ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

MINISTRY OF ICT
Smart Thailand

บทความ
CYBER THREATS 2014

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

MINISTRY OF ICT
Smart Thailand

CYBER THREATS 2014

ชื่อเรื่อง **บทความ Cyber Threats 2014**

โดย ThaiCERT

เรียบเรียงโดย สุรางคณา วายุภาพ, ชัยชนะ มิตรพันธ์,
สรณันท์ จิวะสุรัตน์, สันต์ทศน์ สุริยันต์,
ธงชัย แสงศิริ, พรพรหม ประภากิตติกุล,
เสฏฐวุฒิ แสนนาม, เจษฎา ช้างสีสังข์,
ธงชัย ศิลปวรางกูร, แสนชัย ฐิโนทัย,
โชติกา สินโน, กรรณิกา ภัทรวิศิษฏ์สัณธ์,
ณัฐโชติ ดุสิตานนท์, อรรถวัฒน์ โปร่งเมฆ และทีมไทยเซิร์ต

พิมพ์ครั้งที่ 1 พฤษภาคม 2558

พิมพ์จำนวน 3,000 เล่ม

ราคา 300 บาท

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
(Thailand Computer Emergency Response Team : ThaiCERT)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.)
Electronic Transactions Development Agency (Public Organization : ETDA)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพมหานคร 10310

โทรศัพท์ : 0 2123 1212 | โทรสาร : 0 2120 1200

อีเมล : office@thaicert.or.th

เว็บไซต์ไทยเซิร์ต : www.thaicert.or.th
เว็บไซต์ สพธอ. : www.etda.or.th
เว็บไซต์กระทรวงฯ : www.mict.go.th

คำนำ

ในยุคที่เทคโนโลยีด้านสารสนเทศมีบทบาทและความสำคัญในทุกระดับ ตั้งแต่ประชาชน องค์กร และประเทศ โดยเฉพาะอย่างยิ่งสังคมไทยที่กำลังขับเคลื่อนไปสู่ Digital Economy โดยการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ให้เข้ากับกิจกรรมทางเศรษฐกิจและสังคมเพื่อให้ทุกภาคเศรษฐกิจก้าวหน้าไปได้ทันโลกและสามารถแข่งขันในโลกสมัยใหม่ ซึ่งสิ่งที่มีความสำคัญไม่ยิ่งหย่อนไปกว่าการพัฒนาโครงสร้างพื้นฐานดิจิทัล คือการสร้างความมั่นคงปลอดภัยและความเชื่อมั่นในการทำธุรกรรมด้วยเทคโนโลยีดิจิทัล

ก้าวสู่ปีที่ 4 ที่ไทยเซิร์ตภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้บริการรับมือ วิเคราะห์ และดำเนินการประสานงานเพื่อแก้ไขปัญหาภัยคุกคามด้านสารสนเทศ นอกเหนือจากภารกิจในการแก้ไขปัญหาที่เกิดขึ้นแล้ว หนึ่งในบทบาทสำคัญของไทยเซิร์ตในเชิงรุกคือการเพิ่มขีดความสามารถของทรัพยากรบุคคลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีกิจกรรมสร้างความตระหนักและพัฒนาทักษะความรู้ต่าง ๆ เช่น การซ้อมรับมือภัยคุกคาม รวมถึงการเผยแพร่บทความแจ้งเตือนภัยคุกคามที่ส่งผลกระทบต่อประชาชนและความมั่นคงของประเทศ และบทความสร้างความตระหนักและความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้สามารถป้องกันตนเองและองค์กรจากการถูกสอดแนมหรือขโมยข้อมูล

นอกจากการศึกษาและคัดเลือกข่าวสารที่อาจส่งผลกระทบต่อผู้ใช้งานในประเทศไทย เพื่อนำมาวิเคราะห์และเผยแพร่ในรูปแบบบทความ ไทยเซิร์ตยังได้เพิ่มช่องทางในรูปแบบข่าวสั้นเป็นประจำผ่านเว็บไซต์ และ Twitter เพื่อให้การเผยแพร่ข่าวสารเข้าถึงผู้ใช้งานอินเทอร์เน็ตได้ง่าย รวดเร็ว และทันต่อเหตุการณ์ ส่งผลให้หลาย ๆ ครั้งที่มีการแจ้งเตือนภัยคุกคามสำคัญ ๆ เช่น หน้าเว็บไซต์ธนาคารปลอมที่หลอกขโมยไอดี/รหัสผ่านสำหรับ e-Banking ก็ทำให้เข้าถึงผู้ใช้งานทั่วไปจำนวนมากได้อย่างรวดเร็วผ่านการบอกต่อ ๆ กันในรูปแบบ Retweet นอกจากนี้ ไทยเซิร์ตยังให้บริการ

อีเมลส่งข่าวรายสัปดาห์ เพื่อตอบสนองต่อผู้ที่ใช้อีเมลเป็นช่องทางหลักและไม่ต้องการติดตามข่าวสารรายวัน

หากมองย้อนไปในปี 2557 เห็นได้ว่านอกเหนือจากช่องโหว่จะพบได้ในอุปกรณ์ทั่วไปที่ใช้งานไม่ว่าจะเป็น คอมพิวเตอร์ที่ติดตั้งระบบปฏิบัติการ Windows หรือ MAC อุปกรณ์พกพาทั้งระบบปฏิบัติการ Android และ iOS เราเริ่มพบเห็นภัยคุกคามในอุปกรณ์ประเภท Internet of Things เช่น Smart TV ที่สามารถแอบฟังการสนทนาผ่านไมโครโฟน หรือช่องโหว่ที่เปิดโอกาสให้ดักรับข้อมูลที่มีการส่งระหว่าง Smartwatch กับ Smartphone นอกจากนี้ยังเห็นการโจมตีที่เกิดขึ้นในประเทศไทยรูปแบบต่าง ๆ ไม่ว่าจะเป็นการเผยแพร่มัลแวร์บน Smartphone เพื่อขโมย SMS การเผยแพร่แอปพลิเคชันธนาคารปลอม หรือการแฮกบัญชีไลน์เพื่อหลอกให้ซื้อ iTunes Gift Card ซึ่งจะเห็นได้ว่า ภัยคุกคามเหล่านี้มีการพัฒนาและเปลี่ยนแปลงรูปแบบไปเรื่อย ๆ และไม่ได้ไกลตัวเลย

หนังสือเล่มนี้รวบรวมบทความและข่าวสั้นที่เผยแพร่ผ่านเว็บไซต์ของไทยเซิร์ต (www.thaicert.or.th) ในปี 2557 โดยแบ่งออกเป็น 5 ส่วนคือ บทความแจ้งเตือนและข้อแนะนำสำหรับผู้ใช้งานทั่วไป บทความแจ้งเตือนและข้อแนะนำสำหรับผู้ดูแลระบบ บทความทั่วไป บทความเชิงเทคนิค และข่าวสั้น ทีมผู้จัดทำหวังเป็นอย่างยิ่งว่า หนังสือเล่มนี้จะมีส่วนช่วยให้ผู้อ่านตระหนักถึงผลกระทบและความสำคัญของภัยคุกคามบนโลกไซเบอร์ รวมถึงสามารถป้องกันตนเองและองค์กร เพื่อสร้างความมั่นคงปลอดภัยให้กับสังคมออนไลน์ของประเทศไทย

สุรางคณา วายุภาพ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สารบัญ

บทความ แจ้งเตือน และข้อแนะนำ สำหรับ ผู้ใช้งานทั่วไป

ระวังภัย ช่องโหว่
เราเตอร์ TP-LINK ผู้ไม่หวังดี สามารถควบคุมเราเตอร์ของเหยื่อได้

วันที่ประกาศ : 20 มกราคม 2557
ปรับปรุงล่าสุด : 22 มกราคม 2557
เรื่อง : ระวังภัย ช่องโหว่ เราเตอร์ TP-LINK ผู้ไม่หวังดี สามารถควบคุมเราเตอร์ของเหยื่อได้
ประเภทภัยคุกคาม : Intrusion

ข้อมูลทั่วไป

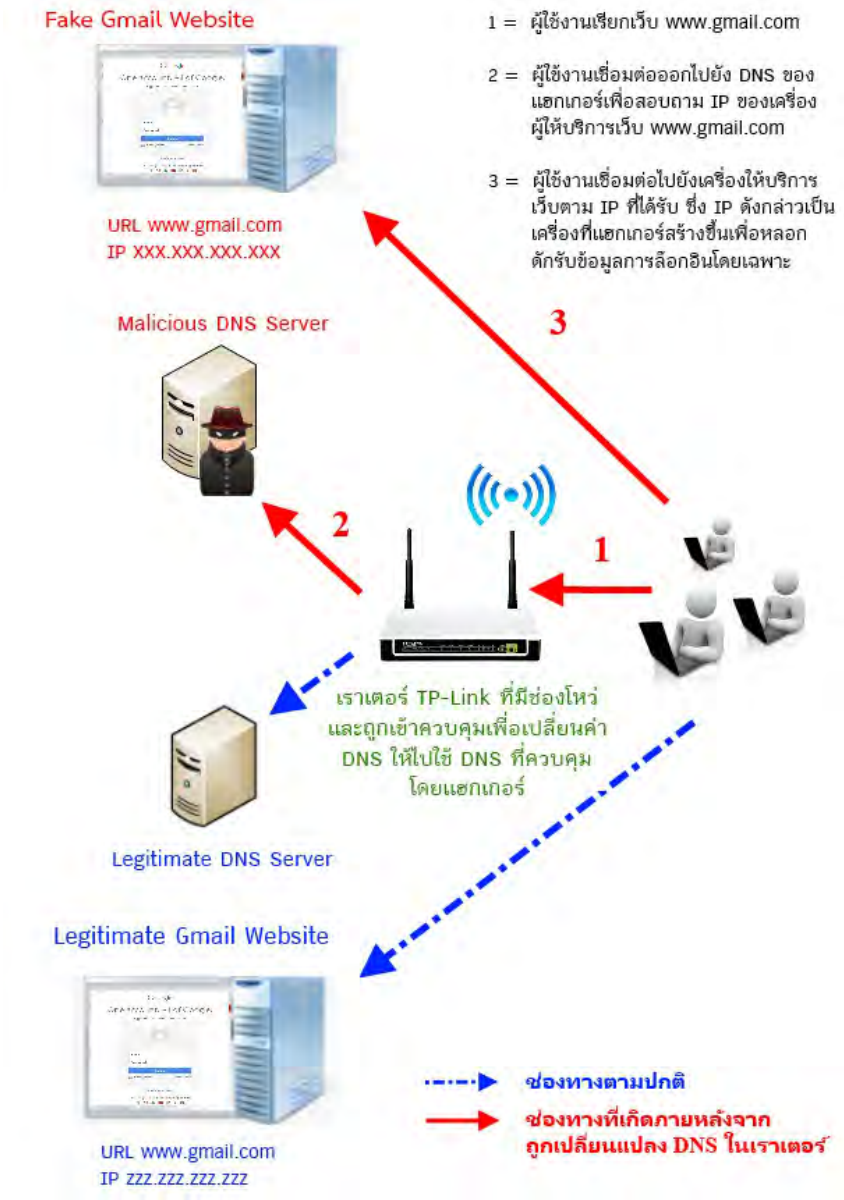
เมื่อวันที่ 15 มกราคม 2557 นาย ABDELLI Nassereddine ชาวแอลจีเรีย ได้เปิดเผยรายงานผ่านเว็บไซต์ The Hacker News ถึงช่องโหว่ในเราเตอร์ยี่ห้อ TP-LINK รุ่น TD-W8951ND ซึ่งเป็นเราเตอร์ที่บริษัท Algerie Telecom ผู้ให้บริการด้านโทรคมนาคมรายใหญ่ของแอลจีเรีย ได้จัดจำหน่ายให้กับผู้ใช้อินเทอร์เน็ตตามบ้าน โดยช่องโหว่ดังกล่าวมีที่มาจากการค้นพบว่า ผู้ใช้สามารถเข้าถึงหน้าต่างการอัปเกรด Firmware และ Romfile (ไฟล์ที่เก็บการตั้งค่าต่าง ๆ ในเราเตอร์) และสามารถดาวน์โหลด Romfile ของเราเตอร์ได้โดยไม่จำเป็นต้องล็อกอินแต่อย่างใด ผ่านทาง URL: http://<ip-address>/rpFWUpload.html ซึ่งจากการวิเคราะห์ Romfile เพิ่มเติมด้วยวิธีการ Reverse Engineering ทำให้สามารถถอดรหัสผ่านของบัญชี Administrator ของเราเตอร์ออกมาอยู่ในรูปของ Plain Text ได้ **[1] [2]**

ผลกระทบ

ผู้ไม่หวังดีสามารถเข้าควบคุมเราเตอร์ของเหยื่อ เพื่อแก้ไขการตั้งค่าและนำไปสู่การโจมตีในรูปแบบต่าง ๆ ได้ทันที

ตัวอย่างการโจมตี

ผู้ไม่หวังดีทำการเปลี่ยนแปลงการตั้งค่า DNS ในเราเตอร์ที่มีช่องโหว่ เพื่อให้ผู้ใช้งานเรียกใช้งาน DNS อันตรายที่ผู้ไม่หวังดีสร้างขึ้น ในทางเทคนิคจะเรียกเทคนิคดังกล่าวว่าเป็นการโจมตีแบบ DNS Hijacking โดยสถานการณ์สมมติตามตัวอย่างในรูปที่ 1 การโจมตีของผู้ไม่หวังดีมีจุดประสงค์เพื่อขโมยบัญชีการเข้าใช้งานอีเมล Gmail ของผู้ใช้งาน โดย DNS ของผู้ไม่หวังดีจะ Redirect ผู้ใช้งานไปยังเครือข่ายของผู้ไม่หวังดี แทนที่จะไปยังเว็บไซต์ Gmail.com ที่เป็นเครือข่ายที่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถขโมยข้อมูลการล็อกอินที่ผู้ใช้งานป้อนเข้าสู่ระบบได้ทันที



รูปที่ 1 ตัวอย่างการโจมตีด้วยเทคนิค DNS Hijacking

ระบบที่ได้รับผลกระทบ

เราเตอร์ยี่ห้อ TP-LINK รุ่น TD-W8951ND ตามที่ปรากฏในข่าว

และจากการตรวจสอบในเบื้องต้น ไทยเซิร์ตพบเราเตอร์รุ่นต่อไปนี้ที่ได้รับผลกระทบจากช่องโหว่ดังกล่าวเช่นเดียวกัน

- TD854W
- TD-8816
- TD-8817
- TD-8840T
- TD-W8101G
- TD-W8151N
- TD-W8901G
- TD-W8901N
- TD-W8961NB
- TD-W8961ND

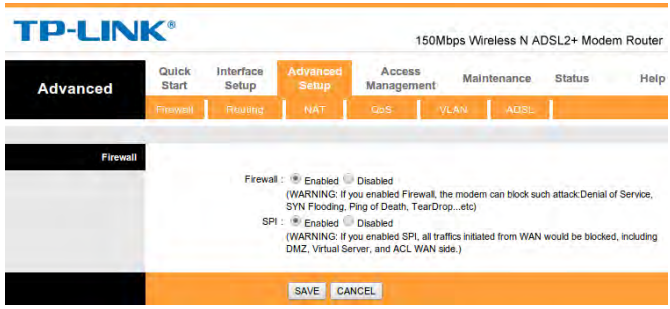
ข้อแนะนำในการป้องกันและแก้ไข

เนื่องจากยังไม่พบการออกแพตช์สำหรับแก้ไขช่องโหว่ดังกล่าวจากบริษัทผู้พัฒนา ทางไทยเซิร์ตจึงได้ประสานงานกับผู้พัฒนาเพื่อแจ้งปัญหาและสอบถามข้อมูลเพิ่มเติม แล้วแต่ยังไม่ได้รับการตอบกลับ อย่างไรก็ตามผู้ใช้งานสามารถใช้วิธีการป้องกันการเข้าถึงหน้าเว็บบริหารจัดการเราเตอร์จากเครือข่ายอินเทอร์เน็ต ด้วยการเปิดการใช้งาน SPI หรือ เลือกใช้งานฟังก์ชัน ACL (Access Control List) ซึ่งเป็นฟังก์ชันที่ใช้ในการจำกัดการเข้าถึงบริการต่าง ๆ ตามเงื่อนไขที่สร้างขึ้นที่มีอยู่ในเราเตอร์ TP-LINK เพื่อลดความเสี่ยงจากการถูกโจมตีช่องโหว่ดังกล่าวได้ โดยหลักการคือ ปิดการเชื่อมต่อหน้าบริหารจัดการจากเครือข่ายภายนอก เท่ากับว่าผู้ไม่หวังดีที่พยายามเชื่อมต่อผ่านอินเทอร์เน็ตจะไม่สามารถเข้าถึงหน้าล็อกอิน หรือหน้าดาวน์โหลดข้อมูล Romfile ของอุปกรณ์เราเตอร์ได้ แต่อย่างไรก็ตามผู้ใช้งานจำเป็นต้องควรพึงระวังสำหรับการตั้งค่าที่ผิดวิธี รวมถึงสิ่งสำคัญที่สุดคือผู้ใช้งานควรรีบอัปเดตแพตช์จากเว็บไซต์ผู้พัฒนาทันทีที่มีการแก้ไขปัญหาแล้ว หรือสามารถติดตามข้อมูลอัปเดตได้ผ่านบทความแจ้งเตือนนี้ได้เช่นกัน โดยไทยเซิร์ตจะรีบแจ้งเตือนทันทีที่มีการอัปเดตจากผู้เกี่ยวข้อง

วิธีการที่ 1 เปิดการใช้งาน SPI เพื่อป้องกันการเข้าถึงหน้าเว็บบริหารจัดการเราเตอร์

1. ภายหลังจากการล็อกอินเข้าสู่หน้าบริหารจัดการเราเตอร์แล้วให้คลิกที่ Advanced Setup -> Firewall แล้วตั้งค่าตามในรูปที่ 2 จากนั้นคลิกปุ่ม SAVE เป็นอันเสร็จสิ้น

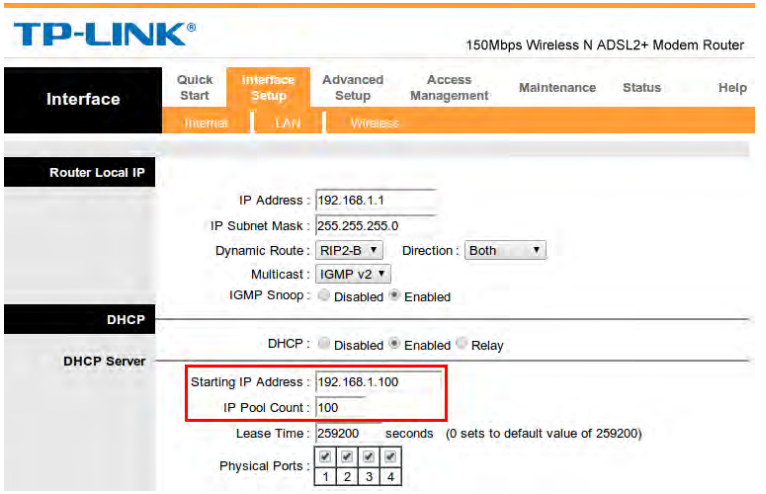
การตั้งค่าดังกล่าว จะเป็นการเปิดการทำงานของ SPI ซึ่งจะเป็นการปิดการเชื่อมต่อทั้งหมด ที่สร้างจากภายนอก ไม่ให้สามารถเชื่อมต่อเข้ามายังเราเตอร์ได้



รูปที่ 2 หน้าต่างการตั้งค่า SPI ของอุปกรณ์เราเตอร์รุ่น TD-W8951ND

วิธีการที่ 2 การตั้งค่า ACL (Access Control List)

1. ภายหลังจากการล็อกอินเข้าสู่หน้าบริหารจัดการเราเตอร์แล้วให้คลิกที่ Interface Setup -> LAN ตรวจสอบตรงช่อง Starting IP Address และ IP Pool Count จากตัวอย่างรูปที่ 3 จะพบว่า Starting IP Address คือ 192.168.1.100 และข้อมูล IP Pool Count คือ 100 แสดงว่าไอพีแอดเดรสภายในจะมีค่าได้ในช่วงตั้งแต่ 192.168.1.100 - 192.168.1.199

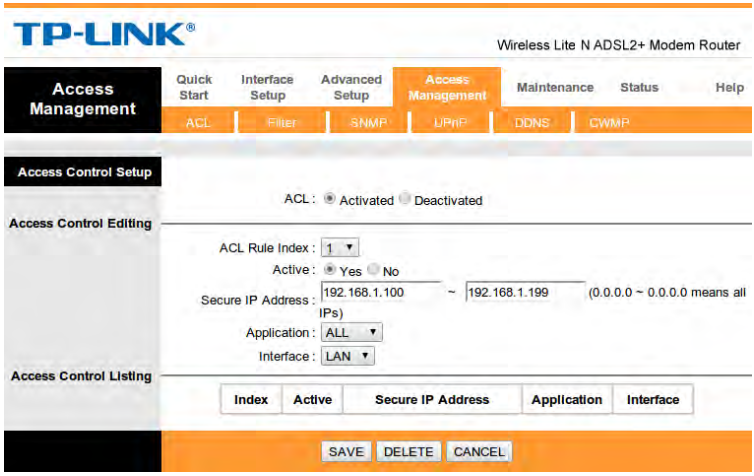


รูปที่ 3 หน้าต่างการตั้งค่าไอพีแอดเดรสของเครือข่ายภายในของอุปกรณ์เราเตอร์รุ่น TD-W8951ND

2. คลิกที่ Access Management -> ACL แล้วตั้งค่าตามในรูปที่ 4 ดังต่อไปนี้

- ACL: Activated
- Active: Yes
- Secure IP Address: ให้ระบุช่วงของไอพีแอดเดรสจากค่าที่ได้ในข้อ 1
- Application: ALL
- Interface: LAN

จากนั้นคลิกปุ่ม SAVE เป็นอันเสร็จสิ้น



รูปที่ 4 หน้าต่างการตั้งค่า ACL ของอุปกรณ์เราเตอร์รุ่น TD-W8951ND

บริการตรวจสอบช่องโหว่ของเราเตอร์ TP-LINK

ไทยเซิร์ตได้เปิดให้บริการตรวจสอบช่องโหว่ตามที่อ้างถึงในบทความนี้ โดยผู้ใช้งานสามารถตรวจสอบได้ตามลิงก์ต่อไปนี้ https://al2014us001.thaicert.or.th/

อ้างอิง
1. http://thehackernews.com/2014/01/TP-LINK-Routers-password-hacking.html
2. http://rootatnasro.wordpress.com/2014/01/11/how-i-saved-your-a-from-the-zynos-rom-0-attack-full-disclosure

ระวังภัย มัลแวร์
Oldboot บนระบบปฏิบัติการ Android ฝังตัวอยู่ในพาร์ทิชัน Boot ติดตั้งตัวเองใหม่ทุกครั้งที่เปิดเครื่อง

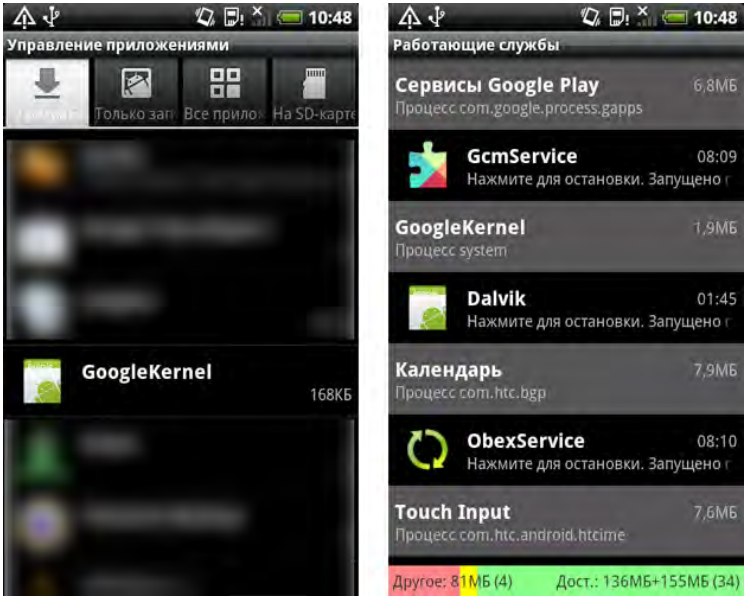
วันที่ประกาศ : 29 มกราคม 2557
ปรับปรุงล่าสุด : 29 มกราคม 2557
เรื่อง : ระวังภัย มัลแวร์ Oldboot บนระบบปฏิบัติการ Android ฝังตัวอยู่ในพาร์ทิชัน Boot ติดตั้งตัวเองใหม่ทุกครั้งที่เปิดเครื่อง
ประเภทภัยคุกคาม : Malicious Code

ข้อมูลทั่วไป

เมื่อวันที่ 24 มกราคม 2557 บริษัท Doctor Web ผู้พัฒนาโปรแกรมแอนติไวรัสจากประเทศรัสเซีย และบริษัท Qihoo 360 Technology จากประเทศจีน ได้รายงานการค้นพบมัลแวร์ในระบบปฏิบัติการ Android ที่ฝังตัวอยู่ในส่วนที่ใช้ในการบู๊ตระบบปฏิบัติการ เพื่อโหลดตัวเองขึ้นมาทำงานตั้งแต่ตอนเปิดเครื่อง และติดตั้งตัวเองใหม่แม้จะลบออกจากเครื่องไปแล้ว โดยข้อมูลของ Doctor Web พบว่ามีผู้ตกเป็นเหยื่อของมัลแวร์ตัวนี้แล้วกว่า 350,000 คน ซึ่งในจำนวนนี้มีผู้เสียหายที่อยู่ในประเทศไทยด้วย [1] แต่จากข้อมูลของ Qihoo 360 Technology พบว่าแค่เฉพาะในประเทศจีนมีผู้ที่ติดมัลแวร์นี้ไปแล้วกว่า 500,000 คน [2]

มัลแวร์ตัวนี้มีชื่อว่า Oldboot (หรืออีกชื่อหนึ่งคือ Android.Oldboot) ถือเป็นมัลแวร์ตัวแรกที่ใช้วิธีการติดตั้งตัวเองลงในพาร์ทิชัน Boot ของระบบปฏิบัติการ Android ซึ่งเป็นพาร์ทิชันที่ใช้เก็บไฟล์สำหรับการบู๊ตระบบปฏิบัติการ (ทางนักวิจัยจากทั้งสองบริษัทเรียกมัลแวร์ประเภทนี้ว่า Bootkit)

วิธีการที่มัลแวร์ติดตั้งตัวเองลงในพาร์ทิชัน Boot นั้นปัจจุบันยังไม่ทราบแน่ชัดว่าทำได้อย่างไร เนื่องจากเป็นพาร์ทิชันที่ได้รับการป้องกันเอาไว้ไม่ให้สามารถแก้ไขข้อมูลได้โดยใช้วิธีการตามปกติ แต่เครื่องที่ติดมัลแวร์ดังกล่าว ผู้ใช้จะพบความผิดปกติคือมีแอปพลิเคชันประเภทโฆษณาถูกติดตั้งอยู่ในเครื่องเป็นจำนวนมาก และเมื่อตรวจสอบดูรายชื่อแอปพลิเคชันที่ติดตั้งอยู่ในเครื่อง จะพบแอปพลิเคชันที่ชื่อ GoogleKernel ซึ่งไม่สามารถลบออกได้ด้วยวิธีปกติ ดังรูปที่ 1



รูปที่ 1 แอปพลิเคชัน GoogleKernel ที่พบในเครื่องที่ติดมัลแวร์ (ที่มา: Doctor Web [1])

นอกจากนี้ ตัวมัลแวร์ Oldboot ยังแก้ไขไฟล์ /init.RC เป็นไฟล์สคริปต์ที่ใช้กำหนดค่าการบู๊ตระบบปฏิบัติการ เพื่อให้โหลดไฟล์ของมัลแวร์ขึ้นมาทำงานโดยอัตโนมัติทุกครั้งที่เปิดเครื่อง

เมื่อผู้ใช้เปิดเครื่อง ตัวระบบจะอ่านค่าจากไฟล์ init.RC แล้วเรียกใช้งานไฟล์ imei_chk โดยไฟล์ดังกล่าวนี้ทำหน้าที่ Extract ไฟล์ GoogleKernel.apk ลงใน /system/app และไฟล์ libgooglekernel.so ลงใน /system/lib

ไฟล์ imei_chk จะเปิด Service ไว้เชื่อมต่อกับเครื่อง C&C Server แล้วให้แอปพลิเคชัน GoogleKernel เรียกใช้ฟังก์ชันจากไฟล์ไลบรารี libgooglekernel.so เพื่อรอรับคำสั่งจาก C&C server มาทำงานต่อ คำสั่งใด ๆ ก็ตามที่ C&C Server ส่งมาจะมีการรันด้วยสิทธิ์ของ Root

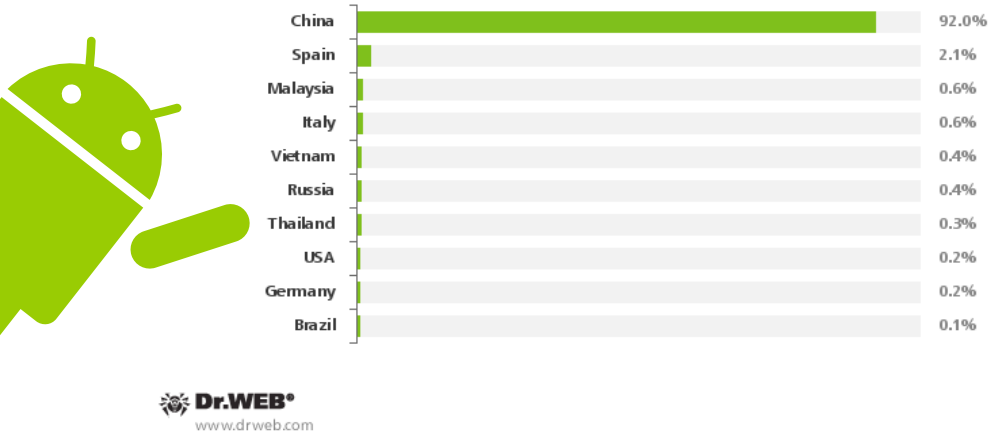
เนื่องจากโค้ดของมัลแวร์ ส่วนที่อยู่ในพาร์ทิชัน Boot นั้นไม่สามารถลบออกได้ด้วยวิธีการปกติ ทำให้ถึงแม้ว่าจะหาวิธี Uninstall แอปพลิเคชัน GoogleKernel ซึ่งเป็นมัลแวร์ออกได้ เมื่อรีสตาร์ทเครื่องใหม่ ไฟล์ imei_chk ก็จะยังคงทำงาน และตัวมัลแวร์ก็จะยังสามารถติดตั้งตัวเองลงในเครื่องใหม่อีกครั้งได้อยู่ดี

ผลกระทบ

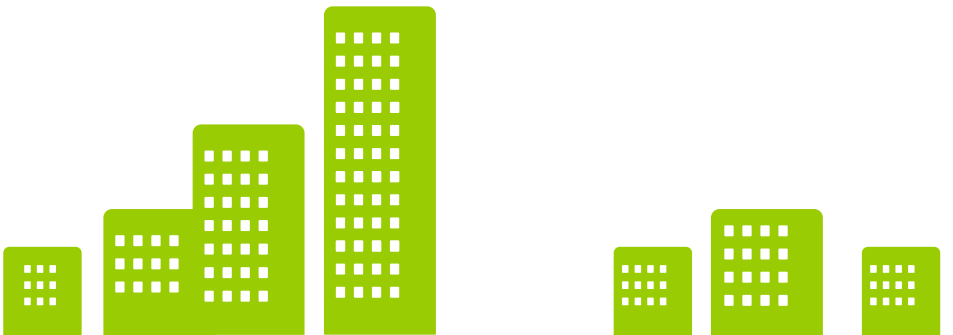
เครื่องที่ติดมัลแวร์ อาจถูกผู้ไม่หวังดีควบคุมให้ทำตามคำสั่ง ในลักษณะ Botnet เช่น ดาวน์โหลดแอปพลิเคชันมัลแวร์มาติดตั้งเพิ่มเติม ดักฟังข้อมูล โทรศัพท์หรือส่ง SMS ออกไปเอง ขโมยไฟล์ ขโมยรหัสผ่าน โจมตีเครื่องอื่น ๆ หรือแม้กระทั่งดาวน์โหลดเฟิร์มแวร์ที่ถูกผู้ไม่หวังดีแก้ไขมาติดตั้งลงในเครื่อง นอกจากนี้ รูปแบบการทำงานของมัลแวร์ชนิดนี้ ยังทำให้การลบมัลแวร์ออกจากเครื่องโทรศัพท์เป็นไปได้ยากกว่าปกติ ดังที่กล่าวไว้ข้างต้นด้วย

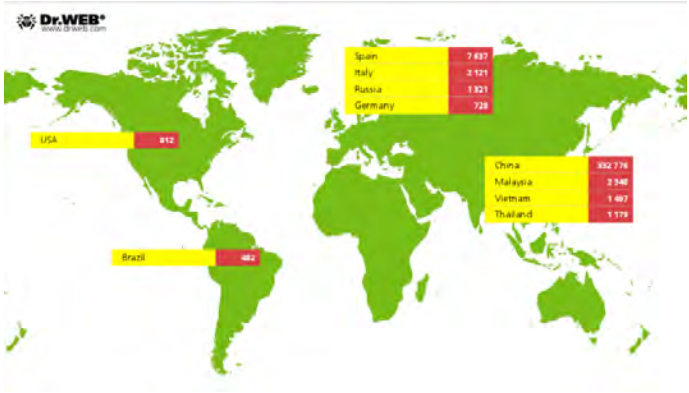
ระบบที่ได้รับผลกระทบ

อ้างอิงข้อมูลของ Doctor Web พบว่ามีอุปกรณ์ที่ติดมัลแวร์ตัวนี้ประมาณ 300,000 เครื่อง หรือคิดเป็น 92% อยู่ในประเทศจีน ดังรูปที่ 2 และ 3 ซึ่งอาจเป็นไปได้ว่ามัลแวร์ตัวนี้มีเจตนาเพื่อโจมตีผู้ใช้งานที่อยู่ในประเทศจีนเป็นหลัก ในประเทศไทยพบว่ามีเครื่องที่ตกเป็นเหยื่อประมาณ 0.3% หรือประมาณ 1,000 เครื่อง



รูปที่ 2 สถิติประเทศที่ติดมัลแวร์ คิดเป็นเปอร์เซ็นต์ (ที่มา: Doctor Web [2])





รูปที่ 3 สถิติประเทศที่ติดมัลแวร์ ตามจำนวนที่พบ (ที่มา: Doctor Web [2])

ข้อแนะนำในการป้องกันและแก้ไข

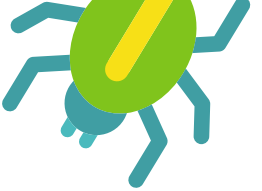
ปัจจุบันยังไม่มีข้อมูลว่ามัลแวร์มีการแพร่กระจายอย่างไร และวิธีการที่มัลแวร์ใช้ในการติดตั้งตัวเองลงในพาร์ทิชัน Boot นั้นทำได้อย่างไร แต่จากการสันนิษฐานของทาง Qihoo 360 Technology คาดว่าน่าจะเกิดจากการ Flash ไฟล์ boot.IMG ที่ถูกสร้างขึ้นเป็นพิเศษให้มีมัลแวร์ชนิดนี้ฝังอยู่ ซึ่ง boot.IMG นี้ เป็นส่วนที่จะติดตั้งตัวเองลงในพาร์ทิชัน Boot ของ Firmware Image ทุกครั้งที่มีการติดตั้ง Firmware Image ใหม่

วิธีการที่เป็นไปได้มากที่สุดที่จะทำให้เครื่องติดมัลแวร์ตัวนี้ คือการฝังโค้ดของมัลแวร์ไว้ใน Custom Firmware Image แล้วแฟลช Firmware Image ดังกล่าวลงในเครื่อง ซึ่งทาง Qihoo 360 Technology พบว่าในร้านขายอุปกรณ์ IT ในประเทศจีน มีการขายโทรศัพท์มือถือ Android ที่ถูกติดตั้ง Custom Firmware Image ซึ่งฝังมัลแวร์ตัวนี้มาด้วย

ทาง Qihoo 360 Technology ได้พัฒนาแอปพลิเคชันที่ใช้ตรวจสอบว่าเครื่องที่ใช้งานอยู่ถูกมัลแวร์ Oldboot ฝังตัวอยู่หรือไม่ โดยผู้ใช้สามารถดาวน์โหลดแอปพลิเคชันดังกล่าวมาตรวจสอบได้จากเว็บไซต์ของ Qihoo 360 Technology

หากพบว่าเครื่องที่ใช้งานอยู่ได้ติดมัลแวร์ไปแล้ว การลบแอปพลิเคชันของมัลแวร์ออกจากเครื่องไม่สามารถช่วยอะไรได้ เพราะเมื่อเปิดเครื่องขึ้นมาใหม่ ตัวมัลแวร์ก็จะถูกติดตั้งลงในเครื่องได้อีก รวมถึงการทำ Factory Reset ก็ไม่สามารถช่วยได้เพราะส่วนมากการทำ Factory Reset เป็นแค่การลบไฟล์ Config หรือข้อมูลของผู้ใช้งานเท่านั้น โดย Firmware Image ยังคงไม่มีการเปลี่ยนแปลง

วิธีการที่น่าจะดีที่สุดเพื่อใช้กำจัดมัลแวร์ชนิดนี้ คือการติดตั้ง Firmware ที่มาจากผู้ผลิตโดยตรง ซึ่งอาจต้องตรวจสอบวิธีการกับบริษัทผู้ผลิตอุปกรณ์แต่ละราย เพราะอุปกรณ์แต่ละรุ่นอาจมีวิธีการแตกต่างกัน หรืออาจจะต้องนำเครื่องเข้ารับบริการที่ศูนย์บริการ



อีกวิธีการที่ทาง Doctor Web แนะนำในการป้องกันมัลแวร์ตัวนี้หรือมัลแวร์ที่มีการทำงานใกล้เคียงกัน คือควรระวังการซื้ออุปกรณ์ Android ที่ไม่ทราบแหล่งที่มา (ซึ่งอาจรวมไปถึงอุปกรณ์ที่ไม่มีข้อมูลผู้ผลิตที่ชัดเจน) และควรติดตั้ง Firmware Image ที่มาจากแหล่งที่น่าเชื่อถือเท่านั้น

อ้างอิง

1. http://news.drweb.com/show/?i=4206&lng=en&c=5
2. http://blogs.360.cn/360mobile/2014/01/17/oldboot-the-first-bootkit-on-android/

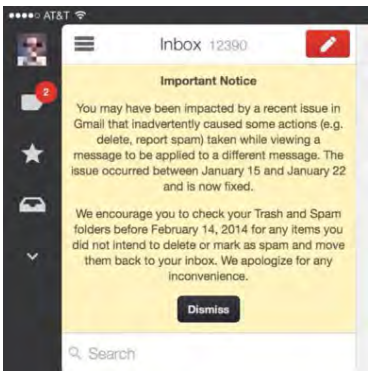
ระวังภัย Gmail ทำงานผิดพลาด อีเมลปกติบางฉบับถูกส่งไปอยู่ในกล่องสแปม/ถังขยะ ผู้ใช้ควรตรวจสอบก่อนอีเมลถูกลบไปอย่างถาวร

วันที่ประกาศ : 30 มกราคม 2557
ปรับปรุงล่าสุด : 30 มกราคม 2557
เรื่อง : ระวังภัย Gmail ทำงานผิดพลาด อีเมลปกติบางฉบับถูกส่งไปอยู่ในกล่องสแปม/ถังขยะ ผู้ใช้ควรตรวจสอบก่อนอีเมลถูกลบไปอย่างถาวร
ประเภทภัยคุกคาม : Other

ข้อมูลทั่วไป

เมื่อประมาณวันที่ 28 มกราคม 2557 Google แจ้งเตือนผู้ใช้บริการ Gmail ว่าพบความผิดพลาดในฟังก์ชันการทำงานของระบบ ส่งผลให้เมื่อผู้ใช้สั่งลบหรือกำหนดให้อีเมลฉบับใดฉบับหนึ่งเป็นจดหมายขยะ ระบบจะลบหรือกำหนดอีเมลฉบับอื่นให้เป็นจดหมายขยะแทน โดยความผิดพลาดนี้เกิดขึ้นกับผู้ใช้บริการบางราย และปัจจุบันปัญหานี้ได้รับการแก้ไขแล้ว

ผู้ใช้บริการบางรายที่อาจได้รับผลกระทบจากปัญหาดังกล่าว เมื่อล็อกอินเข้าใช้งาน Gmail จะพบข้อความแจ้งเตือนดังตัวอย่างในรูปที่ 1 ซึ่งเป็นแอปพลิเคชัน Gmail บน iOS ปัญหาที่เกิดขึ้นอาจมีความเกี่ยวข้องกับเหตุการณ์ที่ Gmail และบริการอื่น ๆ ของ Google ทำงานผิดพลาดและไม่สามารถให้บริการได้เมื่อวันที่ 24 มกราคม 2557 **[1]**



รูปที่ 1 ตัวอย่างการแจ้งเตือนของ Gmail

ผลกระทบ

อีเมลที่ส่งเข้ามาใน Inbox ของผู้ใช้ Gmail ระหว่างวันที่ 15 - 22 มกราคม 2557 อาจถูกส่งไปอยู่ในถังขยะหรือถูกจัดให้เป็นสแปม และหากผู้ใช้ไม่เข้าไปตรวจสอบและย้ายอีเมลดังกล่าวกลับคืนสู่กล่อง Inbox ภายในวันที่ 14 กุมภาพันธ์ 2557 อีเมลเหล่านั้นจะถูกลบออกไปอย่างถาวร

ระบบที่ได้รับผลกระทบ

ปัญหานี้เกิดขึ้นกับผู้ใช้บางราย และเกิดขึ้นกับบริการ Gmail บางระบบ เช่น แอปพลิเคชัน Gmail บน iOS, เว็บไซต์ Gmail เวอร์ชันมือถือ และบริการ Gmail แบบ Offline เป็นต้น

ข้อแนะนำในการป้องกันและแก้ไข

Google ได้แจ้งให้ผู้ใช้ที่คาดว่าจะได้รับผลกระทบ เข้าไปตรวจสอบอีเมลในกล่อง Trash และ Spam เพื่อกู้คืนอีเมลเหล่านั้นออกมาก่อนที่จะถูกลบออกไปอย่างถาวรภายในวันที่ 14 กุมภาพันธ์ 2557

อย่างไรก็ตาม ผู้ใช้ที่ไม่ได้รับข้อความแจ้งเตือนเรื่องปัญหาดังกล่าว ควรตรวจสอบอีเมลในกล่อง Trash และ Spam ด้วยเพื่อความแน่ใจ

อ้างอิง

1. http://googleblog.blogspot.com/2014/01/todays-outage-for-several-google.html

ระวังภัย Yahoo Mail ถูกแฮก ผู้ใช้งานควรรีบเปลี่ยนรหัสผ่านทันที

วันที่ประกาศ : 1 กุมภาพันธ์ 2557
ปรับปรุงล่าสุด : 1 กุมภาพันธ์ 2557
เรื่อง : ระวังภัย Yahoo Mail ถูกแฮก ผู้ใช้งานควรรีบเปลี่ยนรหัสผ่านทันที
ประเภทภัยคุกคาม : Intrusion

ข้อมูลทั่วไป

เมื่อวันที่ 30 มกราคม 2557 เว็บไซต์ Blog ของ Yahoo ผู้ให้บริการฟรีอีเมลรายใหญ่ของโลก ได้แจ้งเตือน **[1]** ผู้ใช้งานบริการอีเมล ให้ทราบถึงการตรวจพบการเข้าถึงข้อมูลบัญชีผู้ใช้งานที่ผิดปกติ อันน่าจะเกิดมาจากการถูกเจาะเข้าสู่ฐานข้อมูลของระบบ Third Party บางระบบ (เนื่องจากไม่พบร่องรอยการเจาะเข้าสู่ระบบของ Yahoo Mail โดยตรง) ทำให้ผู้ไม่หวังดีสามารถเข้าถึงและขโมยข้อมูลบัญชีผู้ใช้งานรวมถึงรหัสผ่านออกไปได้ โดยพบว่าผู้ไม่หวังดีได้นำข้อมูลบัญชีผู้ใช้งานที่ขโมยได้มาใช้เข้าถึงบริการ Yahoo Mail ในเวลาต่อมา

ผลกระทบ

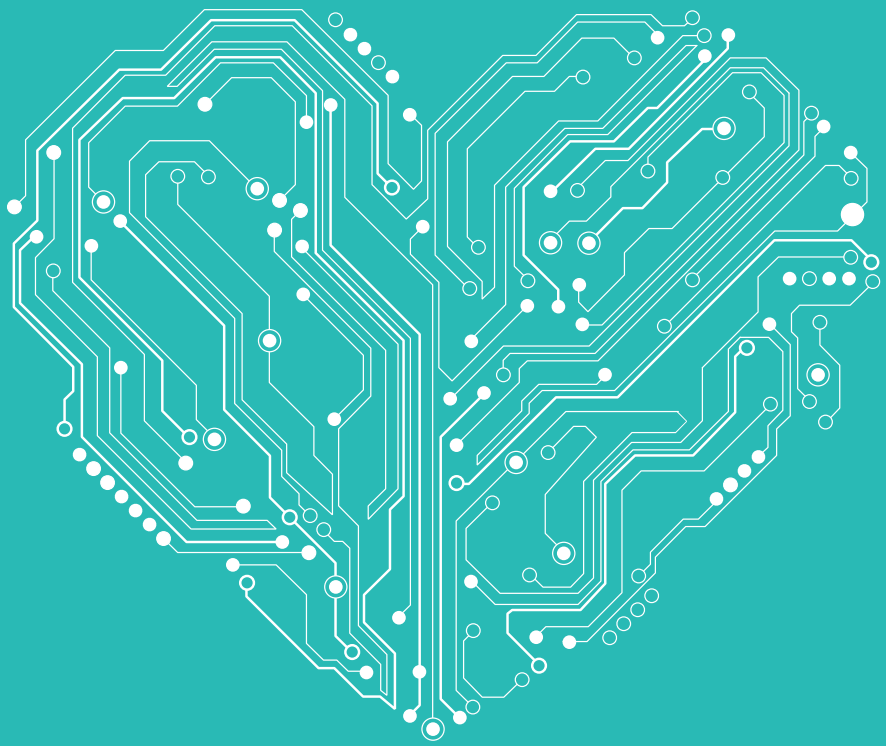
Yahoo ได้แจ้งว่าขณะนี้ได้มีการเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานที่คาดว่าจะได้รับผลกระทบเรียบร้อยแล้ว โดยผู้ใช้งานที่ได้รับผลกระทบจะพบข้อความการแจ้งให้เปลี่ยนรหัสผ่านทันที หรืออาจได้รับข้อมูลการแจ้งเตือนดังกล่าวในช่องทางสำรองของผู้ใช้งาน เช่น SMS เป็นต้น โดยปัจจุบัน Yahoo ได้เปิดให้บริการ Two Factor Authentication ซึ่งมีการเพิ่มมาตรการรักษาความมั่นคงปลอดภัยสูงกว่าวิธีการล็อกอินในลักษณะเดิม เนื่องจากการจะล็อกอินเข้าสู่ระบบจำเป็นต้องยืนยันตัวตนด้วย 2 องค์ประกอบคือ รหัสผ่าน และรหัส SMS ที่ได้จากโทรศัพท์มือถือ

ข้อแนะนำในการป้องกันและแก้ไข

จากกรณีการโจมตีดังกล่าว ถึงแม้ว่าทาง Yahoo จะระบุว่าได้มีการแก้ไขปัญหาในส่วนของบัญชีผู้ใช้งานที่ถูกขโมยไปแล้ว แต่อย่างไรก็ตามผู้ใช้งาน Yahoo Mail ทุกท่านควรรีบเปลี่ยนรหัสผ่านในทันที เพื่อป้องกันโอกาสที่จะเกิดความผิดพลาดจากการตรวจสอบ และควรเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เช่น เปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น รวมถึงควรหลีกเลี่ยงการใช้งานรหัสผ่านเดียวกันในทุกระบบ เพื่อป้องกันโอกาสในการถูกขโมยบัญชีการใช้งานอื่น ๆ ในกรณีที่ระบบใดระบบหนึ่งถูกขโมยข้อมูลออกไปได้ เช่น ไม่ควรตั้งรหัสผ่านของบริการอีเมลเหมือนกับรหัสผ่านของบัญชี Facebook เป็นต้น โดยส่วนหนึ่งผู้ใช้งานสามารถศึกษาวิธีการเข้าใช้งาน Yahoo Mail อย่างมั่นคงปลอดภัย ตามบทความที่ Yahoo Mail จัดทำขึ้น ตามลิงก์นี้ [2]

อ้างอิง

1. http://yahoo.tumblr.com/post/75083532312/important-security-update-for-yahoo-mail-users
2. https://help.yahoo.com/kb/SLN2080.html



ระวังภัย ช่องโหว่ใน Adobe Flash Player ผู้ไม่หวังดีสามารถควบคุมเครื่องได้ (CVE-2014-0497)

วันที่ประกาศ : 7 กุมภาพันธ์ 2557
ปรับปรุงล่าสุด : 7 กุมภาพันธ์ 2557
เรื่อง : ระวังภัย ช่องโหว่ใน Adobe Flash Player ผู้ไม่หวังดีสามารถควบคุมเครื่องได้ (CVE-2014-0497)
ประเภทภัยคุกคาม : Other

ข้อมูลทั่วไป

เมื่อวันที่ 4 กุมภาพันธ์ 2557 บริษัท Adobe ได้แจ้งเตือนช่องโหว่ของโปรแกรม Adobe Flash Player ที่มีผลกับผู้ใช้งานระบบปฏิบัติการ Windows, Mac OS X และ Linux **[1]** ผู้โจมตีสามารถใช้ช่องโหว่ดังกล่าวในการสั่งประมวลผลคำสั่งใด ๆ บนเครื่องคอมพิวเตอร์ของเหยื่อได้จากระยะไกลได้ (Remote Code Execution) ช่องโหว่นี้มีหมายเลข CVE-2014-0497

บริษัท Kaspersky ได้รายงานการค้นพบไฟล์ SWF ที่โจมตีผ่านช่องโหว่นี้ โดยรูปแบบการโจมตีที่พบคือคำสั่งอันตรายที่อยู่ในไฟล์ SWF จะตรวจสอบระบบปฏิบัติการบนเครื่องของเหยื่อ จากนั้นจะติดตั้งโปรแกรมที่อนุญาตให้ผู้ไม่หวังดีเชื่อมต่อเข้ามาควบคุมเครื่องของผู้ใช้ **[2]**

ผลกระทบ

เครื่องคอมพิวเตอร์ที่เปิดไฟล์ SWF ที่มีคำสั่งไม่พึงประสงค์ อาจถูกผู้ไม่หวังดีสั่งประมวลผลคำสั่งไม่พึงประสงค์จากระยะไกลเพื่อควบคุมเครื่องคอมพิวเตอร์

ระบบที่ได้รับผลกระทบ

- Adobe Flash Player เวอร์ชัน 12.0.0.43 หรือต่ำกว่า ทั้งบนระบบปฏิบัติการ Windows และ Mac OS X
- Adobe Flash Player เวอร์ชัน 11.2.202.335 หรือต่ำกว่า บนระบบปฏิบัติการ Linux

ข้อแนะนำในการป้องกันและแก้ไข

Adobe ได้ออกซอฟต์แวร์อัปเดตเพื่อแก้ไขช่องโหว่นี้แล้ว ผู้ใช้งานระบบปฏิบัติการ Windows และ Mac OS X สามารถติดตั้ง Adobe Flash Player เวอร์ชัน 12.0.0.44 ส่วนผู้ใช้งานระบบปฏิบัติการ Linux สามารถติดตั้ง Adobe Flash Player เวอร์ชัน 11.2.202.335 โดยสามารถดาวน์โหลดซอฟต์แวร์ดังกล่าวได้จากเว็บไซต์ของ Adobe

อ้างอิง

1. http://helpx.adobe.com/security/products/flash-player/apsb14-04.html
2. http://threatpost.com/details-emerge-on-latest-adobe-flash-zero-day-exploit/104068

ระวังภัย ช่องโหว่บนระบบปฏิบัติการ iOS 7.0.x อนุญาตให้ผู้ไม่หวังดีปิดการใช้งานฟังก์ชัน Find My Phone

วันที่ประกาศ : 10 กุมภาพันธ์ 2557
ปรับปรุงล่าสุด : 10 กุมภาพันธ์ 2557
เรื่อง : ระวังภัย ช่องโหว่บนระบบปฏิบัติการ iOS 7.0.x อนุญาตให้ผู้ไม่หวังดีปิดการใช้งานฟังก์ชัน Find My Phone
ประเภทภัยคุกคาม : Intrusions

ข้อมูลทั่วไป

เมื่อวันที่ 7 กุมภาพันธ์ 2557 พบการเผยแพร่ข้อมูลคลิปวิดีโอบนเว็บไซต์ Youtube.com [1] โดยผู้ใช้งานชื่อ Bradley Williams อ้างถึงการค้นพบช่องโหว่บนระบบปฏิบัติการ iOS ในการสั่งปิดการทำงานของ Find My Phone โดยไม่มีการถามรหัสผ่านบัญชี iCloud ซึ่งเป็นฟังก์ชันที่ใช้ในการค้นหาตำแหน่งที่อยู่ของอุปกรณ์ที่ใช้งาน รวมถึงการบริหารจัดการโทรศัพท์ด้วยการสั่งการจากระยะไกล เช่น การสั่งลบข้อมูล การตั้งค่าล็อกเครื่อง

สำหรับระบบปฏิบัติการ iOS เวอร์ชัน 7 ขึ้นไป บริษัท Apple ได้มีการพัฒนาฟังก์ชัน iCloud: Activation Lock [2] ซึ่งกำหนดให้ต้องทำการล็อกอินผ่านบัญชี iCloud ก่อนที่จะมีการสั่งปิดการใช้งานฟังก์ชัน Find My Phone ได้ แต่ช่องโหว่ดังกล่าวทำให้ผู้ไม่หวังดีสามารถปิดการทำงานของ Find My Phone บนอุปกรณ์ iOS โดยไม่มีการถามรหัสผ่านของบัญชี iCloud ของผู้ใช้งานก่อน

ผลกระทบ

ในกรณีที่อุปกรณ์ iOS ตกอยู่ในมือของผู้ไม่หวังดี ทำให้ผู้ไม่หวังดีสามารถปิดการทำงานของ Find My Phone ได้แม้ไม่รู้รหัสผ่าน iCloud ของผู้ใช้ เพียงแต่สามารถเข้าถึงหน้า Home ของโทรศัพท์ได้เท่านั้น ซึ่งอาจเกิดจากผู้ใช้งานไม่ได้ล็อกหน้าจอด้วย Passcode หรือใช้ Passcode ที่ผู้ไม่หวังดีสามารถคาดเดาได้ ส่งผลให้ข้อมูลสำคัญของผู้ใช้งานรั่วไหล เพราะผู้ใช้งานไม่สามารถค้นหาตำแหน่ง หรือสั่งลบข้อมูลในโทรศัพท์เมื่อสูญหาย หรือถูกขโมยได้อีกต่อไป

ระบบที่ได้รับผลกระทบ

ระบบปฏิบัติการ iOS เวอร์ชัน 7.0.x หรือต่ำกว่า

ข้อแนะนำในการป้องกันและแก้ไข

ทางบริษัท Apple กำลังพัฒนา iOS เวอร์ชัน 7.1 (ปัจจุบันเผยแพร่เป็นเวอร์ชันสำหรับนักพัฒนาอยู่) ซึ่งในเวอร์ชันนี้ได้มีการแก้ไขปัญหาช่องโหว่ดังกล่าวเรียบร้อยแล้ว และคาดว่าอาจมีการเผยแพร่ให้ใช้งานอย่างเป็นทางการ ร่วมกับฟังก์ชันอื่น ๆ ที่พัฒนาเพิ่มเติม ในช่วงเดือนมีนาคม 2557 [3] แต่อย่างไรก็ตามผู้ใช้งานจำเป็นต้องพึงระวังเก็บโทรศัพท์หรืออุปกรณ์ต่าง ๆ ไว้ใกล้ตัวเพื่อป้องกันการถูกขโมย รวมถึงตั้งค่า Passcode สำหรับล็อกเครื่องเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอีกด้วย

อ้างอิง

1. http://www.youtube.com/watch?v=K7VelNyEMf8
2. http://support.apple.com/kb/PH13695
3. http://9to5mac.com/2014/02/07/apple-currently-plans-to-ship-ios-7-1-in-march/

ระวังภัย ช่องโหว่ 0-day ใน Internet Explorer 9, 10 (CVE-2014-0322) หน่วยงานในสหรัฐฯ ถูกโจมตีแล้ว

วันที่ประกาศ : 20 กุมภาพันธ์ 2557
ปรับปรุงล่าสุด : 20 กุมภาพันธ์ 2557
เรื่อง : ระวังภัย ช่องโหว่ 0-day ใน Internet Explorer 9, 10 (CVE-2014-0322) หน่วยงานในสหรัฐฯ ถูกโจมตีแล้ว
ประเภทภัยคุกคาม : Intrusion

9

ข้อมูลทั่วไป

เมื่อวันที่ 13 กุมภาพันธ์ 2557 บริษัท Fireeye ได้ออกมาประกาศผ่านเว็บไซต์เรื่องช่องโหว่ในโปรแกรม Internet Explorer เวอร์ชัน 9 และ 10 ซึ่งอนุญาตให้ผู้ไม่หวังดีสามารถสั่งประมวลผลคำสั่งไม่พึงประสงค์บนเครื่องของเหยื่อจากระยะไกลได้ (Remote Code Execution) **[1]** ช่องโหว่ดังกล่าวนี้ยังอยู่ระหว่างการตรวจสอบและยังไม่มีวิธีแก้ไข

ในการโจมตี ผู้ไม่หวังดีจะสร้างเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ หรือแทรกโค้ดที่มีอันตรายนั้นไว้ในเว็บไซต์ที่ถูกแฮก จากนั้นใช้วิธีการทาง Social Engineering หลอกล่อให้เหยื่อเข้าไปยังเว็บไซต์ดังกล่าว โค้ดอันตรายที่ถูกฝังอยู่ก็จะเริ่มทำงานทันทีที่เหยื่อเข้าเยี่ยมชมหน้าเว็บไซต์

นอกจากนี้ยังมีรายงานว่าผู้ไม่หวังดีได้ฝังโค้ดไว้ในเว็บไซต์ชื่อ U.S. Veterans of Foreign Wars ซึ่งเป็นเว็บไซต์ด้านการทหารแห่งหนึ่งของประเทศสหรัฐอเมริกา เพื่อให้หน้าเว็บไซต์ดังกล่าว Redirect ไปยังหน้าเว็บไซต์ที่มีโค้ดที่โจมตีผ่านช่องโหว่ดังกล่าวนี้ **[2]**

ผลกระทบ

ผู้ไม่หวังดีสามารถสั่งให้เครื่องของเหยื่อประมวลผลคำสั่งจากระยะไกลเพื่อควบคุมเครื่องคอมพิวเตอร์ เพียงแค่หลอกล่อให้เหยื่อเข้าไปยังเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ **[3]**

ระบบที่ได้รับผลกระทบ

Internet Explorer เวอร์ชัน 9 และ 10

10

ข้อแนะนำในการป้องกันและแก้ไข

จากสถิติของเว็บไซต์ TrueHits พบว่าในเดือนมกราคม 2557 ผู้ใช้งานอินเทอร์เน็ตในประเทศไทย ยังมีการใช้งาน Internet Explorer 8 อยู่ถึง 7.93% และ Internet Explorer 9 อยู่ถึง 3.56% ซึ่งผู้ใช้เหล่านี้มีโอกาสเสี่ยงที่จะถูกโจมตีผ่านช่องโหว่ดังกล่าว **[4]** อย่างไรก็ตาม ในขณะนี้ ทาง Microsoft ยังอยู่ระหว่างการตรวจสอบข้อมูล และยังไม่มีแพตช์แก้ไขช่องโหว่ดังกล่าวออกมา สำหรับผู้ที่ใช้ระบบปฏิบัติการ Windows 7 หรือ Windows 8 ควรเปลี่ยนไปใช้ Internet Explorer เวอร์ชัน 11 และสำหรับผู้ที่ใช้ระบบปฏิบัติการ Windows XP ที่ไม่สามารถติดตั้ง Internet Explorer 11 ได้ควรเปลี่ยนไปใช้เบราว์เซอร์อื่นเป็นการชั่วคราว

อย่างไรก็ตามหากจำเป็นต้องใช้ Internet Explorer 9 หรือ 10 ทาง Microsoft ได้มีทางออกชั่วคราวโดยสามารถใช้ทางเลือกดังกล่าวนี้ในการลดความเสียหายที่อาจจะเกิดขึ้นได้โดย **[5]**

- ติดตั้งโปรแกรม Fix It สำหรับช่องโหว่นี้ โดยสามารถดาวน์โหลดและติดตั้งได้จาก https://support.microsoft.com/kb/2934088

- ติดตั้งโปรแกรม EMET และกำหนดค่าให้ใช้งานกับโปรแกรม Internet Explorer ซึ่งทางไทยเซิร์ตเคยเผยแพร่บทความเรื่องวิธีการใช้งาน EMET ไว้แล้ว **[5]**

- กำหนดค่า Security Level ของ Internet และ Local Intranet ใน Internet Explorer ให้เป็น High รวมถึงปิดการทำงานของ ActiveX Controls และ Active Scripting

- กำหนดค่าให้ Internet Explorer ถามการยืนยันจากผู้ใช้ทุกครั้งก่อนที่จะมีการใช้งาน Active Scripting ซึ่งวิธีการกำหนดค่า Security Level ของโปรแกรม Internet Explorer ผู้ใช้สามารถศึกษาได้จากหน้าเว็บไซต์ Security Advisory ของ Microsoft **[6]** ในส่วนหัวข้อ Suggested Actions

อ้างอิง

1. https://www.fireeye.com/blog/threat-research/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
2. http://www.zdnet.com/new-internet-explorer-10-zero-day-exploit-targets-u-s-military-7000026354/
3. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0322
4. http://truehits.net/graph/graph_stat.php#WEB%22%3Ehttp://truehits.net/graph/graph_stat.php#WEB
5. https://www.thaicert.or.th/papers/technical/2013/pa2013te005.html
6. https://technet.microsoft.com/en-us/security/advisory/2934088

ระวังภัย พบแอปพลิเคชันปลอม ของธนาคารในประเทศไทยใน Play Store

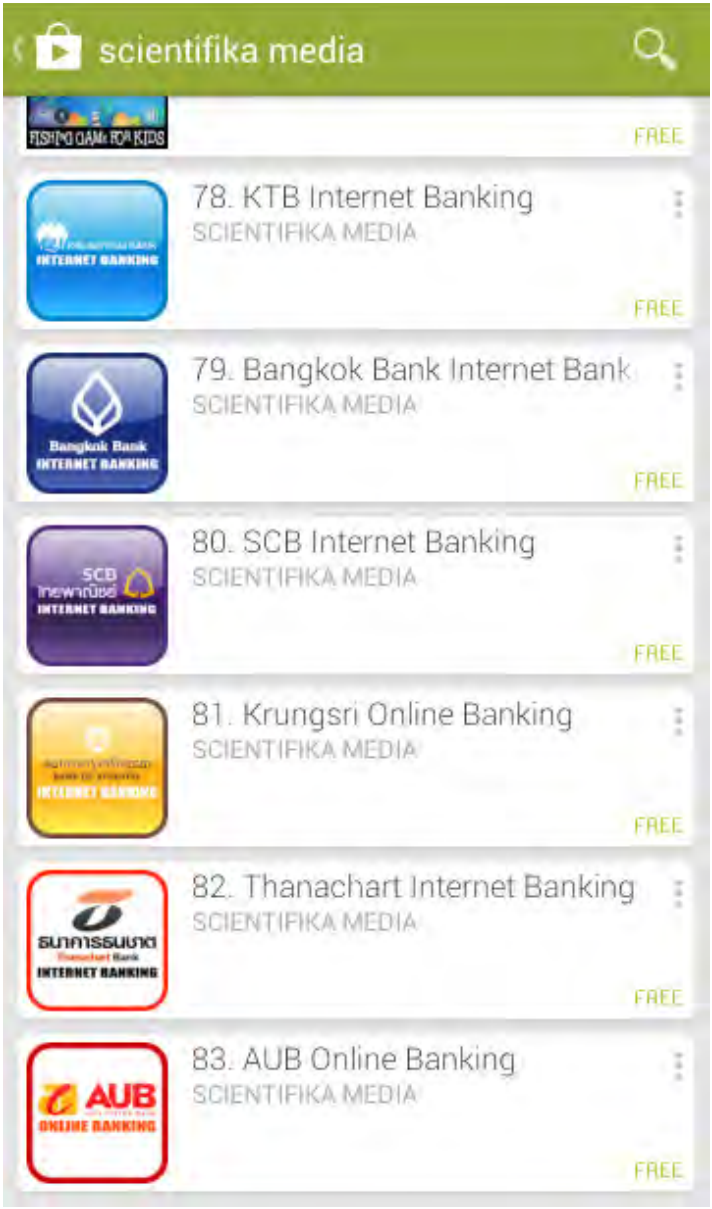
วันที่ประกาศ : 27 มีนาคม 2557
ปรับปรุงล่าสุด : 27 มีนาคม 2557
เรื่อง : ระวังภัย พบแอปพลิเคชันปลอมของธนาคารในประเทศไทยใน Play Store
ประเภทภัยคุกคาม : Fraud

ข้อมูลทั่วไป

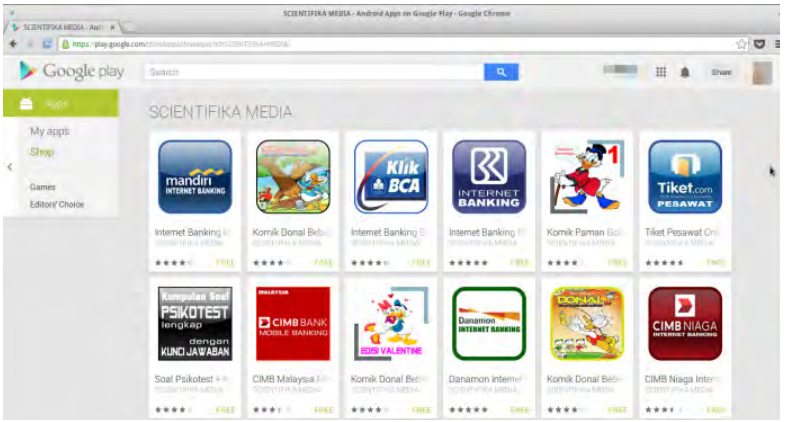
เมื่อวันที่ 26 มีนาคม 2557 ไทยเซิร์ตพบว่าใน Twitter ของธนาคารไทยพาณิชย์ มีการแจ้งเตือนแอปพลิเคชันปลอม ที่พยายามทำให้เข้าใจว่าเป็นแอปพลิเคชันของธนาคารไทยพาณิชย์ ปรากฏอยู่ใน Play Store ของ Google [1] ดังรูปที่ 1

รูปที่ 1 ประกาศใน Twitter ของธนาคารไทยพาณิชย์

จากการตรวจสอบเพิ่มเติม พบว่าแอปพลิเคชันปลอมดังกล่าวสร้างโดยนักพัฒนาที่ใช้ชื่อว่า SCIENTIFIKA MEDIA โดยนำขึ้นสู่ Google Play Store เมื่อวันที่ 25 มีนาคม และยังพบว่าผู้พัฒนารายนี้ ได้พัฒนาแอปพลิเคชันปลอมของธนาคารไทยรวม 5 แห่งคือ ธนาคารกรุงไทย ธนาคารกรุงเทพ ธนาคารไทยพาณิชย์ ธนาคารกรุงศรีอยุธยา และธนาคารธนชาต รวมถึงแอปพลิเคชันปลอมของธนาคารอื่น ๆ ในต่างประเทศด้วย ดังรูปที่ 2 และ 3



รูปที่ 2 แสดงรายการแอปพลิเคชันปลอมของธนาคารไทยบน Google Play Store



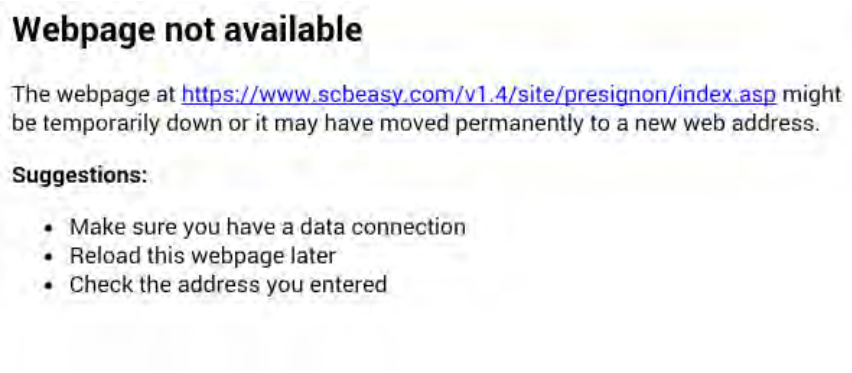
รูปที่ 3 ตัวอย่างรายการแอปพลิเคชันที่พัฒนาโดย SCIENTIFIKA MEDIA ใน Description ของแอปพลิเคชันปลอม พบว่ามีการระบุว่าเป็นแอปพลิเคชันสำหรับแสดงผลหน้าเว็บไซต์ของทางธนาคาร ตามรูปที่ 4

รูปที่ 4 แสดง Description ของแอปพลิเคชัน

เมื่อเรียกใช้งานแอปพลิเคชันปลอม จะพบหน้าจอให้ใส่รหัสผ่านสำหรับเข้าใช้งานบัญชีธนาคารออนไลน์ โดยมีโฆษณาปรากฏอยู่ด้านล่าง ดังรูปที่ 5

รูปที่ 5 แสดงตัวอย่างหน้าหลักของแอปพลิเคชันปลอม

ในกรณีที่โทรศัพท์มือถือหรือแท็บเล็ตไม่ได้เชื่อมต่อกับอินเทอร์เน็ต เมื่อเปิดแอปพลิเคชันดังกล่าวจะพบกับข้อความระบุว่าไม่สามารถเข้าถึงเว็บไซต์ของธนาคารได้ โดยมีลักษณะคล้ายคลึงกับเมื่อเปิดเว็บไซต์บน Web Browser ซึ่ง URL ที่ไม่สามารถเข้าถึงได้นั้นเป็นของเว็บไซต์ธนาคารจริง
ดังรูปที่ 6



รูปที่ 6 แสดงตัวอย่างหน้าหลักของแอปพลิเคชันปลอม ในกรณีที่ไม่ได้เชื่อมต่อกับอินเทอร์เน็ต

และจากการตรวจสอบ Permission ที่แอปพลิเคชันร้องขอ พบว่าทั้ง 5 แอปพลิเคชันต้องการสิทธิ์ในการเชื่อมต่ออินเทอร์เน็ตและแสดงผล Ads เท่านั้น ดังรูปที่ 7

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1" android:versionName="1.0" package="com.scb.internetbanking"
 xmlns:android="http://schemas.android.com/apk/res/android">
   <uses-permission android:name="android.permission.INTERNET" />
   <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
   <meta-data android:name="ADMOB_ALLOW_LOCATION_FOR_ADS" android:value="true" />
   <application android:theme="@*android:style/Theme.NoTitleBar" android:label="@string/app_name"
android:icon="@drawable/ic_launcher">
      <activity android:label="@string/app_name" android:name="SCBInternetBanking"
android:configChanges="keyboard|keyboardHidden|orientation|screenLayout|uiMode|screenSize|
smallestScreenSize">
         <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
         </intent-filter>
      </activity>
      <activity android:name="com.google.ads.AdActivity" android:configChanges="keyboard|keyboardHidden|
orientation|screenLayout|uiMode|screenSize|smallestScreenSize" />
   </application>
</manifest>
```

รูปที่ 7 แสดงข้อมูล Permission ที่แอปพลิเคชันร้องขอ

เมื่อดูในโค้ดของโปรแกรม พบว่ามีการทำงานหลัก ๆ อยู่เพียง 2 อย่าง คือใช้ WebView แสดงผลหน้า Login ของธนาคาร และติดต่อกับ Google Ads เพื่อแสดงโฆษณา โดยยังไม่พบโค้ดที่เป็นการดักขโมยข้อมูลหรือโค้ดที่น่าสงสัยว่าเป็นพฤติกรรม

ประสงค์ร้าย และจากการวิเคราะห์โค้ดของแอปพลิเคชันปลอมทั้ง 5 ตัว พบว่ามีลักษณะคล้ายคลึงกัน ต่างกันที่ไอคอนและเว็บไซต์ที่แสดงผลในหน้า WebView เท่านั้น และจากการตรวจสอบการรับส่งข้อมูลโดยใช้โปรแกรม Wireshark ไม่พบว่ามีการดักขโมยข้อมูลส่งไปให้ผู้ไม่หวังดี

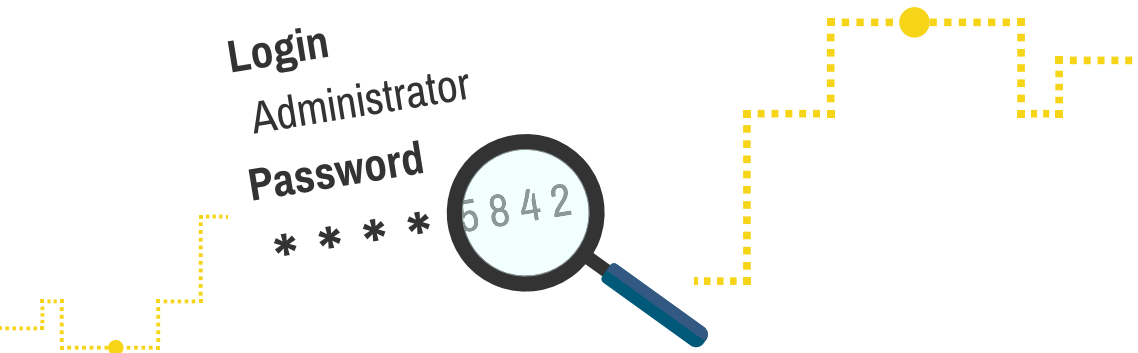
ผลกระทบ

แอปพลิเคชันปลอมกลุ่มนี้เป็นลักษณะของ Web Browser ที่เปิดไปยังหน้า Internet Banking ของแต่ละธนาคารโดยตรง พร้อมทั้งมีการแสดงโฆษณาเพื่อหารายได้ให้กับผู้พัฒนาเท่านั้น โดยยังไม่พบว่ามีพฤติกรรมประสงค์ร้ายในขณะนี้ อย่างไรก็ตาม การใช้งานแอปพลิเคชันลักษณะนี้ในการทำธุรกรรมออนไลน์ถือว่ามีความเสี่ยง เนื่องจากผู้ใช้ไม่สามารถทราบได้ว่าแอปพลิเคชันที่ใช้งานอยู่นั้นมีการขโมยข้อมูลหรือไม่ หรือในอนาคตแอปพลิเคชันที่พบในขณะนี้ไม่มีพฤติกรรมประสงค์ร้าย จะมีการอัปเดตตัวเองเพื่อให้มีความสามารถอื่น ๆ ที่เป็นอันตรายเพิ่มขึ้นหรือไม่ ผู้ใช้งานจึงควรทำธุรกรรมออนไลน์ผ่านทางแอปพลิเคชันที่เป็นทางการของธนาคารเท่านั้น

ข้อแนะนำเบื้องต้นในการตรวจสอบแอปพลิเคชันที่น่าสงสัย

• ตรวจสอบจากชื่อ Developer โดยแอปพลิเคชันที่มาจากธนาคารส่วนใหญ่จะใช้ชื่อธนาคาร โดยมี รายการชื่อ Developer ดังต่อไปนี้

- ธนาคารกรุงไทย: Krung Thai Bank PCL.
- ธนาคารกรุงเทพ: Bangkok Bank PCL
- ธนาคารไทยพาณิชย์: Siam Commercial Bank PCL.
- ธนาคารกรุงศรีอยุธยา: Bank of Ayudhya Public Company Limited



- ธนาคารธนชาต: 2Fellows Network and Design co.,ltd และ Thanachart Bank Plc.

• ตรวจสอบจากจำนวนดาวน์โหลด และรีวิวของผู้ใช้งาน โดยสังเกตแอปพลิเคชันที่มียอดดาวน์โหลดที่ต่ำหรือรีวิวของผู้ใช้งานที่แจ้งถึงความผิดปกติ

• ตรวจสอบจากธนาคาร โดยอาจเข้าไปดูรายละเอียดของแอปพลิเคชันจากเว็บไซต์ของธนาคาร หรือสอบถามจากธนาคารโดยตรง

หากผู้ใช้งานพบแอปพลิเคชันปลอมในลักษณะนี้ หรือแอปพลิเคชันที่มีลักษณะน่าสงสัย หรือเป็นอันตราย สามารถแจ้ง Google เพื่อตรวจสอบและดำเนินการได้ โดยใช้แอปพลิเคชัน Play Store ใน Android เข้าไป ที่หน้าแอปพลิเคชันนั้น เลือกคำสั่ง Flag as inappropriate พร้อมระบุเหตุผล แล้วกด Submit เพื่อส่งข้อมูลให้ Google พิจารณา [2]

อ้างอิง

1. https://twitter.com/scb_thailand/status/448787719846522880
2. https://support.google.com/googleplay/answer/2479847?hl=en

ระวังภัย ช่องโหว่ 0-day ใน WinRAR ผู้ไม่หวังดีสามารถปลอมแปลง Extension ของไฟล์ที่อยู่ภายในไฟล์ .ZIP เพื่อหลอกให้ติดตั้งมัลแวร์

วันที่ประกาศ : 3 เมษายน 2557
ปรับปรุงล่าสุด : 4 เมษายน 2557
เรื่อง : ระวังภัย ช่องโหว่ 0-day ใน WinRAR ผู้ไม่หวังดีสามารถปลอมแปลง Extension ของไฟล์ที่อยู่ภายในไฟล์ .ZIP เพื่อหลอกให้ติดตั้งมัลแวร์
ประเภทภัยคุกคาม : Malicious Code

ข้อมูลทั่วไป

เมื่อวันที่ 23 มีนาคม 2557 นักวิจัยด้านความมั่นคงปลอดภัยชาวอิสราเอลชื่อ Danor Cohen ได้ประกาศการค้นพบช่องโหว่ในโปรแกรม WinRAR ซึ่งทำให้ผู้ไม่หวังดีสามารถปลอมแปลงนามสกุล (Extension) ของไฟล์ที่อยู่ในไฟล์ .ZIP เพื่อหลอกให้ผู้ใช้เปิดใช้งานไฟล์ดังกล่าวได้ **[1]**

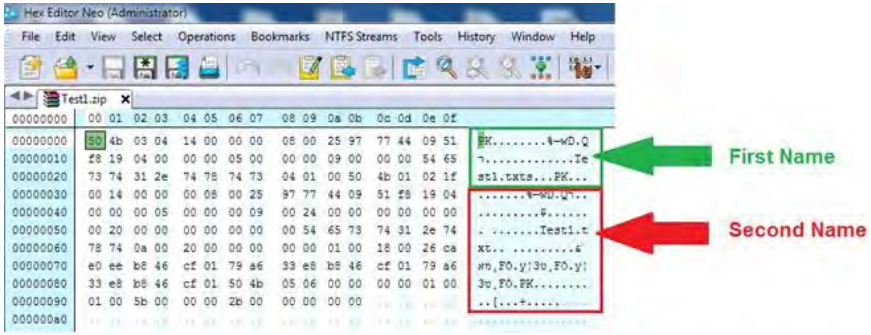
โดยปกติแล้ว โครงสร้างของไฟล์ .ZIP จะเป็นดังรูปที่ 1 โดย Offset ที่ 30 คือชื่อดั้งเดิมของไฟล์ที่อยู่ในไฟล์ .ZIP

Offset	Bytes	Description[25]
0	4	Local file header signature = 0x04034b50 (read as a little-endian number)
4	2	Version needed to extract (minimum)
6	2	General purpose bit flag
8	2	Compression method
10	2	File last modification time
12	2	File last modification date
14	4	CRC-32
18	4	Compressed size
22	4	Uncompressed size
26	2	File name length (*n*)
28	2	Extra field length (*m*)
30	*n*	File name
30+*n*	*m*	Extra field

รูปที่ 1 โครงสร้างของไฟล์ .ZIP

เมื่อใช้โปรแกรม WinRAR สร้างไฟล์ .ZIP ก็จะได้ไฟล์ที่มีโครงสร้างตามรูปที่ 1 แต่ฟังก์ชันสร้างไฟล์ .ZIP ของโปรแกรม WinRAR มีการสร้างข้อมูลส่วนขยายเพิ่มเข้ามาอีก คือส่วนที่เป็นคุณสมบัติของไฟล์ที่อยู่ในไฟล์ .ZIP ซึ่งข้อมูลดังกล่าวมีส่วนของชื่อไฟล์ด้วย ทำให้ในไฟล์ .ZIP มีข้อมูลของชื่อไฟล์ที่อยู่ข้างใน ปรากฏอยู่ 2 ที่

นักวิจัยพบว่า ข้อมูลชื่อไฟล์ที่อยู่ในไฟล์ .ZIP ถูกใช้งานแตกต่างกัน คือชื่อไฟล์ที่แสดงอยู่ในตำแหน่งแรก (ลูกศรสีเขียว) จะเป็นชื่อไฟล์ที่ได้หลังจากที่ Extract ไฟล์ออกมา ซึ่งจะเป็นชื่อไฟล์เดียวกันกับที่แสดงเมื่อใช้โปรแกรม WinRAR เปิดดูไฟล์ .ZIP ในขณะที่ชื่อไฟล์ในตำแหน่งที่สอง (ลูกศรสีแดง) เป็นส่วนอธิบายรายละเอียดของไฟล์ ซึ่งโปรแกรม WinRAR สร้างขึ้นมาเพิ่มเติม ตัวอย่างข้อมูลชื่อไฟล์ที่ปรากฏอยู่ในไฟล์ .ZIP ดังแสดงในรูปที่ 2



รูปที่ 2 ตัวอย่างข้อมูลชื่อไฟล์ที่ปรากฏปรากฏอยู่ในไฟล์ .ZIP

สาเหตุของช่องโหว่ในครั้งนี้ เกิดจากการที่โปรแกรมไม่มีการตรวจสอบว่าชื่อไฟล์ในทั้ง 2 ตำแหน่งนั้นตรงกันหรือไม่ ทำให้ผู้ไม่หวังดีสามารถแก้ไขชื่อไฟล์ให้แสดงผลในโปรแกรม WinRAR เป็นชื่อหนึ่ง แต่เมื่อ Extract ไฟล์ออกมา ปรากฏเป็นอีกชื่อหนึ่งได้

ผลกระทบ

ผู้ไม่หวังดีสามารถใช้โปรแกรม WinRAR สร้างไฟล์ .ZIP ที่ภายในบรรจุโปรแกรมอันตรายไว้ (เช่น ไฟล์ .EXE) แล้วแก้ไขข้อมูลชื่อไฟล์ดังกล่าวให้เป็นไฟล์ที่ไม่น่าจะมีลักษณะอันตราย (เช่น เปลี่ยนนามสกุลเป็นไฟล์ .txt หรือ .mp3) ซึ่งหากผู้ใช้หลงเชื่อและดับเบิลคลิกไฟล์ดังกล่าวจากหน้าต่างโปรแกรม WinRAR ก็จะเป็นการเรียกใช้งานโปรแกรมอันตรายนั้นทันที

ปัจจุบันพบการโจมตีผ่านช่องโหว่นี้แล้ว โดยพบว่ามีการส่งอีเมลที่แนบไฟล์ .ZIP ดังตัวอย่างในรูปที่ 3 ไปยังหน่วยงานสำคัญๆ ในต่างประเทศ เช่น สถานทูต บริษัท หรือหน่วยงานทางทหาร

รูปที่ 3 ตัวอย่างการโจมตีผ่านทางอีเมล

ระบบที่ได้รับผลกระทบ

ในเบื้องต้นนาย Danor แจ้งว่าช่องโหว่ดังกล่าวนี้มีผลกระทบกับโปรแกรม WinRAR เวอร์ชัน 4.2.0 แต่จากการตรวจสอบเพิ่มเติมของบริษัท IntelCrawler พบว่าช่องโหว่นี้มีผลกับโปรแกรม WinRAR ทุกเวอร์ชัน [2]

ข้อแนะนำในการป้องกันและแก้ไข

1. ผู้ใช้งานควรมีความระมัดระวังการเปิดใช้งานไฟล์ต่าง ๆ ที่ได้รับ และพิจารณาอีเมลที่มีการแนบไฟล์ โดยเฉพาะอย่างยิ่งไฟล์ที่บีบอัดด้วยนามสกุล .ZIP ซึ่งอาจเป็นอีเมลของผู้ไม่หวังดีเพื่อหลอกให้ติดมัลแวร์

2. ติดตั้งโปรแกรมแอนติไวรัสที่มีการอัปเดตอยู่เสมอ เพื่อใช้ในการสแกนไฟล์มัลแวร์ที่อาจถูกลักลอบส่งเข้ามาผ่านเทคนิคของช่องโหว่นี้

อ้างอิง

1. http://an7isec.blogspot.co.il/2014/03/winrar-file-extension-spoofing-0day.html
2. http://intelcrawler.com/report_2603.pdf

ระวังภัย ช่องโหว่
Adobe Flash Player ผู้ไม่หวังดี สามารถควบคุมเครื่องได้ (CVE-2014-0515)

วันที่ประกาศ : 29 เมษายน 2557
ปรับปรุงล่าสุด : 29 เมษายน 2557
เรื่อง : ระวังภัย ช่องโหว่ใน Adobe Flash Player ผู้ไม่หวังดี สามารถควบคุมเครื่องได้ (CVE-2014-0515)
ประเภทภัยคุกคาม : Other

ข้อมูลทั่วไป

เมื่อวันที่ 28 เมษายน 2557 บริษัท Adobe ได้แจ้งเตือนช่องโหว่ของโปรแกรม Adobe Flash Player ที่มีผลกับผู้ใช้งานระบบปฏิบัติการ Windows, Mac OS X และ Linux **[1]** ผู้โจมตีสามารถใช้ช่องโหว่ดังกล่าวในการสั่งประมวลผลคำสั่งใด ๆ บนเครื่องคอมพิวเตอร์ของเหยื่อจากระยะไกลได้ (Remote Code Execution) ช่องโหว่นี้มีหมายเลข CVE-2014-0515 อย่างไรก็ตาม แม้ว่าช่องโหว่นี้จะได้รับการประกาศออกมาในระยะเวลาใกล้เคียงกับช่องโหว่ CVE-2014-1776 ของ Internet Explorer **[2]** ซึ่งระบุว่าต้องอาศัย Adobe Flash Player ในการโจมตี แต่ขณะนี้ยังไม่สามารถยืนยันได้ว่า ช่องโหว่นี้มีความเกี่ยวข้องกับช่องโหว่ CVE-2014-1776 หรือไม่

ผลกระทบ

เครื่องคอมพิวเตอร์ที่มีการติดตั้ง Adobe Flash Player เวอร์ชันที่ได้รับผลกระทบ เมื่อเปิดไฟล์ .SWF ที่มีคำสั่งไม่พึงประสงค์ อาจถูกติดตั้งมัลแวร์หรืออาจถูกสั่งให้ประมวลผลคำสั่งไม่พึงประสงค์จากระยะไกลเพื่อควบคุมเครื่องคอมพิวเตอร์

ระบบที่ได้รับผลกระทบ

- Adobe Flash Player เวอร์ชัน 13.0.0.182 หรือต่ำกว่า บนระบบปฏิบัติการ Windows
- Adobe Flash Player เวอร์ชัน 13.0.0.201 หรือต่ำกว่า บนระบบปฏิบัติการ Mac OS X

•Adobe Flash Player เวอร์ชัน 11.2.202.350 หรือต่ำกว่า บนระบบปฏิบัติปฏิบัติการ Linux

ข้อแนะนำในการป้องกันและแก้ไข

Adobe ได้ออกซอฟต์แวร์อัปเดตเพื่อแก้ไขช่องโหว่นี้แล้ว ผู้ใช้งานระบบปฏิบัติการ Windows และ Mac OS X สามารถติดตั้ง Adobe Flash Player เวอร์ชัน 13.0.0.206 ส่วนผู้ใช้งานระบบปฏิบัติการ Linux สามารถติดตั้ง Adobe Flash Player เวอร์ชัน 11.2.202.356 โดยสามารถดาวน์โหลดซอฟต์แวร์ดังกล่าวได้จากเว็บไซต์ของ Adobe **[3]**

อ้างอิง

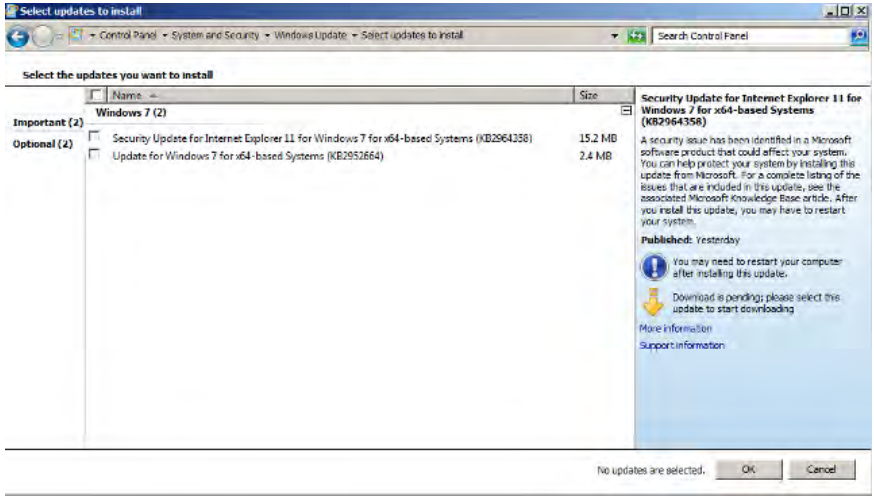
1. http://helpx.adobe.com/security/products/flash-player/apsb14-13.html
2. https://www.thaicert.or.th/alerts/user/2014/al2014us010.html
3. https://www.adobe.com/support/flashplayer/downloads.html

ระวังภัย ช่องโหว่ 0-day ใน Internet Explorer 6 ถึง 11 (CVE-2014-1776)

วันที่ประกาศ : 29 เมษายน 2557
ปรับปรุงล่าสุด : 5 พฤษภาคม 2557
เรื่อง : ระวังภัย ช่องโหว่ 0-day ใน Internet Explorer 6 ถึง 11 (CVE-2014-1776)
ประเภทภัยคุกคาม : Intrusion

ข้อมูลล่าสุด (2 พ.ค. 2557)

ไทยเซิร์ตพบว่า เมื่อวันที่ 1 พฤษภาคม 2557 เวลาประมาณ 23 นาฬิกาตามเวลาของประเทศไทย ไมโครซอฟท์ได้ปล่อยอัปเดตเพื่อปิดช่องโหว่นี้ผ่านระบบ Windows Update เป็นที่เรียบร้อยแล้ว ผู้ใช้สามารถรับการแก้ไขช่องโหว่ได้โดยใช้ Windows Update ได้แล้วในขณะนี้ โดยไทยเซิร์ต แนะนำให้ผู้ใช้งาน Windows เข้าไปตรวจสอบหน้า Windows Update ของตนเองเพื่อให้แน่ใจว่าแพตช์ดังกล่าวได้รับการติดตั้งเรียบร้อยแล้ว ซึ่งแพตช์สำหรับแก้ไขช่องโหว่นี้จะมีหมายเลขเป็น KB2964358 หรือ KB2964444 ขึ้นอยู่กับระบบปฏิบัติการที่ใช้และเวอร์ชันของ Internet Explorer ที่ติดตั้งอยู่ในเครื่อง **[1]**



รูปที่ 1 แสดงแพตช์สำหรับช่องโหว่ที่ปรากฏใน Windows Update ของ IE11 บน Windows 7

นอกจากนี้ ไมโครซอฟท์ได้ระบุว่า Windows XP ที่ถึงแม้จะหมดระยะเวลาสนับสนุนทางเทคนิคไปแล้ว ก็จะได้รับแพตช์สำหรับช่องโหว่นี้ด้วยเป็นกรณีพิเศษด้วย แต่อย่างไรก็ตาม ไมโครซอฟท์ก็ยังแนะนำให้ผู้ใช้งาน Windows XP เปลี่ยนไปใช้ Windows 7 หรือ 8.1 เพื่อให้ได้รับการสนับสนุนทางเทคนิคที่ต่อเนื่อง **[2]**

ข้อมูลทั่วไป

เมื่อวันที่ 26 เมษายน 2557 ไมโครซอฟท์ได้ออกมาประกาศผ่านเว็บเรื่องช่องโหว่ในโปรแกรม Internet Explorer เวอร์ชัน 6 ถึง 11 ซึ่งอนุญาตให้ผู้ไม่หวังดีสามารถสั่งประมวลผลคำสั่งไม่พึงประสงค์บนเครื่องของเหยื่อได้ (Remote Code Execution) **[3]** ช่องโหว่ดังกล่าวนี้ยังอยู่ระหว่างการตรวจสอบและยังไม่มีวิธีแก้ไขโดยตรง

ในการโจมตี ผู้ไม่หวังดีจะสร้างเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ หรือแทรกโค้ดที่มีอันตรายนั้นไว้ในเว็บไซต์ที่ถูกแฮก จากนั้นใช้วิธีการทาง Social Engineering หลอกล่อให้เหยื่อเข้าไปยังเว็บไซต์ดังกล่าว จากนั้นโค้ดอันตรายที่ถูกฝังอยู่ก็จะเริ่มทำงานทันทีที่เหยื่อเข้าเยี่ยมชมหน้าเว็บไซต์

ผลกระทบ

ช่องโหว่ดังกล่าวนี้สามารถโจมตีได้ด้วยการฝังโค้ดอันตรายไว้ในเว็บไซต์ ซึ่งหากผู้ใช้งานเข้าชมเว็บไซต์ที่ผู้ไม่หวังดีเตรียมไว้ อาจถูกติดตั้งมัลแวร์หรืออาจถูกสั่งให้ประมวลผลคำสั่งไม่พึงประสงค์จากระยะไกลเพื่อควบคุมเครื่องคอมพิวเตอร์

จากข้อมูลสถิติของเว็บไซต์ TrueHits พบว่าในเดือนมีนาคม 2557 ผู้ใช้งานอินเทอร์เน็ตในประเทศไทย ยังมีการใช้งาน Internet Explorer อยู่ไม่น้อยกว่า 13.27% **[4]** ซึ่งผู้ใช้เหล่านี้มีโอกาสเสี่ยงที่จะถูกโจมตีผ่านช่องโหว่ดังกล่าว นอกจากนี้ เนื่องจากบริษัทไมโครซอฟท์ได้หยุดการให้การสนับสนุนด้านเทคนิคแก่ Windows XP แล้ว อาจทำให้ผู้ใช้งาน Internet Explorer บนระบบปฏิบัติการดังกล่าว ไม่ได้รับแพตช์แก้ไขช่องโหว่นี้เมื่อมีการปล่อยออกมาด้วย

ระบบที่ได้รับผลกระทบ

Internet Explorer ตั้งแต่เวอร์ชัน 6 ถึง 11

ข้อแนะนำในการป้องกันและแก้ไข

ในขณะนี้ ไมโครซอฟท์ยังอยู่ระหว่างการดำเนินการ และยังไม่มีแพตช์แก้ไขช่องโหว่ดังกล่าวออกมา อย่างไรก็ตาม จากการแนะนำของไมโครซอฟท์ **[3]** ให้ดำเนินการดังต่อไปนี้เพื่อป้องกันผลกระทบที่เกิดจากช่องโหว่ดังกล่าว

1. ติดตั้งโปรแกรม EMET 4.1 หรือ 4.0 และกำหนดค่าให้ใช้งานกับโปรแกรม Internet Explorer ซึ่งทางไทยเซิร์ตเคยเผยแพร่บทความเรื่องวิธีการใช้งาน EMET ไว้แล้ว **[5]**

2. กำหนดค่า Security Level ของ Internet และ Local Intranet ใน Internet Explorer ให้เป็น High รวมถึงปิดการทำงานของ ActiveX Controls และ Active Scripting อย่างไรก็ตามการใช้วิธีการนี้ อาจทำให้บางเว็บไซต์มีปัญหาในการแสดงผลได้

3. หากใช้งาน Internet Explorer เวอร์ชัน 10 และ 11 บน Windows 7 ขึ้นไปที่เป็นระบบปฏิบัติการชนิด 64 บิต ให้เปิดการใช้งาน Enhanced Protected Mode (EPM)

หากว่าไม่สามารถดำเนินโดยวิธีอื่นได้ จากคำแนะนำของ US-CERT อาจพิจารณาเปลี่ยนไปใช้เบราว์เซอร์อื่นเป็นการชั่วคราว **[6]** เช่น Chrome หรือ Firefox จนกว่าบริษัทไมโครซอฟท์จะออกแพตช์มาแก้ไข

นอกจากนี้ ผู้ใช้ควรตั้งค่าการปรับปรุงระบบของ Windows (Windows Update) **[7]** เพื่อให้สามารถอัปเดต Internet Explorer โดยอัตโนมัติ และสำหรับวิธีการอื่น ๆ ที่สามารถป้องกันผลกระทบของช่องโหว่นี้ได้ ผู้ใช้งานสามารถศึกษาเพิ่มเติมได้จากเว็บไซต์ของไมโครซอฟท์ **[3]**

ผู้ใช้ที่ได้ปฏิบัติตามข้อแนะนำในการป้องกันและแก้ไขที่ได้กล่าวไว้ข้างต้น ไทยเซิร์ตแนะนำว่า หากทำการติดตั้ง EMET หรือเปิดการใช้งาน Enhanced Protected Mode (EPM) ไว้ หากไม่พบปัญหาในการใช้งานใด ๆ อาจจะคงใช้งานต่อไปได้โดยไม่ต้องการเปลี่ยนแปลงการตั้งค่า เพื่อเพิ่มความมั่นคงปลอดภัยและลดผลกระทบจากการโจมตีอื่น ๆ ในอนาคต แต่สำหรับผู้ที่ได้กำหนดค่า Security Level ของ Internet และ Local Intranet ใน Internet Explorer ให้เป็น High และปิดการทำงานของ ActiveX Controls และ Active Scripting อาจจะพิจารณาเปลี่ยนค่าใช้งานกลับเป็นค่าเดิมได้ หลังจากได้ติดตั้งแพตช์เรียบร้อยแล้ว

อ้างอิง

1. https://technet.microsoft.com/library/security/ms14-021
2. http://blogs.technet.com/b/msrc/archive/2014/05/01/out-of-band-release-to-address-microsoft-security-advisory-2963983.aspx
3. https://technet.microsoft.com/en-US/library/security/2963983
4. http://truehits.net/graph/graph_stat.php#WEB
5. https://www.thaicert.or.th/papers/technical/2013/pa2013te005.html
6. http://www.us-cert.gov/ncas/current-activity/2014/04/28/Microsoft-Internet-Explorer-Use-After-Free-Vulnerability-Being
7. http://windows.microsoft.com/en-us/windows/turn-automatic-updating-on-off#turn-automatic-updating-on-off=windows-7

ระวังภัย
แอปธนาคารปลอมบน Android

วันที่ประกาศ : 23 พฤษภาคม 2557
ปรับปรุงล่าสุด : 23 พฤษภาคม 2557
เรื่อง : ระวังภัย แอปธนาคารปลอมบน Android
ประเภทภัยคุกคาม : Fraud

เมื่อวันที่ 21 พฤษภาคม 2557 ไทยเซิร์ตได้รับรายงานว่า พบแอปพลิเคชันปลอมของธนาคารในประเทศไทยบนระบบปฏิบัติการ Android ที่พยายามทำให้เข้าใจว่าเป็นแอปพลิเคชันของธนาคารไทยพาณิชย์และธนาคารกสิกรไทยเผยแพร่อยู่ที่เว็บไซต์ downloads.applications.customersecurity.user-3729.com ซึ่งเมื่อตรวจสอบแล้วพบว่าตั้งอยู่ในประเทศออสเตรีย ดังรูปที่ 1 แอปพลิเคชันดังกล่าว เมื่อติดตั้งในเครื่องโทรศัพท์ จะปรากฏหน้าจอดังรูปที่ 2

```
                                :~$ nslookup downloads.applications.customersecu
rity.user-3729.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
downloads.applications.customersecurity.user-3729.com   canonical name = user-37
29.com.
Name:   user-3729.com
Address: 91.194.254.71

                                :~$ whois 91.194.254.71
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '91.194.254.0 - 91.194.255.255'

% No abuse contact registered for 91.194.254.0 - 91.194.255.255

inetnum:        91.194.254.0 - 91.194.255.255
netname:        DIMLINE-NET
descr:          Dimline Ltd.
country:        AT
org:            ORG-DL53-RIPE
```

รูปที่ 1 แสดง DNS Lookup และ Whois ของเว็บไซต์ที่เผยแพร่มัลแวร์

รูปที่ 2 ตัวอย่างหน้าจอแอปพลิเคชันปลอม

จากการตรวจสอบ พบว่าแอปพลิเคชันทั้งสองแอปพลิเคชัน มีหน้าจอที่พยายามแสดงให้ผู้ใช้งานเข้าใจว่า เป็นแอปพลิเคชันที่สามารถสร้างรหัสผ่านโอทีพี (OTP - One Time Password) สำหรับล็อกอินบริการธนาคารทางอินเทอร์เน็ต

รูปที่ 3 สิทธิ (Permission) ที่แอปพลิเคชันสามารถเข้าถึงได้

จากการตรวจสอบสิทธิ (Permission) ที่แอปพลิเคชันร้องขอ พบว่าแอปพลิเคชันดังกล่าวต้องการรับและส่ง SMS รวมถึงความสามารถในการเชื่อมต่อกับอินเทอร์เน็ต ดังรูปที่ 3

- Sent SMS

Timestamp	Number	Data
26.133	+79255419513	357242043237517 268823
27.130	+79255419513	357242043237517 392779
28.130	+79255419513	357242043237517 503281
29.130	+79255419513	357242043237517 503281
32.132	+79255419513	357242043237517 503281
32.133	+79255419513	357242043237517 284674
33.132	+79255419513	357242043237517 209688

รูปที่ 4 แสดงการส่ง SMS ไปยังหมายเลข +79255419513

Network Traffic Analysis

- DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
funnygnommi.com	DNS_TYPE_A		0	udp

รูปที่ 5 แสดงการทำ DNS Lookup เพื่อจะเชื่อมต่อไปยัง funnygnommi.com

เมื่อนำแอปพลิเคชันดังกล่าวไปตรวจสอบกับบริการ Anubis **[1]** พบว่ามีการพยายามส่งข้อมูลบางอย่างผ่าน SMS ไปยังหมายเลขโทรศัพท์ที่อยู่ในประเทศรัสเซีย (+79255419513) และมีพฤติกรรมที่จะพยายามเชื่อมต่อไปยัง funnygnommi.com ดังรูปที่ 4 และ 5 ซึ่งจากการตรวจสอบพบว่าเว็บเซิร์ฟเวอร์ตั้งอยู่ที่ประเทศรัสเซียและยูเครน

ผลกระทบ

ผู้ใช้ที่ติดตั้งแอปพลิเคชันดังกล่าวอาจถูกขโมยข้อมูลสำคัญจาก SMS เช่น ข้อมูลรหัสผ่านโอทีพี สำหรับเข้าทำธุรกรรมทางอิเล็กทรอนิกส์ โดยข้อมูลดังกล่าวอาจถูกนำไปใช้โดยผู้ไม่หวังดีและนำไปสู่การขโมยเงินจากบัญชีธนาคารภายหลังได้

ข้อแนะนำในการป้องกันและแก้ไข

ผู้ใช้งานควรติดตั้งแอปพลิเคชันจากแหล่งที่น่าเชื่อถือเท่านั้น เช่น Google Play Store แต่สำหรับแอปพลิเคชันที่เกี่ยวกับธุรกรรมทางการเงิน ควรเพิ่มความระมัดระวังเป็นพิเศษ เนื่องเคยมีการพบแอปพลิเคชันปลอมของธนาคารในประเทศไทยใน Google Play Store เมื่อเดือนมีนาคม **[2]** มาแล้ว ดังนั้น ผู้ใช้อาจตรวจสอบแอปพลิเคชันที่น่าสงสัยได้โดยวิธีการดังต่อไปนี้

• ตรวจสอบจากชื่อ Developer โดยแอปพลิเคชันที่มาจากธนาคารส่วนใหญ่ที่ใช้ชื่อธนาคาร โดยมีรายการชื่อ Developer ดังต่อไปนี้

- ธนาคารกรุงไทย: Krung Thai Bank PCL.
- ธนาคารกรุงเทพ: Bangkok Bank PCL
- ธนาคารไทยพาณิชย์: Siam Commercial Bank PCL.
- ธนาคารกรุงศรีอยุธยา: Bank of Ayudhya Public Company Limited
- ธนาคารธนชาต: 2Fellows Network and Design co.,ltd และ Thanachart Bank Plc.

• ตรวจสอบจากจำนวนดาวน์โหลด และรีวิวของผู้ใช้งาน โดยสังเกตแอปพลิเคชันที่มียอดดาวน์โหลดที่ต่ำหรือรีวิวของผู้ใช้งานที่แจ้งถึงความผิดปกติ

• ตรวจสอบจากธนาคาร โดยอาจเข้าไปดูรายละเอียดของแอปพลิเคชันจากเว็บไซต์ของธนาคาร หรือสอบถามจากธนาคารโดยตรง

• ตรวจสอบการร้องขอสิทธิ (Permission) ของแอปพลิเคชัน ว่ามีความเหมาะสมหรือไม่ เช่นแอปพลิเคชันที่มีการขอสิทธิในการส่ง SMS ควรทราบว่ามีการส่งไปที่ใด เพื่อจุดประสงค์อะไร

นอกจากนี้ผู้ใช้งานสามารถศึกษาบทความที่ไทยเซิร์ตได้เคยเผยแพร่ ถึงวิธีการตรวจสอบและป้องกันปัญหามัลแวร์ รวมถึงวิธีการใช้งานโทรศัพท์มือถือให้มั่นคงปลอดภัย จากบทความดังต่อไปนี้

- แนวทางการใช้งานโทรศัพท์มือถือให้มั่นคงปลอดภัยจากภัยคุกคาม **[3]**
- รู้ทันและป้องกัน Malware ในระบบปฏิบัติการ Android **[4]**
- รู้ทันและป้องกัน Malware ในระบบปฏิบัติการ Android ตอนที่ 2 **[5]**

สำหรับผู้ดูแลระบบ ในขณะนี้อาจทำการปิดกั้นการเชื่อมต่อไปยังเว็บไซต์ downloads.applications.customersecurity.user-3729.com เป็นการชั่วคราว เพื่อป้องกันไม่ให้ผู้ใช้งานเข้าไปดาวน์โหลดแอปพลิเคชันปลอมนี้ และส่งผลให้ผู้ไม่หวังดีสามารถขโมยข้อมูลของผู้ใช้งานได้

อ้างอิง

1. http://anubis.iseclab.org/?action=result&task_id=147b6b3a6d09692c49976adc25a7e7145&format=html
2. https://www.thaicert.or.th/alerts/user/2014/al2014us008.html
3. http://www.thaicert.or.th/papers/general/2011/pa2011ge010.html
4. http://www.thaicert.or.th/papers/technical/2012/pa2012te003.html
5. http://www.thaicert.or.th/papers/technical/2012/pa2012te011.html

ระวังภัย ช่องโหว่ 0-day ใน Internet Explorer 8 (CVE-2014-1770)

วันที่ประกาศ : 22 พฤษภาคม 2557
เรื่อง : ระวังภัย ช่องโหว่ 0-day ใน Internet Explorer 8 (CVE-2014-1770)
ประเภทภัยคุกคาม : Intrusion

ข้อมูลทั่วไป

เมื่อวันที่ 21 พฤษภาคม 2557 Zero Day Initiative (ZDI) **[1]** ซึ่งเป็นโครงการหนึ่งของบริษัท HP **[2]** ได้ออกมาประกาศผ่านเว็บไซต์เรื่องช่องโหว่ในโปรแกรม Internet Explorer เวอร์ชัน 8 ซึ่งอนุญาตให้ผู้ไม่หวังดีสามารถสั่งประมวลผลคำสั่งไม่พึงประสงค์บนเครื่องของเหยื่อได้ (Remote Code Execution) **[3]** โดยระบุว่าได้มีการค้นพบช่องโหว่นี้ตั้งแต่เดือนตุลาคม ปี 2556 และแจ้งไปยังบริษัทไมโครซอฟท์แล้ว แต่จนถึงปัจจุบันนี้ก็ยังไม่ได้มีการออกแพตช์มาแก้ไขช่องโหว่ดังกล่าวแต่อย่างใด

ในการโจมตี ผู้ไม่หวังดีจะสร้างเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ หรือแทรกโค้ดที่มีอันตรายนั้นไว้ในเว็บไซต์ที่ถูกแฮก จากนั้นใช้วิธีการทาง Social Engineering หลอกล่อให้เหยื่อเข้าไปยังเว็บไซต์ดังกล่าว จากนั้นโค้ดอันตรายที่ถูกฝังอยู่ก็จะเริ่มทำงานทันทีที่เหยื่อเข้าเยี่ยมชมหน้าเว็บไซต์ การโจมตีนี้มีรูปแบบเช่นเดียวช่องโหว่ที่เคยมีการแจ้งเตือนไปก่อนหน้านี้ในเว็บไซต์ของไทยเซิร์ต **[4]** เพียงแต่อาศัยช่องโหว่ที่แตกต่างกันเท่านั้น

ผลกระทบ

ช่องโหว่ดังกล่าวนี้สามารถโจมตีได้ด้วยการฝังโค้ดอันตรายไว้ในเว็บไซต์ ซึ่งหากผู้ใช้งานเข้าชมเว็บไซต์ที่ผู้ไม่หวังดีเตรียมไว้ อาจถูกติดตั้งมัลแวร์หรืออาจถูกสั่งให้ประมวลผลคำสั่งไม่พึงประสงค์จากระยะไกลได้ (Remote Code Execution)

จากข้อมูลสถิติของเว็บไซต์ TrueHits พบว่าในเดือนเมษายน 2557 ผู้ใช้งานอินเทอร์เน็ตในประเทศไทย ยังมีการใช้งาน Internet Explorer เวอร์ชัน 8 นี้อยู่ไม่น้อยกว่า 6.66% **[5]** ซึ่งผู้ใช้เหล่านี้มีโอกาสเสี่ยงที่จะถูกโจมตีผ่านช่องโหว่ดังกล่าว อย่างไรก็ตาม เมื่อพิจารณาจากข้อมูลย้อนหลังในเว็บไซต์ TrueHits จะเห็นได้ว่า จำนวนผู้ใช้ Internet Explorer เวอร์ชันนี้มีแนวโน้มลดลงตามลำดับ

แต่เนื่องจาก Internet Explorer เวอร์ชัน 8 นี้ เป็นเวอร์ชันสุดท้ายที่ยังสามารถใช้งานได้กับ Windows XP โดยไม่สามารถอัปเกรดเป็นเวอร์ชันที่ใหม่กว่านี้ได้อีกแล้ว ผู้ที่ยังใช้งาน Windows XP อยู่ จึงเป็นกลุ่มที่ตกอยู่ในความเสี่ยง แม้ว่าจะไม่ได้ใช้ Internet Explorer เวอร์ชัน 8 เป็นเว็บเบราว์เซอร์หลักก็ตาม เนื่องจากซอฟต์แวร์อื่น ๆ ที่อยู่ในเครื่องคอมพิวเตอร์ อาจมีการเรียกใช้ความสามารถของ Internet Explorer ในการแสดงเอกสาร HTML ทำให้มีโอกาสที่โปรแกรม Internet Explorer ที่มีช่องโหว่นี้ ถูกเรียกใช้งานขึ้นมาโดยที่ผู้ใช้งานไม่ทราบ และเป็นช่องทางให้ผู้ไม่หวังดีทำการโจมตีได้

ระบบที่ได้รับผลกระทบ

Internet Explorer เวอร์ชัน 8 ในระบบปฏิบัติการ Windows ทุกเวอร์ชัน

ข้อแนะนำในการป้องกันและแก้ไข

ในขณะนี้ ยังไม่มีแพตช์แก้ไขช่องโหว่ดังกล่าวออกมา และยังไม่มีการแถลงข่าวใด ๆ จากไมโครซอฟท์เกี่ยวกับช่องโหว่นี้ อย่างไรก็ตาม ผู้ที่ใช้งานระบบปฏิบัติการ Windows เวอร์ชัน Vista ขึ้นไป สามารถอัปเกรด Internet Explorer เป็นเวอร์ชัน 9 หรือใหม่กว่าได้ เพื่อป้องกันผลกระทบจากช่องโหว่นี้ แต่สำหรับผู้ที่ยังต้องใช้งาน Windows XP อยู่ และไม่สามารถอัปเกรด Internet Explorer ได้ จากคำแนะนำของ ZDI ผู้ใช้งานสามารถปฏิบัติตามคำแนะนำต่อไปนี้เพื่อลดผลกระทบของช่องโหว่ได้

1. ติดตั้งโปรแกรม EMET 4.1 และกำหนดค่าให้ใช้งานกับโปรแกรม Internet Explorer ซึ่งทางไทยเซิร์ตเคยเผยแพร่บทความเรื่องวิธีการใช้งาน EMET ไว้แล้ว **[6]**

2. กำหนดค่า Security Level ของ Internet, Local Intranet และ Restricted Sites ใน Internet Explorer ให้เป็น High รวมถึงปิดการทำงานของ ActiveX Controls และ Active Scripting อย่างไรก็ตามการใช้วิธีการนี้ อาจทำให้บางเว็บไซต์มีปัญหาในการแสดงผลได้

นอกจากนี้ ผู้ใช้ควรตั้งค่าการปรับปรุงระบบของ Windows (Windows Update) **[7]** เพื่อให้สามารถอัปเดต Internet Explorer โดยอัตโนมัติ ในกรณีที่อาจมีการเผยแพร่แพตช์สำหรับช่องโหว่นี้ หรือช่องโหว่อื่น ๆ ในอนาคตจากไมโครซอฟท์

อ้างอิง

1. http://zerodayinitiative.com
2. http://www8.hp.com/us/en/software-solutions/enterprise-security.html
3. http://zerodayinitiative.com/advisories/ZDI-14-140
4. https://thaicert.or.th/alerts/user/2014/al2014us010.html
5. http://truehits.net/graph/graph_stat.php#WEB
6. https://www.thaicert.or.th/papers/technical/2013/pa2013te005.html
7. http://windows.microsoft.com/en-us/windows/turn-automatic-updating-on-off#turn-automatic-updating-on-off=windows-7

ระวังภัย Apple
เผยแพร่อัปเดตของ Safari เพื่อแก้ไขช่องโหว่ Remote Code Execution ผู้ใช้งานควรอัปเดตทันที

วันที่ประกาศ : 24 พฤษภาคม 2557
เรื่อง : Apple เผยแพร่อัปเดตของ Safari เพื่อแก้ไขช่องโหว่ Remote Code Execution ผู้ใช้งานควรอัปเดตทันที
ประเภทภัยคุกคาม : Intrusion

ข้อมูลทั่วไป

เมื่อวันที่ 21 พฤษภาคม 2557 บริษัท Apple ได้เผยแพร่อัปเดตของโปรแกรมเว็บเบราว์เซอร์ Safari ซึ่งเป็นเว็บเบราว์เซอร์ที่ติดตั้งอยู่ในระบบปฏิบัติการ Mac OS X จากรายละเอียดที่ปรากฏในเว็บไซต์ของ Apple **[1]** ระบุว่ามีการแก้ไขช่องโหว่ในลักษณะ Remote Code Execution จำนวน 22 รายการ ซึ่งในการโจมตี ผู้ไม่หวังดีจะสร้างเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ หรือแทรกโค้ดที่มีอันตรายนั้นไว้ในเว็บไซต์ที่ถูกแฮก จากนั้นใช้วิธีการทาง Social Engineering หลอกล่อให้เหยื่อเข้าไปยังเว็บไซต์ดังกล่าว โค้ดอันตรายที่ถูกฝังอยู่ก็จะเริ่มทำงานทันทีที่เหยื่อเข้าเยี่ยมชมหน้าเว็บไซต์

ผลกระทบ

ช่องโหว่ดังกล่าวนี้สามารถโจมตีได้ด้วยการฝังโค้ดอันตรายไว้ในเว็บไซต์ ซึ่งหากผู้ใช้งานเข้าชมเว็บไซต์ที่ผู้ไม่หวังดีเตรียมไว้ อาจถูกติดตั้งมัลแวร์หรืออาจถูกสั่งให้ประมวลผลคำสั่งไม่พึงประสงค์จากระยะไกลได้ (Remote Code Execution)

จากข้อมูลสถิติของเว็บไซต์ TrueHits พบว่าในเดือนเมษายน 2557 ผู้ใช้งานอินเทอร์เน็ตในประเทศไทย มีการใช้งานโปรแกรม Safari อยู่ไม่น้อยกว่า 25.29% **[2]** ซึ่งผู้ใช้เหล่านี้ส่วนหนึ่งใช้งานโปรแกรม Safari บนระบบปฏิบัติการ Mac OS X ซึ่งมีโอกาสเสี่ยงที่จะถูกโจมตีผ่านช่องโหว่ดังกล่าวได้

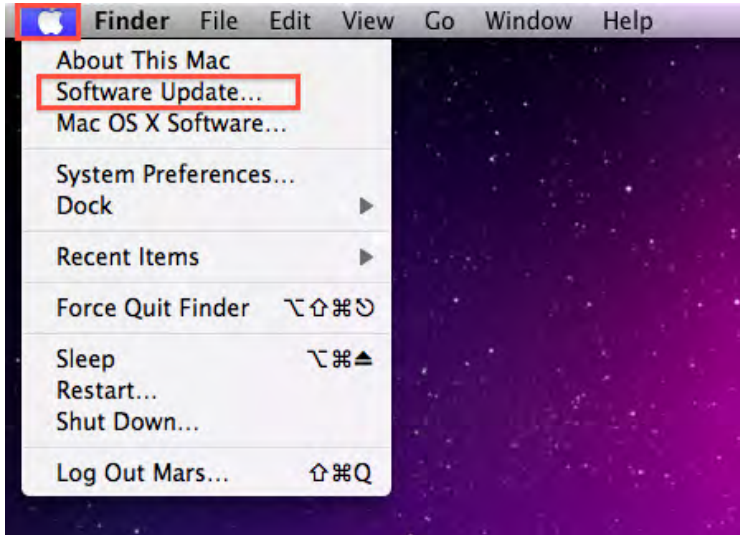
ระบบที่ได้รับผลกระทบ

โปรแกรม Safari ในระบบปฏิบัติการ Mac OS X

ข้อแนะนำในการป้องกันและแก้ไข

จากข้อมูลที่ปรากฏในเว็บไซต์ของ Apple นั้น ระบุว่ามีการเผยแพร่อัปเดตผ่านระบบ Software Update ของระบบปฏิบัติการ Mac OS X **[3]** ซึ่งผู้ใช้งานสามารถเข้าไปตรวจสอบสถานะการอัปเดตได้ที่ Apple Menu -> Software Update ดังรูปที่ 1

โปรแกรม Safari ที่ได้รับการอัปเดตอย่างถูกต้องแล้วจะเป็นเวอร์ชัน 7.0.4 สำหรับ Mac OS X 10.9 และ เวอร์ชัน 6.1.4 สำหรับ Mac OS X 10.8 และ 10.7



รูปที่ 1 แสดงเมนู Software Update ของ Mac OS X (ภาพจาก discussions.apple.com)

อย่างไรก็ตาม ในเว็บไซต์ของ Apple ยังไม่ได้มีการกล่าวถึงอัปเดตสำหรับผู้ที่ใช้ Mac OS X 10.6 หรือต่ำกว่า ข้อมูลของเว็บไซต์ Computerworld **[4]** และ The Inquirer **[5]** ระบุว่า Apple จะไม่มีการเผยแพร่อัปเดตสำหรับ Mac OS X 10.6 และต่ำกว่าอีกแล้ว ผู้ใช้งาน Mac OS X เวอร์ชันดังกล่าว จึงควรพิจารณาอัปเกรด Mac OS X ให้เป็นเวอร์ชันที่ใหม่กว่า เพื่อให้สามารถรับการอัปเดตด้านความมั่นคงปลอดภัยจาก Apple ต่อไป

อ้างอิง

1. http://support.apple.com/kb/HT6254
2. http://truehits.net/graph/graph_stat.php#WEB
3. http://support.apple.com/kb/HT1222
4. http://www.computerworld.com/s/article/9246609/Apple_retires_Snow_Leopard_from_support_leaves_1_in_5_Macs_vulnerable_to_attacks
5. http://www.theinquirer.net/inquirer/news/2331684/apples-end-of-support-for-snow-leopard-leaves-mac-users-open-to-malware

TrueCrypt ประกาศหยุดพัฒนา แจ้งเตือนให้ย้ายไปใช้งานโปรแกรมเข้ารหัสลับข้อมูลตัวอื่น

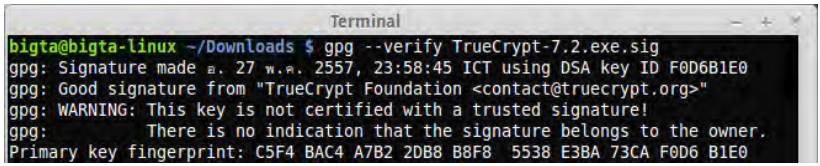
วันที่ประกาศ : 29 เมษายน 2557
เรื่อง : TrueCrypt ประกาศหยุดพัฒนา แจ้งเตือนให้ย้ายไปใช้งานโปรแกรมเข้ารหัสลับข้อมูลตัวอื่น
ประเภทภัยคุกคาม : Other

ข้อมูลทั่วไป

เมื่อวันที่ 28 พฤษภาคม 2557 เว็บไซต์ทางการของโปรแกรม TrueCrypt (www.truecrypt.org) ซึ่งเป็นโปรแกรมที่ใช้สำหรับเข้ารหัสลับข้อมูล ได้ประกาศว่าจะหยุดพัฒนาโปรแกรมนี้ตั้งแต่เดือนพฤษภาคม 2557 เป็นต้นไป และได้ขึ้นข้อความแจ้งเตือนว่าการใช้งานโปรแกรม TrueCrypt จะไม่มั่นคงปลอดภัยเพราะอาจมีช่องโหว่ด้านความมั่นคงปลอดภัยที่จะไม่ถูกแก้ไข **[1]** ข้อความที่ปรากฏในหน้าเว็บไซต์ TrueCrypt เป็นดังรูปที่ 1

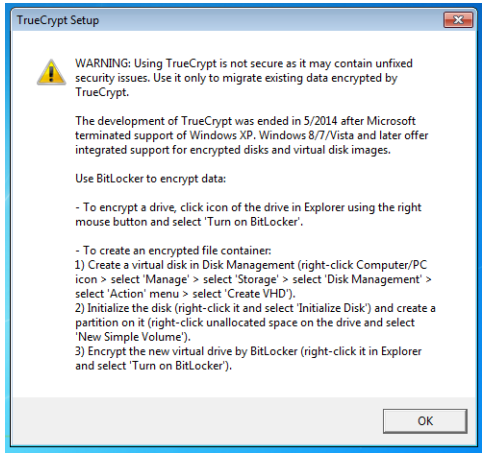
รูปที่ 1 ประกาศบนหน้าเว็บไซต์ TrueCrypt

ที่ด้านล่างสุดของหน้าเว็บไซต์ มีลิงก์สำหรับดาวน์โหลดโปรแกรม TrueCrypt เวอร์ชัน 7.2 ซึ่งเป็นเวอร์ชันล่าสุด จากการตรวจสอบ Signature พบว่าถูก Sign เมื่อวันที่ 28 พฤษภาคม 2557 เวลา 6:58:45 โดยใช้ key ID F0D6B1E0 ดังรูปที่ 2



รูปที่ 2 การตรวจสอบ Signature ของโปรแกรม TrueCrypt

เมื่อดับเบิลคลิกไฟล์ติดตั้ง จะพบหน้าต่างแจ้งเตือนว่าโปรแกรม TrueCrypt ไม่มั่นคงปลอดภัย และให้ย้ายข้อมูลออกไปใส่ในโปรแกรมที่มีการเข้ารหัสลับข้อมูลที่ดีกว่า ดังรูปที่ 3



รูปที่ 3 หน้าต่างแจ้งเตือนว่าโปรแกรม TrueCrypt ไม่มั่นคงปลอดภัย

จากการทดสอบ ทางไทยเซิร์ตพบว่าโปรแกรม TrueCryt เวอร์ชัน 7.2 ไม่สามารถเข้ารหัสลับข้อมูลได้ ทำได้เพียงอ่านข้อมูลจาก TrueCrypt Volumn เท่านั้น

อย่างไรก็ตาม ทาง TrueCrypt ไม่ได้ระบุถึงเหตุผลทางเทคนิคที่ทำให้ต้องหยุดพัฒนาโปรแกรมดังกล่าว และจากข้อมูลของโครงการ TrueCrypt Audit ซึ่งเป็นโครงการตรวจสอบซอร์สโค้ดของโปรแกรม TrueCrypt เพื่อหาช่องโหว่ด้านความมั่นคงปลอดภัย ก็ไม่ปรากฏข้อมูลรายละเอียดในเรื่องนี้ **[2]** นอกจากนี้ ทางทีมพัฒนา TrueCrypt นั้นไม่ได้เปิดเผยตัวตน ทำให้ในขณะนี้ยังไม่มีใครสามารถติดต่อทีมพัฒนาเพื่อสอบถามข้อมูลเพิ่มเติมได้ **[3]**

ผลกระทบ

เนื่องจากโปรแกรม TrueCrypt หยุดพัฒนา ทำให้ผู้ที่ใช้งานโปรแกรม TrueCrypt อาจถูกโจมตีผ่านช่องโหว่ที่ไม่มีการแก้ไข (0-day) หรือข้อมูลที่ถูกเข้ารหัสลับไว้อาจถูก

เปิดอ่านโดยผู้ไม่หวังดีได้

ระบบที่ได้รับผลกระทบ

โปรแกรม TrueCrypt ทุกเวอร์ชัน

ข้อแนะนำในการป้องกันและแก้ไข

ทาง TrueCrypt ได้แนะนำให้เปลี่ยนไปใช้งานโปรแกรมเข้ารหัสลับข้อมูลตัวอื่นที่มีความมั่นคงปลอดภัยมากกว่า สำหรับผู้ที่ใช้งานระบบปฏิบัติการ Windows Vista/7/8 ตัวระบบปฏิบัติการมีฟังก์ชัน BitLocker ซึ่งสามารถใช้เข้ารหัสลับข้อมูลในฮาร์ดดิสก์ได้ ซึ่งทาง TrueCrypt ได้แนะนำให้ผู้ใช้ย้ายข้อมูลออกจากไดรฟ์ที่เป็น TrueCrypt มาใส่ในไดรฟ์ที่เป็น BitLocker

สำหรับผู้ที่ใช้งานระบบปฏิบัติการ Linux หรือ Mac OS X ทาง TrueCrypt แนะนำให้ย้ายข้อมูลออกไปใส่ในพาร์ทิชันที่เข้ารหัสลับข้อมูลโดยโปรแกรมที่รองรับระบบปฏิบัติการนั้น ๆ **[4]** เช่น FileVault ใน Mac OS X หรือ LUKS ใน Linux เป็นต้น

อ้างอิง

1. http://truecrypt.sourceforge.net/
2. http://istruecryptauditedyet.com/
3. https://isc.sans.edu//diary/True+Crypt+Compromised++Removed?/18177
4. http://truecrypt.sourceforge.net/OtherPlatforms.html

ระวังภัย มัลแวร์
GameOver มีผู้ใช้ในประเทศไทยตกเป็นเหยื่อแล้วกว่าสามพันสี่ร้อยราย

วันที่ประกาศ : 5 มิถุนายน 2557
เรื่อง : ระวังภัย มัลแวร์ GameOver มีผู้ใช้ในประเทศตกเป็นเหยื่อแล้วกว่าสามพันสี่ร้อยราย
ประเภทภัยคุกคาม : Malicious Code

ข้อมูลทั่วไป

เมื่อวันที่ 2 มิถุนายน 2557 กระทรวงยุติธรรม ประเทศสหรัฐอเมริกา ได้ประกาศผ่านเว็บไซต์ว่า มีการเข้ายึดเครื่องคอมพิวเตอร์ C&C ของมัลแวร์ประเภท Botnet ที่ชื่อ GameOver โดยความร่วมมือของ FBI, Europol, National Crime Agency ประเทศอังกฤษ รวมถึงบริษัทด้าน IT Security อย่าง Symantec, Trend Micro, McAfee และหน่วยงานอื่น ๆ ในปฏิบัติการชื่อ Tovar **[1]**

GameOver เป็นมัลแวร์สายพันธุ์ตระกูลเดียวกับมัลแวร์ Zeus มีจุดประสงค์เพื่อขโมยข้อมูลสำคัญที่เกี่ยวกับการทำธุรกรรมออนไลน์ **[1]** และมีความสามารถดาวน์โหลดมัลแวร์อื่น ๆ เข้ามาในเครื่องได้อีก โดยข้อมูลจากบางแหล่งข่าว เช่น KrebsonSecurity **[2]** และ Nakedsecurity **[3]** ระบุว่า GameOver มีการดาวน์โหลดมัลแวร์ CryptoLocker มาติดในเครื่องของเหยื่อด้วย ซึ่งไทยเซิร์ตได้เคยเผยแพร่บทความเกี่ยวกับมัลแวร์ CryptoLocker นี้มาแล้ว **[4]**

การแพร่ระบาดของมัลแวร์ GameOver นั้นมีหลายรูปแบบเช่น วิธีการ Social Engineering หรืออาศัยช่องโหว่ของซอฟต์แวร์ โดยรายงานในปี พ.ศ. 2555 ของ Dell SecureWorks ระบุว่าได้พบการระบาดของมัลแวร์ดังกล่าวผ่านการส่งสแปม **[5]**

จากปฏิบัติการ Tovar ดังกล่าว ไทยเซิร์ตได้รับข้อมูลจาก US-CERT ซึ่งเป็นหน่วยงาน CSIRT ระดับประเทศของสหรัฐฯ รายงานว่ามีเครื่องคอมพิวเตอร์ในประเทศไทยจำนวนไม่ต่ำกว่า 3,400 เครื่องที่ติดมัลแวร์ GameOver และพยายามติดต่อกลับไปยัง C&C ที่ควบคุมไว้โดยเจ้าหน้าที่ของสหรัฐฯ ซึ่งไทยเซิร์ตได้ประสานงานไปยัง ISP เพื่อให้ดำเนินการต่อไปเป็นที่เรียบร้อยแล้ว

ถึงแม้ว่าเครื่องคอมพิวเตอร์ C&C จะควบคุมไว้ได้แล้ว แต่ก็ยังไม่สามารถแน่ใจได้ว่ามัลแวร์ที่ไม่ได้รับคำสั่งจาก C&C จะยังสามารถแสดงพฤติกรรมที่ไม่พึงประสงค์ ทำให้เกิดอันตรายแก่ผู้ที่ตกเป็นเหยื่อได้อีกหรือไม่ ผู้สงสัยว่าจะตกเป็นเหยื่อของมัลแวร์จึงควรตรวจสอบและกำจัดมัลแวร์โดยเร็วที่สุด

ผลกระทบ

เครื่องคอมพิวเตอร์ที่ติดมัลแวร์ GameOver อาจถูกขโมยข้อมูลสำคัญต่าง ๆ ที่เกี่ยวกับธุรกรรมออนไลน์ เช่น รหัสผ่าน ข้อมูลดังกล่าวอาจถูกนำไปใช้โดยผู้ไม่หวังดีและนำไปสู่การขโมยเงินจากบัญชีธนาคารภายหลัง และอาจถูกติดตั้งมัลแวร์ CryptoLocker ที่สามารถเข้ารหัสลับข้อมูล ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ และไฟล์ประเภทอื่น ๆ ในเครื่องคอมพิวเตอร์ของเหยื่อ ทำให้ไม่สามารถใช้งานไฟล์ข้อมูลดังกล่าวได้

ระบบที่ได้รับผลกระทบ

ผู้ที่สงสัยว่าตกเป็นเหยื่อของมัลแวร์ GameOver และ / หรือ มัลแวร์ CryptoLocker บนระบบปฏิบัติการ Windows

ข้อแนะนำในการป้องกันและแก้ไข

1. ติดตั้งโปรแกรมแอนติไวรัสที่ถูกลิขสิทธิ์ และอัปเดตฐานข้อมูลของโปรแกรมแอนติไวรัสอย่างสม่ำเสมอ เพื่อช่วยให้สามารถตรวจจับและป้องกันมัลแวร์ใหม่ ๆ ได้

2. หากสงสัยว่าจะตกเป็นเหยื่อของมัลแวร์นี้ หรือมัลแวร์อื่น ๆ ที่อยู่ในกลุ่ม Zeus ผู้ใช้งานควรเปลี่ยนรหัสผ่านในบัญชีต่าง ๆ ทันที เนื่องจากมีความเป็นไปได้ว่ารหัสผ่านอาจถูกขโมยโดยมัลแวร์ในเครื่องคอมพิวเตอร์

3. ควรตรวจสอบช่องโหว่ต่าง ๆ ของซอฟต์แวร์ที่ใช้งาน กับบริษัทผู้ผลิต หรือจากแหล่งข้อมูลทางด้าน Security ที่น่าเชื่อถืออยู่เสมอ และดำเนินการปรับปรุงซอฟต์แวร์ตามข้อแนะนำเพื่อแก้ไขช่องโหว่ในทันที

4. สำหรับมัลแวร์ GameOver ผู้ใช้งานสามารถใช้โปรแกรมเพื่อกำจัดมัลแวร์ที่ทาง US-CERT ได้แนะนำ **[6]** โดยมีรายละเอียดดังนี้

F-Secure

http://www.f-secure.com/en/web/home_global/online-scanner (WindowsVista, 7 and 8)

http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142 (Windows XP)

Heimdal

http://goz.heimdalsecurity.com (Microsoft Windows XP, Vista, 7, 8 and 8.1)

Microsoft

http://www.microsoft.com/security/scanner/en-us/default.aspx (Windows

8.1, Windows 8, Windows 7, Windows Vista, and Windows XP)

Sophos

http://www.sophos.com/VirusRemoval (Windows XP (SP2) and above)

Symantec

http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network (Windows XP, Windows Vista and Windows 7)

Trend Micro

http://www.trendmicro.com/threatdetector (Windows XP, Windows Vista, Windows 7, Windows 8/8.1, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2)

5. สำหรับเครื่องคอมพิวเตอร์ที่ติด CryptoLocker สามารถศึกษาวิธีการป้องกันและแก้ไขได้ที่ https://www.thaicert.or.th/papers/technical/2013/pa2013te011.html

อ้างอิง

1. http://www.justice.gov/opa/pr/2014/June/14-crm-584.html
2. http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/
3. http://nakedsecurity.sophos.com
4. https://www.thaicert.or.th/papers/technical/2013/pa2013te011.html
5. http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/
6. https://www.us-cert.gov/ncas/alerts/TA14-150A

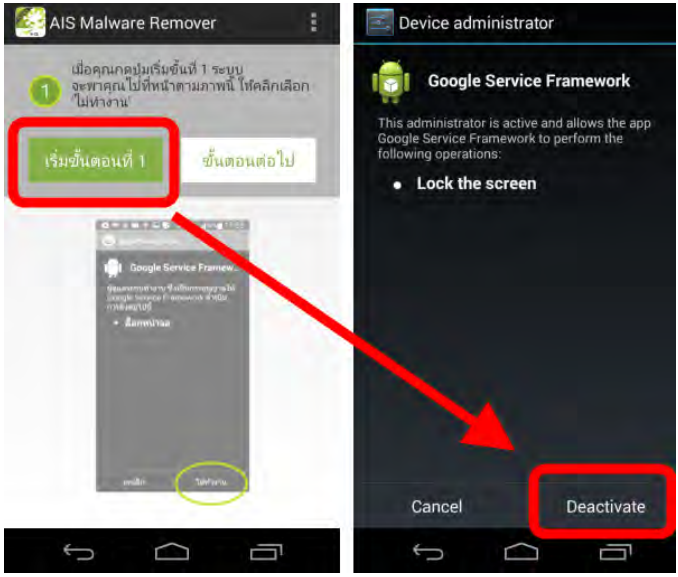
ระวังภัย มัลแวร์ใน Android (แจ้ง.apk, รับทราบ.apk) **แพร่กระจายด้วยการส่ง SMS**

วันที่ประกาศ : 13 สิงหาคม 2557
ปรับปรุงล่าสุด : 26 สิงหาคม 2557
เรื่อง : ระวังภัย มัลแวร์ใน Android (แจ้ง.apk, รับทราบ.apk) แพร่กระจายด้วยการส่ง SMS
ประเภทภัยคุกคาม : Malicious Code

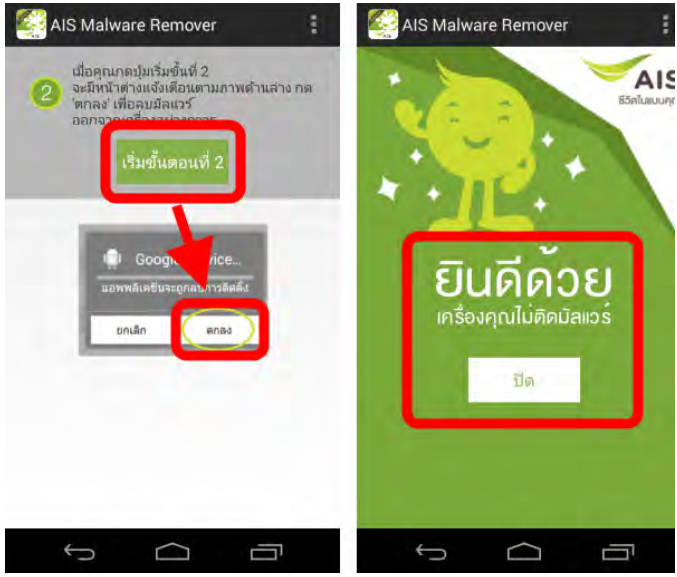
รูปที่ 1 ตัวอย่างแอปพลิเคชัน “AIS Malware Remover”

ปรับปรุงข้อมูลล่าสุด

วันที่ 26 สิงหาคม 2557 ไทยเซิร์ตได้รับแจ้งข้อมูลอีกครั้งถึงการเปลี่ยนลิงก์ที่ใช้เผยแพร่ไฟล์มัลแวร์ (แจ้ง.apk) มาเป็น http://goo.gl/INFLXN อย่างไรก็ตามจากการประสานงานแก้ไขปัญหาและตรวจสอบล่าสุดพบว่าลิงก์ทั้งหมดที่เกี่ยวข้องกับกรณีนี้ถูกปิดกั้นการเข้าถึงแล้ว รวมถึงทางบริษัท AIS ได้พัฒนาแอปพลิเคชันสำหรับอำนวยความสะดวกให้ผู้ใช้งานได้ตรวจสอบและถอนการติดตั้งมัลแวร์ตัวดังกล่าวบนระบบปฏิบัติการ Android โดยใช้ชื่อแอปพลิเคชันว่า “AIS Malware Remover” ผู้ใช้งานสามารถดาวน์โหลดได้แล้วที่ Google Play โดยมีตัวอย่างการใช้งานตามรูปที่ 1-3



รูปที่ 2 ตัวอย่างการทำงานของแอปพลิเคชันในขั้นตอนที่ 1 (ยกเลิกการให้สิทธิ Device Administration)

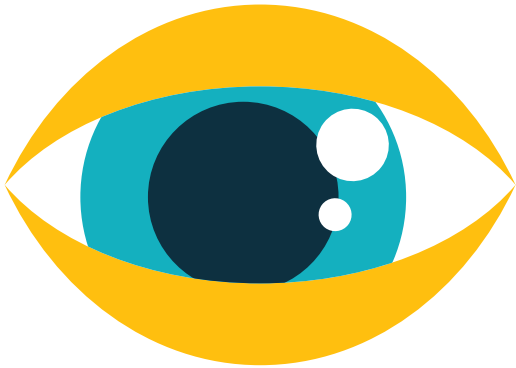


รูปที่ 3 ตัวอย่างการทำงานของแอปพลิเคชันในขั้นตอนที่ 2 (ถอนการติดตั้งแอปพลิเคชันมัลแวร์)

วันที่ 23 สิงหาคม 2557 ไทยเซิร์ตได้รับแจ้งข้อมูลอีกครั้ง ถึงการเปลี่ยนลิงก์ที่ใช้เผยแพร่ไฟล์มัลแวร์ (รับทราบ.apk) มาเป็น http://goo.gl/AjT773 อย่างไรก็ตามจากการตรวจสอบล่าสุดพบว่าลิงก์ที่ได้รับแจ้งในวันที่ 22 สิงหาคม 2557 ได้ถูกปิดกั้นและไม่สามารถเข้าถึงได้แล้ว และหากผู้ใช้งานท่านใดพบลิงก์มัลแวร์ที่เปลี่ยนแปลงไป สามารถแจ้งเข้ามายังไทยเซิร์ตเพื่อให้ประสานปิดกั้นการเข้าถึงได้ทันที

วันที่ 22 สิงหาคม 2557 ไทยเซิร์ตได้รับแจ้งข้อมูลเพิ่มเติมว่าผู้ไม่หวังดีมีการเปลี่ยนลิงก์ที่ใช้เผยแพร่ไฟล์มัลแวร์มาเป็น http://goo.gl/q87XnM เนื่องจากลิงก์ที่พบในวันที่ 21 สิงหาคม 2557 นั้นถูกปิดกั้นและไม่สามารถเข้าถึงได้แล้ว โดยพบว่าเมื่อคลิกลิงก์ดังกล่าวจะมีการ Redirect ไปยังเว็บไซต์ Dropbox เพื่อดาวน์โหลดไฟล์มัลแวร์ชื่อ รับทราบ.apk มาติดตั้ง และเมื่อมีการนำไฟล์มัลแวร์ทั้งหมดมาทำการ Decompile พบว่าซอร์สโค้ดของไฟล์มัลแวร์ แจ้ง.apk (พบในวันที่ 13 สิงหาคม 2557) ไฟล์มัลแวร์ รับทราบ.apk (พบในวันที่ 21 สิงหาคม 2557) ไฟล์มัลแวร์ รับทราบ.apk (พบในวันที่ 22 สิงหาคม 2557) มีการทำงานเหมือนกันทุกประการ ซึ่งจากการวิเคราะห์เพิ่มเติมทำให้คาดเดาได้ว่าการเผยแพร่มัลแวร์ตัวดังกล่าวอาจมีเป้าหมายเพื่อโจมตีผู้ใช้งานระบบธุรกรรมออนไลน์ต่าง ๆ เช่น e-Banking ด้วยการขโมย SMS มาใช้ในการทำธุรกรรมออนไลน์ ตามที่เคยเกิดขึ้นมาแล้วในอดีต

วันที่ 21 สิงหาคม 2557 ไทยเซิร์ตได้รับข้อมูลเพิ่มเติมว่าผู้ไม่หวังดีทำการส่งข้อความ SMS ไปยังผู้ใช้งานกลุ่มหนึ่ง โดยมีความพยายามเปลี่ยนแปลงข้อความให้แตกต่างไปจากวันที่ 13 สิงหาคม 2557 ว่า รับทราบ.apk และหากผู้ใช้งานคลิกไปยังลิงก์ดังกล่าวจะพบหน้าเว็บไซต์ Dropbox ที่ให้ดาวน์โหลดไฟล์ชื่อ รับทราบ.apk **[1]** มาติดตั้ง ตรวจสอบเบื้องต้นพบว่าค่าแฮชของไฟล์ รับทราบ.apk ไม่ตรงกับค่าแฮชของไฟล์ แจ้ง.apk ที่พบวันที่ 13 สิงหาคม 2557 และเมื่อนำไฟล์มัลแวร์มาทำการ Decompile เพื่อพิจารณาซอร์สโค้ดดู ทำให้สามารถยืนยันได้ว่าเป็นไฟล์มัลแวร์ตัวเดิม ที่มีฟังก์ชันการทำงานเหมือนเดิมทุกประการ โดยในความหมายของการทำให้ค่าแฮชของไฟล์มัลแวร์ไม่ตรงนั้น อาจหมายความว่าแฮกเกอร์ต้องการทำให้การตรวจสอบมัลแวร์เป็นไปได้ยากขึ้น เนื่องจากในกรณีดังกล่าวหากพบว่าไฟล์มัลแวร์มีค่าแฮชที่ตรงกัน ก็จะทำให้สามารถยืนยันได้ทันทีว่าเป็นมัลแวร์ตัวเดียวกัน



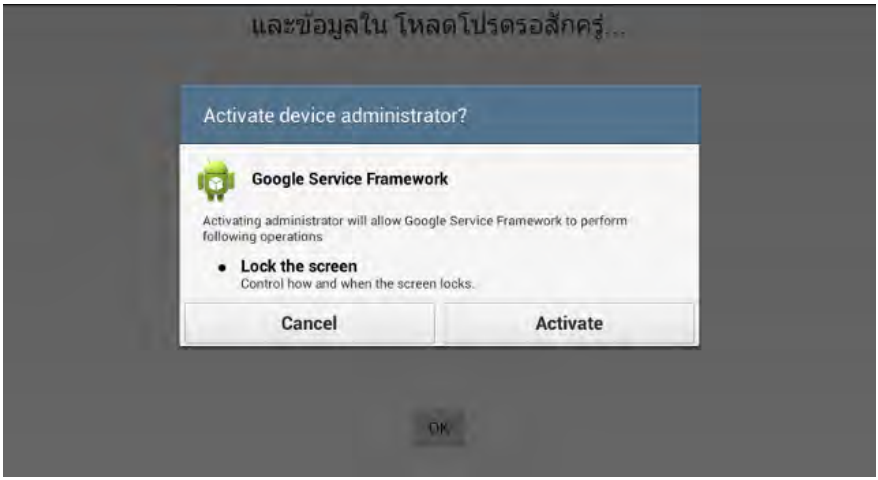
ข้อมูลทั่วไป

เมื่อวันที่ 13 สิงหาคม 2557 ไทยเซิร์ตได้รับรายงานว่ามีผู้ใช้งานโทรศัพท์มือถือระบบปฏิบัติการ Android ได้รับ SMS ข้อความ “(ชื่อผู้ติดต่อในโทรศัพท์), แจ้งให้ทราบการจัดส่งของคุณ http://goo.gl/NPD8sdb>” ซึ่งเมื่อเปิดลิงก์จะพาไปยังหน้าเว็บไซต์ Dropbox ซึ่งเป็นเว็บไซต์บริการรับฝากไฟล์ เพื่อดาวน์โหลดไฟล์ชื่อ “แจ้ง.apk” เมื่อติดตั้งแอปพลิเคชันจากไฟล์ .apk ดังกล่าวลงในเครื่องแล้ว แอปพลิเคชันนี้จะลักลอบส่ง SMS ออกไปยังหมายเลขโทรศัพท์อื่น ๆ ที่บันทึกอยู่ในเครื่อง เพื่อแพร่กระจายมัลแวร์ไปยังผู้ใช้รายอื่น **[2] [3]** จากการตรวจสอบโดยไทยเซิร์ตพบว่า แอปพลิเคชันดังกล่าวมีลักษณะเป็นโปรแกรมไม่พึงประสงค์ ผู้ใช้งานโทรศัพท์มือถือระบบปฏิบัติการ Android ควรตรวจสอบ SMS ที่น่าสงสัยและหลีกเลี่ยงการดาวน์โหลดหรือติดตั้งแอปพลิเคชันดังกล่าว

จากการวิเคราะห์ไฟล์ .apk ไทยเซิร์ตพบว่าแอปพลิเคชันดังกล่าวมีการร้องขอสิทธิ์การทำงาน (Permission) ที่น่าสงสัย ซึ่งการขอสิทธิ์ในลักษณะนี้ แอปพลิเคชันสามารถขโมยข้อมูลหรือทำให้ผู้ที่ติดตั้งแอปพลิเคชันดังกล่าวเสียเงินค่าส่ง SMS เป็นจำนวนมากได้ นอกจากนี้ แอปพลิเคชันยังมีการร้องขอสิทธิ Device Administration ในการล็อกหน้าจอ ซึ่งเป็นที่น่าสังเกตว่าการร้องขอสิทธิดังกล่าวอาจมีจุดประสงค์อื่นที่ไม่ดีด้วย

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="2" android:versionName="2.0" package="com.example.google.service"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.WRITE_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <application android:theme="@style/AppTheme" android:label="@string/activity_name" android:icon="@drawable/i
        <activity android:label="@string/app_name" android:name="com.example.google.service.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <service android:name="com.example.google.service.Services">
            <intent-filter>
                <action android:name="com.example.google.service.Services" />
            </intent-filter>
        </service>
        <receiver android:name="com.example.google.service.SMSServiceBootReceiver">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED" />
            </intent-filter>
        </receiver>
        <receiver android:name="com.example.google.service.SMSReceiver">
            <intent-filter android:priority="800">
                <action android:name="android.provider.Telephony.SMS_RECEIVED" />
            </intent-filter>
        </receiver>
        <receiver android:name="TaskRequest" />
        <receiver android:label="@string/app_name" android:name="com.example.google.service.MyDeviceAdminReceiver"
            <meta-data android:name="android.app.device_admin" android:resource="@xml/device_admin_sample" />
```

รูปที่ 4 สิทธิ์ที่แอปพลิเคชันสามารถเข้าถึงได้

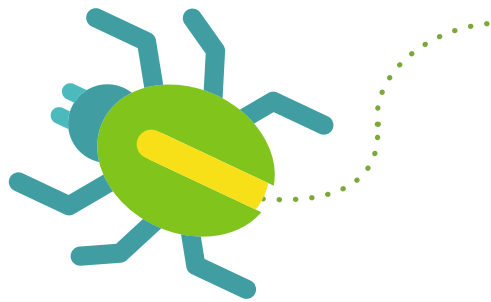


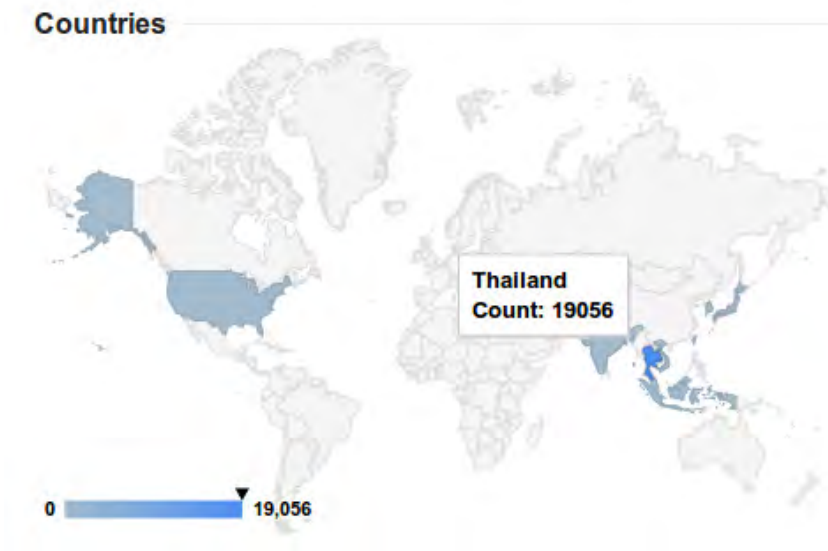
รูปที่ 5 การร้องขอสิทธิ Device Administration เมื่อเปิดแอปพลิเคชัน

ผลกระทบ

ผู้ใช้ที่ติดตั้งแอปพลิเคชันดังกล่าวลงในเครื่องอาจถูกขโมยข้อมูลรายชื่อผู้ติดต่อหรือข้อมูลอื่น ๆ

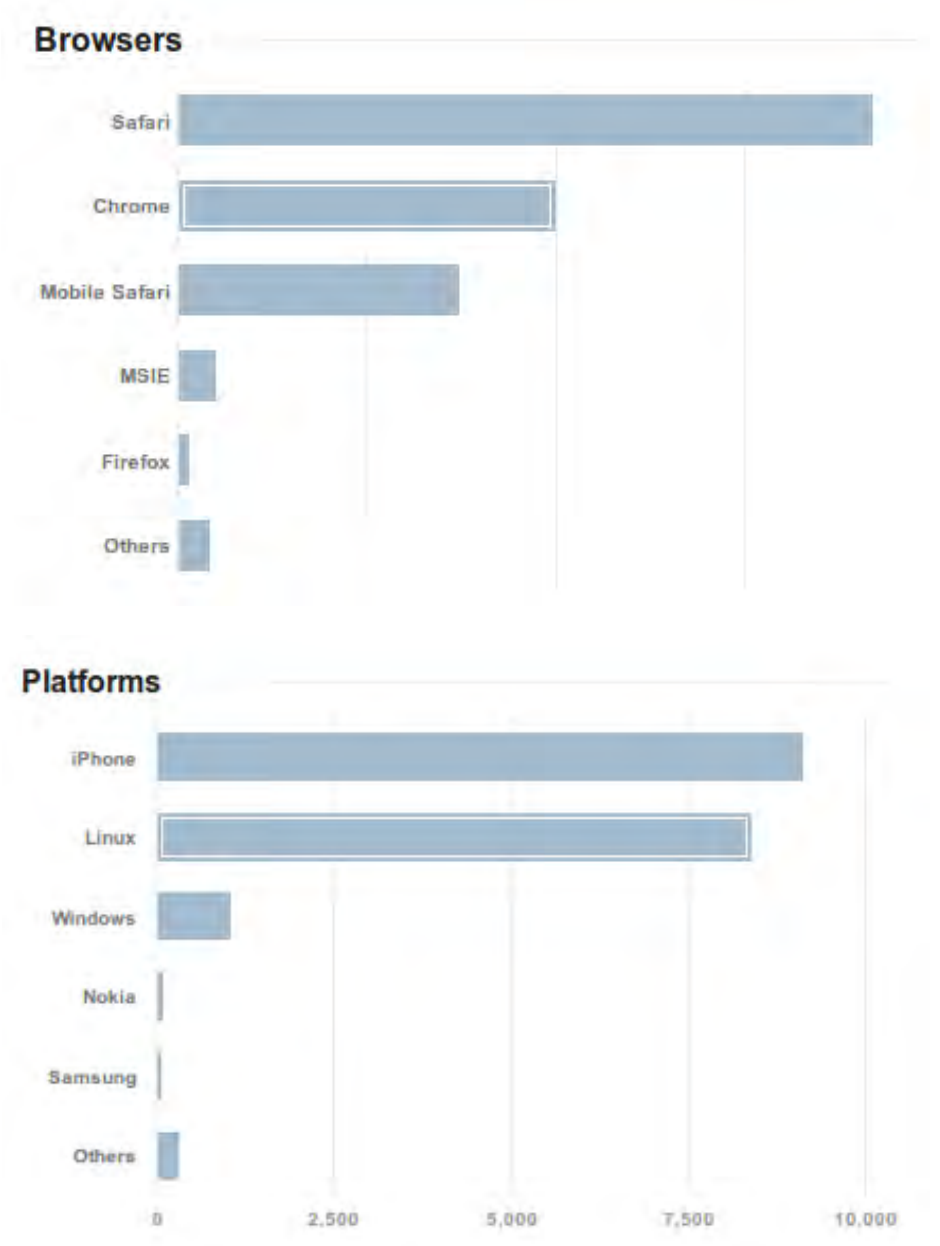
ผู้ใช้ที่ติดตั้งแอปพลิเคชันดังกล่าวลงในเครื่องอาจต้องเสียค่าบริการ SMS ที่แอปพลิเคชันดังกล่าวลักลอบแอบส่งข้อความเป็นจำนวนมาก





รูปที่ 6 สถิติการคลิกลิงก์ที่เผยแพร่มัลแวร์
จำแนกตามประเทศ เมื่อวันที่ 13 ส.ค. 2557 เวลา 12:41 น.

เมื่อตรวจสอบผลกระทบต่อผู้ใช้ในประเทศไทยจากสถิติของการคลิกลิงก์ที่เผยแพร่มัลแวร์ (http://goo.gl/NPD8sd) พบว่ามีการสร้างลิงก์ดังกล่าวตั้งแต่วันที่ 12 สิงหาคม โดยมีผู้ใช้ในประเทศไทยคลิกลิงก์นี้ถึง 19,056 ครั้ง **[4]**



รูปที่ 7 สถิติการคลิกลิงก์ที่เผยแพร่มัลแวร์ จำแนกตามเว็บเบราว์เซอร์และระบบปฏิบัติการ

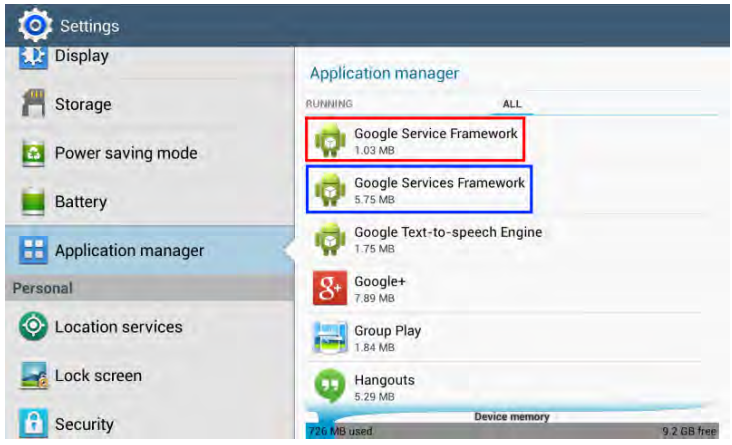
จากสถิติข้างต้นพบว่ามีผู้ใช้งานที่เข้าถึง URL ดังกล่าวจากระบบปฏิบัติการ iOS เป็นจำนวนกว่า 9,288 ครั้ง ซึ่งผู้ใช้งานในกลุ่มนี้น่าจะไม่ได้รับผลกระทบเนื่องจากใช้งานคนละระบบปฏิบัติการกัน และนอกจากนี้ จากสถิติที่จำแนกตามระบบปฏิบัติการ ที่พบว่าเป็นระบบปฏิบัติการ Linux จำนวนกว่า 9,000 ครั้ง มีความเป็นไปได้ว่า ผู้ใช้เข้าถึง URL จากโทรศัพท์มือถือระบบปฏิบัติการ Android เนื่องจากเว็บเบราว์เซอร์ในระบบปฏิบัติการ Android มักจะแสดงตัวเป็นระบบปฏิบัติการ Linux

ระบบที่ได้รับผลกระทบ

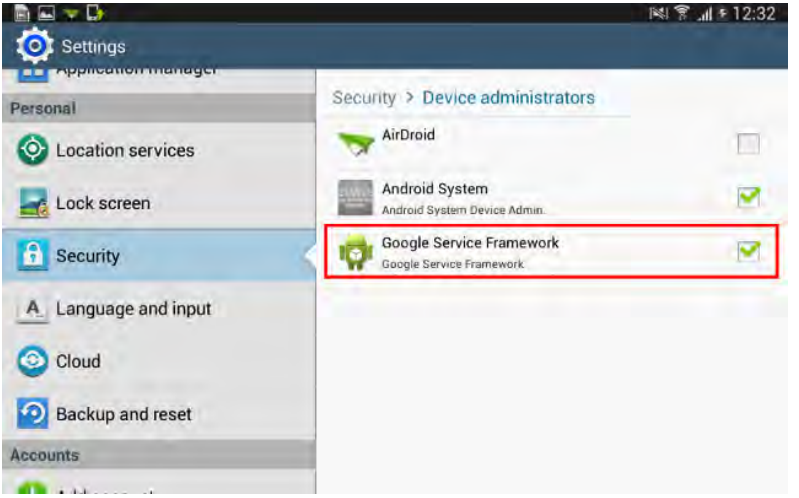
ผู้ใช้งานโทรศัพท์มือถือหรืออุปกรณ์ที่ใช้ระบบปฏิบัติการ Android

ข้อแนะนำในการป้องกันและแก้ไข

เมื่อติดตั้งแอปพลิเคชันดังกล่าวลงในเครื่อง แอปพลิเคชันอันตรายนี้จะใช้ชื่อว่า Google Service Framework ซึ่งตั้งชื่อคล้ายคลึงกับแอปพลิเคชันจริงที่ชื่อว่า Google Services Framework (มี s ต่อท้าย Service) ดังนั้น ผู้ใช้งานที่ติดตั้งแอปพลิเคชันดังกล่าวไปแล้ว ให้รีบถอนการติดตั้งแอปพลิเคชัน โดยเข้าไปที่ Settings > Security > Device Administrators แล้วติ๊กเครื่องหมายถูกหลังแอปพลิเคชัน Google Service Framework ออกเพื่อถอนการให้สิทธิ์ Device Administration จากนั้นให้ถอนการติดตั้งแอปพลิเคชันนี้ตามขั้นตอนปกติ



รูปที่ 8 แอปพลิเคชันปลอม (Google Service Framework)
ที่ตั้งชื่อคล้ายคลึงกับแอปพลิเคชันจริง (Google Services Framework)



รูปที่ 9 หน้าจัดการสิทธิ Device Administration ของแอปพลิเคชัน

ทั้งนี้ ผู้ใช้งานควรติดตั้งแอปพลิเคชันจากแหล่งที่น่าเชื่อถือเท่านั้น เช่น Google Play Store แต่อย่างไรก็ตาม แม้จะเป็นแอปพลิเคชันที่อยู่ใน Google Play Store ก็ควรเพิ่มความระมัดระวังเป็นพิเศษ เนื่องจากเคยพบแอปพลิเคชันปลอมใน Google Play Store เมื่อเดือนมีนาคม 2557 **[5]** มาแล้ว ดังนั้น ผู้ใช้อาจตรวจสอบแอปพลิเคชันที่น่าสงสัยได้โดยวิธีการดังต่อไปนี้

- ตรวจสอบจากจำนวนดาวน์โหลด และรีวิวของผู้ใช้งาน โดยสังเกตแอปพลิเคชันที่มียอดดาวน์โหลดที่ต่ำหรือรีวิวของผู้ใช้งานที่แจ้งถึงความผิดปกติ

- ตรวจสอบการร้องขอสิทธิ (Permission) ของแอปพลิเคชันว่ามีความเหมาะสมหรือไม่ เช่นแอปพลิเคชันที่มีการขอสิทธิในการส่ง SMS และ Internet Access ควรพิจารณาว่ามีการร้องขอสิทธิดังกล่าวเพื่อจุดประสงค์ใด

นอกจากนี้ผู้ใช้งานยังสามารถศึกษาบทความที่ไทยเซิร์ตได้เคยเผยแพร่วิธีการตรวจสอบและป้องกันปัญหามัลแวร์ รวมถึงวิธีการใช้งานโทรศัพท์มือถือให้มั่นคงปลอดภัย จากบทความดังต่อไปนี้

- แนวทางการใช้งานโทรศัพท์มือถือให้มั่นคงปลอดภัยจากภัยคุกคาม **[6]**
- รู้ทันและป้องกัน Malware ในระบบปฏิบัติการ Android **[7]**
- รู้ทันและป้องกัน Malware ในระบบปฏิบัติการ Android ตอนที่ 2 **[8]**

สำหรับผู้ดูแลระบบ ในขณะนี้อาจทำการปิดกั้นการเชื่อมต่อไปยังเว็บไซต์ http://goo.gl/NPD8sd เพื่อป้องกันไม่ให้ผู้ใช้งานเข้าไปดาวน์โหลดแอปพลิเคชันนี้ และปิดกั้นการเชื่อมต่อกับหมายเลขไอพี 213.163.72.147 เพื่อป้องกันมัลแวร์นี้ติดต่อกลับไปยังผู้ไม่หวังดี ทั้งนี้ ไทยเซิร์ตกำลังอยู่ในระหว่างการตรวจสอบวิเคราะห์เพิ่มเติมถึงพฤติกรรมของมัลแวร์ดังกล่าว และจะนำข้อมูลมาอัปเดตให้ทราบอีกครั้ง

อ้างอิง

1. http://pantip.com/topic/32480183
2. http://pantip.com/topic/32443108
3. http://pantip.com/topic/32444404
4. https://goo.gl/#analytics/goo.gl/NPD8sd/all_time
5. https://www.thaicert.or.th/alerts/user/2014/al2014us008.html
6. https://www.thaicert.or.th/papers/general/2011/pa2011ge010.html
7. https://www.thaicert.or.th/papers/technical/2012/pa2012te003.html
8. https://www.thaicert.or.th/papers/technical/2012/pa2012te011.html

เตือนภัยแฮกไลน์ (LINE) หลอกให้ซื้อ **iTunes Gift Card พร้อมวิธีป้องกันตนเอง**

วันที่ประกาศ : 11 ตุลาคม 2557
ปรับปรุงล่าสุด : 11 ตุลาคม 2557
เรื่อง : เตือนภัยแฮกไลน์ (LINE) หลอกให้ซื้อ iTunes Gift Card พร้อมวิธีป้องกันตนเอง
ประเภทภัยคุกคาม : Intrusion

โจรจ๋ำขอเวลาหนูเปลี่ยน Password ก่อน อย่าเพิ่งแฮก LINE หนู !!!

จากที่ไทยเซิร์ตเคยนำเสนอบทความเรื่อง “Risk on LINE” **[1]** และเรื่อง “ไทยเซิร์ตพบช่องโหว่ของแอปพลิเคชัน LINE แฮกเกอร์สามารถดักรับข้อมูลบนเครือข่าย LAN/WiFi และอ่านบทสนทนาได้ทันที” **[2]** ซึ่งมีเนื้อหาเกี่ยวกับปัญหาด้านความมั่นคงปลอดภัยของการใช้งานแอปพลิเคชันไลน์ (LINE) และช่องโหว่ LINE ที่ไทยเซิร์ตตรวจพบนั้น ปัจจุบันถึงแม้จะมีการแก้ไขปัญหาทั้งหมดโดยผู้พัฒนาแล้ว แต่จากสถานการณ์ล่าสุดที่ไทยเซิร์ตได้รับแจ้งเกี่ยวกับการแฮกบัญชีใช้งานของ LINE รวมถึงพบข้อมูลในสื่อสังคมออนไลน์ที่มีเนื้อหาคล้ายกันเป็นจำนวนมาก

ในส่วนนี้ขอยกตัวอย่างเนื้อหาจากเว็บไซต์พันทิป หมายเลข 32643838 **[3]** มีใจความเกี่ยวกับการขอความช่วยเหลือเรื่องถูกแฮก LINE แล้วนำไปแอบอ้างสร้างความเสียหายให้กับเพื่อนของเหยื่อ จากสถานการณ์ดังกล่าวมีผู้แชร์ข้อมูลเพิ่มเติมถึงสถานการณ์ที่ประสบกับตนเองหรือเพื่อนในลักษณะคล้ายกัน ขยายวงกว้างขึ้นเรื่อย ๆ ทำให้ผู้ใช้งานหลายคนเกิดความสงสัยและมีความกังวลต่อความมั่นคงปลอดภัยในการใช้งาน LINE ไทยเซิร์ตจึงได้วิเคราะห์สถานการณ์ที่เกิดขึ้น และประสานงานกับผู้ที่เกี่ยวข้องเพื่อประเมินหาสาเหตุของ

สถานการณ์ดังกล่าว โดยได้สรุปภาพรวมที่เกี่ยวกับสถานการณ์ที่เกิดขึ้นในมุมมองของทั้งผู้ดูแลระบบ และความเสี่ยงของผู้ใช้งานที่สามารถถูกแฮก LINE ผลกระทบของปัญหาที่สามารถเกิดทั้งในมุมมองของเหยื่อและเพื่อนรอบข้าง พร้อมทั้งจัดเตรียมข้อแนะนำสำหรับผู้ใช้งานที่เป็นประโยชน์ เพื่อให้สามารถรับมือกับปัญหาที่อาจเกิดขึ้นกับตนเองและให้รู้วิธีการใช้งาน LINE ที่มีความมั่นคงปลอดภัย โดยมีรายละเอียดดังต่อไปนี้

วิเคราะห์สถานการณ์เบื้องต้น

รูปที่ 1 อ้างอิงข้อมูลจากเว็บไซต์พันทิปกรณีที่ผู้เสียหายถูกขโมยบัญชีใช้งาน LINE และถูกนำไปใช้ในการสวมรอย เพื่อหลอกลวงเพื่อนของเหยื่อให้ทำการซื้อบัตร iTunes Gift Card ให้ แต่กรณีดังกล่าวเพื่อนของเหยื่อรู้ตัวก่อนทำให้ไม่มีความเสียหายเกิดขึ้น

ลำดับการหลอกลวง (สรุปจากข้อมูลที่พบบนเว็บไซต์พันทิป)

1. เพื่อนของผู้ใช้งานตัวจริง (เหยื่อ) ได้รับข้อความขอความช่วยเหลือให้ซื้อบัตร iTunes Gift Card แต่เนื่องจากมีการใช้งานภาษาที่ค่อนข้างผิดปกติ คล้ายกับว่าแปลมาจากโปรแกรมแปลภาษา เช่น Google Translate เพื่อนคนดังกล่าวจึงเกิดความสงสัย และหาทางปฏิเสธคำขอ

2. เพื่อนคนดังกล่าวติดต่อกลับไปหาเหยื่อ ทำให้ทราบว่าข้อความดังกล่าวไม่ได้ส่งออกจากเหยื่อ และน่าจะถูกแฮกบัญชีใช้งาน LINE

3. เหยื่อพยายามหาทางกู้คืนบัญชีใช้งาน LINE ด้วยการเปลี่ยนรหัสผ่าน แต่ไม่เป็นผล

4. บัญชีใช้งาน LINE ของเหยื่อถูกลบออกในลักษณะที่ไม่สามารถกู้คืนได้ (ฟังก์ชัน Delete Account)

จากการประเมินสถานการณ์ ผู้ไม่หวังดีมีลักษณะการใช้งานภาษาไทยที่ค่อนข้างจะผิดไปจากปกติ คล้ายกับแปลภาษาไทยมาจากโปรแกรมแปลภาษา และอาจมีความเป็นไปได้ว่าผู้ไม่หวังดีเป็นกลุ่มบุคคลจากต่างประเทศ โดยจุดประสงค์ของการกระทำดังกล่าวต้องการหลอกเพื่อนของเหยื่อให้หลงเชื่อซื้อบัตร iTunes Gift Card ให้ แต่เนื่องจากในเหตุการณ์ดังกล่าวเพื่อนของเหยื่อเกิดความสงสัย จึงทำให้ไม่หลงเชื่อกลลวงดังกล่าว ทั้งนี้บัตร iTunes Gift Card มีคุณสมบัติเหมือนกับบัตรเติมเงินที่ใช้ในการซื้อเพลง ภาพยนตร์ แอปพลิเคชัน ฯลฯ บน iTunes Store, App Store, iBooks Store หรือ Mac App Store สำหรับผู้ที่ใช้อุปกรณ์ของ Apple เช่น iPhone, iPad และ MacBook **[4]** ซึ่งหากผู้ไม่หวังดีได้รหัสของบัตรแล้ว จะสามารถนำไปเติมเงินเข้าบัญชี Apple ID ของตนเองเพื่อซื้อสินค้าได้ทันที

จากสถานการณ์ดังกล่าว ไทยเซิร์ตได้มีการตรวจสอบเพิ่มเติมกับผู้เสียหายหลายราย โดยได้ข้อมูลที่สามารถบ่งชี้ได้ว่าผู้ใช้งานดังกล่าวถูกขโมยข้อมูลบัญชีใช้งาน LINE ส่วนที่เป็นบัญชีอีเมล (Registered Email) และรหัสผ่านออกไปได้ ซึ่งผู้ไม่หวังดีนำบัญชีใช้งานดังกล่าวมาล็อกอินที่เครื่องโทรศัพท์มือถืออีกเครื่องหนึ่ง ส่งผลให้ในช่วงเวลาดังกล่าว ผู้ใช้งานตัวจริงไม่สามารถใช้งาน LINE บนโทรศัพท์มือถือได้ (เซสชันการใช้งาน LINE จะหลุดทันที) เนื่องจาก LINE ไม่อนุญาตให้ล็อกอินบนโทรศัพท์มือถือพร้อมกัน 2 เครื่องในช่วงเวลาเดียวกัน พร้อมกับผู้ไม่หวังดีมีการเข้ามาเปลี่ยนการตั้งค่าของ LINE ในส่วนต่าง ๆ เพื่อป้องกันการเข้ามาล็อกอินซ้ำของผู้ใช้งานตัวจริง เช่น ตั้งค่าไม่อนุญาตให้มีการล็อกอินผ่านทาง LINE บนเครื่อง PC และทำการเปลี่ยนรหัสผ่านบัญชีใช้งานที่ใช้ล็อกอิน LINE ใหม่ เป็นต้น

ไทยเซิร์ตตรวจสอบจากข้อมูลข่าวย้อนหลังไปตั้งแต่เดือนมิถุนายน 2557 โดยพบเนื้อหาของข่าวเกี่ยวกับการตรวจพบการขโมยข้อมูลบัญชีผู้ใช้งาน LINE มากกว่า 300 กรณีในประเทศญี่ปุ่น **[5]** ซึ่งกรณีดังกล่าวเป็นการตรวจพบเนื่องจากมีกรณีหลอกลวงเกี่ยวกับทางการเงิน และมีความคล้ายคลึงกับเหตุการณ์ที่เกิดขึ้นในประเทศไทยอยู่ ณ ขณะนี้ แต่อย่างไรก็ตาม ขณะนั้นทางตัวแทนจากบริษัทผู้พัฒนา LINE ให้สัมภาษณ์ว่าข้อมูลดังกล่าวไม่ได้เกิดจากการโจมตีฐานข้อมูลของ LINE แต่อย่างใด

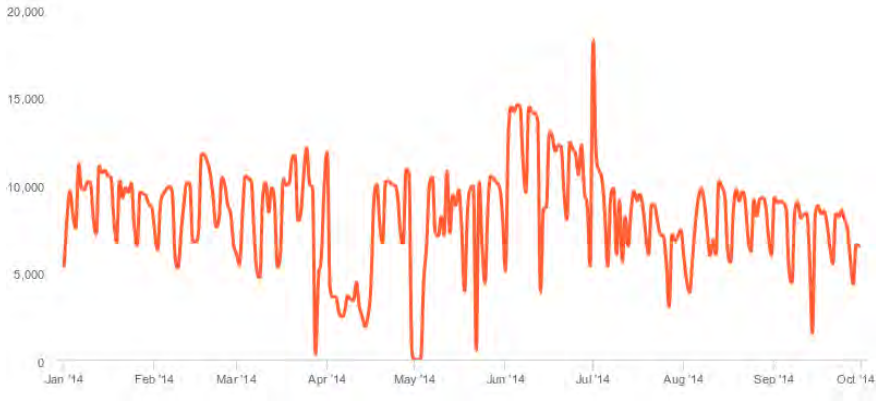
ไทยเซิร์ตยังได้ทำการประสานไปยังผู้ดูแลระบบของ LINE ที่ประเทศญี่ปุ่น เพื่อขอให้ยืนยันสถานการณ์การโจมตีที่เกิดขึ้นในปัจจุบันตามที่ได้กล่าวมาข้างต้น โดยผู้ดูแลระบบ LINE แจ้งว่าไม่พบการบุกรุกหรือขโมยข้อมูลที่ฝั่งเซิร์ฟเวอร์ของ LINE แต่อย่างใด การโจมตีผู้ใช้งานดังกล่าวน่าจะมีที่มาจากที่ผู้ใช้งานมีพฤติกรรมเสี่ยงในมุมต่าง ๆ ส่งผลให้ผู้ไม่หวังดีสามารถขโมยข้อมูลการล็อกอินบัญชีอีเมลไปได้

ล่าสุดเมื่อวันที่ 8 ตุลาคมที่ผ่านมาในช่องทาง LINE Official ในส่วนของ “LINE ประเทศไทย” ได้มีการออกประกาศแจ้งเตือนผู้ใช้งาน เพื่อให้ระวังการเปิดเผยข้อมูลส่วนตัว เช่น LINE ID หรือข้อมูลรหัสผ่าน พร้อมทั้งแนะนำให้ผู้ใช้งานเปลี่ยนรหัสผ่านอย่างต่อเนื่องเพื่อความมั่นคงปลอดภัย และยืนยันว่า LINE เป็นแพลตฟอร์มที่มั่นคงปลอดภัยในระดับสากลอีกด้วย ดังแสดงในรูปที่ 2

รูปที่ 2 ข้อมูลแจ้งเตือนจาก LINE ประเทศไทย

บัญชีใช้งาน LINE ถูกแฮกได้อย่างไรบ้าง

สืบเนื่องจากสถานการณ์ล่าสุดที่ทางผู้ดูแลระบบ LINE ยืนยันว่าไม่ได้มีการบุกรุกหรือขโมยข้อมูลที่ฝั่งเซิร์ฟเวอร์ LINE ทำให้มีการวิเคราะห์มุ่งเป้าประเด็นไปยังฝั่งผู้ใช้งานที่อาจมีการใช้งานที่มีความเสี่ยง ส่งผลให้เกิดการขโมยข้อมูลบัญชีใช้งาน LINE ได้ดังนี้



รูปที่ 3 สถิติการตรวจพบเครื่องคอมพิวเตอร์ในประเทศไทยที่ติดมัลแวร์ประเภท Banking Trojan ระหว่างเดือนมกราคมถึงกันยายน 2557 ไทยเซิร์ต

1. เครื่องผู้ใช้งานติดมัลแวร์ (หรือที่คนทั่วไปรู้จักกันในนามของ ไวรัสคอมพิวเตอร์) จากสถิติที่ไทยเซิร์ตได้รับแจ้งเกี่ยวกับการตรวจพบเครื่องคอมพิวเตอร์ในประเทศไทยที่ติดมัลแวร์ประเภทที่มีความสามารถในการขโมยข้อมูลทางการเงิน (Banking Trojan) ระหว่างเดือนมกราคมถึงกันยายน 2557 นับตามจำนวนหมายเลขไอพีที่ไม่ซ้ำในแต่ละวัน ตามรูปที่ 3 นั้น มีประเด็นที่น่าสนใจว่าเครื่องคอมพิวเตอร์ไม่น้อยกว่า 10,000 เครื่องในประเทศไทย มีโอกาสเสี่ยงที่จะถูกขโมยข้อมูลบัญชีใช้งานระบบต่าง ๆ รวมถึงบัญชีใช้งาน LINE ด้วย

2. ผู้ใช้งานส่งข้อมูลล็อกอินบัญชีใช้งาน LINE ให้กับผู้ไม่หวังดีเอง โดยข้อมูลดังกล่าวไทยเซิร์ตตรวจสอบพบบนเว็บไซต์พันทิปว่ามีผู้หลงเชื่อข้อมูลจากผู้ไม่หวังดี ว่าสามารถโกงไอเท็มของเกมใน LINE ได้ โดยมีการส่งข้อมูลการล็อกอินบัญชีใช้งาน LINE ให้กับผู้ไม่หวังดี เพื่อใช้ในกระบวนการ ตามรูปที่ 4

รูปที่ 4 ตัวอย่างของการส่งข้อมูลส่วนบุคคลให้กับผู้ไม่หวังดี เพื่อใช้ในการโกงเกม [6]

จากรูปแบบการหลอกลวงดังกล่าวและข้อมูลที่พบ ทำให้ทราบว่ายังมีผู้ที่หลงเชื่อกรอกข้อมูลส่งให้ผู้ไม่หวังดีอยู่จริง แสดงให้เห็นว่ากลุ่มผู้ใช้งานอีกส่วนหนึ่งที่ยังคงมีความเสี่ยงในเรื่องของการถูกขโมยข้อมูลจากช่องทางดังกล่าวได้เช่นกัน

3. ผู้ใช้งานมีการใช้งานรหัสผ่านเดียวกันทุกระบบ หากรหัสผ่านใดรหัสผ่านหนึ่งรั่วไหลหรือถูกขโมยออกไป จะเกิดสถานการณ์ที่ทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านของบัญชีใช้งาน LINE ได้ทันที ซึ่งกลุ่มเสี่ยงของผู้ใช้งานประเภทนี้ คาดว่าจะมีอยู่เป็นจำนวนหนึ่ง และอาจถูกขโมยด้วยวิธีการต่าง ๆ นอกเหนือจากข้อ 1 และ 2 เช่น การใช้งาน WiFi สาธารณะและถูกดักรับข้อมูลการล็อกอิน หรือการตั้งรหัสผ่านที่ง่ายต่อการคาดเดา เป็นต้น โดยยกตัวอย่างกรณีที่เกิดขึ้นในอดีตเมื่อระบบของ Twitter ถูกแฮก ทำให้ข้อมูลบัญชีใช้งานถูกขโมยออกไปจำนวนหนึ่ง ส่งผลให้มีผู้ใช้งานจำนวนหนึ่งที่ถูกแฮกอีเมลและบริการอื่น ๆ เพิ่มเติม

LINE มั่นคงปลอดภัยแค่ไหน

ถึงแม้ว่าปัจจุบันจะยังไม่มีข้อสรุปสุดท้ายเกี่ยวกับการแฮกที่เกิดขึ้นว่าเป็นการแฮกที่ฝั่งผู้ใช้งานจริง หรือเซิร์ฟเวอร์ของ LINE ถูกเจาะเข้าถึงเพื่อเอาข้อมูลบัญชีใช้งาน LINE ออกมา ซึ่งยังคงเป็นประเด็นที่ทางไทยเซิร์ตให้ความสำคัญและเฝ้าติดตามและประเมินสถานการณ์ของปัญหาต่อไป แต่สิ่งสำคัญที่ผู้ใช้งานทุกคนควรทราบคือปัญหาเรื่องจุดอ่อนหรือช่องโหว่อันนำมาซึ่งการแฮกบัญชีใช้งาน LINE ได้นั้น ไม่ได้ขึ้นอยู่กับปัจจัยด้านความมั่นคงปลอดภัยของระบบ LINE เพียงอย่างเดียว แต่ขึ้นอยู่กับความตระหนักรู้ของผู้ใช้งานอีกด้วย หลายครั้งที่พบว่ามีข่าวเรื่องการแฮกระบบและผู้เกี่ยวข้องได้ทำการแจ้งเตือนผู้ใช้งานให้ทำการเปลี่ยนรหัสผ่าน หากผู้ใช้งานให้ความตระหนักในข้อความที่ได้รับและมองว่าเป็นความรับผิดชอบส่วนหนึ่งต่อการใช้งาน ก็อาจจะทำให้สถานการณ์ดังกล่าวลดระดับความรุนแรงลงได้ หรือพูดอีกนัยหนึ่งคือสามารถรอดพ้นสถานการณ์การถูกแฮกได้

ผู้ใช้งานควรตระหนักและระลึกเสมอว่าระบบทุกระบบที่ใช้งานมีโอกาสพบช่องโหว่ได้ในเวลาภายหลัง ในวันนี้ระบบ LINE อาจกล่าวได้ว่ามั่นคงปลอดภัยตามข้อมูลที่ได้รับจากผู้ดูแลระบบ LINE แต่อย่างไรก็ตามไม่ได้หมายถึงว่าระบบ LINE ไม่มีปัญหาด้านความมั่นคงปลอดภัย เพราะหากวันหนึ่งที่มีผู้พบช่องโหว่ของ LINE ก็คงต้องกลับมาทบทวนกันใหม่ถึงมาตรการและแนวทางการรับมือปัญหาในฝั่งผู้ใช้งาน ดังจะเห็นจากหลายครั้งที่ผ่านมา เช่น การค้นพบช่องโหว่ Heartbleed ซึ่งถูกพบภายหลังจากมีการใช้งานซอฟต์แวร์ OpenSSL มาแล้วมากกว่า 10 ปี เป็นต้น ดังนั้นผู้ใช้งานจึงต้องมีความตระหนักรู้ว่าการจะใช้งานอะไรก็ตามย่อมมีความเสี่ยง จำเป็นต้องพิจารณาการใช้งานให้รอบคอบ และหากพบความผิดปกติใด ๆ เกี่ยวกับการใช้งาน จำเป็นต้องแจ้งให้ทางผู้ดูแลทราบในทันที เพื่อหาสาเหตุและความผิดปกติที่เกิดขึ้น อย่างไรก็ตามในส่วนของปัญหาที่เกิดกับ LINE ไทยเซิร์ตจะติดตามและวิเคราะห์ปัญหาอย่างต่อเนื่อง หากผู้ใช้งานท่านใดมีข้อมูลเพิ่มเติมสามารถแจ้งเข้ามาได้ตามช่องทาง office@thaicert.or.th ทางไทยเซิร์ตยินดีรับข้อมูลเพื่อมาใช้ในการวิเคราะห์และเผยแพร่แก่ผู้ใช้งานทั่วไปได้รับทราบโดยทั่วกัน

ผลกระทบที่เกิดขึ้นจากการถูกแฮก LINE

ผลกระทบที่เกิดขึ้นสามารถแบ่งออกเป็น 2 ส่วน โดยอธิบายได้ดังนี้

1. ผู้ใช้งาน LINE ที่ถูกแฮกบัญชีใช้งาน (เหยื่อ) มีโอกาสถูกสวมรอยและนำบัญชีดังกล่าวมาใช้เพื่อหลอกลวงเพื่อนของเหยื่อให้เสียทรัพย์ในลักษณะต่าง ๆ ได้ และท้ายที่สุดบัญชีใช้งาน LINE ของเหยื่ออาจถูกเปลี่ยนแปลงหรือลบทิ้งทันที เมื่อผู้ไม่หวังดีรู้ว่าเหยื่อกำลังรู้ตัวว่าถูกแฮก

2. ผู้ใช้งาน LINE ที่อยู่ใน Contact ของเหยื่อ มีโอกาสพบการหลอกลวงให้กระทำการซื้อสินค้า อย่างในกรณีนี้คือ iTunes Gift Card หรือในอนาคตอาจพบรูปแบบการหลอกลวงในลักษณะที่เปลี่ยนแปลงไปได้อีก ซึ่งหากผู้ใช้งานหลงเชื่อแล้ว ไม่ว่ากรณีใดก็อาจก่อให้เกิดการเสียทรัพย์ได้

การรับมือเมื่อถูกแฮก LINE และข้อแนะนำในการใช้งาน LINE ให้มีความมั่นคงปลอดภัย

ถึงแม้วันนี้จะยังไม่ทราบแน่ชัดถึงสาเหตุของการแฮก LINE และผู้อ่านเองอาจจะไม่ได้ตกอยู่ในสถานการณ์ของการเป็นเหยื่อ แต่อย่างไรก็ตามผู้ใช้งาน LINE ทุกท่าน ควรเรียนรู้ถึงวิธีการป้องกันและรับมือด้วยตนเอง เพื่อให้สามารถใช้งาน LINE ได้อย่างมั่นคงปลอดภัย และสามารถรับมือกับสถานการณ์ที่ตนเองอาจถูกแฮก LINE ได้

ข้อแนะนำในการรับมือ เมื่อตนเองถูกแฮก LINE (อาจทราบจากคนรอบข้างในลักษณะปัญหาที่กล่าวข้างต้น หรือพบว่าเซสชันที่ใช้งานบนโทรศัพท์หลุดออก) ให้รีบดำเนินการดังต่อไปนี้

1. ล็อกอิน LINE บนโทรศัพท์มือถือด้วยบัญชีใช้งานที่เคยสมัครไว้

1.1 หากสมัครด้วยบัญชีอีเมล ให้ทำการล็อกอินด้วยบัญชีอีเมลก่อน แต่ถ้าล็อกอินไม่ผ่านให้ไปยังข้อ 1.2

1.2 ในกรณีที่ผู้ใช้งานมีการ Link บัญชีใช้งาน Facebook เข้ากับบัญชีใช้งาน LINE อยู่แล้ว ให้ทำการล็อกอินด้วยบัญชี Facebook แต่ถ้าล็อกอินไม่ผ่านให้ไปยังข้อ 1.3

1.3 หากยังไม่สามารถล็อกอินได้ให้ลองทำการรีเซ็ตรหัสผ่านด้วยฟังก์ชัน “Forgot my password”

1.4 หากยังพบว่าทำตามขั้นตอนที่ 1.1-1.3 แล้วไม่สามารถล็อกอิน LINE ได้อยู่ ให้รีบประสานงานแจ้งความผิดปกติกับผู้ดูแลระบบ LINE ทันที **[7]**

2. เมื่อล็อกอินจากข้อ 1 ได้แล้ว ให้รีบพิจารณาตรวจสอบความผิดปกติในส่วนการตั้งค่า LINE บนโทรศัพท์ และรีบดำเนินการปรับปรุงค่าดังต่อไปนี้

2.1 ตรวจสอบว่ามีคนล็อกอิน LINE บนเครื่อง PC อยู่หรือไม่

ขั้นตอนการตรวจสอบการล็อกอิน LINE บนเครื่อง PC

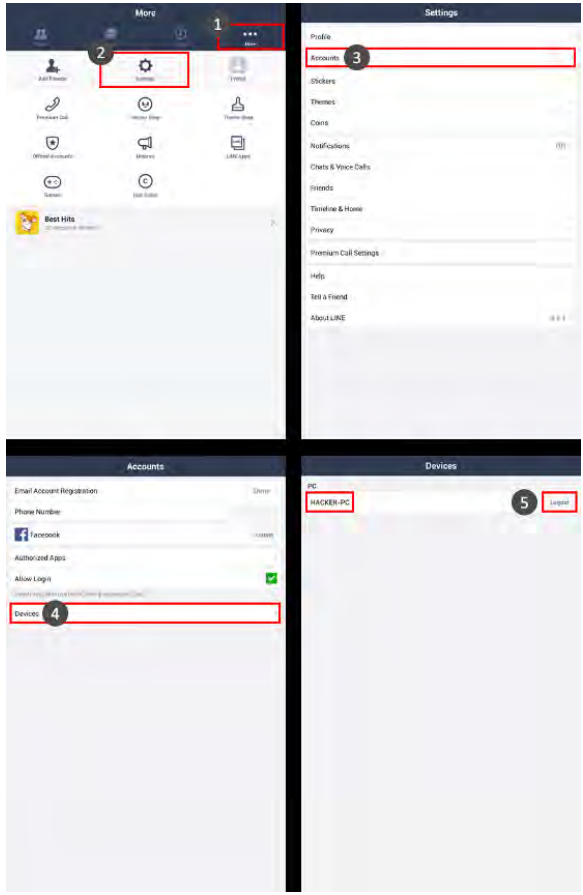
1) เปิดแอปพลิเคชัน LINE แล้วเลือกเมนู More

2) เลือกเมนู Settings

3) เลือกเมนู Accounts

4) เลือกเมนู Devices

5) ตรวจสอบว่ามีคอมพิวเตอร์ที่กำลังล็อกอิน LINE บนเครื่อง PC อยู่หรือไม่ หากพบว่ามีชื่อคอมพิวเตอร์ที่ไม่ใช่ของตนเองกำลังล็อกอินอยู่ ให้กดปุ่ม Logout (หมายเหตุ: ชื่อคอมพิวเตอร์จะแสดงเป็นตัวพิมพ์ใหญ่ทั้งหมด)



รูปที่ 5 ขั้นตอนการตรวจสอบการล็อกอิน LINE บนเครื่อง PC

2.2 ยกเลิกการใช้งานฟังก์ชัน SNS (Social Network Service) ซึ่งปัจจุบันสามารถเชื่อมต่อกับบัญชีใช้งานของ Facebook ได้ การยกเลิกการใช้งานเพื่อป้องกันโอกาสเสี่ยงอื่น ๆ ที่อาจเกิด เช่น รหัสผ่านบัญชีใช้งาน Facebook ถูกแฮก อันจะทำให้ผู้ไม่หวังดีสามารถล็อกอินเข้าใช้งาน LINE ได้เช่นกัน

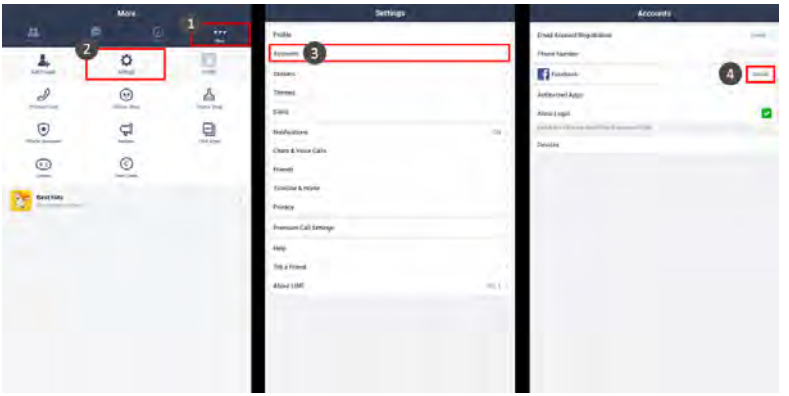
ขั้นตอนการยกเลิกการเชื่อมต่อระหว่าง LINE และ Facebook

1) เปิดแอปพลิเคชัน LINE แล้วเลือกเมนู More

2) เลือกเมนู Settings

3) เลือกเมนู Accounts

4) กดปุ่ม Unlink ที่เมนู Facebook



รูปที่ 6 ขั้นตอนการยกเลิกการเชื่อมต่อระหว่าง LINE และ Facebook

2.3 ตรวจสอบการตั้งค่าบัญชีใช้งาน LINE ในส่วนที่เป็นอีเมล (Email Account Registration) ดูว่าใช้งานเป็นบัญชีชื่อเดิมหรือไม่ หากไม่ใช่ให้รีบเปลี่ยนทันที และหากพบว่ามีการเปลี่ยนไปใช้อีเมลอื่นแล้ว ให้รีบประสานงานแจ้งความผิดปกติกับผู้ดูแลระบบ LINE ทันที **[7]**

ขั้นตอนการตรวจสอบบัญชีใช้งาน LINE ส่วนที่เป็นอีเมล (Email Account Registration)

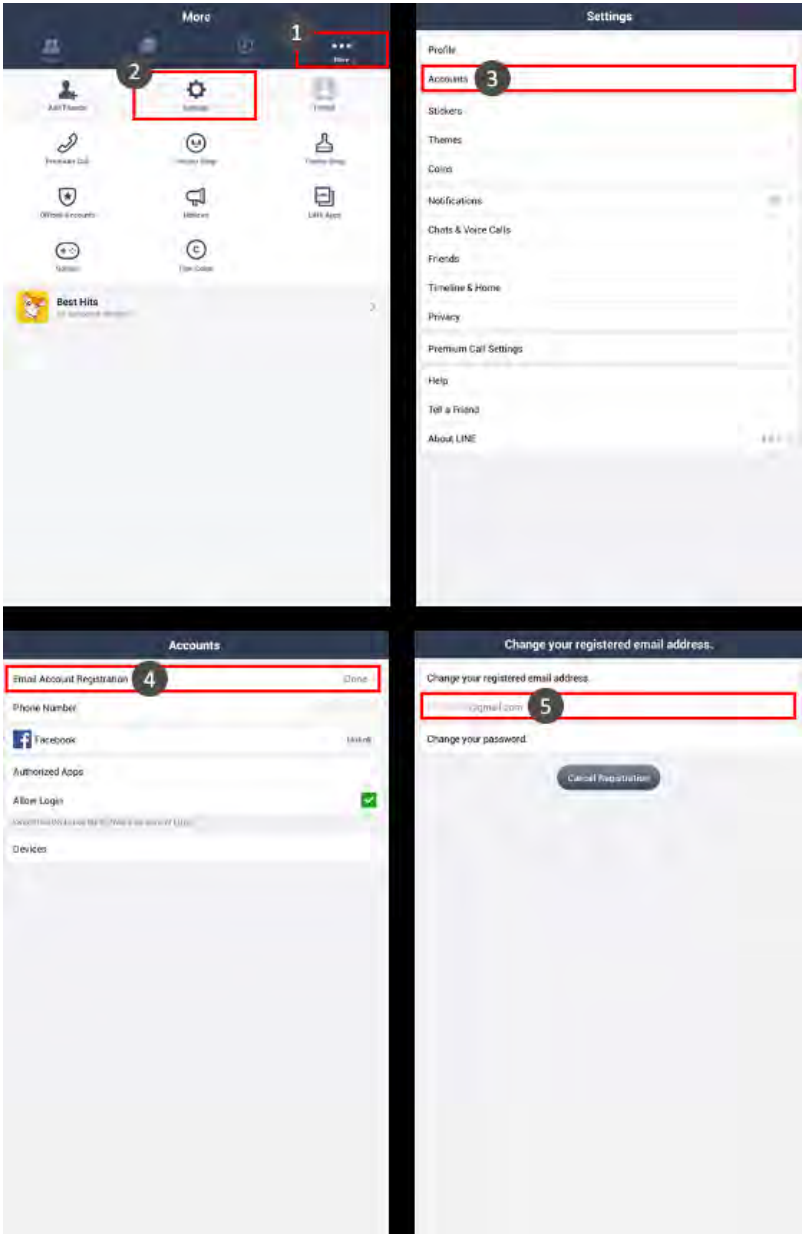
1) เปิดแอปพลิเคชัน LINE แล้วเลือกเมนู More

2) เลือกเมนู Settings

3) เลือกเมนู Accounts

4) เลือกเมนู Email Account Registration

5) ตรวจสอบว่าอีเมลที่ปรากฏเป็นอีเมลที่เคยลงทะเบียนไว้หรือไม่ หากไม่ใช่ให้รีบเปลี่ยนอีเมลด้วยการเลือกเมนู Change your registered email address. ที่อยู่ด้านบนของอีเมล



รูปที่ 7 ขั้นตอนการตรวจสอบบัญชีใช้งาน LINE ส่วนที่เป็นอีเมล

2.4 พิจารณาตั้งค่ารหัสผ่านใหม่สำหรับบัญชีใช้งาน LINE ในส่วนที่เป็นอีเมล อย่างน้อยที่สุดหากสาเหตุของการแฮก LINE อยู่ที่ฝั่งเซิร์ฟเวอร์ของ LINE ก็ยังสามารถลดผลกระทบในฝั่งผู้ใช้งานได้ เนื่องจากข้อมูลรหัสผ่านที่ถูกขโมยออกไปได้จะไม่สามารถใช้งานได้แล้ว รวมถึงต้องไม่ใช้รหัสผ่านเดียวกันในทุกระบบ เช่น อีเมล หรือ Twitter เพื่อป้องกันรหัสผ่านใดรหัสผ่านหนึ่งรั่วไหลและถูกคาดเดาได้

ขั้นตอนการเปลี่ยนรหัสผ่านบัญชีใช้งาน LINE ส่วนที่เป็นอีเมล

1) เปิดแอปพลิเคชัน LINE แล้วเลือกเมนู More

2) เลือกเมนู Settings

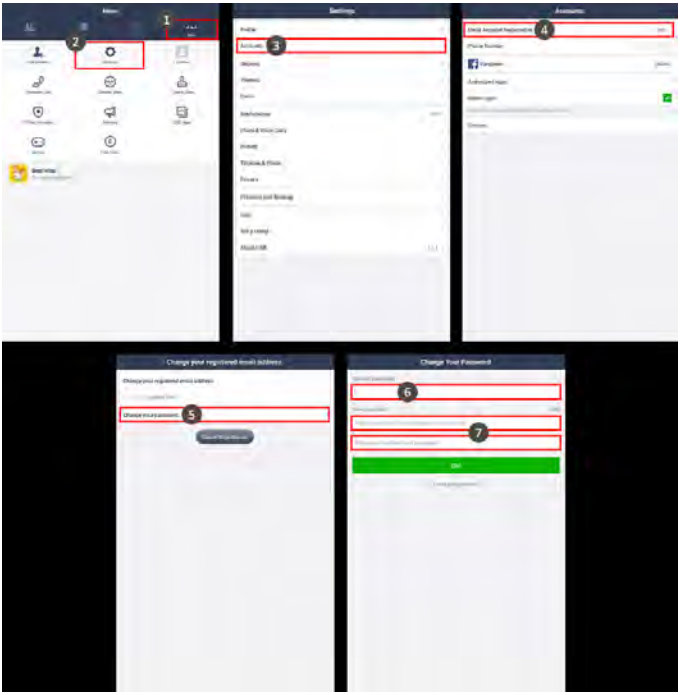
3) เลือกเมนู Accounts

4) เลือกเมนู Email Account Registration

5) เลือกเมนู Change your password.

6) ระบุรหัสผ่านเดิมที่ใช้ในการล็อกอิน LINE บน PC

7) ระบุรหัสผ่านใหม่ที่ต้องการ แล้วกด OK



รูปที่ 8 ขั้นตอนการเปลี่ยนรหัสผ่านบัญชีใช้งาน LINE ส่วนที่เป็นอีเมล

ข้อแนะนำในการใช้งาน LINE ให้มีความมั่นคงปลอดภัย

1. พิจารณาตั้งค่ารหัสผ่านใหม่สำหรับบัญชีใช้งาน LINE ในส่วนที่เป็นอีเมล และ Facebook จำเป็นต้องใช้เป็นรหัสผ่านที่ไม่เคยใช้มาก่อน และรหัสผ่านที่ใช้งานทั้งหมดต้องตั้งให้ไม่เหมือนกัน เพื่อป้องกันกรณีที่บัญชีใช้งานใดบัญชีหนึ่งถูกขโมยแล้วนำมาใช้เชื่อมโยงแฮกไปยังระบบอื่น ๆ ได้ หากพบความผิดปกติให้รีบดำเนินการตามข้อมูลข้างต้นทันที

2. พิจารณาติดตั้งโปรแกรมประเภทแอนติไวรัสและสแกนหาความผิดปกติในเครื่องที่ใช้งาน LINE เนื่องจากมัลแวร์ในปัจจุบันสามารถที่จะขโมยข้อมูลในลักษณะที่เรียกว่า Keylogging ซึ่งอาจเป็นสาเหตุสำคัญทำให้ข้อมูลการล็อกอินของ LINE ถูกขโมยออกไปได้

3. ไม่หลงเชื่อการใช้งานโปรแกรมใด ๆ ก็ตามที่ให้ผู้ใช้งานกรอกข้อมูล Username และ Password ของระบบต่าง ๆ อันอาจเป็นต้นเหตุของการขโมยข้อมูลการล็อกอินของ LINE ออกไปได้

4. อัปเดตโปรแกรม LINE ให้เป็นเวอร์ชันใหม่ล่าสุดเสมอทั้งบนเครื่อง PC และโทรศัพท์มือถือ เนื่องจากบางครั้งผู้พัฒนา LINE มีการออกแพตช์แก้ไขปัญหาช่องโหว่ด้านความมั่นคงปลอดภัยมาด้วย การอัปเดตอย่างสม่ำเสมอสามารถช่วยลดผลกระทบจากปัญหาช่องโหว่บน LINE ได้

5. ติดตามข่าวสารด้านความมั่นคงปลอดภัยจากแหล่งข้อมูลที่น่าเชื่อถือ เพื่ออัปเดตให้รู้เท่าทันกลลวงหรือภัยคุกคามแบบใหม่ และใช้วิจารณญาณในการใช้งานก่อนทุกครั้ง

อ้างอิง

1. https://www.thaicert.or.th/papers/technical/2013/pa2013te015.html
2. https://www.thaicert.or.th/papers/general/2013/pa2013ge010.html
3. http://pantip.com/topic/32643838
4. http://store.apple.com/us/accessories/giftcards
5. http://www.scmp.com/news/asia/article/1536095/users-line-messaging-app-urged-change-passwords-after-hack
6. http://pantip.com/topic/32633178
7. https://contact.line.me/serviceId/10000

บทความ แจ้งเตือน และข้อแนะนำ สำหรับ ผู้ดูแลระบบ

ระวังภัย ช่องโหว่ 0-day ในโปรแกรม Microsoft Word (CVE-2014-1761) โจมตีผ่านไฟล์ RTF

วันที่ประกาศ : 24 มีนาคม 2557
ปรับปรุงล่าสุด : 29 มีนาคม 2557
เรื่อง : ระวังภัย ช่องโหว่ 0-day ในโปรแกรม Microsoft Word (CVE-2014-1761) โจมตีผ่านไฟล์ RTF
ประเภทภัยคุกคาม : Intrusion

ข้อมูลทั่วไป

เมื่อวันที่ 24 มีนาคม 2557 บริษัท Microsoft ได้แจ้งเตือนช่องโหว่ด้านความมั่นคงปลอดภัย (Security Advisory) หมายเลข 2953095 **[1]** เรื่องข้อผิดพลาดในการประมวลผลไฟล์เอกสารประเภท .RTF ในโปรแกรม Microsoft Word ส่งผลให้ผู้ไม่หวังดีสามารถติดตั้งโปรแกรมไม่พึงประสงค์ลงในเครื่องของผู้ใช้ได้ ช่องโหว่นี้มีหมายเลข CVE-2014-1761 **[2]** โดย Microsoft แจ้งว่าพบการโจมตีด้วยช่องโหว่นี้แล้ว

วิธีการโจมตีผ่านช่องโหว่นี้ ผู้ไม่หวังดีจะส่งอีเมลโดยมีข้อความหลอกให้เหยื่อเปิดเอกสารแนบเป็นไฟล์ RTF ที่ภายในเอกสารมีการฝังโค้ดโจมตีผ่านช่องโหว่นี้เอาไว้ เมื่อเปิดเอกสารนั้นขึ้นมาดูก็จะถูกติดตั้งโปรแกรมไม่พึงประสงค์ลงในเครื่อง

ผลกระทบ

ผู้ใช้ที่ใช้ Microsoft Word เปิดไฟล์เอกสาร RTF ที่มีโค้ดอันตรายฝังอยู่ จะถูกติดตั้งโปรแกรมไม่พึงประสงค์ลงในเครื่อง ซึ่งอาจทำลายข้อมูลในเครื่องหรือเปิดโอกาสให้ผู้ไม่หวังดีเชื่อมต่อเข้ามาควบคุมเครื่องจากระยะไกลได้

ระบบที่ได้รับผลกระทบ

- Microsoft Word 2003 Service Pack 3
- Microsoft Word 2007 Service Pack 3
- Microsoft Word 2010 Service Pack 1 และ Service Pack 2 ทั้งเวอร์ชัน 32 bit และ 64 bit
- Microsoft Word 2013 ทั้งเวอร์ชัน 32 bit และ 64 bit
- Microsoft Word 2013 RT
- Microsoft Office for Mac 2011
- Microsoft Word Viewer

- Microsoft Office Compatibility Pack Service Pack 3
- Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 1 และ Service Pack 2
- Word Automation Services on Microsoft SharePoint Server 2013
- Microsoft Office Web Apps 2010 Service Pack 1 และ Service Pack 2
- Microsoft Office Web Apps Server 2013

ข้อแนะนำในการป้องกันและแก้ไข

ปัจจุบันยังอยู่ระหว่างการตรวจสอบและวิเคราะห์สาเหตุ โดยในเบื้องต้น Microsoft ได้แนะนำให้ผู้ใช้ติดตั้งโปรแกรม Fix it **[3]** เพื่อปิดการแสดงผลไฟล์ RTF เป็นการชั่วคราว อย่างไรก็ตาม Fix it นี้เป็นเพียงวิธีการแก้ไขปัญหาเฉพาะหน้าเท่านั้น ผู้ใช้ควรติดตามข่าวสารอย่างสม่ำเสมอและรีบติดตั้งแพตช์จาก Microsoft ทันทีที่สามารถทำได้

การติดตั้ง Fix it นี้อาจก่อให้เกิดปัญหากับโปรแกรมที่มีการเรียกใช้งานไฟล์ RTF หากจำเป็นต้องทำงานโดยใช้ไฟล์เอกสารรูปแบบดังกล่าว และไม่สามารถติดตั้ง Fix it ได้ ทาง Microsoft ได้แนะนำวิธีการลดโอกาสเสี่ยงจากช่องโหว่ ดังนี้

- ตั้งค่าโปรแกรม Microsoft Outlook ให้อ่านอีเมลในแบบ Plaintext **[4]**
- ตั้งค่าโปรแกรม Microsoft Office File Block Policy เพื่อบล็อกไม่ให้โปรแกรม Microsoft Word สามารถเปิดไฟล์ RTF ได้ **[5]**
- ติดตั้งโปรแกรม EMET และตั้งค่าโปรแกรมให้คอยตรวจสอบการทำงานของโปรแกรม Microsoft Word เพื่อช่วยลดผลกระทบที่เกิดจากช่องโหว่นี้

และเนื่องจากปัจจุบันยังไม่มีแพตช์หรือ Fix it สำหรับ Microsoft Office for Mac ออกมา ดังนั้นหากผู้ใช้โปรแกรมดังกล่าวต้องการจะเปิดไฟล์ RTF ให้หลีกเลี่ยงไปใช้โปรแกรมอื่น เช่น TextEdit ซึ่งเป็นโปรแกรมที่มาพร้อมกับระบบปฏิบัติการ OS X ซึ่งสามารถเปิดไฟล์ RTF ได้

ทาง Microsoft ได้ให้ข้อมูลเพิ่มเติมว่า โปรแกรม Wordpad ที่มากับ Windows ไม่ได้รับผลกระทบจากช่องโหว่นี้ ผู้ใช้งานที่ยังจำเป็นต้องทำงานร่วมกับไฟล์ RTF สามารถเปิดไฟล์ดังกล่าวโดยใช้โปรแกรม Wordpad ได้โดยการคลิกขวาที่ไฟล์ RTF เลือกคำสั่ง Open with แล้วเลือกโปรแกรม Wordpad

อ้างอิง

1. https://technet.microsoft.com/en-us/security/advisory/2953095
2. http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1761
3. https://support.microsoft.com/kb/2953095
4. http://office.microsoft.com/en-us/outlook-help/read-email-messages-in-plain-text-HA102748923.aspx
5. http://technet.microsoft.com/library/cc179230

ระวังภัย ช่องโหว่ใน OpenSSL ผู้ไม่หวังดีสามารถขโมยข้อมูลใน Memory จากเครื่องของเหยื่อได้ (Heartbleed, CVE-2014-0160)

วันที่ประกาศ : 9 เมษายน 2557
ปรับปรุงล่าสุด : 19 เมษายน 2557
เรื่อง : ระวังภัย ช่องโหว่ใน OpenSSL ผู้ไม่หวังดีสามารถขโมยข้อมูลใน Memory จากเครื่องของเหยื่อได้ (Heartbleed, CVE-2014-0160)
ประเภทภัยคุกคาม : Other

ข้อมูลทั่วไป

OpenSSL เป็นไลบรารีสำหรับใช้ในการเข้ารหัสลับข้อมูลผ่านโพรโทคอล SSL และ TLS ซึ่งเป็นไลบรารีแบบ Open Source ทำให้ผู้พัฒนาซอฟต์แวร์หลายรายนำไลบรารีดังกล่าวนี้ไปใช้ในซอฟต์แวร์ของตนเอง ตัวอย่างโปรแกรมที่ใช้งานไลบรารี OpenSSL เช่น ระบบปฏิบัติการ Linux, เว็บเซิร์ฟเวอร์, โปรแกรมแซ็ต หรือโปรแกรมสำหรับเชื่อมต่อ VPN เป็นต้น

เมื่อวันที่ 7 เมษายน 2557 ทาง OpenSSL ได้แจ้งเตือนช่องโหว่ในซอฟต์แวร์ OpenSSL เวอร์ชัน 1.0.1 ถึง 1.0.1f **[1]** โดยช่องโหว่ดังกล่าวอยู่ในส่วนของการเชื่อมต่อ TLS/DTLS ในส่วนที่เป็น Heartbeat Extension ที่เอาไว้ตรวจสอบว่าโฮสต์ที่เชื่อมต่ออยู่ด้วยนั้นยังทำงานอยู่หรือไม่ **[2]**

เนื่องจากส่วน Heartbeat Extension อนุญาตให้ระบบใด ๆ ก็ตามสามารถส่ง Request เข้ามาเพื่อให้เครื่องปลายทางตอบกลับ แต่กระบวนการนี้มีความผิดพลาดในขั้นตอนการตรวจสอบข้อมูล ทำให้ในกรณีที่ Request ที่ส่งเข้ามามีการระบุความยาวของข้อมูลที่ส่งกลับมากกว่าขนาดของ Request เครื่องปลายทางจะไปอ่านข้อมูลจากหน่วยความจำของตัวเครื่องออกมา แล้วส่งข้อมูลดังกล่าวกลับไปให้ผู้ที่ร้องขอ **[3]**

ข้อมูลที่เครื่องปลายทางจะส่งกลับไปให้ผู้ที่ร้องขอเป็นข้อมูลขนาด 64 KB จากหน่วยความจำในตำแหน่งที่ใกล้เคียงกับข้อมูลที่โปรเซสของ OpenSSL ใช้งานอยู่ ซึ่งข้อมูลที่อยู่ในหน่วยความจำจะมีการเก็บแบบไม่มีการเข้ารหัสลับ และอาจมีข้อมูลสำคัญเก็บอยู่ในตำแหน่งนี้ เช่น รหัสผ่าน หมายเลขบัตรเครดิต หรือ Private Key ของระบบที่ใช้งาน OpenSSL จึงทำให้มีโอกาสสูงที่ผู้ไม่หวังดีจะเชื่อมต่อเข้ามาเพื่อขโมยข้อมูลสำคัญออกไปจากหน่วยความจำของเครื่องปลายทางได้ **[4]**

ถึงแม้ว่าข้อมูลที่สามารถอ่านได้จากหน่วยความจำของเครื่องปลายทาง จะสามารถนำออกไปได้แค่ครั้งละไม่เกิน 64 KB แต่ผู้ไม่หวังดีก็สามารถที่จะส่ง Request เข้ามา

เรื่อย ๆ เพื่อดึงข้อมูลในส่วนที่เหลือและนำข้อมูลที่ได้ไปปะติดปะต่อให้เป็นข้อมูลเต็ม ๆ ได้

ผลกระทบ

ช่องโหว่นี้มีผลกระทบทั้งกับผู้ใช้ทั่วไปและผู้ให้บริการผ่านอินเทอร์เน็ต ซึ่งทั้งสองกลุ่มนี้มีโอกาสที่จะถูกขโมยข้อมูลสำคัญออกไปจากหน่วยความจำ

ตัวอย่างความเสียหายที่เกิดกับผู้ใช้ทั่วไป เช่น ผู้ใช้เปิดโปรแกรมที่มีการเชื่อมต่อแบบ SSL/TLS ที่พัฒนาโดยใช้ไลบรารี OpenSSL เวอร์ชันที่มีช่องโหว่ หากผู้ใช้มีการเชื่อมต่อแบบ SSL ก็มีโอกาสที่จะถูกผู้ไม่หวังดีขโมยข้อมูลที่อยู่ในหน่วยความจำได้ ขึ้นอยู่กับว่าโปรแกรมที่ใช้งานนั้นคือโปรแกรมอะไร เช่น เว็บเบราว์เซอร์ โปรแกรมรับส่งอีเมล โปรแกรมแช็ต โปรแกรม Cloud Storage หรือโปรแกรมเชื่อมต่อ VPN

ตัวอย่างความเสียหายที่เกิดกับผู้ให้บริการที่เปิดใช้งานเว็บเซิร์ฟเวอร์ที่ใช้การเชื่อมต่อแบบ SSL ซึ่งมีโอกาสสูงที่จะถูกผู้ไม่หวังดีขโมยข้อมูลสำคัญออกไปจากหน่วยความจำ เช่น รหัสผ่านของผู้ที่เข้าใช้งานระบบ หรือ Private Key ที่ใช้ในการเข้ารหัสลับข้อมูล หากผู้ไม่หวังดีได้ข้อมูลในส่วนนี้ไปก็อาจถอดรหัสลับข้อมูลทุกอย่างที่เคยมีการแลกเปลี่ยนผ่านเครื่องเซิร์ฟเวอร์ได้

ระบบที่ได้รับผลกระทบ

ซอฟต์แวร์ OpenSSL เวอร์ชันดังต่อไปนี้ **[5]**

- 1.0.1
- 1.0.1:beta1 ถึง 1.0.1:beta3
- 1.0.1a ถึง 1.0.1f
- 1.0.2-beta1

ผู้ให้บริการอ้างตาม list ของ CERT/CC **[6]**

ข้อแนะนำในการป้องกันและแก้ไข

[สำหรับผู้ดูแลระบบ]

1. ผู้ดูแลระบบควรอัปเดตซอฟต์แวร์ OpenSSL ที่ใช้งานในทันที เมื่ออัปเดตซอฟต์แวร์เสร็จแล้วให้ตรวจสอบหมายเลขเวอร์ชันว่าซอฟต์แวร์ได้รับการอัปเดตแล้ว

สำหรับระบบปฏิบัติการที่บริหารจัดการด้วย DPKG เช่น Debian Ubuntu

dpkg -s openssl

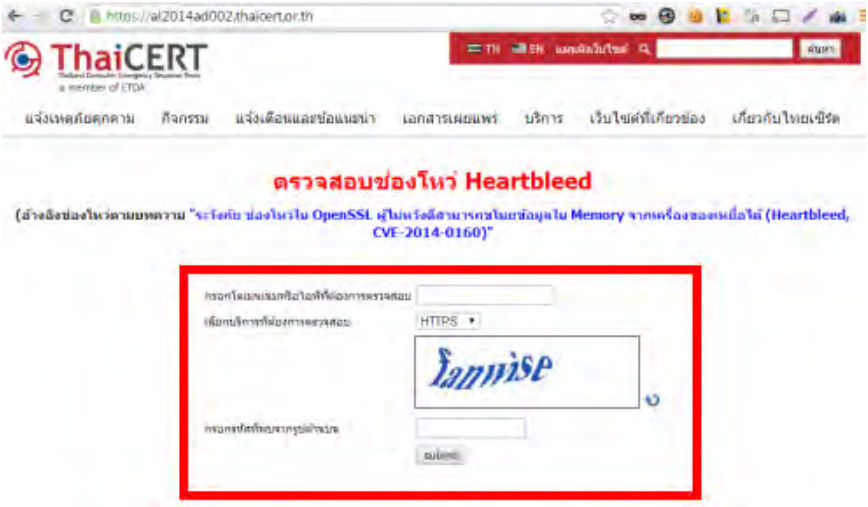
สำหรับระบบปฏิบัติการที่บริหารจัดการด้วย RPM เช่น CentOS Redhat

rpm -q --info openssl

2. เปลี่ยน SSL Certificate ใหม่

อย่างไรก็ตาม เวอร์ชันล่าสุดของซอฟต์แวร์ OpenSSL ที่ได้รับการแก้ไขช่องโหว่นี้แล้วบนระบบปฏิบัติการ Linux นั้น อาจมีหมายเลขเวอร์ชันที่ดูเหมือนเป็นส่วนหนึ่งของเวอร์ชันที่ได้รับผลกระทบดังที่ระบุไว้ข้างต้น เช่น ซอฟต์แวร์ OpenSSL บนระบบปฏิบัติการ Debian เวอร์ชันที่ได้รับการแก้ไขช่องโหว่แล้วคือ 1.0.1e-2+deb7u5 หรือสูงกว่า และในแต่ละระบบปฏิบัติการอาจมีหมายเลขเวอร์ชันล่าสุดที่แตกต่างกันไป ดังนั้น ผู้ใช้จึงควรตรวจสอบจากเว็บไซต์ทางการของแต่ละระบบปฏิบัติการอีกครั้ง เช่น Debian **[7]**, Ubuntu **[8]**, Red Hat Enterprise Linux **[9]** และ FreeBSD **[10]**

3. ผู้ดูแลระบบสามารถตรวจสอบปัญหาของโหว่ดังกล่าว ผ่านบริการของไทยเซิร์ตจัดเตรียมไว้ https://al2014ad002.thaicert.or.th/



รูปที่ 1 หน้าจอแสดงบริการตรวจสอบช่องโหว่ที่ไทยเซิร์ตจัดเตรียมไว้

[สำหรับผู้ใช้งาน]

1. ผู้ใช้งานสามารถตรวจสอบปัญหาของโหว่ดังกล่าว ผ่านบริการที่ไทยเซิร์ตจัดเตรียมไว้ https://al2014ad002.thaicert.or.th/ หากพบว่าบริการที่กำลังจะเข้าใช้งานมีช่องโหว่ Heartbleed ให้หยุดการเข้าใช้งานระบบนั้นก่อนทันที

2. เปลี่ยนรหัสผ่านกับเว็บไซต์ที่เข้าใช้งานด้วยรหัสผ่านใหม่ รวมถึงรหัสผ่านสำหรับการเข้าใช้งาน**ระบบที่ได้รับผลกระทบ** อ้างตาม list ของ CERT/CC **[6]** และในกรณีที่ใช้งานหลายเว็บไซต์หรือระบบ ให้เลือกเปลี่ยนรหัสผ่านที่แตกต่างกัน

3. เมื่อรู้ตัวว่าใช้งาน WiFi สาธารณะให้ระมัดระวังการใช้งานหรือหลีกเลี่ยงเข้า

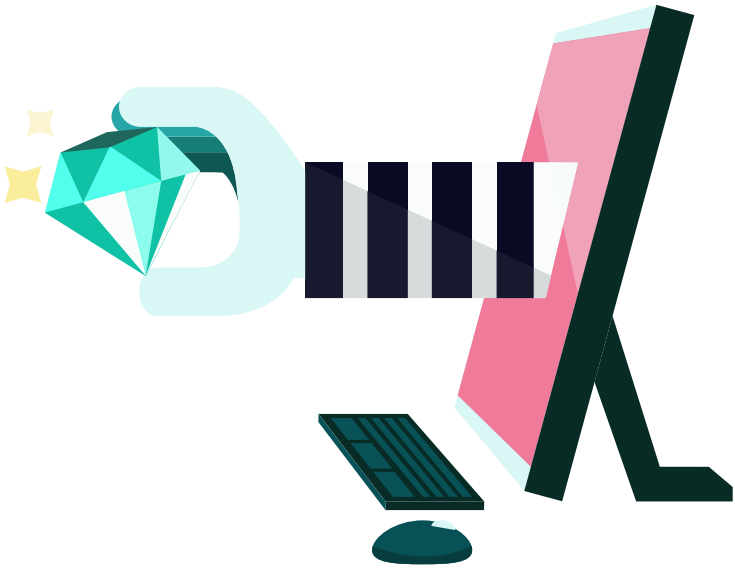
เว็บไซต์ที่มีความสำคัญ เช่น เว็บไซต์ธนาคารออนไลน์ หรือเว็บไซต์อีเมล

4. ตรวจสอบประวัติการล็อกอินเข้าใช้งานระบบที่สำคัญเพื่อให้แน่ใจว่าไม่มีการล็อกอินจากบุคคลอื่น

5. ติดตามข่าวสารเกี่ยวกับปัญหาช่องโหว่ Heartbleed จากเว็บไซต์ที่น่าเชื่อถือหรือบนเว็บไซต์ไทยเซิร์ต

บริการตรวจสอบช่องโหว่ Heartbleed

ไทยเซิร์ตได้เปิดให้บริการตรวจสอบช่องโหว่ตามที่อ้างถึงในบทความนี้ โดยผู้ใช้งานสามารถตรวจสอบได้ตามลิงก์ต่อไปนี้ http://al2014ad002.thaicert.or.th/



อ้างอิง

1. https://www.openssl.org/news/secadv_20140407.txt
2. https://tools.ietf.org/html/rfc6520
3. http://heartbleed.com
4. http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html
5. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
6. http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=720951&SearchOrder=4
7. http://www.debian.org/security/2014/dsa-2896
8. http://www.ubuntu.com/usn/usn-2165-1
9. https://rhn.redhat.com/errata/RHSA-2014-0376.html
10. http://www.freebsd.org/security/advisories/FreeBSD-SA-14:06.openssl.asc

ระวังภัย มัลแวร์
SynoLocker แพร่ระบาดบนอุปกรณ์ NAS ของ Synology

วันที่ประกาศ : 5 สิงหาคม 2557
เรื่อง : ระวังภัย มัลแวร์ SynoLocker แพร่ระบาดบนอุปกรณ์ NAS ของ Synology
ประเภทภัยคุกคาม : Malicious Code

ข้อมูลทั่วไป

เมื่อวันที่ 3 สิงหาคม 2557 มีผู้ใช้หลายรายได้รายงานถึงการแพร่ระบาดของมัลแวร์บนอุปกรณ์ประเภท Network-attached Storage (NAS) ที่ผลิตโดยบริษัท Synology Inc. **[1]** โดยมัลแวร์ดังกล่าวมีชื่อเรียกว่า SynoLocker ซึ่งเป็นมัลแวร์ประเภท Ransomware ที่มีพฤติกรรมในการเข้ารหัสลับข้อมูลที่เก็บอยู่บน NAS เพื่อไม่ให้ผู้ใช้สามารถเข้าถึงข้อมูลของตนได้ จากนั้นมัลแวร์จะแสดงข้อความข่มขู่ให้ผู้ใช้ชำระเงิน เพื่อดำเนินการถอดรหัสลับข้อมูลดังกล่าว

ผู้ใช้จะสามารถสังเกตความผิดปกติระหว่างการใช้งานหาก NAS ติดมัลแวร์ได้โดยเมื่อผู้ใช้เข้าสู่หน้าหลักของระบบจัดการ จะพบข้อความที่แสดงโดยมัลแวร์ ระบุให้ผู้ใช้เข้าไปยังเว็บไซต์ http://cypherxffttr7hho.onion ผ่านโปรแกรม Tor Browser แล้วชำระเงินด้วย Bitcoin เป็นจำนวน 0.6 BTC เพื่อขอรับ Private Key ในการถอดรหัสลับข้อมูลดังรูปที่ 1 และ 2

SynoLocker™

Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available here.

Follow these simple steps if files recovery is needed:

1. Download and install Tor Browser.
2. Open Tor Browser and visit http://cypherxffttr7hho.onion. This link works **only** with the Tor Browser.
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is **18z9v3tQSI9mEg8yDBkVXJ5krvqCvtqXL2** (also visible here).
5. Follow the instructions on the decryption page once a valid decryption key has been acquired.

Technical details about the encryption process:

- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwritten with random bits before being deleted from the hard drive.
- The encrypted file is renamed to the original filename.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.
- Once a valid decryption key is provided, the software search each files for a specific string stored in all encrypted files.
- When the string is found, the software extracts and decrypts the unique 256-bit AES key needed to restore that file.

Note: Without the decryption key, all encrypted files will be lost forever.

รูปที่ 1 ข้อความที่แสดงโดยมัลแวร์ให้ผู้ใช้ชำระเงิน

รูปที่ 2 ขั้นตอนการชำระเงินบนเว็บไซต์ของผู้ไม่หวังดี (ที่มา: korben.info [2])

ผลกระทบ

ผู้ใช้จะไม่สามารถเข้าถึงข้อมูลที่เก็บอยู่ภายใน NAS ได้

ระบบที่ได้รับผลกระทบ

อุปกรณ์ประเภท NAS ของบริษัท Synology Inc. ที่ติดตั้งระบบปฏิบัติการ DiskStation Manager (DSM) เวอร์ชันต่อไปนี้

- DSM 4.3 เวอร์ชันต่ำกว่า 4.3-3827
- DSM 4.2 หรือ 4.1 เวอร์ชันต่ำกว่า 4.2-3243
- DSM 4.0 เวอร์ชันต่ำกว่า 4.0-2259

ข้อแนะนำในการป้องกันและแก้ไข

เมื่อวันที่ 4 สิงหาคม 2557 ทาง Synology ได้ประกาศผ่านทางเว็บไซต์ทางการเกี่ยวกับมัลแวร์ดังกล่าว โดยแนะนำให้ผู้ใช้ปิดการทำงานของ NAS ทันทีที่พบว่าติดมัลแวร์ เพื่อหยุดการทำงานของมัลแวร์ที่กำลังเข้ารหัสลับข้อมูลในเครื่อง และติดต่อฝ่าย Support ของ Synology เพื่อให้เจ้าหน้าที่ตรวจสอบและวิเคราะห์ต่อไป **[3]**

ต่อมาในวันที่ 5 สิงหาคม 2557 ทาง Synology ได้มีการระบุเพิ่มเติมว่า ช่องโหว่ที่มัลแวร์ใช้โจมตีเป็นช่องโหว่ที่มีการแก้ไขไปแล้วตั้งแต่เดือนธันวาคม 2556 และแนะนำให้ผู้ที่ยังไม่ได้อัปเดตระบบปฏิบัติการของ NAS ในช่วงเวลาดังกล่าว อัปเดตระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดเพื่อป้องกันการโจมตีของมัลแวร์

จากข้อมูลข้างต้น ไทยเซิร์ตแนะนำให้ผู้ใช้ NAS ของ Synology ทำการอัปเดตระบบปฏิบัติการของ NAS ให้เป็นเวอร์ชันล่าสุด โดยอ้างอิงหมายเลขเวอร์ชันจากเว็บไซต์ทางการของ Synology **[4]** ตลอดจนพิจารณาปิดกั้นการเชื่อมต่อ ไม่ให้ผู้ใช้งานบนอินเทอร์เน็ตสามารถเข้าถึง NAS ได้โดยตรง แต่ให้เชื่อมต่อผ่านบริการ VPN ที่ไม่ได้ทำงานอยู่บน NAS ดังกล่าว เช่น บริการ VPN ของเราเตอร์ในระบบเครือข่าย หรือ OpenVPN เท่านั้น นอกจากนี้ควรเปลี่ยนรหัสผ่านผู้ใช้งานให้มีความแข็งแกร่งมากขึ้น ทั้งนี้หากมีความคืบหน้าประการใด ไทยเซิร์ตจะนำข้อมูลมาอัปเดตให้ทราบอีกครั้ง โดยสามารถติดตามข่าวสารต่าง ๆ ผ่านทาง Twitter ของไทยเซิร์ตได้ที่ @ThaiCERT **[5]**

อ้างอิง

1. http://forum.synology.com/enu/viewtopic.php?f=3&t=88716
2. http://korben.info/synolocker.html
3. http://forum.synology.com/enu/viewtopic.php?f=108&t=88770#p333891
4. http://www.synology.com/en-global/support/download
5. https://twitter.com/thaicert

ระวังภัย ช่องโหว่ใน Drupal และ WordPress ผู้ไม่หวังดีสามารถโจมตีระบบในลักษณะ DoS ได้

วันที่ประกาศ : 8 สิงหาคม 2557
เรื่อง : ระวังภัย ช่องโหว่ใน Drupal และ WordPress ผู้ไม่หวังดีสามารถโจมตีระบบในลักษณะ DoS ได้
ประเภทภัยคุกคาม : DoS (Denial-of-Service)

ข้อมูลทั่วไป

เมื่อวันที่ 6 สิงหาคม 2557 เว็บไซต์ทางการของ Drupal ได้ประกาศพบช่องโหว่ในซอฟต์แวร์ Drupal ซึ่งเป็นเครื่องมือในการจัดการเนื้อหา (CMS) โดยเกิดช่องโหว่ในส่วนประกอบของ XML-RPC และ OpenID ที่เปิดโอกาสให้ผู้ไม่หวังดีสามารถโจมตีเว็บไซต์ในลักษณะ DoS ผ่านช่องโหว่ดังกล่าวได้ **[1]** โดยจะส่งผลให้การใช้งาน CPU และ Memory ตลอดจนการเชื่อมต่อฐานข้อมูลเพิ่มขึ้นมากผิดปกติ จนทำให้เว็บไซต์ไม่สามารถทำงานได้ตามปกติ จนต้องหยุดให้บริการในที่สุด

ช่องโหว่นี้ยังมีผลกระทบกับระบบ WordPress ด้วย เนื่องจากมีการใช้งานส่วนประกอบ XML-RPC เช่นกัน ดังที่มีการแจ้งเตือนในเว็บไซต์ของ WordPress ในวันเดียวกัน **[2]**

ผลกระทบ

เว็บไซต์ที่ใช้งานระบบ Drupal หรือ WordPress เวอร์ชันที่ได้รับผลกระทบ อาจถูกโจมตีจนไม่สามารถให้บริการได้

ระบบที่ได้รับผลกระทบ

- Drupal เวอร์ชัน 6.x ที่เก่ากว่าเวอร์ชัน 6.33
- Drupal เวอร์ชัน 7.x ที่เก่ากว่า 7.31
- WordPress เวอร์ชันเก่ากว่า 3.9.2

ข้อแนะนำในการป้องกันและแก้ไข

ผู้ดูแลระบบ Drupal และ WordPress สามารถอัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขช่องโหว่นี้แล้ว จากเว็บไซต์ทางการของ Drupal **[3]** และ WordPress **[4]** แต่หากไม่สามารถอัปเดตเวอร์ชันซอฟต์แวร์ให้เป็นเวอร์ชันที่แก้ไขแล้วดังกล่าวได้ ผู้ดูแลระบบสามารถใช้วิธีลบหรือจำกัดการเข้าถึง xml-rpc.php ในเครื่องเซิร์ฟเวอร์ที่ติดตั้ง Drupal หรือ WordPress และปิดการใช้งาน OpenID ในระบบ Drupal เพื่อป้องกันการโจมตีช่องโหว่ดังกล่าว อย่างไรก็ตาม ไทยเซิร์ตแนะนำให้ผู้ดูแลระบบอัปเดตเวอร์ชันของ Drupal และ WordPress หรือซอฟต์แวร์อื่น ๆ ในเครื่องบริการเว็บให้เป็นเวอร์ชันใหม่ตามที่ผู้ผลิตซอฟต์แวร์แนะนำเสมอ เพื่อป้องกันผลกระทบจากช่องโหว่ต่าง ๆ ที่อาจมีการค้นพบในอนาคต

อ้างอิง

1. https://www.drupal.org/SA-CORE-2014-004
2. https://wordpress.org/news/2014/08/wordpress-3-9-2/
3. https://www.drupal.org/project/drupal
4. https://wordpress.org/download/

ระวังภัย ช่องโหว่ในซอฟต์แวร์ Bash ผู้ไม่หวังดีสามารถส่งคำสั่งไม่พึงประสงค์ไปประมวลผลยังเครื่องของเหยื่อได้ทันที (Shellshock, CVE-2014-6271, CVE-2014-7169)

วันที่ประกาศ : 26 กันยายน 2557
ปรับปรุงล่าสุด : 8 ตุลาคม 2557
เรื่อง : ระวังภัย ช่องโหว่ในซอฟต์แวร์ Bash ผู้ไม่หวังดีสามารถส่งคำสั่งไม่พึงประสงค์ไปประมวลผลยังเครื่องของเหยื่อได้ทันที (Shellshock, CVE-2014-6271, CVE-2014-7169)
ประเภทภัยคุกคาม : Intrusion

ปรับปรุงข้อมูลล่าสุด

เมื่อวันที่ 29 กันยายน 2557 ไทยเซิร์ตได้รับข้อมูลว่าผู้พัฒนาซอฟต์แวร์ Bash ได้มีการเผยแพร่แพตช์สำหรับแก้ไขปัญหาช่องโหว่ออกมาอีก 2 ครั้ง คือในวันที่ 27 และ 28 กันยายน 2557 (ตามเวลาของประเทศไทย) โดยเป็นแพตช์ที่ใช้แก้ไขปัญหาช่องโหว่ CVE-2014-7169 ที่กล่าวถึงในการแจ้งเตือนนี้ และช่องโหว่ใหม่ คือ CVE-2014-7186 และ CVE-2014-7187 ซึ่งเป็นช่องโหว่ในรูปแบบ Buffer Overflow โดยเวอร์ชันที่เป็นทางการของซอฟต์แวร์ Bash ที่แก้ไขล่าสุดจะเป็น 4.0.41 **[1]**, 4.1.14 **[2]**, 4.2.50 **[3]** และ 4.3.27 **[4]** สำหรับผู้ที่ติดตั้งซอฟต์แวร์ Bash ผ่านระบบบริการจัดการซอฟต์แวร์แพ็กเกจ (Package Management) บนระบบปฏิบัติการ Linux ให้ตรวจสอบจากเอกสาร Changelog ของซอฟต์แวร์ Bash เวอร์ชันล่าสุดของ Distribution ที่ใช้งานอยู่ว่า มีการระบุถึงการแก้ไขช่องโหว่ใน CVE ทั้งหมดที่ระบุในการแจ้งเตือนนี้หรือไม่ เพื่อให้แน่ใจว่าไม่ได้รับผลกระทบจากช่องโหว่ดังกล่าว

ข้อมูลทั่วไป

โดยปกติการใช้งานระบบปฏิบัติการประเภทยูนิกซ์ (Unix หรือ Unix-liked) อย่างเช่น Linux หรือ FreeBSD มีการออกแบบมาให้ใช้งานในลักษณะ Command Line มาตั้งแต่ต้น ถึงแม้ปัจจุบันจะมีการพัฒนาให้มีการทำงานผ่าน Graphic User Interface (GUI) แต่การทำงานในลักษณะ Command Line ที่ใช้งานผ่านซอฟต์แวร์ประเภท Shell ก็ยังถือเป็นส่วนประกอบพื้นฐานสำคัญของระบบปฏิบัติการประเภทยูนิกซ์ที่ยังไม่สามารถยกเลิกการใช้งานได้ เนื่องจากยังมีแอปพลิเคชันอื่น ๆ อีกเป็นจำนวนมากที่ยังต้องการความสามารถของ Shell ในการทำงาน ตัวอย่างของซอฟต์แวร์ที่ทำงานเป็น Shell เช่น Csh Ksh Ash Dash หรือ Bash ซอฟต์แวร์ Bash ถือเป็นซอฟต์แวร์ประเภท Shell

ที่ได้รับความนิยมสูงสุด เนื่องจากมีการนำมาใช้เป็นซอฟต์แวร์ Shell หลักของระบบปฏิบัติการ Linux เกือบทุก Distribution ตัวอย่างของแอปพลิเคชันที่มีการเรียกใช้ซอฟต์แวร์ Bash ในการทำงานนี้ เช่น เว็บแอปพลิเคชันประเภท CGI และแอปพลิเคชันระบบ เช่น DHCP ที่มีการทำงานร่วมกับซอฟต์แวร์ Shell เพื่อรับค่าผ่านพารามิเตอร์บางอย่างมาประมวลผล

เมื่อวันที่ 24 กันยายน 2557 บริษัท Akamai ซึ่งให้บริการเครือข่ายส่งคอนเทนต์ความเร็วสูง (Content Delivery Network) ได้เผยแพร่บทความในเว็บไซต์ blogs.akamai.com โดยมีเนื้อหาว่านักวิจัยของ Akamai ชื่อ Stephane Chazelas **[5]** ได้ค้นพบช่องโหว่เกี่ยวกับซอฟต์แวร์ Bash เรียกว่า Shellshock ช่องโหว่ดังกล่าวทำให้ผู้ไม่หวังดีสามารถสั่งรันคำสั่งไม่พึงประสงค์บนเครื่องให้บริการของระบบได้ทันที และได้มีการยืนยันจากบริษัทแล้วถึงปัญหาช่องโหว่ดังกล่าว รวมถึงมีการเผยแพร่ข้อมูลช่องโหว่ดังกล่าวไปยังเว็บไซต์ CVE แล้วเช่นกัน **[6]**

ทางเว็บไซต์ผู้พัฒนาซอฟต์แวร์ Bash ได้เผยแพร่แพตช์อัปเดตสำหรับแก้ไขช่องโหว่ CVE-2014-6271 ซึ่งสามารถตรวจสอบได้ในหัวข้อ “ข้อแนะนำในการป้องกันและแก้ไข”

อย่างไรก็ตามจากสถานการณ์ดังกล่าว ยังมีผู้ตรวจพบว่าถึงแม้จะมีการอัปเดตแล้วแต่ก็ยังสามารถโจมตีช่องโหว่ของซอฟต์แวร์ Bash ได้อยู่ เพียงแต่เปลี่ยนแปลงวิธีการในการโจมตี **[7]** โดยในกรณีการโจมตีนี้ถือว่าเป็นรูปแบบการค้นพบช่องโหว่ใหม่และได้มีการออกหมายเลข CVE เพิ่มเติมในกรณีดังกล่าวแล้ว โดยมีหมายเลขเป็น CVE-2014-7169 **[8]**

สำหรับช่องโหว่ CVE-2014-7169 นี้ ตรวจสอบพบว่าหนึ่งในทีมผู้พัฒนาซอฟต์แวร์ Bash ชื่อ Chet Ramey ได้ทำการเผยแพร่แพตช์สำหรับแก้ไขปัญหาช่องโหว่ดังกล่าว **[9]** และจากการตรวจสอบเพิ่มเติมพบว่า Debian **[10]** และ Ubuntu **[11]** ได้มีการเผยแพร่อัปเดตของซอฟต์แวร์ Bash ซึ่งแก้ปัญหาช่องโหว่ตามข้อมูลของ CVE ทั้ง 2 ส่วนแล้ว อย่างไรก็ตามสำหรับผู้ใช้งานระบบปฏิบัติการ Linux ใน Distribution อื่น ๆ สามารถติดตามการแก้ไขปัญหาได้จากเว็บไซต์ทางการของแต่ละ Distribution

สำหรับผู้ใช้งานระบบปฏิบัติการ Mac OS X เวอร์ชันล่าสุด 10.9.5 พบว่ามีการติดตั้งซอฟต์แวร์ Bash เวอร์ชัน 3.2.51 ซึ่งจากการตรวจสอบข้อมูลข่าวบนอินเทอร์เน็ตพบว่าขณะนี้ทาง Apple ได้รับทราบปัญหานี้แล้ว และทาง Apple จะเผยแพร่เวอร์ชันอัปเดตของซอฟต์แวร์ Bash ในเร็ว ๆ นี้ **[12]**

ผลกระทบ

ช่องโหว่นี้มีผลกระทบทั้งผู้ใช้และระบบที่ให้บริการ ซึ่งทั้งสองกลุ่มนี้มีโอกาสที่จะถูกโจมตีจากช่องโหว่ดังกล่าว เพื่อสั่งให้ประมวลผลคำสั่งไม่พึงประสงค์จากระยะไกล หรือที่เรียกว่า Remote Code Execution ส่งผลให้เครื่องคอมพิวเตอร์ถูกควบคุม

[ตัวอย่างผลกระทบที่เกิดกับผู้ใช้]

1. ผู้ใช้งานที่ใช้ระบบปฏิบัติการที่ได้รับผลกระทบเชื่อมต่อกับ WiFi ที่ผู้ไม่หวังดีเตรียมไว้ ก็มีโอกาสที่ผู้ใช้งานจะถูกโจมตีผ่าน DHCP โดยผู้ไม่หวังดีสามารถใช้วิธีการฝัง

คำสั่งไม่พึงประสงค์และส่งเข้ามาทางพารามิเตอร์ของ DHCP ซึ่งเครื่องผู้ใช้งานจะรับคำสั่งดังกล่าวมาประมวลผลในทันที

[ตัวอย่างผลกระทบที่เกิดกับระบบ]

2. ผู้ให้บริการที่มีการใช้งานเว็บแอปพลิเคชันประเภท CGI เช่น PHP-CGI ที่มีการรับส่งค่าผ่านซอฟต์แวร์ Bash สามารถถูกโจมตีได้ โดยผู้ไม่หวังดีสามารถใช้วิธีการส่งคำสั่งไม่พึงประสงค์ผ่านพารามิเตอร์ของ HTTP Header และเครื่องให้บริการเว็บจะรับคำสั่งดังกล่าวมาประมวลผลในทันที อย่างไรก็ตามจากการตรวจสอบพบว่าการใช้งานของ PHP ผ่าน Mod PHP ของ Apache ในรูปแบบปกติ หรือลักษณะอื่น ๆ ที่คล้ายคลึงกันจะไม่ได้รับผลกระทบ เนื่องจากไม่ได้ใช้วิธีการส่งค่าพารามิเตอร์ในลักษณะเดียวกับ CGI

อย่างไรก็ตาม รูปแบบของการโจมตีด้วยช่องโหว่ดังกล่าวอาจไม่ได้จำกัดอยู่ในกรณีที่ระบุมาเท่านั้น และอาจจะไม่ได้มีการค้นพบในช่วงเวลานี้ ซึ่งหากมีความคืบหน้าใด ๆ ทางไทยเซิร์ตจะอัปเดตให้ทราบต่อไป

ระบบที่ได้รับผลกระทบ

สามารถตรวจสอบผลกระทบของช่องโหว่ดังกล่าวได้ 2 ทาง

1. ทดสอบรันคำสั่ง **[7]**

$env X='() { (a)=>\' bash -c “echo date”

จากคำสั่งดังกล่าว เป็นการสร้างไฟล์ชื่อ echo และมีข้อมูลวันเวลาอยู่ภายใน หากผู้ใช้พบไฟล์ดังกล่าวแสดงว่าระบบที่ใช้งานมีช่องโหว่ของซอฟต์แวร์ Bash อยู่ ดังรูปที่ 1

```
$ env X='() { (a)=>\' bash -c "echo date"
bash: X: line 1: syntax error near unexpected token `='
bash: X: line 1: `'
bash: error importing function definition for `X'
$ ls
echo
$ cat echo
Fri Sep 26 10:31:29 ICT 2014
```

รูปที่ 1 การทดสอบรันคำสั่งเพื่อตรวจสอบช่องโหว่ของซอฟต์แวร์ Bash

2. ตรวจสอบเวอร์ชันของซอฟต์แวร์ Bash ที่ใช้งาน โดยพิมพ์คำสั่ง bash --version ดังตัวอย่างในรูปที่ 2

```
nd@ubuntu:~$ bash --version
GNU bash, version 4.3.11(1)-release (i686-pc-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/
```

รูปที่ 2 การตรวจสอบเวอร์ชันของซอฟต์แวร์ Bash

[เวอร์ชันที่ได้รับผลกระทบจาก CVE-2014-6271]

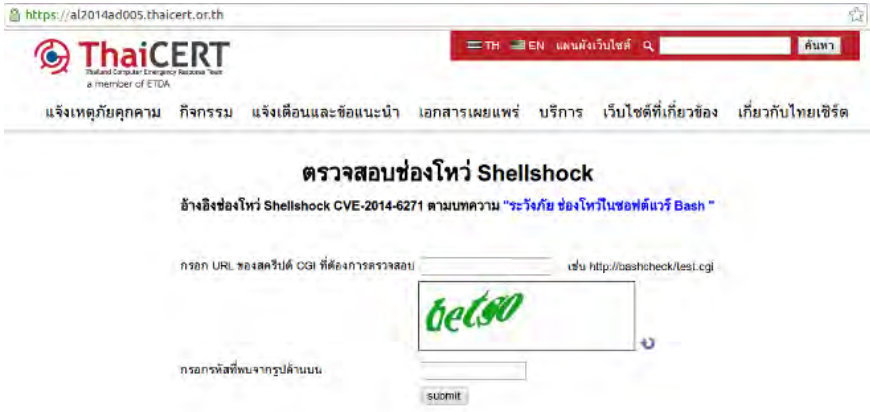
ระบบที่ใช้งานซอฟต์แวร์ Bash ในเวอร์ชัน 3.0.17 , 3.1.18 , 3.2.52 , 4.1.12 , 4.2.48 , 4.3.25 หรือต่ำกว่า

[เวอร์ชันที่ได้รับผลกระทบจาก CVE-2014-7169]

ระบบที่ใช้งานซอฟต์แวร์ Bash ในทุกเวอร์ชัน ยกเว้นที่มีการอัปเดต Patch ของช่องโหว่ CVE-2014-7169 เช่น ซอฟต์แวร์ Bash ใน Debian และ Ubuntu

เวอร์ชันของซอฟต์แวร์ Bash บนระบบปฏิบัติการ Linux นั้น อาจมีหมายเลขเวอร์ชันที่ดูเหมือนเป็นส่วนหนึ่งของเวอร์ชันที่ได้รับผลกระทบดังที่ระบุไว้ข้างต้น แต่ในความเป็นจริงรูปแบบการบริหารจัดการบนระบบปฏิบัติการ Linux นั้น อาจจะไม่ได้มีการใช้งานซอฟต์แวร์เวอร์ชันล่าสุดเสมอไป แต่มีการ Patch เพื่อแก้ไขปัญหาช่องโหว่เรียบร้อยแล้ว ดังนั้น ผู้ใช้งานจึงควรตรวจสอบจากเว็บไซต์ทางการของแต่ละ Distribution อีกครั้ง เช่น Debian **[13]** Ubuntu **[14]** Red Hat Enterprise Linux **[15]** หรือตรวจสอบจากเอกสาร Changelog ของซอฟต์แวร์ Bash ใน Distribution ที่ใช้งานอยู่

3. ผู้ให้บริการที่มีการใช้งานเว็บแอปพลิเคชันประเภท CGI สามารถตรวจสอบปัญหาช่องโหว่ดังกล่าว ผ่านบริการของไทยเซิร์ตจัดเตรียมไว้ https://al2014ad005.thaicert.or.th ดังรูปที่ 3



รูปที่ 3 หน้าจอแสดงบริการตรวจสอบช่องโหว่ที่ไทยเซิร์ตจัดเตรียมไว้

ข้อแนะนำในการป้องกันและแก้ไข

1. อัปเดตซอฟต์แวร์ Bash ให้เป็นเวอร์ชันที่ได้รับการแก้ไขปัญหาช่องโหว่แล้ว

1.1 เพื่อแก้ไขปัญหาช่องโหว่ตาม CVE-2014-6271 ผู้ใช้สามารถอัปเดต Patch สำหรับซอฟต์แวร์

Bash ในเวอร์ชันต่างๆดังต่อไปนี้ **[16]**

- Bash 4.3 Patch 25 **[17]**
- Bash 4.2 Patch 48 **[18]**
- Bash 4.1 Patch 12 **[19]**
- Bash 4.0 Patch 39 **[20]**
- Bash 3.2 Patch 52 **[21]**
- Bash 3.1 Patch 18 **[22]**
- Bash 3.0 Patch 17 **[23]**

1.2 เพื่อแก้ไขช่องโหว่ตาม CVE-2014-7169 ผู้ที่ใช้ Debian และ Ubuntu สามารถอัปเดต Bash เป็นเวอร์ชันล่าสุดด้วยคำสั่ง apt-get update แต่ในกรณีของการใช้งานระบบปฏิบัติการอื่น ๆ ผู้ใช้งานควรตรวจสอบจากเว็บไซต์ทางการอีกครั้งและหากพบว่ามีการเผยแพร่ Patch ใด ๆ เพิ่มเติม ทางไทยเซิร์ตจะแจ้งข้อมูลให้ทราบต่อไป

2. พิจารณาเปลี่ยนไปใช้งาน Shell อื่นทดแทนก่อน จนกว่าจะมีการอัปเดต Patch สมบูรณ์ แต่อย่างไรก็ตามควรมีการพิจารณาผลกระทบกรณีอื่นที่อาจส่งผลจากการเปลี่ยนแปลง

3. พิจารณายกเลิกการใช้งานบริการหรือส่วนประกอบที่อาจได้รับผลกระทบและยังไม่สามารถดำเนินการ Patch ได้ ณ ขณะนี้ เพื่อลดความเสี่ยงจากการถูกโจมตีและเข้าควบคุมระบบ

อ้างอิง

1. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00281.html
2. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00280.html
3. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00279.html
4. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00278.html
5. https://blogs.akamai.com/2014/09/environment-bashing.html
6. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
7. https://twitter.com/taviso/status/514887394294652929
8. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169
9. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00123.html
10. https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=762760
11. http://www.ubuntu.com/usn/usn-2363-2
12. http://www.imore.com/apple-working-quickly-protect-os-x-against-shellshock-exploit
13. https://www.debian.org/security
14. http://www.ubuntu.com/usn/
15. https://access.redhat.com/security/updates/active/
16. http://ftp.gnu.org/gnu/bash/
17. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00081.html
18. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00082.html
19. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00083.html
20. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00084.html
21. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00085.html
22. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00087.html
23. http://lists.gnu.org/archive/html/bug-bash/2014-09/msg00086.html

ระวังภัย ช่องโหว่โพรโทคอล
SSL เวอร์ชัน 3 ผู้ไม่หวังดีสามารถถอดรหัสลับข้อมูลที่รับส่งกับเซิร์ฟเวอร์ได้ (Poodle, CVE-2014-3566)

วันที่ประกาศ : 18 ตุลาคม 2557
ปรับปรุงล่าสุด : 18 ตุลาคม 2557
เรื่อง : ระวังภัย ช่องโหว่โพรโทคอล SSL เวอร์ชัน 3 ผู้ไม่หวังดีสามารถถอดรหัสลับข้อมูลที่รับส่งกับเซิร์ฟเวอร์ได้ (Poodle, CVE-2014-3566)
ประเภทภัยคุกคาม : Other

ข้อมูลทั่วไป

SSL เป็นโพรโทคอลสำหรับใช้เข้ารหัสลับข้อมูลที่รับส่งกันระหว่างเครื่องผู้ใช้งานกับเครื่องให้บริการ เช่น การใช้งานเว็บไซต์ผ่าน HTTPS การใช้งานดาวน์โหลดไฟล์ผ่าน FTPS เป็นต้น โดยการใช้งานโพรโทคอลดังกล่าวจะต้องมีการยอมรับการเชื่อมต่อทั้งส่วนของโปรแกรมในฝั่งผู้ใช้งาน และระบบที่ฝั่งเครื่องให้บริการ ซึ่งโพรโทคอล SSL พัฒนาขึ้นครั้งแรกโดยบริษัท Netscape อดีตผู้พัฒนาเว็บเบราว์เซอร์ชื่อดัง โพรโทคอล SSL เวอร์ชัน 1.0 นั้นไม่เคยได้รับการเผยแพร่ให้ใช้งานจริง โพรโทคอล SSL เวอร์ชัน 2.0 ออกมาในปี 1995 แต่หลังจากที่เผยแพร่ออกมาก็ค้นพบว่ามีช่องโหว่อยู่มากมาย จึงปรับปรุงใหม่เป็น SSL เวอร์ชัน 3.0 ที่ออกมาในปี 1996

ต่อมา ทางบริษัท Netscape ได้ส่งโพรโทคอล SSL เวอร์ชัน 3.0 เข้าไปยังหน่วยงาน IETF เพื่อขอรับรองมาตรฐาน โดยได้พัฒนาออกมาเป็นโพรโทคอล TLS เวอร์ชัน 1.0 เผยแพร่ในปี 1999 ซึ่งในทางเทคนิคแล้วก็เป็นโพรโทคอล SSL เวอร์ชัน 3.0 ที่ปรับปรุงและเปลี่ยนชื่อใหม่ **[1]** ปัจจุบันโพรโทคอล TLS พัฒนามาถึงเวอร์ชัน 1.3 โดยมีการประกาศร่างเอกสารส่งให้ IETF ในช่วงเมษายนปี 2557 ที่ผ่านมา

เมื่อวันที่ 14 ตุลาคม 2557 นักวิจัยของ Google ประกาศพบช่องโหว่ในโพรโทคอล SSL เวอร์ชัน 3.0 ซึ่งช่องโหว่ดังกล่าวนี้ส่งผลให้ผู้ไม่หวังดีสามารถถอดรหัสลับข้อมูลที่รับส่งเพื่ออ่านเนื้อหาของข้อมูลได้ **[2]** ทาง Google เรียกชื่อช่องโหว่นี้ว่า POODLE (Padding Oracle On Downgraded Legacy Encryption) หมายเลขช่องโหว่ CVE-2014-3566

ถึงแม้ว่าโพรโทคอล SSL เวอร์ชัน 3.0 จะเป็นโพรโทคอลเก่าตั้งแต่เกือบ 20 ปีที่แล้ว แต่ก็ยังพบว่ามีเครื่องให้บริการหลายส่วน รวมถึงโปรแกรมเบราว์เซอร์เวอร์ชันเก่า หรือแอปพลิเคชันบางตัวที่ยังคงอนุญาตให้ใช้การเชื่อมต่อผ่านโพรโทคอล SSL เวอร์ชัน 3.0 อยู่ ซึ่งก็อาจส่งผลให้ข้อมูลของผู้ใช้งานที่มีการรับส่งกับเซิร์ฟเวอร์ ตกอยู่ในความเสี่ยงได้

ผลกระทบ

ข้อมูลที่รับส่งระหว่างเครื่องผู้ใช้งานกับเครื่องให้บริการที่ยังใช้งานโพรโทคอล SSL เวอร์ชัน 3.0 สามารถถูกผู้ไม่หวังดีดักรับและเปิดอ่านข้อมูลในลักษณะของข้อความที่ไม่ได้เข้ารหัสลับได้ ส่งผลให้ข้อมูลสำคัญ เช่น ข้อมูลการล็อกอิน ข้อมูลการใช้งาน ถูกขโมยออกไปได้ **[3]**

ระบบที่ได้รับผลกระทบ

เซิร์ฟเวอร์ให้บริการหลายส่วน รวมไปถึงโปรแกรมเบราว์เซอร์เวอร์ชันเก่า หรือแอปพลิเคชันบางตัวที่ยังคงอนุญาตแอปพลิเคชัน หรือเซิร์ฟเวอร์ที่ยังคงใช้การรับส่งข้อมูลผ่านโพรโทคอล SSL เวอร์ชัน 3.0 เช่น Internet Explorer เวอร์ชัน 6

ข้อแนะนำในการป้องกันและแก้ไข

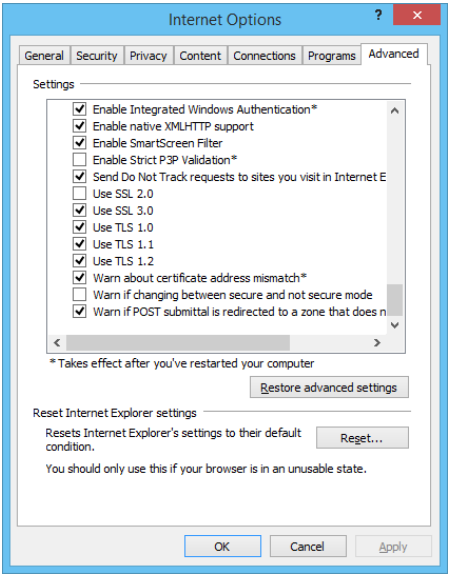
ปัจจุบันพบว่า โปรแกรมที่พัฒนาขึ้นมักจะให้ใช้งานโพรโทคอลสำหรับการเข้ารหัสลับข้อมูลในสมัยใหม่รองรับการเชื่อมต่อผ่านโพรโทคอล TLS/SSL ตั้งแต่เวอร์ชันล่าสุด (TLS 1.2) ลงไปจนถึงเวอร์ชันเก่าสุด (SSL 2.0) เช่น การใช้งาน HTTPS ซึ่งมีการเรียกใช้งานผ่านเว็บเบราว์เซอร์ โดยตัวเบราว์เซอร์จะส่งคำร้องขอเชื่อมต่อด้วยโพรโทคอลเวอร์ชันล่าสุดไปให้ทางเซิร์ฟเวอร์ก่อนเสมอ ถ้าหากเซิร์ฟเวอร์ไม่รองรับถึงจะปรับลดการเชื่อมต่อมายังเวอร์ชันของโพรโทคอลที่ต่ำกว่า ซึ่งในกรณีนี้ ผู้ใช้งานอาจถูกผู้ไม่หวังดีดักรับข้อมูลระหว่างทาง และทำการหลอกให้เชื่อมต่อกับเซิร์ฟเวอร์ผ่านโพรโทคอล SSL เวอร์ชัน 3.0 แทนที่จะเป็นโพรโทคอลเวอร์ชันใหม่ที่มั่นคงปลอดภัยกว่าได้

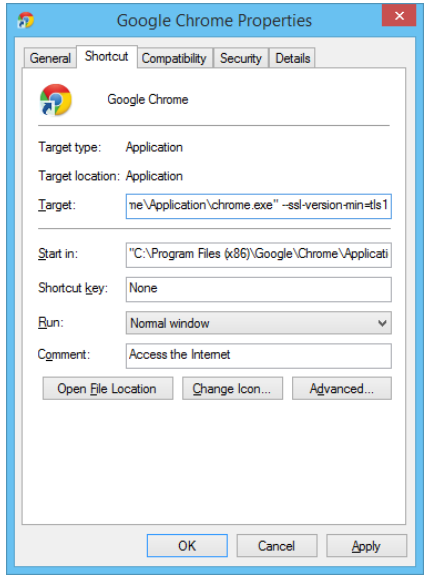
การแก้ไขปัญหา สามารถทำได้โดยการปิดการทำงานของ SSL เวอร์ชัน 3.0 ซึ่งสามารถทำได้ทั้ง 2 ส่วนคือทั้งผู้ใช้งาน (User) และผู้ดูแลระบบ (Administrator) โดยวิธีการตั้งค่าของแต่ละโปรแกรมหรือระบบที่ใช้งานนั้นมีความแตกต่างกันออกไป แต่จะขอยกตัวอย่างการปิดการทำงานของ SSL เวอร์ชัน 3.0 ในส่วนของผู้ใช้งานที่มีการใช้งาน HTTPS ผ่านโปรแกรมเบราว์เซอร์ต่าง ๆ ดังนี้

ปรับการตั้งค่าของเบราว์เซอร์ให้ยกเลิกการใช้งาน SSL เวอร์ชัน 3.0

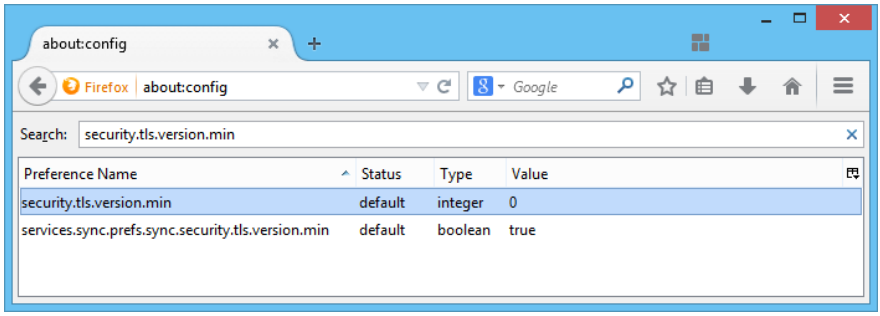
• Internet Explorer 6 รองรับการเชื่อมต่อผ่านโพรโทคอล TLS 1.0 แต่ถูกปิดการใช้งานไว้ ผู้ใช้สามารถเปิดใช้งาน TLS 1.0 และปิด SSL 2.0/SSL 3.0 ได้จากหน้าต่าง Internet Options แต่เนื่องจากว่า Internet Explorer 6 นั้นหยุดพัฒนาแล้ว และโพรโทคอล TLS 1.0 ที่มีให้ใช้งานนั้นก็มีช่องโหว่ ผู้ใช้งานที่ยังใช้ Internet Explorer 6 จึงควรอัปเดตเบราว์เซอร์ให้เป็นเวอร์ชันใหม่โดยเร็วที่สุด

• ผู้ใช้งาน Internet Explorer ทุกเวอร์ชัน สามารถปิดไม่ให้มีการใช้งาน SSL เวอร์ชัน 3.0 ได้ด้วยการเข้าไปที่ Control Panel เลือก Internet Options คลิกที่แท็บ Advanced ตรงช่อง Settings เอาเครื่องหมายถูกออกจากช่อง Use SSL 3.0

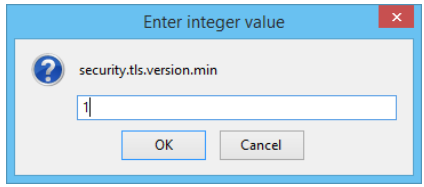




• Google Chrome เวอร์ชันล่าสุด ทาง Google ได้มีการอัปเดตเพื่อลดผลกระทบจากปัญหาช่องโหว่ SSL เวอร์ชัน 3.0 แล้ว แต่ยังมีการเปิดใช้งานโพรโทคอลนี้อยู่ หากผู้ใช้ต้องการปิดการทำงานของโพรโทคอล SSL เวอร์ชัน 3.0 สามารถทำได้โดยการคลิกขวาที่ไอคอนของ Google Chrome เลือก Properties คลิกที่แท็บ Shortcut ในช่อง Target เพิ่มข้อความ --ssl-version-min=tls1 จากนั้นกด OK แล้วเปิด Google Chrome ขึ้นมาใหม่ จะเป็นการเปิดใช้งานโดยไม่อนุญาตให้มีการเชื่อมต่อผ่านโพรโทคอล SSL 3.0



• Mozilla Firefox พิมพ์ในช่อง Address Bar ว่า about:config ในช่อง Search พิมพ์คำว่า security.tls.version.min จากนั้นดับเบิลคลิกค่าในช่อง Value เพื่อเปลี่ยนค่าจาก 0 ให้เป็น 1



• กดปุ่ม OK จากนั้นปิด Firefox แล้วเปิดใหม่

• หรือหากไม่ต้องการเข้าไปตั้งค่าเอง สามารถติดตั้ง Extension ชื่อ SSL Version Control **[4]** เพื่อบังคับไม่ให้มีการเชื่อมต่อโพรโทคอล SSL เวอร์ชัน 3.0

• สำหรับ Safari ใน Mac OS X 10.10 Yosemite, Mac OS X 10.9 Mavericks และ Mac OS X 10.8 Mountain Lion ผู้ใช้งานสามารถติดตั้ง Security Update 2014-005 เพื่อแก้ปัญหาดังกล่าวได้ **[5] [6]**

อ้างอิง

1. http://en.wikipedia.org/wiki/Transport_Layer_Security
2. https://www.openssl.org/~bodo/ssl-poodle.pdf
3. https://www.imperialviolet.org/2014/10/14/poodle.html
4. https://addons.mozilla.org/en-US/firefox/addon/ssl-version-control/
5. https://support.apple.com/kb/HT6531
6. https://zmap.io/sslv3/browsers.html

ระวังภัย ช่องโหว่ใน Drupal
ผู้ไม่หวังดีสามารถขโมยข้อมูลในฐานข้อมูลได้

วันที่ประกาศ : 1 ธันวาคม 2557
ปรับปรุงล่าสุด : 1 ธันวาคม 2557
เรื่อง : ระวังภัย ช่องโหว่ใน Drupal ผู้ไม่หวังดีสามารถขโมยข้อมูลในฐานข้อมูลได้
ประเภทภัยคุกคาม : Intrusion

ข้อมูลทั่วไป

เมื่อวันที่ 15 ตุลาคม 2557 ทางเว็บไซต์ผู้พัฒนาซอฟต์แวร์ Drupal ได้ประกาศว่าพบช่องโหว่ประเภท SQL Injection ในซอฟต์แวร์ Drupal ซึ่งเป็นซอฟต์แวร์บริหารจัดการเนื้อหาบนเว็บไซต์ (CMS) โดยช่องโหว่ดังกล่าวมีการพบใน Database Abstraction API ซึ่งเป็นส่วนประกอบหลักที่ใช้ในการเชื่อมต่อกับฐานข้อมูล (Database) เพื่ออ่านหรือแก้ไขข้อมูล **[1]**

ผลกระทบ

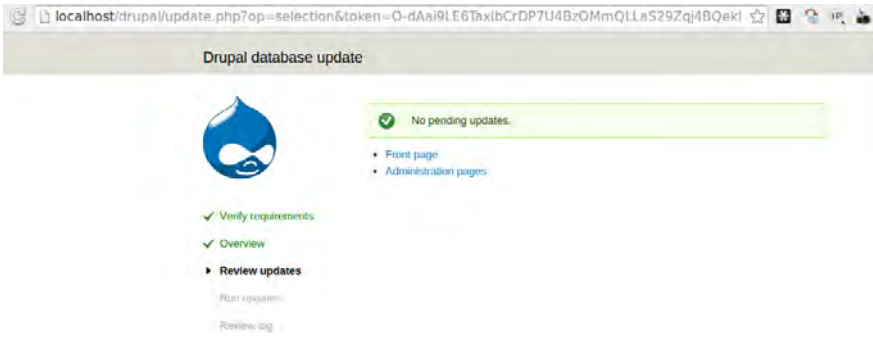
ผู้ไม่หวังดีสามารถโจมตีเว็บไซต์ที่มีช่องโหว่ดังกล่าว ในลักษณะอ่านหรือแก้ไขฐานข้อมูลที่เชื่อมต่อกับเว็บไซต์ได้

ระบบที่ได้รับผลกระทบ

Drupal เวอร์ชัน 7.x ที่เก่ากว่า 7.32

ข้อแนะนำในการป้องกันและแก้ไข

ผู้ดูแลเว็บไซต์ที่ใช้ซอฟต์แวร์ Drupal สามารถตรวจสอบและอัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขช่องโหว่ด้วย update.PHP ใน Directory ที่ติดตั้ง Drupal ดังรูปที่ 1 **[2]**



รูปที่ 1 การอัปเดตซอฟต์แวร์ด้วย update.PHP

หากไม่สามารถอัปเดตเวอร์ชันซอฟต์แวร์ให้เป็นเวอร์ชันที่แก้ไขแล้วดังกล่าวได้ ผู้ดูแลระบบที่ใช้ซอฟต์แวร์ Drupal สามารถติดตั้งแพตช์ (Patch) เพื่อปิดช่องโหว่ในไฟล์ที่ชื่อ database.INC **[1]** โดยการดาวน์โหลดแพตช์จาก https://www.drupal.org/files/issues/SA-CORE-2014-005-D7.patch มายัง Directory ที่ติดตั้ง Drupal จากนั้นให้ติดตั้งแพตช์ด้วยคำสั่ง patch -p1 < SA-CORE-2014-005.patch **[3]** ทั้งนี้ผู้ดูแลเว็บไซต์ควรทำการสำรองข้อมูลก่อนที่จะทำการอัปเดตซอฟต์แวร์หรือติดตั้งแพตช์

อ้างอิง

1. https://www.drupal.org/SA-CORE-2014-005
2. http://www.dummies.com/how-to/content/running-drupal-updatephp.html
3. https://www.drupal.org/patch/apply

บทความทั่วไป

ข้อแนะนำสำหรับผู้ที่ยังใช้งาน Windows XP หลังวันที่ 8 เมษายน 2557

ผู้เขียน : เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่ : 6 กุมภาพันธ์ 2557
ปรับปรุงล่าสุด : 6 กุมภาพันธ์ 2557

ใน Windows ทุกเวอร์ชันที่ Microsoft วางจำหน่าย ต่างมีระยะเวลาการสนับสนุนทางเทคนิค เริ่มตั้งแต่วันแรกที่ผลิตภัณฑ์ออกวางจำหน่าย และสิ้นสุดลงหลังจากที่ผลิตภัณฑ์นั้นหยุดวางจำหน่ายในระยะเวลาหนึ่ง

Windows XP เริ่มวางจำหน่ายครั้งแรกเมื่อวันที่ 25 ตุลาคม 2544 และได้หยุดวางจำหน่ายไปตั้งแต่วันที่ 30 มิถุนายน 2551 ถึงแม้ตัวผลิตภัณฑ์หยุดวางจำหน่ายไปนานหลายปีแล้ว แต่ทาง Microsoft เองก็ยังออกแพตช์แก้ไขช่องโหว่ออกมาอยู่เรื่อย ๆ จนในที่สุดทาง Microsoft ก็ตัดสินใจประกาศว่าจะสิ้นสุดระยะเวลาการสนับสนุนทางเทคนิคให้กับ Windows XP ลงในวันที่ 8 เมษายน 2557 **[1]**

การสิ้นสุดระยะเวลาสนับสนุนทางเทคนิคนั้นหมายความว่าจะไม่มีการออกแพตช์แก้ไขข้อผิดพลาด หรือแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยอีกต่อไป รวมถึงไม่มีบริการให้คำปรึกษาแบบออนไลน์ด้วย ดังนั้นหลังจากวันที่ 8 เมษายน 2557 หากมีผู้ค้นพบช่องโหว่ที่สามารถใช้โจมตี Windows XP ได้ ช่องโหว่นั้นก็จะไม่ได้รับการแก้ไข และจะคงอยู่ไปตลอดกาล

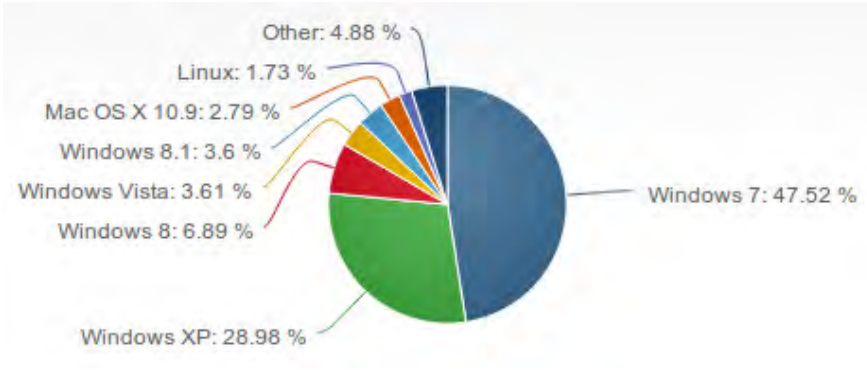
ความเสี่ยงที่จะเกิดขึ้นหลังสิ้นสุดระยะเวลาการสนับสนุน

ทาง Microsoft เองก็รับรู้ถึงปัญหา และได้ออกมาแจ้งเตือนความเสี่ยงที่จะเกิดขึ้นกับผู้ที่ยังคงใช้งาน Windows XP ต่อหลังจากวันที่สิ้นสุดระยะเวลาการสนับสนุน โดยหนึ่งในปัญหาที่อาจจะเกิดขึ้นคือการโจมตีระบบที่ใช้งาน Windows XP ผ่านช่องโหว่ที่ยังไม่มีการแก้ไข (0-day)

โดยปกติ Microsoft จะออกแพตช์ Security Update เป็นประจำทุกเดือน เพื่อแก้ไขปัญหาช่องโหว่ด้านความมั่นคงปลอดภัยของระบบปฏิบัติการและซอฟต์แวร์อื่น ๆ ซึ่งมีหลายครั้งที่พบว่าเป็นช่องโหว่ที่มีผลกับระบบปฏิบัติการตั้งแต่ Windows XP ขึ้นมาจนถึง Windows เวอร์ชันล่าสุด พอทาง Microsoft ออกแพตช์แก้ไขช่องโหว่ก็จะออกให้กับระบบปฏิบัติการทุกตัวที่ได้รับผลกระทบ

ปัญหาก็คือ หากมีการค้นพบช่องโหว่ใน Windows เวอร์ชันอื่น และทาง Microsoft ออกแพตช์มาแก้ กลุ่มแฮกเกอร์สามารถนำแพตช์นั้น ๆ มาทำ Reverse Engineer เพื่อศึกษาช่องโหว่ของระบบที่แพตช์นั้นใช้แก้ไข และหากพบว่าช่องโหว่นั้นเกิดกับส่วนประกอบที่มีใน Windows XP ด้วย แฮกเกอร์ก็สามารถใช้ข้อมูลนี้ในการสร้างเครื่องมือโจมตี Windows XP ได้ **[2]**

หากดูข้อมูลจากเว็บไซต์ NetMarketShare **[3]** ซึ่งรวบรวมสถิติผู้ใช้งานอินเทอร์เน็ตจากทั่วโลก พบว่าในเดือนธันวาคม 2556 มีผู้ที่ยังใช้งาน Windows XP อยู่มากถึง 28.98% ดังรูปที่ 1



รูปที่ 1 สถิติระบบปฏิบัติการที่มีผู้ใช้งานในเดือนธันวาคม 2556
(ที่มา: NetMarketShare [3])

หากมีคนพัฒนาโปรแกรมที่โจมตีระบบปฏิบัติการ Windows XP ผ่านช่องโหว่ของเว็บเบราว์เซอร์ แล้วโพสต์คำสั่งสำหรับโจมตีลงในเว็บไซต์ที่มีผู้ใช้งานอยู่เป็นประจำวันละ 100 คน เราก็น่าจะพอประมาณความเสียหายคร่าว ๆ ได้ว่าอย่างน้อยก็มีคนเกือบ 30 คน ตกเป็นเหยื่อของการโจมตีครั้งนี้

ตัวอย่างที่ยกมาอาจจะยังเห็นภาพไม่ชัดเจนนัก แต่หากลองคิดว่าถ้าเกิดเป็นการโจมตีเว็บไซต์ข่าวที่ไหนซักแห่ง ที่มีคนเข้ามาอ่านวันละประมาณหลักหมื่นหลักแสนคน แล้วฝังมัลแวร์ที่ใช้ขโมยเงินลงในเครื่องของผู้ใช้ (เหมือนอย่างเหตุการณ์ที่เคยเกิดขึ้นมาแล้วก่อนหน้านี้ **[4]**) ความเสียหายที่เกิดขึ้นก็จะมากจนน่ากลัว

ข้อมูลสำคัญที่เป็นความลับ อาจไม่ใช่แค่ข้อมูล Username/Password สำหรับเข้าใช้งานเว็บไซต์ หรือข้อมูลการทำธุรกรรมออนไลน์เสมอไป ทุกวันนี้คนจำนวนมากใช้สมาร์ตโฟน/แท็บเล็ต และเชื่อมต่ออุปกรณ์ดังกล่าวเข้ากับเครื่องคอมพิวเตอร์เพื่อโอนถ่ายหรือสำรองข้อมูล ซึ่งอาจมีการเก็บภาพส่วนตัว หรือ SMS ที่เป็นความลับสำรองไว้ในเครื่องด้วย หากมีมัลแวร์ที่สามารถขโมยข้อมูลออกจากเครื่องได้ พวกภาพลับ คลิปลับ หรือข้อมูลอื่น ๆ ที่เป็นความลับก็อาจหลุดออกไปสู่สาธารณะได้

ข้อแนะนำสำหรับผู้ที่ยังต้องการใช้งาน Windows XP ต่อ

วิธีที่ง่ายที่สุดที่จะลดความเสี่ยงจากปัญหาที่จะเกิดขึ้นหลัง Windows XP หมดระยะเวลาการสนับสนุน คือการอัปเกรดไปใช้ Windows เวอร์ชันที่ใหม่กว่า เพราะใน Windows เวอร์ชันใหม่ ๆ ทาง Microsoft ได้มีการพัฒนาความสามารถด้านความมั่นคงปลอดภัยเพิ่มขึ้น จึงทำให้ระบบโดยรวมมีความมั่นคงปลอดภัยมากกว่า Windows XP โดยทาง

Microsoft ได้บอกว่า Windows 8 นั้นมั่นคงปลอดภัยกว่า Windows XP ถึง 21 เท่า และมั่นคงปลอดภัยกว่า Windows 7 ถึง 6 เท่า **[5]**

หากว่าสเปคเครื่องที่ใช้อยู่ สามารถอัปเกรดเป็น Windows เวอร์ชันใหม่ได้ และความจำเป็นที่จะต้องใช้ Windows XP มีเพียงแค่ต้องการรันซอฟต์แวร์เวอร์ชันเก่าที่รองรับเฉพาะ Windows XP ก็สามารถอัปเกรดมาใช้ระบบปฏิบัติการเวอร์ชันใหม่ได้ แล้วใช้งาน Windows XP Mode หรือติดตั้ง Windows XP ใน Virtual Machine เพื่อเรียกใช้โปรแกรมที่ต้องการ Windows XP โดยเฉพาะ

ใช้งาน Windows XP Mode บน Windows 7

Windows 7 มีฟีเจอร์หนึ่งที่ชื่อ Windows XP Mode ซึ่งเป็นการนำ Windows XP มารันผ่านโปรแกรม Microsoft Virtual PC โดยมีความสามารถพิเศษคือสามารถแยกเฉพาะหน้าต่างของตัวโปรแกรมที่อยู่ใน Virtual PC มาแสดงผลบนหน้าจอ เสมือนว่าเป็นการรันแอปพลิเคชันบนระบบปฏิบัติการปกติ **[6]** ดังรูปที่ 2

รูปที่ 2 ตัวอย่างการรันโปรแกรมของ Windows XP บน Windows 7 โดยใช้ Windows XP Mode (ที่มา: Microsoft [6])

เนื่องจากการทำงานของ Windows XP Mode เป็นการทำงานผ่าน Virtual Machine ซึ่งเป็นการจำลองเครื่องคอมพิวเตอร์ขึ้นมาเพื่อเรียกใช้งานระบบปฏิบัติการอีกทีหนึ่ง จึงทำให้สามารถใช้งานฟังก์ชันต่าง ๆ ของ Windows XP รวมถึงติดตั้งโปรแกรมที่รองรับเฉพาะ Windows XP ลงใน Windows XP Mode ได้

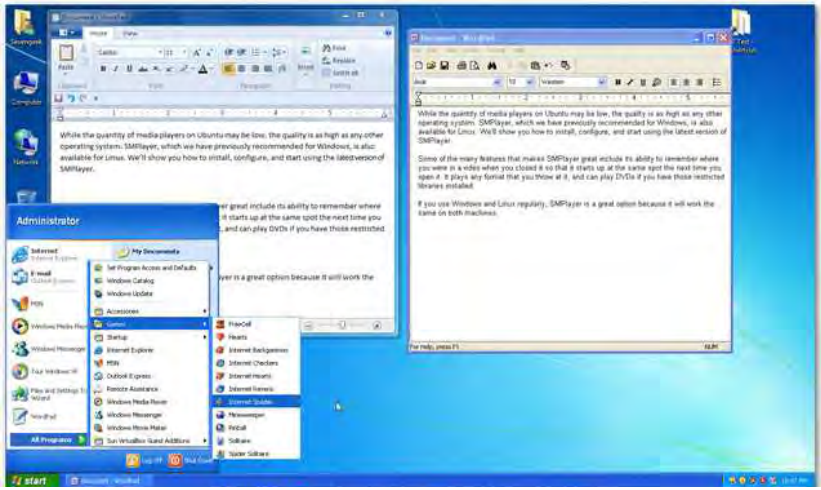
Windows XP Mode สามารถดาวน์โหลดมาใช้งานได้ฟรีจากเว็บไซต์ของ Microsoft **[7]** อย่างไรก็ตาม Windows XP Mode สามารถทำงานได้เฉพาะบน Windows 7 เวอร์ชัน Professional, Enterprise และ Ultimate เท่านั้น

ถึงแม้ว่า Windows XP Mode จะสิ้นสุดระยะเวลาการสนับสนุนในวันที่ 8 เมษายน 2557 ไปพร้อม ๆ กับ Windows XP ด้วยก็ตาม แต่การใช้งาน Windows XP ผ่าน Virtual PC ที่เป็นระบบจำลอง และใช้งานฟีเจอร์เท่าที่จำเป็นจริง ๆ จะช่วยลดความเสี่ยงได้มากกว่า

ใช้งาน Windows XP ผ่าน Virtual Machine

เนื่องจาก Windows 8 ไม่มี License ของ Windows XP ติดมาด้วย จึงไม่สามารถใช้งาน Windows XP Mode ได้เหมือนกับ Windows 7 แต่ก็ยังสามารถใช้วิธีการติดตั้ง Windows XP ลงในซอฟต์แวร์ Virtual Machine แล้วเรียกใช้งานโปรแกรมที่จำเป็นจาก Virtual Machine แทนได้

โปรแกรม Virtual Machine อย่าง VMWare หรือ VirtualBox ก็มีฟีเจอร์ที่สามารถทำงานได้เหมือนกับ Windows XP Mode โดยของ VirtualBox นั้นชื่อว่า Seamless Mode ส่วนของ VMWare ชื่อว่า Unity Mode **[8]** ซึ่งในการใช้งานฟีเจอร์เหล่านี้ หลังจากที่ติดตั้ง Windows XP ลงใน Virtual Machine เรียบร้อยแล้ว ต้องติดตั้ง Guest Addition หรือ VMWare Tools ลงใน Windows XP ที่อยู่ใน Virtual Machine ด้วย **[9]** ตัวอย่างการรัน Windows XP ผ่าน Seamless Mode ของ Virtual Box เป็นดังรูปที่ 3



รูปที่ 3 ตัวอย่างการรัน Windows XP ผ่าน Seamless Mode ของ Virtual Box
(ที่มา: How To Geek [9])

แต่หากการอัปเกรดไปใช้ Windows เวอร์ชันใหม่ หรือเปลี่ยนไปใช้ระบบปฏิบัติการอื่นอย่าง Linux หรือ Mac OS X นั้นไม่สามารถทำได้ และยังยืนยันว่าต้องใช้ Windows XP ต่อจริง ๆ ก็ยังพอมีทางที่จะช่วยให้ผู้ใช้ Windows XP พอเอาตัวรอดจากการตกเป็นเป้าโจมตีของผู้ไม่หวังดีได้ แต่อย่างไรก็ตาม วิธีที่จะแนะนำต่อไปนี้ก็เป็นเพียงแค่การลดผลกระทบจากความเสียหาย (Mitigation) ไม่ใช่วิธีการแก้ปัญหา เพราะปัญหาจริง ๆ นั้นจะยังคงอยู่และจะไม่ได้รับการแก้ไขแต่อย่างใด

เปลี่ยนไปใช้เบราว์เซอร์อื่นที่ไม่ใช่ Internet Explorer

Microsoft เลิกพัฒนา Internet Explorer ให้กับ Windows XP แล้ว โดย Internet Explorer เวอร์ชันใหม่สุดที่สามารถติดตั้งลงใน Windows XP ได้คือ Internet Explorer 8 **[10]** ที่ออกมาตั้งแต่วันที่ 22 กุมภาพันธ์ 2554 หรือเกือบ 3 ปีที่แล้ว (ปัจจุบัน Internet Explorer เวอร์ชันล่าสุดคือเวอร์ชัน 11)

ใน Internet Explorer เวอร์ชันหลัง ๆ ทาง Microsoft ได้มีการพัฒนาความสามารถด้านความมั่นคงปลอดภัยเพิ่มขึ้น เช่น การจัดการ ActiveX Control การปกป้องความเป็นส่วนตัวของผู้ใช้ การตรวจสอบและแจ้งเตือนเว็บไซต์หลอกลวง (Phishing) การจัดการ Add-on เป็นต้น ซึ่งฟีเจอร์ต่าง ๆ เหล่านี้ช่วยให้ผู้ที่ใช้ Internet Explorer เวอร์ชันใหม่ ๆ มีความมั่นคงปลอดภัยมากกว่าผู้ที่ใช้ Internet Explorer เวอร์ชันเก่า

การที่ยังคงใช้ Internet Explorer 8 ซึ่งเป็นเบราว์เซอร์เวอร์ชันเก่าที่มีอายุกว่า 3 ปี มีโอกาสเสี่ยงสูงที่จะถูกโจมตี ไม่ว่าจะเป็นการโจมตีจาก Phishing **[11]** **[12]** หรือการโจมตีผ่านช่องโหว่ของเบราว์เซอร์ **[13]** ดังนั้นเพื่อความมั่นคงปลอดภัยควรเปลี่ยนมาใช้เบราว์เซอร์ตัวอื่นที่มีความมั่นคงปลอดภัยมากกว่าและมีการอัปเดตอย่างสม่ำเสมอ **[14]** เช่น Mozilla Firefox **[15]** หรือ Google Chrome **[16]** เป็นต้น

เปลี่ยนไปใช้โปรแกรมเล่นไฟล์มัลติมีเดียตัวอื่นที่ไม่ใช่ Windows Media Player

Windows Media Player เป็นโปรแกรมที่ใช้สำหรับเล่นไฟล์มัลติมีเดีย เช่น เพลง หรือ วิดีโอ ซึ่งก็ได้รับความนิยมอยู่ในระดับหนึ่ง แต่ชะตากรรมของ Windows Media Player นั้นยังไม่แน่นอนว่าจะมีการพัฒนาต่อหรือไม่ เพราะหลังจาก Windows Media Player 12 ที่ออกมาตั้งแต่ปี 2552 หลังจากนั้นมาทาง Microsoft ก็ไม่ได้มีการพัฒนาเวอร์ชันใหม่ ๆ ของ Windows Media Player ออกมาอีกเลย มีเพียงการอัปเดตช่องโหว่ให้เท่านั้น

Windows Media Player เวอร์ชันล่าสุดที่สามารถติดตั้งลงใน Windows XP ได้คือเวอร์ชัน 11 **[17]** ซึ่งออกมาตั้งแต่ปี 2549 ปัญหาที่จะเกิดขึ้นหลังจากที่ Windows XP หมดระยะเวลาสนับสนุน คือช่องโหว่ของ Windows Media Player ใน Windows XP จะไม่ได้รับการแก้ไข ซึ่งช่องโหว่บางอย่างเป็นช่องโหว่อันตราย ตัวอย่างช่องโหว่ที่เคยเกิดขึ้นมาก่อนหน้านี้ เช่น ช่องโหว่ CVE-2012-0003 ที่เมื่อผู้ใช้เปิดเว็บไซต์หรือเปิดไฟล์ MIDI ที่มีโค้ดอันตรายฝังอยู่ จะถูกผู้ไม่หวังดีติดตั้งโปรแกรมอันตรายลงในเครื่องแล้วเข้ามาควบคุมเครื่องได้ในทันที เป็นต้น **[18]**

ในการใช้งานเพื่อความมั่นคงปลอดภัย ควรหลีกเลี่ยงโปรแกรม Windows Media Player แล้วเปลี่ยนไปใช้งานโปรแกรมเล่นไฟล์มัลติมีเดียตัวอื่นแทน เช่น Media Player Classic **[19]** หรือ VLC **[20]** ซึ่งเป็นโปรแกรม Open Source ที่ได้รับความนิยมและมีการอัปเดตช่องโหว่ด้านความมั่นคงปลอดภัยอยู่เป็นประจำ ตัวอย่างหน้าจอโปรแกรม Media Player Classic เป็นดังรูปที่ 4

รูปที่ 4 ตัวอย่างหน้าจอโปรแกรม Media Player Classic
(ที่มา: MPC-HC [19])

ติดตั้งและใช้งานโปรแกรมแอนติไวรัส

การติดตั้งโปรแกรมแอนติไวรัสและหมั่นอัปเดตฐานข้อมูลอย่างสม่ำเสมอก็สามารถช่วยให้การตรวจจับไวรัส/โทรจัน หรือมัลแวร์อื่น ๆ ได้ถูกต้องแม่นยำขึ้น อีกทั้งโปรแกรมแอนติไวรัสเวอร์ชันใหม่ ๆ หลายตัวก็มีฟีเจอร์ในการตรวจจับแอปพลิเคชันที่ต้องสงสัยว่าน่าจะเป็นมัลแวร์ โดยดูจากพฤติกรรมการทำงานของแอปพลิเคชันนั้น ๆ ซึ่งก็ช่วยให้สามารถตรวจจับมัลแวร์เวอร์ชันใหม่ ๆ ที่ยังไม่ได้มีข้อมูลอยู่ในฐานข้อมูลของโปรแกรมแอนติไวรัสได้

โปรแกรม Microsoft Security Essentials เป็นโปรแกรมแอนติไวรัสที่พัฒนาโดย Microsoft เนื่องจากการหยุดสนับสนุนทางเทคนิคให้กับ Windows XP นั้นรวมถึงการหยุดสนับสนุนเรื่องความมั่นคงปลอดภัยด้วย ทาง Microsoft จึงได้ตัดสินใจที่หยุดสนับสนุนโปรแกรม Microsoft Security Essentials โดยจะถอดลิงก์ของไฟล์ติดตั้งโปรแกรมนี้ออกจากหน้าเว็บไซต์ ตั้งแต่วันที่ 8 เมษายน 2557 เป็นต้นไป แต่จะยังคงออกอัปเดตฐานข้อมูลมัลแวร์ให้ถึงวันที่ 14 กรกฎาคม 2558 **[21]**

ถึงแม้ Microsoft จะไม่พัฒนาความสามารถอะไรเพิ่มเติมให้กับ Microsoft Security Essentials แล้ว แต่ผู้ผลิตโปรแกรมแอนติไวรัสหลายเจ้าก็ยังยืนยันที่จะพัฒนาโปรแกรมให้รองรับ Windows XP และอัปเดตฐานข้อมูลการตรวจจับมัลแวร์ต่อไปอย่างน้อยอีก 1-2 ปี **[22] [23]** ดังนั้นผู้ใช้ที่ยังใช้งาน Microsoft Security Essentials อยู่ หลังจากวันที่ 8 เมษายน 2557 ควรเปลี่ยนไปใช้แอนติไวรัสตัวอื่นเพื่อความมั่นคงปลอดภัย

ติดตั้งและใช้งานโปรแกรม Firewall

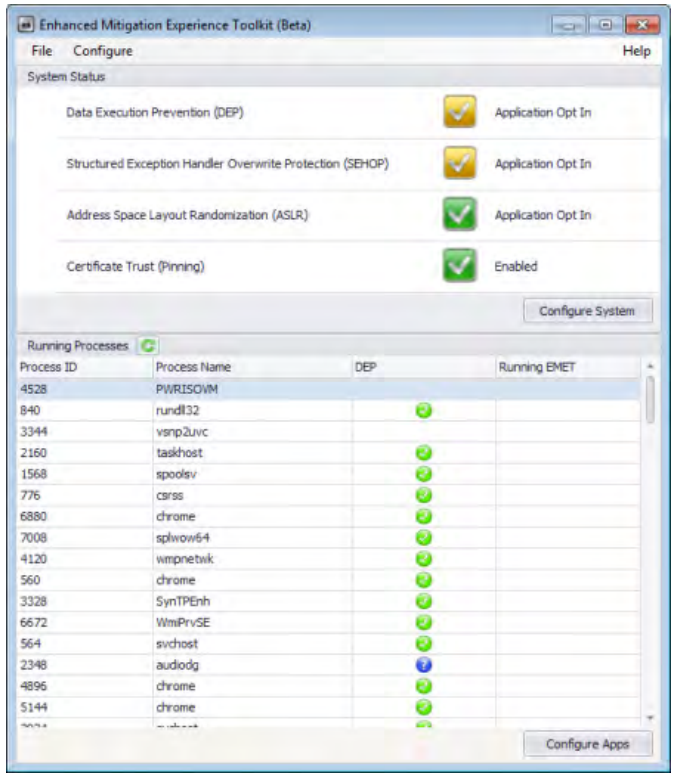
ถึงแม้ว่าใน Windows XP เองจะมีโปรแกรม Windows Firewall ติดตั้งมาให้ด้วย (เริ่มมีตั้งแต่สมัย Windows XP Service Pack 2) แต่ความสามารถของโปรแกรมนี้ก็มีจำกัด คือสามารถป้องกันได้แค่การโจมตีจากเครือข่ายภายนอกเข้ามาที่เครื่อง (Inbound) แต่ไม่สามารถตรวจสอบหรือป้องกันการส่งข้อมูลออกไปจากเครื่องได้ (Outbound) **[24]**

เนื่องจากโปรแกรม Firewall ที่มาพร้อมกับ Windows XP นั้นมีความสามารถน้อย และในอนาคตอาจมีช่องโหว่ที่สามารถถูกโจมตีได้และไม่มีวิธีการแก้ไข ดังนั้นเพื่อความมั่นคงปลอดภัยควรปิดการทำงานของโปรแกรม Windows Firewall แล้วเปลี่ยนไปใช้โปรแกรม Firewall ยี่ห้ออื่นที่มีความสามารถและมีความมั่นคงปลอดภัยมากกว่า

โปรแกรมแอนติไวรัสบางยี่ห้อมีเวอร์ชัน Internet Security ซึ่งจะมีโปรแกรม Firewall แถมมาให้ด้วย และอาจมีโปรแกรมประเภท Browser Plugin ที่ช่วยตรวจสอบความมั่นคงปลอดภัยเวลาใช้งานเว็บเบราว์เซอร์ ซึ่งผู้ใช้อาจพิจารณาใช้งานโปรแกรมต่าง ๆ เหล่านี้แทนโปรแกรมที่ติดตั้งมาพร้อมกับระบบ

ใช้งาน EMET เพื่อลดผลกระทบจากความเสี่ยง

EMET เป็นเครื่องมือที่ Microsoft พัฒนาขึ้นมาใช้เพิ่มความมั่นคงปลอดภัยให้กับระบบ โดยสามารถ “บังคับ” แอปพลิเคชันที่พัฒนาโดยผู้พัฒนาภายนอก ให้สามารถใช้ฟีเจอร์ด้านความมั่นคงปลอดภัยใหม่ ๆ ที่อยู่ในระบบปฏิบัติการได้ เพื่อช่วยให้การโจมตีจากผู้ไม่หวังดีสามารถทำได้ยากขึ้นและมีโอกาสสำเร็จน้อยลง หรือหากโจมตีได้สำเร็จก็เกิดความเสียหายน้อยกว่าปกติ ตัวอย่างหน้าจอโปรแกรม EMET เป็นดังรูปที่ 5



รูปที่ 5 ตัวอย่างหน้าจอโปรแกรม EMET

นอกจากนี้ EMET ยังมีระบบความมั่นคงปลอดภัยบางอย่างที่มีการหยิบยกมาจาก Windows เวอร์ชันใหม่ ๆ ให้สามารถทำงานบน Windows XP ได้ด้วย เช่น SEHOP ที่หยิบยกมาจาก Windows Vista Service Pack 1 **[25]** ผู้ใช้งาน Windows XP สามารถดาวน์โหลด EMET มาใช้งานได้ฟรีจากเว็บไซต์ของ Microsoft **[26]** โดยสามารถศึกษาวิธีการใช้งานและข้อมูลเพิ่มเติมได้จากบทความของไทยเซิร์ต **[27] [28]**

รันโปรแกรมผ่าน Sandbox Mode

Sandbox ในโลกความเป็นจริงก็เป็นกล่องทรายที่เราสามารถวาดเขียน หรือก่อกองทรายให้เป็นรูปร่างอะไรก็ได้ พอทำเสร็จก็ลบทิ้งแล้วสร้างใหม่ได้เรื่อย ๆ คำว่า Sandbox ในทาง Computer Security ก็มีลักษณะคล้าย ๆ กัน คือเป็นการแบ่งกั้นพื้นที่เอาไว้เพื่อใช้รันโปรแกรมอะไรสักอย่างนึง ซึ่งสิ่งที่เกิดขึ้นจากการรันโปรแกรมนี้จะไม่ส่งผลกระทบกับระบบจริง และเราสามารถล้างข้อมูลใน Sandbox ได้เรื่อย ๆ เช่นกัน

โดยปกติแล้วการรันโปรแกรมผ่าน Sandbox Mode จะทำผ่านโปรแกรมประเภทจำลองระบบ Sandbox ซึ่งการทำงานหลัก ๆ ของโปรแกรมเหล่านี้ก็จะเป็นการคัดลอก

ไฟล์สำคัญ ๆ ของระบบที่มีการเปลี่ยนแปลง รวมทั้ง Registry ต่าง ๆ ที่ได้รับการแก้ไขเข้ามาเก็บไว้ในสภาพแวดล้อมของ Sandbox และเมื่อมีการรันโปรแกรมในโหมด Sandbox ก็จะเอาข้อมูลที่อยู่ใน Sandbox Mode ไปใช้งานแทน เพื่อไม่ให้เกิดผลกระทบหรือเกิดความเสียหายกับระบบจริง รวมทั้งไฟล์ที่มีการสร้างโดยโปรแกรมที่รันในโหมด Sandbox ก็จะเก็บอยู่ในส่วนที่กั้นไว้เป็น Sandbox ด้วยเช่นกัน

ตัวอย่างโปรแกรมที่สามารถจำลอง Sandbox Mode เพื่อเอาโปรแกรมอื่น ๆ มารันใน Sandbox ได้ เช่น Sandboxie **[29]**, BufferZone **[30]**, ReturNil **[31]** เป็นต้น อย่างไรก็ตาม การรันโปรแกรมใน Sandbox Mode เป็นเพียงการจำกัดการทำงานของโปรแกรมไม่ให้ส่งผลกระทบกับไฟล์หรือการตั้งค่าในระบบจริง แต่อาจไม่สามารถแน่ใจได้ 100% ว่าการทำงานทุกอย่างจะจำกัดอยู่ใน Sandbox ไปทั้งหมด เพราะมีโอกาสที่โปรแกรม Sandbox จะมีช่องโหว่ ทำให้โปรแกรมที่รันอยู่สามารถทะลุ Sandbox Mode ออกมาได้ **[32]**

สรุป

หลังจาก Microsoft หยุดสนับสนุน Windows XP ในวันที่ 8 เมษายน 2557 ทางที่ดีที่สุดในการที่จะใช้งานคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยอยู่คือการอัปเกรดไปใช้ระบบปฏิบัติการ Windows เวอร์ชันใหม่ (หรือเปลี่ยนไปใช้ระบบปฏิบัติการ เช่น Linux หรือ OS X) การที่ยังฝืนใช้งาน Windows XP ต่อไปถึงแม้จะหมดระยะเวลาสนับสนุนแล้ว ก็มีแต่จะเพิ่มความเสี่ยงที่จะทำให้เครื่องคอมพิวเตอร์เกิดปัญหา เช่น ติดมัลแวร์ ถูกควบคุมโดยผู้ไม่หวังดี หรือถูกขโมยข้อมูลสำคัญออกไปจากเครื่องได้

ข้อแนะนำต่าง ๆ ที่อยู่ในบทความนี้ เป็นเพียงแค่การยื้อเวลาเพื่อให้ผู้ใช้สามารถมีเวลาเตรียมการเพื่อที่จะย้ายข้อมูลและงานที่สำคัญ ๆ ที่ผูกติดกับ Windows XP อยู่ ไปทำงานบนระบบปฏิบัติการตัวอื่นที่มั่นคงปลอดภัยกว่า เพราะไม่ว่าอย่างไรก็ตาม ในอีกไม่กี่ปีข้างหน้า ชะตากรรมของ Windows XP เองก็คงจะเหมือนกับ Windows เวอร์ชันเก่าตัวอื่น ๆ เช่น Windows 95/98 ที่ปัจจุบันนี้ไม่มีผู้ผลิตฮาร์ดแวร์ทำไดรเวอร์ออกมารองรับ และไม่มีนักพัฒนาซอฟต์แวร์สนใจทำแอปพลิเคชันให้อีกต่อไป หรือหากเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เป็นเวอร์ชันที่เก่ามากจนไม่สามารถอัปเกรดมาใช้ Windows เวอร์ชันใหม่ได้ อายุขัยของฮาร์ดแวร์ในเครื่องก็มีระยะเวลาจำกัด (เช่น 5-10 ปี) ซึ่งเมื่อเวลานั้นมาถึง ผู้ที่ยังคงใช้งาน Windows XP อยู่ก็คงต้องเปลี่ยนไปใช้งานระบบปฏิบัติการเวอร์ชันที่ใหม่กว่าอยู่ดีนั่นเอง

อ้างอิง

1. http://windows.microsoft.com/en-us/windows/lifecycle
2. http://blogs.technet.com/b/security/archive/2013/08/06/the-risk-of-running-windows-xp-after-support-ends.aspx
3. http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0
4. https://thaicert.or.th/alerts/user/2013/al2013us008.html
5. http://www.itworld.com/consumerization-it/372106/windows-7-has-6-times-more-security-threats-windows-8-according-microsoft
6. http://windows.microsoft.com/th-th/windows7/install-and-use-windows-xp-mode-in-windows-7
7. http://windows.microsoft.com/th-th/windows7/products/features/windows-xp-mode
8. http://www.howtogeek.com/171145/use-virtualboxs-seamless-mode-or-vmwares-unity-mode-to-seamlessly-run-programs-from-a-virtual-machine/
9. http://www.howtogeek.com/howto/12183/how-to-run-xp-mode-in-virtualbox-on-windows-7/
10. http://windows.microsoft.com/en-us/internet-explorer/downloads/ie-8
11. https://thaicert.or.th/papers/general/2012/pa2012ge007.html
12. https://thaicert.or.th/papers/general/2012/pa2012ge011.html
13. https://thaicert.or.th/papers/general/2012/pa2012ge008.html
14. http://www.pcmag.com/article2/0,2817,2365692,00.asp
15. https://www.mozilla.org/en-US/firefox/new/
16. https://www.google.com/intl/th/chrome/
17. http://windows.microsoft.com/th-th/windows/download-windows-media-player
18. http://blog.trendmicro.com/trendlabs-security-intelligence/malware-leveraging-midi-remote-code-execution-vulnerability-found/
19. http://mpc-hc.org/
20. http://www.videolan.org/vlc/
21. http://blogs.technet.com/b/mmpc/archive/2014/01/15/microsoft-antimalware-support-for-windows-xp.aspx
22. http://www.bitdefender.com/news/bitdefender-extends-antimalware-support-for-xp-users-2858.html
23. http://blog.kaspersky.com/xp-is-there-life-after-the-end-of-support/
24. http://www.bleepingcomputer.com/tutorials/how-to-configure-windows-xp-firewall/
25. http://krebsonsecurity.com/2013/06/windows-security-101-emet-4-0/
26. http://support.microsoft.com/kb/2458544
27. https://thaicert.or.th/papers/technical/2012/pa2012te004.html
28. https://thaicert.or.th/papers/technical/2013/pa2013te005.html
29. http://www.sandboxie.com/
30. http://www.trustware.com/
31. http://www.returnilvirtualsystem.com/
https://media.blackhat.com/bh-ad-10/Ridley/BlackHat-AD-2010-Ridley-Escaping-The-Sandbox-slides.pdf

เราเตอร์ที่ใช้ภายในบ้าน กับปัญหาด้านความมั่นคงปลอดภัย

ผู้เขียน : ธงชัย ศิลปวรางกูร
วันที่เผยแพร่ : 31 มีนาคม 2557
ปรับปรุงล่าสุด : 31 มีนาคม 2557

ผู้ที่ติดตามข่าวสารด้านเทคโนโลยีต่าง ๆ อยู่เป็นประจำ อาจสังเกตว่าในช่วงไม่กี่เดือนที่ผ่านมา มีการรายงานข่าวเกี่ยวกับปัญหาด้านความมั่นคงปลอดภัยของเราเตอร์ที่ใช้งานตามบ้านและออฟฟิศขนาดเล็กที่มักเรียกกันว่า SOHO Router อยู่ไม่น้อย ไม่ว่าจะเป็นข่าวการแฮกเราเตอร์ของผู้ใช้งานรูปแบบต่าง ๆ หรือช่องโหว่ของเราเตอร์ที่เปิดโอกาสให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต อันที่จริงข่าวในลักษณะนี้ปรากฏให้เห็นเป็นระยะอยู่แล้ว แต่เนื่องจากในช่วงที่ผ่านมามีข้อมูลที่น่าสนใจอยู่หลายเรื่องและเป็นเรื่องที่มีผลกระทบต่อผู้ใช้งานทั่วไปโดยตรง จึงขอหยิบยกข่าวส่วนหนึ่งที่เกิดขึ้นตั้งแต่ต้นปี เพื่อให้ได้ทราบถึงสถานการณ์ และผลกระทบที่เกิดจากการโจมตีในรูปแบบต่าง ๆ ดังนี้

ในต่างประเทศนั้น มีหน่วยงานหลายแห่งที่ทำการสำรวจ วิเคราะห์ และค้นพบข้อมูลด้านปัญหาความมั่นคงปลอดภัยที่เกี่ยวข้องกับเราเตอร์ที่ใช้งานตามบ้านอยู่หลายเรื่อง เริ่มจากผลการวิเคราะห์ของ Tripwire's Vulnerability and Exposure Research Team ที่พบว่า กว่าร้อยละ 80 ใน 25 อันดับแรกของเราเตอร์ที่ขายดีที่สุดในเว็บไซต์ Amazon มีช่องโหว่ และกว่าร้อยละ 34 ของเราเตอร์ที่มีช่องโหว่นั้น มีเอกสารระบุวิธีการโจมตีช่องโหว่เหล่านั้นเผยแพร่ในอินเทอร์เน็ตอยู่แล้ว เห็นได้ว่า ผู้ใช้ที่มีความเสี่ยงที่จะตกเป็นเหยื่อของผู้ไม่หวังดีโดยไม่รู้ตัวนั้นมีค่อนข้างมาก และจากการสำรวจผู้ที่ทำงานในสายไอทีในเรื่องของหลักการกำหนดค่าด้านความมั่นคงปลอดภัยของเราเตอร์ยังพบอีกว่า มีจำนวนไม่น้อยที่ไม่ได้ปฏิบัติตามหลักดังกล่าว เช่น ไม่ได้เปลี่ยนรหัสผ่านของผู้ดูแลระบบที่เป็นค่าตั้งต้น และไม่ได้อัปเดตเฟิร์มแวร์ให้เป็นเวอร์ชันล่าสุด **[1]**

ถัดมาเป็นเรื่องของช่องโหว่ในเราเตอร์ยี่ห้อ Asus ที่มีการเผยแพร่ออกมานานแล้ว แต่เพิ่งจะเป็นข่าวอีกครั้ง เนื่องจากมีผู้พบไฟล์แปลกปลอมภายในฮาร์ดดิสก์ที่เชื่อมต่อเข้ากับเราเตอร์ผ่านพอร์ต USB ภายในไฟล์มีข้อความแจ้งเตือนว่าข้อมูลภายในฮาร์ดดิสก์ของเขานั้นสามารถเข้าถึงได้จากอินเทอร์เน็ต **[2]** ช่องโหว่ในลักษณะนี้ถึงแม้ว่าอาจจะไม่ได้ส่งผลกระทบต่อคนส่วนใหญ่ เนื่องจากผู้ใช้งานตามบ้านทั่วไปมักไม่ค่อยได้ใช้งานพอร์ต USB บนเราเตอร์ แต่ช่องโหว่ดังกล่าวก็แสดงให้เห็นข้อเท็จจริงที่ว่า ไม่ใช่แค่ตัวเราเตอร์เองเท่านั้นที่อาจมีช่องโหว่ให้สามารถเข้าควบคุมได้ แต่อุปกรณ์เก็บข้อมูลที่เชื่อมต่อเข้ากับเราเตอร์โดยตรงก็มีความเสี่ยงที่จะถูกเข้าถึงจากอินเทอร์เน็ตเช่นกัน ซึ่งแม้กระทั่งผู้ใช้

ที่มีความรู้ความเข้าใจในการตั้งค่าอุปกรณ์เครือข่ายก็อาจไม่ได้คาดคิดว่าจะมีช่องโหว่ในลักษณะนี้เกิดขึ้น

อีกข่าวหนึ่งที่น่าสนใจไม่น้อยไปกว่าเรื่องของช่องโหว่ต่าง ๆ คือเรื่องของงานวิจัยจากสหราชอาณาจักร ที่ทำการทดลองโดยสร้างมัลแวร์ที่ชื่อ Chameleon ซึ่งมีความสามารถในการแพร่กระจายตัวเองไปยัง Access Point เครื่องอื่น ๆ ในละแวกเดียวกันผ่าน WiFi ติดตั้งเฟิร์มแวร์ที่มีมัลแวร์ฝังอยู่ลงใน Access Point ที่ตกเป็นเป้าหมาย และดักรับข้อมูลของผู้ใช้ที่กำลังเชื่อมต่ออุปกรณ์ของตนเองเข้ากับ Access Point นั้น **[3]** ทั้งนี้ในสถานการณ์จริงยังมีปัจจัยอื่นหลายอย่างที่ส่งผลกระทบต่อการทำงานของมัลแวร์ดังกล่าว เช่น จำนวน Access Point ที่อยู่ในบริเวณเดียวกันกับตัวที่ติดมัลแวร์ ระยะห่างระหว่าง Access Point แต่ละเครื่อง และการตั้งค่าด้านความมั่นคงปลอดภัยของตัว Access Point เอง แต่อย่างน้อยการทดลองดังกล่าวก็พิสูจน์ให้เห็นถึงความเป็นไปได้ที่จะเกิดการโจมตีลักษณะนี้ขึ้นในอนาคต

นอกจากนี้ยังมีการค้นพบการโจมตีเราเตอร์ยี่ห้อ Linksys โดยผู้ให้บริการอินเทอร์เน็ตในประเทศสหรัฐอเมริกา ซึ่งนักวิจัยจาก Internet Storm Center ของ SANS ได้ทำการวิเคราะห์เพิ่มเติมแล้วพบว่าการโจมตีดังกล่าวเกิดจากมัลแวร์ตัวหนึ่งที่มีชื่อเรียกเล่นในตอนนี้ว่า TheMoon ซึ่งหากมัลแวร์โจมตีเราเตอร์ได้สำเร็จ ก็จะทำการดาวน์โหลดไฟล์มัลแวร์เพิ่มเติมลงในเราเตอร์ แล้วสแกนหาเราเตอร์ตัวอื่น ภายในเครือข่ายที่ถูกมัลแวร์ระบุเป้าหมายไว้ ซึ่งปัจจุบันถึงยังไม่สามารถสรุปได้ว่าจุดประสงค์ของมัลแวร์ดังกล่าวคืออะไร แต่ก็มีการสันนิษฐานว่าเราเตอร์ที่ถูกโจมตีอาจถูกสั่งการและควบคุมโดยผู้ไม่หวังดีได้ เนื่องจากพบหลักฐานที่น่าสงสัยภายในไฟล์มัลแวร์ดังกล่าว สำหรับเทคนิคที่มัลแวร์ใช้ในการโจมตีสามารถศึกษาได้จากเว็บไซต์ Internet Storm Center **[4][5][6][7]** ส่วนในบทความนี้จะขอกล่าวถึงแต่เพียง**ข้อมูลทั่วไป**เท่านั้น

ในอีกด้านหนึ่ง นักวิจัยจากบริษัท Dr. Web ของรัสเซียได้ตรวจสอบพบโทรจันบนคอมพิวเตอร์ที่ชื่อ Rbrute ซึ่งทำการโจมตีเราเตอร์ด้วยการสุ่มรหัสผ่าน หากโจมตีสำเร็จ โทรจันดังกล่าวจะแก้ไขการตั้งค่า DNS ภายในเราเตอร์ ทำให้แทนที่จะสามารถเข้าชมเว็บไซต์ตามปกติ ผู้ใช้งานจะถูกพาเข้าไปยังเว็บไซต์หลอกลวง เช่น หน้าดาวน์โหลดโปรแกรม Google Chrome ปลอมแทน เพื่อหลอกให้ดาวน์โหลดโปรแกรมซึ่งมีมัลแวร์ชื่อ Sality ฝังอยู่ โดยมัลแวร์ดังกล่าวสามารถดาวน์โหลดโทรจัน Rbrute กลับมาทำงานซ้ำในรูปแบบเดิมได้ เราเตอร์ที่ได้รับผลกระทบจากโทรจันนี้มีหลายยี่ห้อ ไม่ว่าจะเป็น D-Link, TP-LINK และ ZTE สำหรับรายละเอียดต่าง ๆ รวมถึงเวอร์ชันของเราเตอร์ที่ได้รับผลกระทบสามารถดูได้จากเว็บไซต์ Dr. Web **[8]**

สำหรับในประเทศไทยเอง ข่าวหนึ่งที่ได้รับความสนใจค่อนข้างมากก็คือเรื่องของช่องโหว่ในเราเตอร์ยี่ห้อ TP-LINK ที่ทำให้ไม่ว่าใครก็ตามที่เชื่อมต่ออินเทอร์เน็ตสามารถขโมยรหัสผ่านของเราเตอร์ไปได้ ซึ่งหลังจากที่เกิดข่าวช่องโหว่นี้ขึ้น ไทยเซิร์ตได้เผยแพร่บทความแจ้งเตือนเกี่ยวกับช่องโหว่ดังกล่าว และได้ติดต่อประสานงานไปยังทาง TP-LINK เพื่อแจ้งปัญหาและสอบถามข้อมูลเพิ่มเติมแล้ว **[9]** และในภายหลังยังพบอีกว่ามีเราเตอร์

บางยี่ห้อที่ใช้เฟิร์มแวร์เดียวกันกับของ TP-LINK แล้วพบช่องโหว่ในลักษณะเดียวกัน เช่น ZyXEL และ Billion บางเวอร์ชัน อย่างไรก็ตาม จากการสำรวจของไทยเซิร์ตนับตั้งแต่ที่มีการเผยแพร่ข่าวของช่องโหว่ดังกล่าวตั้งแต่กลางเดือนมกราคม 2557 จนถึงปัจจุบัน กลับพบว่า จำนวนเราเตอร์ที่มีความเสี่ยงที่จะถูกโจมตีโดยช่องโหว่ดังกล่าวลดลงในสัดส่วนที่เล็กน้อยมาก แสดงให้เห็นว่าผู้ใช้ส่วนใหญ่อาจยังไม่ทราบถึงข่าวดังกล่าว ส่วนทาง TP-LINK เองก็ได้ออกประกาศผ่านทางเว็บไซต์เกี่ยวกับช่องโหว่ดังกล่าวแล้วเช่นกัน **[10]** แต่ปัจจุบันยังไม่มีประกาศเกี่ยวกับเฟิร์มแวร์เวอร์ชันใหม่ออกมาแต่อย่างใด

ในส่วนของสถิติจำนวนเราเตอร์ที่ตกเป็นเหยื่อนั้น แม้ว่าจะยังไม่สามารถระบุได้ชัดเจน แต่จากรายงานของ Team Cymru ซึ่งได้วิเคราะห์การโจมตีเราเตอร์ที่ใช้งานตามบ้านตั้งแต่ต้นปี 2557 ด้วยช่องโหว่ต่าง ๆ พบว่า มีเราเตอร์กว่า 3 แสนเครื่องทั่วโลกที่ตกเป็นเหยื่อในการโจมตี โดยประเทศไทยติดอยู่ในอันดับที่ 4 มีจำนวนเราเตอร์ที่ถูกโจมตีในหลักหมื่นเครื่อง **[11]** ทั้งนี้รายงานดังกล่าวแสดงให้เห็นถึงจำนวนผู้ที่ตกเป็นเหยื่อเพียงส่วนหนึ่งเท่านั้น เนื่องจากในโลกนี้ย่อมมีผู้ไม่หวังดีที่จะทำการโจมตีอยู่อีกหลายกลุ่ม และอาจใช้ช่องโหว่ในการโจมตีที่แตกต่างกันออกไป

นอกจากข่าวเกี่ยวกับช่องโหว่และรายงานสถิติต่าง ๆ แล้ว ยังมีผู้ใช้งานในประเทศไทยหลายรายที่เริ่มพบความผิดปกติในการใช้งานอินเทอร์เน็ต ด้วยการที่เราเตอร์ของผู้ใช้ถูกแก้ไขการตั้งค่า DNS ส่งผลให้เมื่อเข้าเว็บไซต์ชื่อดังอย่าง google.com หรือ youtube.com แล้ว แทนที่เว็บเบราว์เซอร์จะแสดงหน้าเว็บของจริง แต่กลับแสดงเป็นหน้าเว็บที่หลอกให้ดาวน์โหลดตัวอัปเดตโปรแกรม Adobe Flash Player ซึ่งอันที่จริงแล้วเป็นมัลแวร์ **[12]** ซึ่งหากผู้ใช้ทั่วไปที่พบความผิดปกติในลักษณะคล้ายคลึงกับแบบนี้ไม่ได้มีความรู้ความเข้าใจในด้านระบบเครือข่ายคอมพิวเตอร์แล้ว ก็แทบจะไม่สามารถหาสาเหตุและแก้ไขปัญหาดังกล่าวด้วยตนเองได้เลย

จากข่าวที่ยกตัวอย่างมาข้างต้นทั้งหมดทำให้เห็นได้ชัดว่า อุปกรณ์เครือข่ายที่ใช้ตามบ้านโดยเฉพาะเราเตอร์ซึ่งย่อมมีในทุกบ้านที่ติดตั้งอินเทอร์เน็ต มีความเสี่ยงสูงที่จะถูกโจมตีจากผู้ไม่หวังดีได้หลากหลายช่องทางและรูปแบบ อย่างไรก็ดี แนวทางการตรวจสอบและป้องกันไม่ให้ตนเองตกเป็นเหยื่อสามารถทำได้ไม่ยาก แต่ต้องทำการป้องกันหลายอย่างควบคู่กันดังนี้

- เนื่องจากจุดเริ่มต้นของการโจมตีส่วนใหญ่ เกิดจากผู้ที่อยู่ภายนอกระบบเครือข่ายของผู้ใช้มีโอกาสที่จะสามารถเข้าถึงเราเตอร์ของผู้ใช้ได้ ดังนั้นสำหรับผู้ใช้ทั่วไปที่ไม่ได้มีความต้องการใช้งานอะไรเป็นพิเศษอยู่แล้ว สิ่งที่ควรทำเป็นอันดับแรกก็คือการตัดโอกาสเหล่านั้น ด้วยการปิดการทำงานของ Remote Management เพื่อป้องกันไม่ให้ผู้อื่นในอินเทอร์เน็ตสามารถเข้าถึงเราเตอร์ของเราได้ วิธีที่สามารถทำได้ในเราเตอร์แทบทุกตัวก็คือการกำหนด Access Control List (ACL) ให้เฉพาะผู้ใช้ภายในเครือข่ายของเราที่สามารถเข้าถึงหน้าล็อกอินของเราเตอร์ได้ โดยแนวทางการตั้งค่าอย่างง่ายก็คืออนุญาตให้ IP Address ใดๆ สามารถเข้าถึงเราเตอร์ได้เฉพาะจาก LAN Interface ในเราเตอร์บางยี่ห้อจะมีฟังก์ชัน Stateful Packet Inspection (SPI) ที่เมื่อเปิดการทำงานแล้วก็จะส่งผลให้ทุกการเชื่อมต่อจากภายนอกมาที่เราเตอร์ผ่าน WAN Interface ไม่สามารถทำได้

ซึ่งก็สามารถใช้ได้ผลเช่นเดียวกันกับการกำหนด ACL ทั้งนี้ในเราเตอร์บางตัวอาจมีฟังก์ชันให้เลือกเพื่อเปิดหรือปิดการทำงาน Remote Management โดยตรงได้เลย

• ในขณะเดียวกัน แม้ว่าบางช่องโหว่สามารถป้องกันได้ด้วยการปิดการทำงานของ Remote Management แต่ผู้ใช้คนอื่นที่เชื่อมต่ออยู่ภายในเครือข่ายเดียวกันกับเราก็มีโอกาสที่โจมตีผ่านช่องโหว่ดังกล่าวได้อยู่ดี ดังนั้นหลักปฏิบัติเดิมที่มักได้ยินอยู่เป็นประจำไม่ว่าจะเป็นการตั้งค่ารหัสผ่านของเราเตอร์ รวมถึงรหัสผ่านของ WPA, WPA2 ฯลฯ ให้มีความแข็งแกร่ง (8 หลักขึ้นไป มีตัวอักษร ตัวเลข และอักขระพิเศษผสมกัน ไม่ควรใช้ข้อมูลส่วนตัวเป็นส่วนหนึ่งของรหัสผ่าน ฯลฯ) หมั่นอัปเดตเฟิร์มแวร์ของเราเตอร์ และการ Logout ทุกครั้งหลังจากที่ตั้งค่าเราเตอร์เสร็จสิ้น ก็เป็นสิ่งที่ไม่ควรละเลยแต่อย่างใด ในเรื่องรหัสผ่านของเราเตอร์นั้นอาจมีเหตุผลบางอย่างที่ทำให้ผู้ใช้ไม่เปลี่ยนรหัสผ่านที่เป็นค่าตั้งต้น เช่น ถ้าหากพบปัญหาระหว่างการใช้งาน ผู้ให้บริการจะได้สามารถล็อกอินเข้าเราเตอร์มาแก้ไขปัญหาได้ในทันที ซึ่งในความคิดเห็นส่วนตัวของผู้เขียนนั้น ไม่ว่าด้วยเหตุผลใดก็ตามควรเปลี่ยนรหัสผ่านดังกล่าว เนื่องจากรหัสผ่านเดิมของเราเตอร์ที่ติดตั้งโดยผู้ให้บริการเป็นรหัสผ่านที่ทุกคนสามารถค้นหาได้โดยง่ายอยู่แล้ว และเป็นหนึ่งในจุดอ่อนสำคัญที่ผู้ไม่หวังดีใช้ในการโจมตี

• หลาย ๆ ท่านคงทราบว่า การตั้งค่า Wireless Security แบบ WEP นั้นถูกแฮกได้อย่างง่ายดายมาเป็นเวลานานแล้ว ปัจจุบันจึงมักจะเห็นการตั้งค่าแบบ WPA2 เป็นส่วนใหญ่ แต่บางท่านอาจยังไม่ทราบว่า ฟังก์ชัน WiFi Protected Setup (WPS) ที่มักมาพร้อมกับเราเตอร์ในปัจจุบันนั้นเป็นอีกช่องทางหนึ่งที่เปิดโอกาสให้ผู้ไม่หวังดีสามารถแฮกได้ภายในไม่กี่ชั่วโมง และช่องโหว่ดังกล่าวมีการเปิดเผยออกมานานแล้วเช่นกัน ดังนั้นสิ่งที่ควรทำในอันดับต้น เมื่อมีการตั้งค่าเราเตอร์ใหม่ก็คือการปิดการทำงานของ WPS และตรวจสอบซ้ำอีกครั้งว่าฟังก์ชัน WPS ปิดการทำงานแล้วจริง ด้วยการลบข้อมูลการเชื่อมต่อกับเครือข่ายที่เคยมีอยู่บนคอมพิวเตอร์แล้วทำการเชื่อมต่อใหม่อีกครั้ง หากคอมพิวเตอร์มีการแนะนำให้ผู้ใช้สามารถกดปุ่ม WPS บนเราเตอร์เพื่อทำการเชื่อมต่ออัตโนมัติได้ แสดงว่า WPS ยังไม่ได้ปิดการทำงานจริง ซึ่งสาเหตุที่ควรตรวจสอบซ้ำเนื่องจากมีเราเตอร์บางยี่ห้อที่แม้จะตั้งค่าให้ปิดการทำงานของ WPS แล้วแต่อันที่จริงยังมีการทำงานอยู่

• ในช่วงนี้มีผู้ใช้หลายรายที่พบปัญหาเราเตอร์มีการแก้ไขการตั้งค่า DNS ดังนั้นผู้ใช้ควรตรวจสอบการตั้งค่า DNS ภายในเราเตอร์อย่างสม่ำเสมอ (สามารถศึกษาวิธีการตรวจสอบการตั้งค่า DNS ในคอมพิวเตอร์และเราเตอร์ได้จากเว็บไซต์ OpenDNS **[13]**) การตั้งค่า DNS ในเราเตอร์โดยทั่วไปมีอยู่ด้วยกัน 2 แบบ คือการตั้งค่าให้รับ IP Address ของ DNS Server จากผู้ให้บริการอินเทอร์เน็ต และการตั้งค่าโดยกำหนด IP Address ของ DNS Server ด้วยตนเอง ซึ่งวิธีการตรวจสอบ IP Address ของ DNS Server ในเบื้องต้นว่าเป็นของผู้ไม่หวังดีหรือไม่สามารถทำได้ด้วยการใช้บริการ WHOIS **[14]** แล้วระบุ IP Address ดังกล่าวเพื่อค้นหา หากพบว่าเป็น IP Address ของผู้ให้บริการรายเดียวกันกับที่เราใช้ก็สามารถตอบได้ในระดับหนึ่งว่ามั่นคงปลอดภัย แต่วิธีนี้อาจใช้ไม่ได้ผลกับผู้ไม่หวังดีที่เปิดบริการ DNS Server ในเครือข่ายของผู้ให้บริการรายเดียวกันกับที่เราใช้ ดังนั้นหากผู้ใช้ไม่สามารถแยกแยะได้ชัดเจนว่าเป็น DNS Server ที่เชื่อถือได้

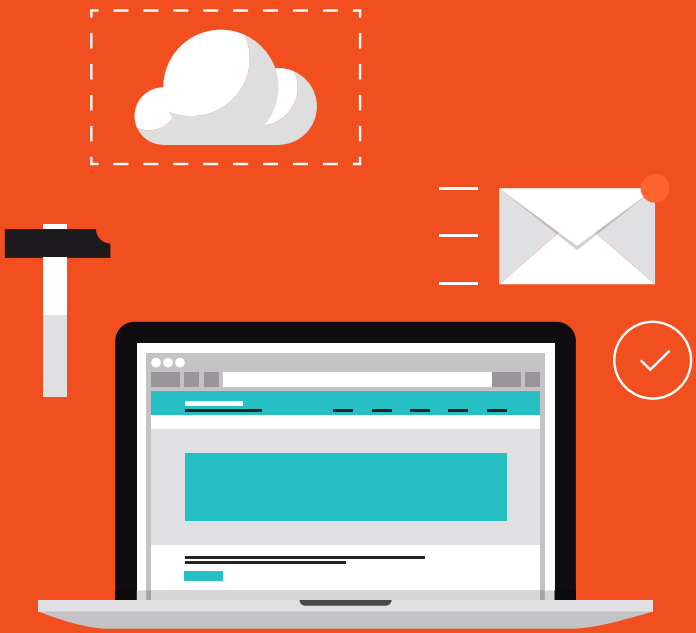
หรือไม่ ให้ทำการระบุ IP Address ของ DNS Server ที่มีความน่าเชื่อถือลงในเราเตอร์ เช่น DNS Server ของ Google จะมีหมายเลขเป็น 8.8.8.8 และ 8.8.4.4 **[15]**

• สำหรับผู้ที่มีความรู้ในการตั้งค่าระบบเครือข่ายต่าง ๆ คำแนะนำสุดท้ายก็คือให้เลือกซื้อเราเตอร์ที่รองรับการติดตั้งเฟิร์มแวร์จากนักพัฒนาภายนอก เช่น DD-WRT **[16]**, OpenWRT **[17]** และ Tomato **[18]** ที่เป็นเวอร์ชันใหม่ได้ เพราะหากมีผู้ค้นพบช่องโหว่ในเฟิร์มแวร์ที่มาพร้อมกับเราเตอร์แล้วยังไม่มีอัปเดตออกมาจากทางผู้ผลิต ผู้ใช้ยังมีโอกาสที่จะเปลี่ยนไปใช้เฟิร์มแวร์ตัวอื่นเพื่อหลีกเลี่ยงช่องโหว่เหล่านั้น อีกทั้งเฟิร์มแวร์จากนักพัฒนาภายนอกเหล่านี้มักมีฟังก์ชันให้ผู้ใช้สามารถปรับแต่งได้อย่างมากมาย ทั้งนี้ผู้ใช้ควรศึกษาขั้นตอนการติดตั้งและตั้งค่าเฟิร์มแวร์เหล่านี้ให้ดีก่อนลงมือทำจริง

ปัญหาเหล่านี้ ต้องอาศัยความร่วมมือระหว่างผู้ใช้และผู้ให้บริการจึงจะทำให้การตรวจสอบและป้องกันเหตุภัยคุกคามเป็นไปอย่างมีประสิทธิภาพ ซึ่งในปัจจุบันนั้นผู้ใช้ทั่วไปยังไม่ได้มีความตระหนักรู้และเข้าใจในปัญหาด้านความมั่นคงปลอดภัยเท่าที่ควร และทางผู้ให้บริการก็ยังไม่ได้มีการเผยแพร่ข่าวสารและวิธีการตรวจสอบป้องกันจากเหตุภัยคุกคามให้กับผู้ใช้อย่างทั่วถึง ผู้เขียนจึงหวังว่าจะเห็นความร่วมมือในลักษณะดังกล่าวเกิดขึ้น เนื่องจากการโจมตีเหล่านี้สามารถทำได้ไม่ยากและส่งผลกระทบต่อผู้ใช้ตรง และภัยในลักษณะนี้คาดว่าจะทวีความรุนแรงมากขึ้นเรื่อย ๆ ต่อไปในอนาคต

อ้างอิง

1. http://www.tripwire.com/state-of-security/top-security-stories/majority-soho-wireless-routers-security-vulnerabilities
2. http://arstechnica.com/security/2014/02/dear-asus-router-user-youve-been-pwned-thanks-to-easily-exploited-flaw
3. http://jis.eurasipjournals.com/content/2013/1/2
4. https://isc.sans.edu/forums/diary/Suspected+Mass+Exploit+Against+Linksys+E1000+E1200+Routers/17621
5. https://isc.sans.edu/diary/Linksys+Worm+Captured/17630
6. https://isc.sans.edu/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633
7. https://isc.sans.edu/diary/A+few+updates+on+%22The+Moon%22+worm/17855
8. http://www.net-security.org/malware_news.php?id=2731
9. https://thaicert.or.th/alerts/user/2014/al2014us001.html
10. http://www.tplink.com/ca/article/?faqid=569
11. https://www.team-cymru.com/ReadingRoom/Whitepapers/2013/TeamCymruSOHOPharming.pdf
12. http://pantip.com/topic/31775473
13. https://store.opendns.com/setup
14. http://who.is
15. https://developers.google.com/speed/public-dns
16. http://www.dd-wrt.com
17. https://openwrt.org
18. http://www.polarcloud.com/tomato



ข้อแนะนำในการป้องกัน ไม่ให้เด็กกดซื้อ In-App Purchase โดยไม่ตั้งใจ

ผู้เขียน : เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่ : 4 กรกฎาคม 2557
ปรับปรุงล่าสุด : 6 กรกฎาคม 2557

เมื่อวันที่ 22 มิถุนายน 2557 หนังสือพิมพ์ไทยหลายฉบับได้เผยแพร่ข่าวว่าเด็กชายเล่นเกม Cookie Run แล้วได้รับบิลเรียกเก็บเงินเป็นแสนบาท โดยเนื้อข่าวระบุว่าเด็กคนดังกล่าวทำตามคลิปใน YouTube ที่อ้างว่าเป็นวิธีการซื้อไอเทมในเกมโดยไม่ต้องจ่ายเงิน และลองปฏิบัติตาม แต่ปรากฏว่าในเวลาต่อมาถูกเรียกเก็บเงินจากผู้ให้บริการโทรศัพท์มือถือเป็นค่าไอเทมโดยมียอดค่าใช้จ่ายกว่าสองแสนบาท [1]

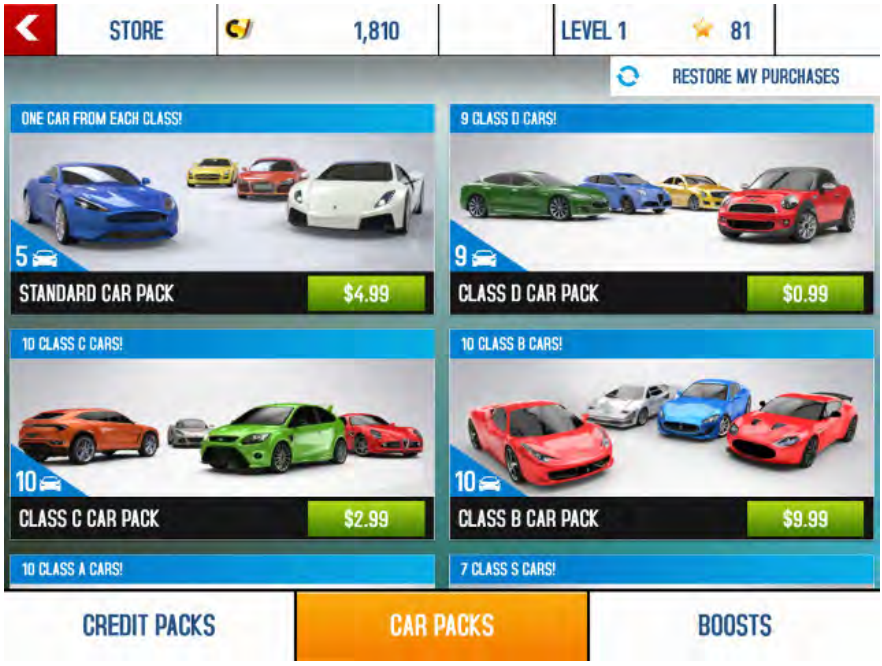
ทาง AIS ซึ่งเป็นผู้ให้บริการโทรศัพท์มือถือที่เด็กชายคนดังกล่าวใช้บริการอยู่ ได้ให้ข้อมูลว่า ค่าใช้จ่ายดังกล่าวนั้นเกิดจากการใช้บริการ Carrier Billing ซึ่งเป็นการจ่ายเงินซื้อสินค้าใน Google Play Store โดยหักเงินผ่านทางผู้ให้บริการโทรศัพท์มือถือ สำหรับกรณีที่เกิดขึ้นนี้ทางผู้ใช้บริการได้เปิดใช้งานเป็นแบบรายเดือน และทาง AIS ยังไม่ได้มีมาตรการควบคุมเพดานค่าใช้จ่าย จึงทำให้เด็กคนดังกล่าวสามารถซื้อของในเกมเป็นมูลค่ากว่าสองแสนบาทได้ [2]

ภายหลังจากที่เกิดปัญหาดังกล่าว ทาง AIS ได้ปิดระบบการจ่ายเงินผ่านบริการ Carrier Billing ไปเป็นการชั่วคราว และแถลงข่าวว่าจะยกเลิกค่าบริการให้กับลูกค้าที่กดซื้อสินค้าและบริการโดยรู้เท่าไม่ถึงการณ์ ล่าสุดทาง กสทช. ได้เข้ามากำกับดูแลการให้บริการ Carrier Billing ของผู้ให้บริการโทรศัพท์มือถือในประเทศไทยแล้ว [3]

จากข่าวข้างต้น ผู้ปกครองหลายท่านที่ให้บุตรหลานโดยเฉพาะเด็กเล็ก ๆ ใช้งานโทรศัพท์มือถือหรือแท็บเล็ต อาจไม่เข้าใจว่าเหตุการณ์ดังกล่าวนี้เกิดขึ้นได้อย่างไร และอาจมีความกังวลว่าเด็กอาจจะเผลอไปกดซื้อของในเกมผ่านระบบ In-App Purchase จนหมดเงินไปหลายแสนบาทแบบที่เกิดขึ้นในข่าวได้ บทความนี้จะอธิบายสาเหตุและวิธีการป้องกันความเสียหายที่จะเกิดขึ้นจากเหตุการณ์ดังกล่าว

In-App Purchase คืออะไร

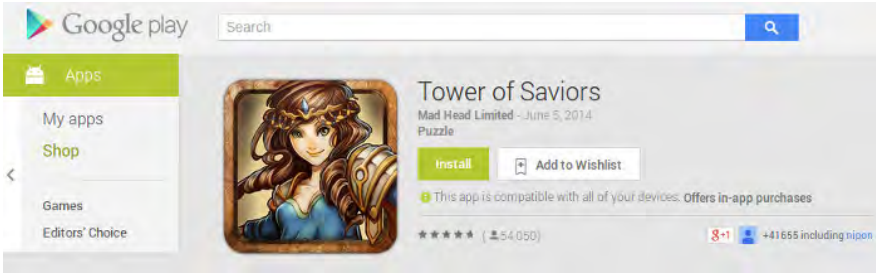
In-App Purchase คือชื่อเรียกวิธีการจ่ายเงินจริงเพื่อซื้อความสามารถหรือคุณสมบัติพิเศษของตัวแอปพลิเคชัน เช่น จ่ายเงินเพื่อปิดหน้าจอแสดงโฆษณา หรืออัปเกรดความสามารถของแอปพลิเคชันให้ทำงานได้มากกว่าเวอร์ชันฟรี เป็นต้น ถ้าเป็นเกม โดยเฉพาะเกมในโทรศัพท์มือถือ จะนิยมใช้ In-App Purchase ในการซื้อสิ่งของมาอัปเกรดความสามารถให้กับตัวละครในเกม เช่น ซื้ออาวุธหายากที่ไม่สามารถหาได้ด้วยการเล่นเกมตามปกติ หรือซื้อของเพิ่มพลังชีวิตให้ตัวละครสามารถอยู่ในเกมได้นานขึ้น เป็นต้น ตัวอย่างหน้าจอเกมที่มี In-App Purchase เป็นดังรูปที่ 1



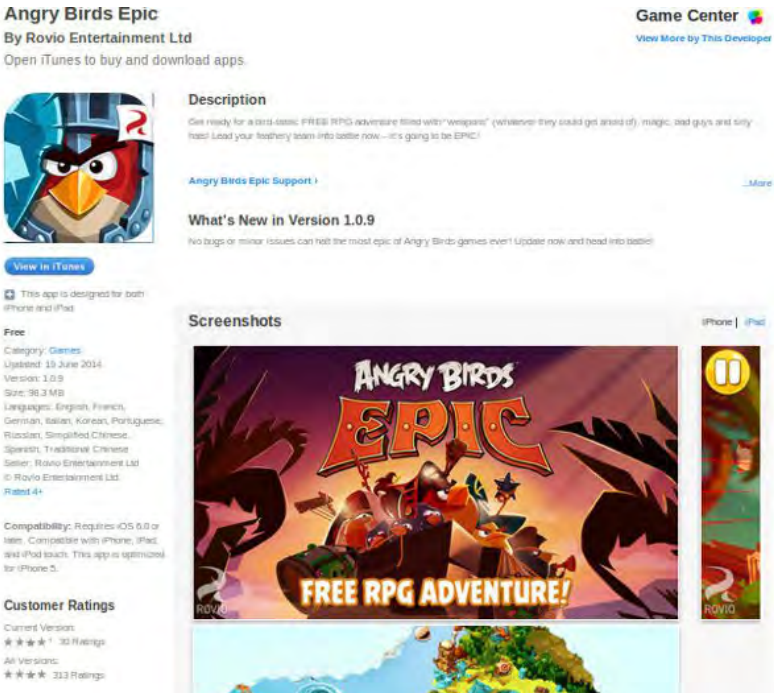
รูปที่ 1 ตัวอย่างหน้าจอ In-App Purchase ในเกม

เกมในโทรศัพท์มือถือส่วนใหญ่มักจะออกแบบมาให้รองรับระบบ In-App Purchase และทำระบบเกมออกมาเอื้อให้คนจ่ายเงินเพื่อซื้อของมาเพิ่มความสามารถให้ตัวละคร เนื่องจากการจ่ายเงินผ่านโทรศัพท์มือถือนั้นสามารถทำได้ง่าย และในหลายครั้งการซื้อของในเกมราคาประมาณ 30-60 บาท สามารถทำให้ตัวละครเก่งขึ้นได้เร็วกว่าการนั่งเล่นเกมเป็นสิบชั่วโมง ทำให้คนตัดสินใจจ่ายเงินเพื่อซื้อของเหล่านี้ได้ง่ายกว่า โดยเฉพาะอย่างยิ่งถ้าเป็นเกมที่สามารถเล่นเพื่อเอาคะแนนไปแข่งขันกับคนอื่น ๆ ได้ก็จะยิ่งทำให้คนยอมจ่ายเงินเพื่อซื้อของในเกมมากขึ้นไปอีก

ใน Google Play Store และ Apple App Store แอปพลิเคชันไหนที่มีระบบ In-App Purchase จะมีข้อความระบุไว้ชัดเจน ดังรูปที่ 2 และ 3 เพียงแต่ว่าใน Play Store นั้นจะไม่มีรายละเอียดบอกว่า In-App Purchase ของแต่ละแอปพลิเคชันมีอะไรบ้าง และแต่ละรายการมีราคาเท่าไหร่



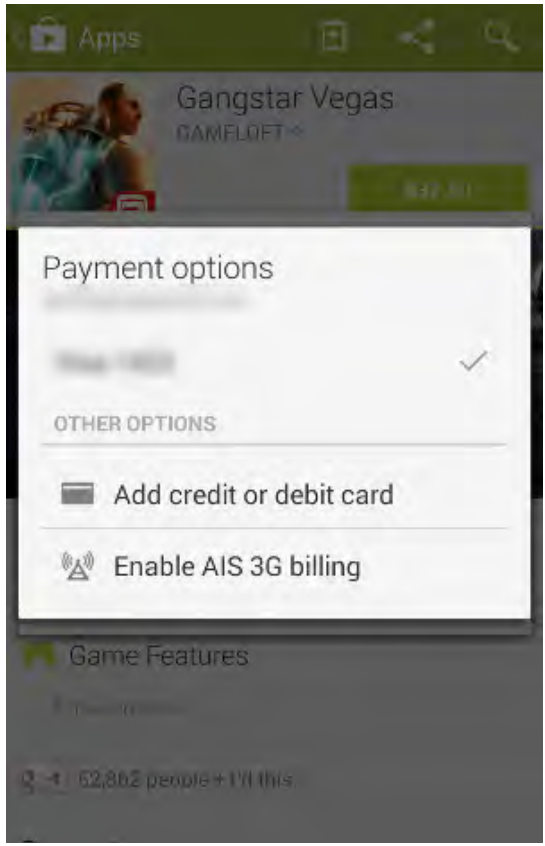
รูปที่ 2 หน้าดาวน์โหลดของ Play Store
บอกว่าแอปพลิเคชันมี In-App Purchase แต่ไม่บอกรายละเอียด



รูปที่ 3 หน้าดาวน์โหลดของ App Store มีข้อมูล
รายการ In-App Purchase พร้อมราคา

วิธีซื้อ In-App Purchase

การจ่ายเงินเพื่อซื้อ In-App Purchase สามารถทำได้เหมือนการซื้อแอปตามปกติ โดยหลัก ๆ แล้วในประเทศไทยสามารถทำได้ 2 วิธีคือจ่ายผ่านบัตรเครดิตและจ่ายผ่าน Carrier Billing ดังตัวอย่างในรูปที่ 4 (AIS 3G Billing)



รูปที่ 4 ตัวอย่างวิธีการจ่ายเงินเพื่อซื้อแอปพลิเคชัน
จาก Play Store

จ่ายผ่านบัตรเครดิต

ใช้วิธีสมัครบัตรเครดิตแล้วผูกข้อมูลของบัตรเข้ากับบัญชีที่ใช้งานในโทรศัพท์มือถือ แต่หากไม่มีบัตรเครดิตก็สามารถใช้บัตรเดบิตแทนได้ ซึ่งจะแตกต่างจากบัตรเครดิตตรงที่การหักเงินจะหักออกจากเงินที่มีอยู่ในบัญชี และใช้เงินได้เท่ากับจำนวนเงินที่มีอยู่ ไม่ใช่การจ่ายเงินล่วงหน้าแบบบัตรเครดิต

จ่ายผ่าน Carrier Billing

เปลี่ยนจากการจ่ายเงินผ่านบัตรเครดิต มาเป็นการจ่ายเงินผ่านผู้ให้บริการโทรศัพท์มือถือแทน ซึ่งในปัจจุบันนี้มีผู้ให้บริการโทรศัพท์มือถืออยู่ 2 ค่ายที่ให้บริการ Carrier Billing คือ AIS รองรับการจ่ายเงินซื้อสินค้าและบริการผ่าน Google Play Store **[4]** และ DTAC รองรับการซื้อแอปพลิเคชันผ่าน Windows Phone Store **[5]** แต่สำหรับระบบปฏิบัติการ iOS นั้น ขณะนี้ยังไม่มีการเปิดให้บริการ Carrier Billing ในประเทศไทย

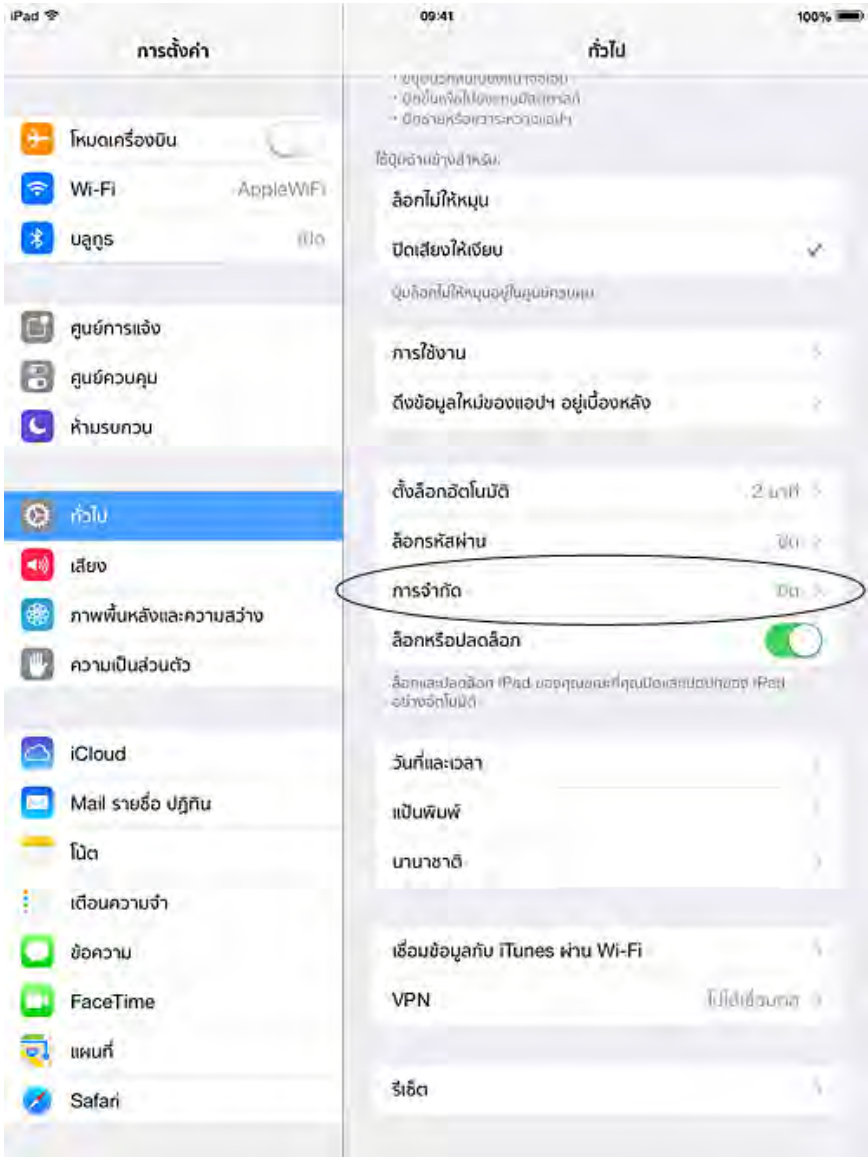
ผู้ให้บริการบางราย (เช่น LINE) มีระบบ Store เป็นของตัวเอง และรองรับการจ่ายเงินเพื่อซื้อของใน Store โดยการใช้บัตรเงินสดหรือบัตรเติมเงินโทรศัพท์มือถือ ซึ่งทำให้ผู้ที่ไม่มีบัตรเครดิตและไม่ได้ใช้เครือข่ายโทรศัพท์ที่รองรับ Carrier Billing สามารถซื้อของจาก Store ได้ **[6]**

การกดซื้อแอปพลิเคชันหรือซื้อ In-App Purchase โดยปกติแล้วถ้าหากเป็นระบบปฏิบัติการ Android ที่มีการผูกข้อมูลบัตรเครดิตหรือ Carrier Billing ไว้แล้ว จะสามารถกดซื้อได้เลยโดยไม่จำเป็นต้องมีการยืนยันตัวบุคคลอีก แต่หากเป็นระบบปฏิบัติการ iOS จะมีหน้าจอให้ใส่รหัสผ่านของ Apple ID เมื่อมีการซื้อสินค้าทุกครั้ง

วิธีป้องกันปัญหาเด็กกดซื้อ In-App Purchase โดยไม่ตั้งใจ

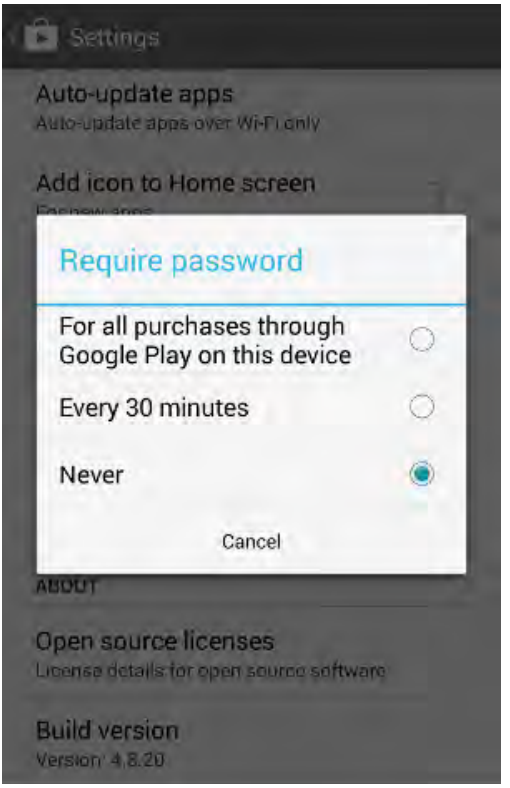
ถ้าพ่อแม่ซื้อโทรศัพท์มือถือหรือแท็บเล็ตให้ลูกใช้เล่นเกม ก็ไม่ควรไปผูกบัตรเครดิตหรือผูกข้อมูลการจ่ายเงินไว้กับบัญชีที่ล็อกอินไว้ในเครื่องนั้น เพราะการใส่ข้อมูลเหล่านี้ไว้ก็เหมือนกับการฝากกระเป๋าเงินไว้ที่เด็ก ซึ่งเด็กจะหยิบเงินออกมาใช้เมื่อไหร่ก็ได้

ในระบบปฏิบัติการ iOS มีฟังก์ชันจำกัดสิทธิ์การใช้งาน (Restriction) ซึ่งผู้ปกครองสามารถกำหนดได้ว่าให้ลูกสามารถใช้งานแอปพลิเคชันอะไรได้บ้าง รวมถึงตั้งรหัสผ่านสำหรับใช้ในการซื้อสินค้าจาก Store ได้ด้วย (เป็นคนละรหัสผ่านกับรหัสผ่านที่ใช้ใน Apple ID) โดยวิธีการเปิดใช้งานสามารถทำได้โดยไปที่การตั้งค่า และทำตามวิธีที่อธิบายไว้ในเว็บไซต์ของ Apple ดังรูปที่ 5 **[7]**



รูปที่ 5 การตั้งค่าการจำกัดในระบบปฏิบัติการ iOS

สำหรับระบบปฏิบัติการ Android สามารถตั้งค่าที่แอปพลิเคชัน Play Store ได้ว่าต้องการให้ใส่รหัสผ่าน Google Account ทุกครั้งที่มีการสั่งซื้อสินค้าจาก Play Store หรือไม่ ดังรูปที่ 6 โดยสามารถเปิดดูวิธีการตั้งค่าได้จากเว็บไซต์ของ Google **[8]**



รูปที่ 6 การตั้งค่าให้ใส่รหัสผ่านทุกครั้งที่สั่งซื้อสินค้าจาก Play Store

อย่างไรก็ตาม วิธีการนี้ไม่ใช่วิธีการที่มั่นคงปลอดภัยนัก เพราะยังมีจุดอ่อนที่สามารถเข้าไป Clear Data ของแอปพลิเคชัน Play Store เพื่อให้สามารถกดซื้อโดยไม่ต้องใส่รหัสยืนยันได้ หรือในบางกรณีการอัปเดตเวอร์ชันของ Play Store หรืออัปเกรดระบบปฏิบัติการ ก็อาจมีการเคลียร์ข้อมูลเก่าของ Play Store ซึ่งก็อาจทำให้การตั้งค่าในส่วนนี้กลับมาเป็นเหมือนเดิมได้

ในระบบปฏิบัติการ Android เวอร์ชันปัจจุบัน (Android 4.4 KitKat) ยังไม่มีระบบจำกัดสิทธิ์การใช้งานที่ครอบคลุมและป้องกันได้ดีพอเหมือนกับ iOS ดังนั้นผู้ปกครองที่ให้เด็กใช้มือถือหรือแท็บเล็ตที่เป็นระบบปฏิบัติการ Android และมีการผูกข้อมูลการจ่ายเงินไว้ในบัญชี ก็อาจจะมีความเสี่ยงมากกว่าอุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS

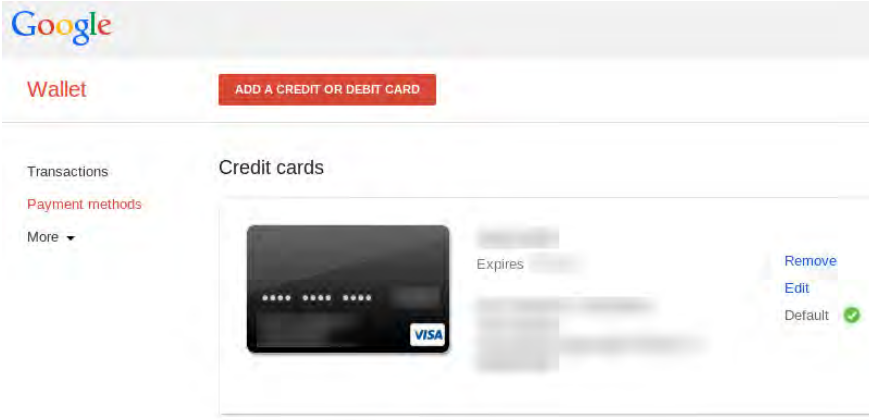
ข้อแนะนำและวิธีการป้องกัน

ปัญหาของการซื้อของผ่านระบบออนไลน์นั้นไม่ใช่มีแค่ว่าเด็กจะเอามือถือไปกดซื้อของในเกมได้อย่างเดียว ทางผู้ใหญ่เองหากวางโทรศัพท์มือถือทิ้งไว้หรือถูกขโมย แล้วไม่มีการตั้งค่าล็อกหน้าจอไว้ ก็อาจถูกผู้ไม่หวังดีกดซื้อสินค้าหรือบริการต่าง ๆ จนเงินหมดบัญชีได้ พึงระลึกไว้เสมอว่าหากมีการผูกข้อมูลการจ่ายเงินเข้ากับตัวอุปกรณ์ใด ๆ แล้ว ให้ถือว่าอุปกรณ์นั้นเป็นกระเป๋าเงินหรือเป็นบัตร ATM ที่พร้อมจะกดเงินออกได้ตลอดเวลา ดังนั้นการให้ความสำคัญกับอุปกรณ์เหล่านี้จึงควรให้อยู่ในระดับเดียวกับการระวังรักษากระเป๋าเงิน

การตั้งรหัสผ่านล็อกหน้าจอ รวมถึงกำหนดรหัสผ่านสำหรับจ่ายเงินซื้อสินค้า ก็สามารถช่วยป้องกันความเสียหายได้ในระดับหนึ่ง รวมทั้งการตั้งค่าติดตามมือถือหายและล้างข้อมูลในเครื่องจากระยะไกล (Remote Wipe) ก็สามารถช่วยลดความเสียหายหากมือถือสูญหายหรือถูกขโมยได้

หากตั้งค่าให้ซื้อสินค้าผ่านบัตรเครดิต ควรตรวจสอบข้อมูลการซื้อสินค้าอย่างสม่ำเสมอ หากพบว่ามีรายการสั่งซื้อสินค้าที่ผิดปกติ ควรรีบแจ้งทางธนาคารและเจ้าของ Store ทันที หรือหากใช้บริการ Carrier Billing ก็ควรใช้บริการโทรศัพท์แบบเติมเงิน เพื่อที่จะสามารถควบคุมปริมาณเงินที่จะใช้ซื้อบริการแบบออนไลน์ได้

หากไม่ต้องการให้มีข้อมูลการจ่ายเงินอยู่ในบัญชีที่ใช้ในเครื่อง สามารถเอาข้อมูลเหล่านั้นออกได้ โดยหากเป็น Android ให้ไปที่เว็บไซต์ Google Wallet (https://wallet.google.com) จากนั้นล็อกอินด้วย Google Account ในด้านซ้ายมือ เลือก วิธีชำระเงิน แล้วลบรายการบัตรเครดิตออก ตัวอย่างหน้าจอเป็นดังรูปที่ 7 และ 8 หากใส่ข้อมูล Carrier Billing ไว้ก็สามารถนำรายการดังกล่าวออกได้จากหน้าจอนี้เช่นกัน

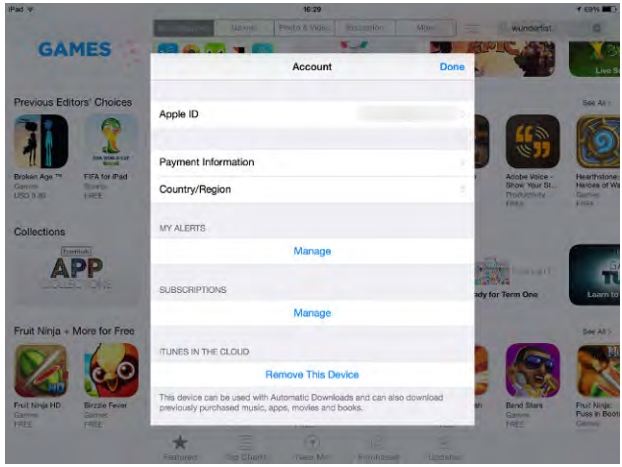


รูปที่ 7 ตัวอย่างหน้าจอการตั้งค่า Google Wallet
เมื่อเข้าจากเบราว์เซอร์ในคอมพิวเตอร์

รูปที่ 8 ตัวอย่างหน้าจอการตั้งค่า Google Wallet เมื่อเข้าจากโทรศัพท์มือถือ

ล่าสุดเมื่อวันที่ 2 กรกฎาคม 2557 ทาง กสทช. ได้แถลงผลการหารือร่วมกับผู้ให้บริการ โดยได้ข้อสรุปว่าในอนาคตเมื่อมีการซื้อสินค้าผ่าน Google Play Store จะต้องมีให้ใส่รหัสผ่าน เพื่อยืนยันทุกครั้ง กำหนดให้ผู้ซื้อสามารถซื้อสินค้าได้ครั้งละไม่เกิน 1,000 บาท และให้คิดค่าซื้อสินค้ารวมกับค่าใช้บริการโทรศัพท์ **[9]** อย่างไรก็ตามถึงแม้ว่าทาง AIS จะแจ้งว่าสามารถเปิดให้บริการ Carrier Billing ได้อีกครั้งในวันที่ 22 กรกฎาคม 2557 แต่จากการตรวจสอบของไทยเซิร์ตในวันที่ 3 กรกฎาคม 2557 พบว่าสามารถทำการใช้งานบริการ Carrier Billing ได้จากซิมโทรศัพท์มือถือของ AIS ที่ซื้อมาใหม่ และสามารถกดซื้อสินค้าได้โดยไม่จำเป็นต้องใส่รหัสผ่านก่อนซื้อแต่อย่างใด

สำหรับผู้ที่ใช้งานระบบปฏิบัติการ iOS สามารถแก้ไขข้อมูลการจ่ายเงินได้จากแอป App Store หรือ iTunes Store จากในเครื่องได้เลย โดยเข้าไปที่เมนู Payment Information ดังรูปที่ 9 หรือจะทำผ่านโปรแกรม iTunes บนคอมพิวเตอร์ก็ได้ **[10]**



รูปที่ 9 ตัวอย่างหน้าจอการตั้งค่าบัญชี Apple ID

การขอคืนเงินในกรณีที่เผลอกดซื้อสินค้าโดยไม่ตั้งใจ

ในระบบปฏิบัติการ Android หากกดซื้อแอปพลิเคชันมาแล้วพบว่าใช้งานไม่ถูกใจ หรือกดซื้อผิด สามารถลบแอปพลิเคชันนั้นออกจากเครื่องได้ภายใน 15 นาทีหลังจากกดซื้อ ซึ่งระบบจะไม่หักเงินออกจากบัญชี แต่หากลบแล้วกดซื้อแอปเดิมซ้ำอีกครั้ง จะไม่สามารถขอเงินคืนได้อีก หากต้องการได้เงินคืน ต้องส่งเรื่องไปยัง Google เพื่อพิจารณาคืนเงินให้ **[11]**

สำหรับระบบปฏิบัติการ iOS หากต้องการขอเงินคืน สามารถไปที่เว็บไซต์ของ Apple (http://reportaproblem.apple.com/) เพื่อส่งเรื่องไปแจ้งปัญหาได้ หรือทำผ่านโปรแกรม iTunes ก็ได้ **[12]** ทั้งนี้ ทาง Apple ยินดีเงินคืนให้ในกรณีที่ตรวจสอบแล้วพบว่าการซื้อของนั้นเกิดจากเด็กกดซื้อ In-App Purchase โดยไม่ตั้งใจ **[13]**

อ้างอิง

1. http://www.thairath.co.th/content/431346
2. http://www.thannews.th.com/index.php?option=com_content&view=article&id=236034&-catid=176&Itemid=524#.U6ffvf77sjj
3. http://www.posttoday.com/%E0%B8%94%E0%B8%B4%E0%B8%88%E0%B8%B4%E0%B8%95%E0%B8%AD%E0%B8%A5%E0%B9%84%E0%B8%A5%E0%B8%9F%E0%B9%8C/302368/
4. http://www.ais.co.th/googleplay/
5. http://www.thairath.co.th/content/367150
6. http://help.line.me/webstore/web?lang=th&contentId=705
7. http://support.apple.com/kb/HT4213?viewlocale=th_TH&locale=th_TH
8. https://support.google.com/googleplay/answer/1626831?hl=th
9. http://www.twitlonger.com/show/n_1s2b45o
10. http://support.apple.com/kb/HT1918?viewlocale=th_TH
11. https://support.google.com/googleplay/answer/134336?hl=th
12. http://ioshacker.com/how-to/get-refund-app-purchased-app-store
13. http://recode.net/2014/01/15/apple-agrees-to-ftc-consent-decree-over-in-app-purchases/

ไทยเซิร์ตพบรูปแบบการฝังแอปพลิเคชันอันตราย ลงในระบบ Google Adsense โจมตีผู้ใช้งาน Android

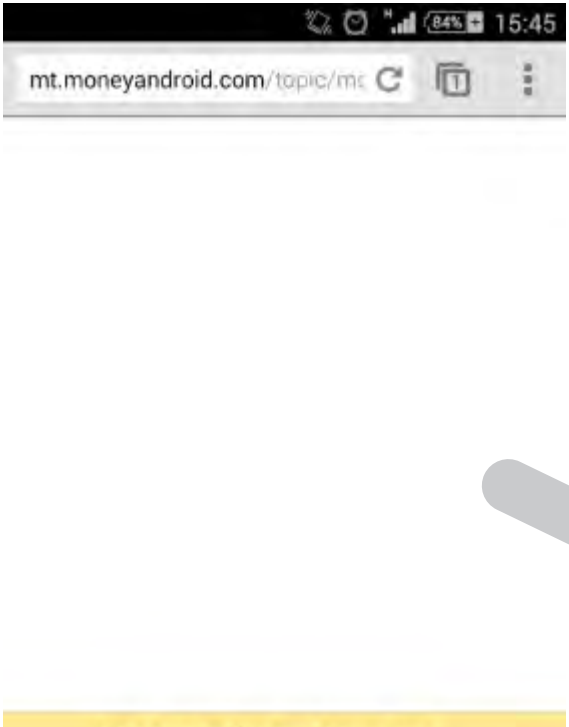
ผู้เขียน : เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่ : 7 สิงหาคม 2557
ปรับปรุงล่าสุด : 7 สิงหาคม 2557

ในช่วงปลายเดือนกรกฎาคมที่ผ่านมา ทีมไทยเซิร์ตได้พบว่าเมื่อเข้าเว็บไซต์ในประเทศไทยหลายแห่งโดยใช้เบราว์เซอร์ในโทรศัพท์มือถือ Android (เช่น Chrome for Android) จะปรากฏ Popup ขึ้นมาเป็นภาษาที่อ่านไม่ออก และสามารถกดได้แค่ปุ่ม OK เพียงอย่างเดียว ดังรูปที่ 1 และ 2 ซึ่งตัวอย่าง Popup ดังกล่าวมาจากเว็บไซต์ mt.moneyandroid.com

รูปที่ 1 ตัวอย่างหน้าจอ Popup ให้ดาวน์โหลดโปรแกรม Adobe Flash Player

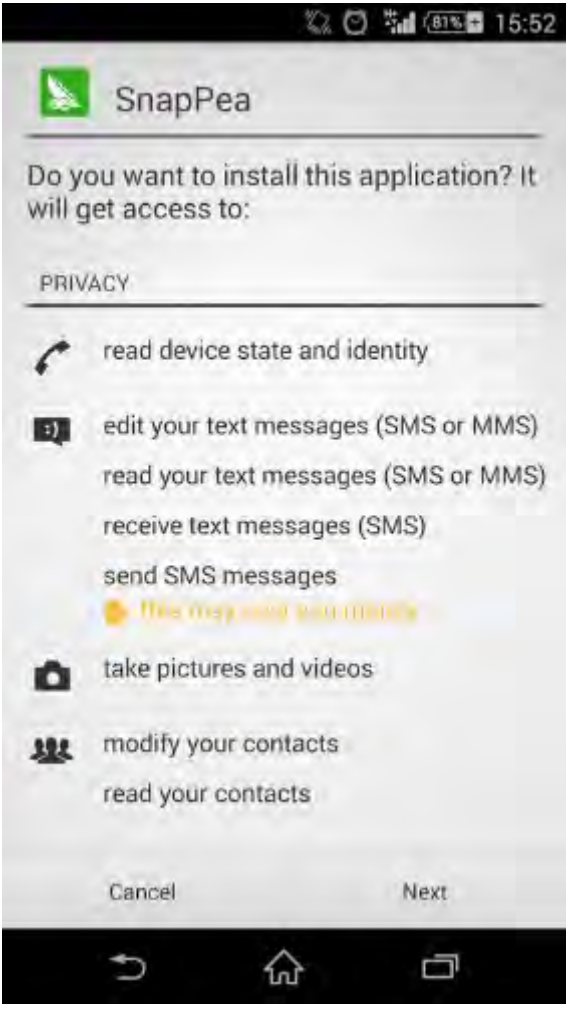
รูปที่ 2 ตัวอย่างหน้าจอ Popup ให้ดาวน์โหลดโปรแกรม SnapPea

ไม่ว่าผู้ใช้จะกดปุ่ม OK หรือกดปุ่ม Back ที่ตัวเครื่อง ก็จะถูกเปลี่ยนเส้นทาง (Redirect) ไปยังเว็บไซต์ mt.moneyandroid.com เพื่อให้ดาวน์โหลดไฟล์ .apk ซึ่งเป็นแอปพลิเคชันของ Android มาติดตั้ง ดังรูปที่ 3 ในบางรายพบว่าถูก Redirect ไปยังหน้าเว็บไซต์ที่ให้กรอกหมายเลขโทรศัพท์มือถือเพื่อให้สมัครใช้บริการรับข่าวสารผ่าน SMS เป็นรายสัปดาห์ ซึ่งจะมีการคิดค่าส่ง SMS ในราคาที่สูง



รูปที่ 3 ตัวอย่างหน้าจอที่ให้ดาวน์โหลดไฟล์ .apk

เมื่อตรวจสอบข้อมูลของแอปพลิเคชันที่ดาวน์โหลดได้จากเว็บไซต์ดังกล่าว พบว่ามีการร้องขอสิทธิ (Permission) ที่น่าสงสัยเป็นจำนวนมาก เช่น อ่านหรือส่ง SMS, ถ่ายภาพ, ถ่ายวิดีโอ, อ่านข้อมูลใน SD Card, เพิ่มหรือลบบัญชีผู้ใช้งานในเครื่อง, เพิ่มหรือลบโปรแกรมในเครื่อง รวมถึงแก้ไขการตั้งค่าระบบ เป็นต้น ดังรูปที่ 4



รูปที่ 4 ตัวอย่างสิทธิที่แอปพลิเคชัน SnapPea ร้องขอ

อย่างไรก็ตาม ข้อความ Popup ไม่ได้ปรากฏขึ้นมาทุกครั้งที่ผู้ใช้งานเข้าเยี่ยมชมเว็บไซต์ที่กล่าวถึงข้างต้น แต่จะแสดงขึ้นมาเป็นแบบสุ่ม และจากการสุ่มตรวจสอบไทยเซิร์ตพบว่ามีเว็บไซต์ที่ได้รับผลกระทบทั้งในประเทศไทยและต่างประเทศ

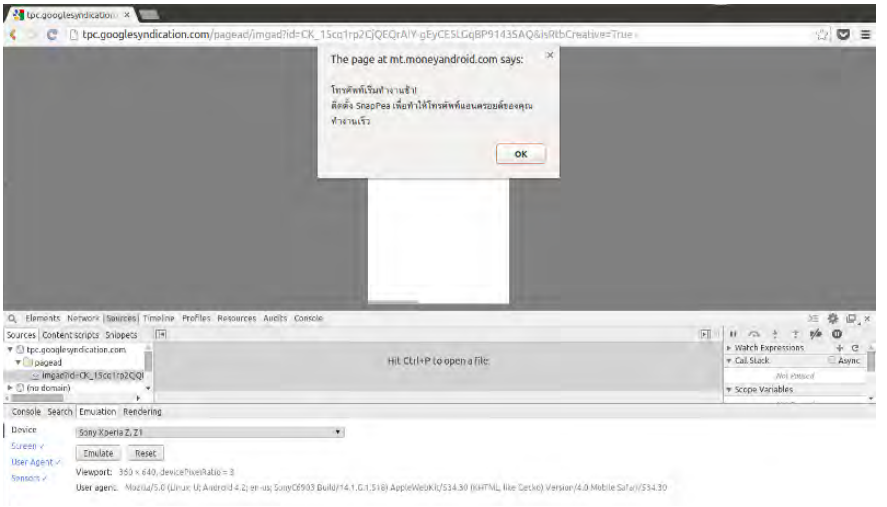
วิเคราะห์สาเหตุ

จากการวิเคราะห์พบว่า Popup ดังกล่าวมาจากโฆษณาที่แสดงใน Google Adsense ซึ่งเป็นระบบโฆษณาที่ Google เปิดให้ผู้พัฒนาเว็บไซต์สามารถนำโค้ดของ Adsense ไปแปะในหน้าเว็บไซต์เพื่อให้ Google จ่ายเงินให้ตามจำนวนผู้เข้าชมโฆษณา ซึ่งระบบการแสดงผลโฆษณาของ Google Adsense สามารถตั้งค่าให้แสดงโฆษณาได้ 3 รูปแบบ คือ Image, Text และ Rich Media หากเลือกแบบ Rich Media ผู้ลงโฆษณาสามารถใส่สคริปต์พิเศษเข้าไปในโฆษณาได้ (เช่น JavaScript หรือ HTML Tag) จึงเป็นช่องทางให้สามารถเลือกใส่สคริปต์ไม่ประสงค์ดีลงไปในตัวโฆษณาได้ ดังตัวอย่างโฆษณาตาม URL ด้านล่างนี้

http://tpc.googlesyndication.com/pagead/imgad?id=CK_15cq1rp2CjQEQrAIY-gEyCE5LGqBP9143SAQ&isRtbCreative=True

รูปที่ 5 โฆษณาแสดงผลเป็นรูปภาพเมื่อเปิดดูด้วยเบราว์เซอร์ของเครื่องคอมพิวเตอร์

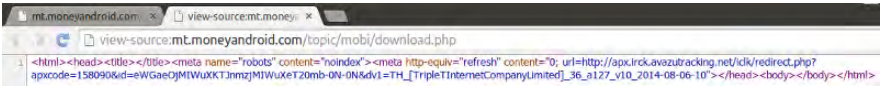
เมื่อเปิด URL ดังกล่าวผ่านเบราว์เซอร์ของเครื่องคอมพิวเตอร์ จะปรากฏเป็นรูปภาพธรรมดา ดังรูปที่ 5 แต่เมื่อเปิด URL เดียวกันนี้โดยใช้เบราว์เซอร์ในโทรศัพท์มือถือ Android จะพบ Popup ขึ้นมา และถูกบังคับให้ไปยังหน้าเว็บไซต์อื่นเพื่อดาวน์โหลดแอปพลิเคชันชื่อ SnapPea ดังรูปที่ 6 ซึ่งในรูปดังกล่าวทางทีมไทยเซิร์ตได้ตั้งค่าโปรแกรม Google Chrome ให้จำลองตัวเองว่าเป็นเบราว์เซอร์ของโทรศัพท์มือถือ Android เพื่อตรวจสอบพฤติกรรม



รูปที่ 6 โฆษณาไม่แสดงผล แต่จะมี Popup
ปรากฏเมื่อเปิดดูด้วยเบราว์เซอร์ของโทรศัพท์มือถือ Android

เมื่อกดปุ่ม OK จะถูก Redirect ไปยังหน้าเว็บไซต์ mt.moneyandroid.com/topic/mobi/download.php ซึ่งจะแสดงผลเป็นหน้าจอว่าง ๆ และมีไฟล์ชื่อ Click_me_to_install_SnapPea_avazu_thai_snappea.apk ให้ดาวน์โหลด อย่างไรก็ตาม เมื่อตรวจสอบไฟล์ดังกล่าวกับเว็บไซต์ Virustotal ยังไม่พบว่ามีอันตราย **[1]**

ซอร์สโค้ดของหน้าเว็บไซต์ดังกล่าวเป็นดังรูปที่ 7 (ดูซอร์สโค้ดได้ที่เว็บไซต์ Pastebin) **[2]** ซึ่งจะเป็นการ Redirect ไปยังลิงก์สำหรับดาวน์โหลดไฟล์ .apk ดังกล่าว



รูปที่ 7 ซอร์สโค้ดของเว็บไซต์ที่ให้ดาวน์โหลดไฟล์ .apk

การโจมตีผ่าน Google Adsense

ผู้ไม่หวังดีลงโฆษณากับ Google Adsense โดยฝังโค้ดที่เป็น JavaScript ไว้ (ดูซอร์สโค้ดได้ที่เว็บไซต์ Pastebin) **[3]** เมื่อเบราว์เซอร์รันสคริปต์จากโค้ดดังกล่าว จะไปดาวน์โหลดสคริปต์ตัวถัดมาซึ่งเป็น iframe ที่มองไม่เห็นและเป็นสคริปต์สำหรับ Redirect ไปยังเว็บไซต์ปลายทางที่ผู้ไม่หวังดีต้องการ (ดูซอร์สโค้ดได้ที่เว็บไซต์ Pastebin) **[4]**

เทคนิคการโจมตีผ่าน Google Adsense นี้ไม่ใช่รูปแบบใหม่ เพราะก่อนหน้านี้เคยเกิดเหตุเช่นเดียวกันนี้มาแล้วหลายครั้ง เช่น การฝังสคริปต์ให้ Redirect ไปยังหน้าดาวน์โหลด Java หรือ Adobe Flash Player ปลอม **[5]** เพื่อหลอกผู้ใช้ Windows

แต่ในกรณีล่าสุดที่ทางไทยเซิร์ตตรวจพบนี้ เป็นการโจมตี Google Adsense โดยมีเป้าหมายที่ผู้ใช้งานระบบปฏิบัติการ Android โดยเฉพาะ ซึ่งถึงแม้ว่าแอปพลิเคชัน SnapPea ที่ผู้ใช้ถูกบังคับให้ดาวน์โหลดไปติดตั้งนั้น เมื่อลองสแกนผ่านเว็บไซต์ Virustotal แล้วไม่พบว่ามีอันตรายก็ตาม แต่เนื่องจากแอปพลิเคชันดังกล่าวมีการขอสิทธิต่าง ๆ ที่มีโอกาสสร้างความเสียหายต่อระบบได้ จึงไม่สมควรที่จะติดตั้งลงในเครื่อง

นอกจากนี้ ยังไม่มีอะไรรับประกันได้ว่าผู้ที่ลงโฆษณาด้วยวิธีการเช่นนี้จะไม่เปลี่ยนจากแอปพลิเคชัน SnapPea เป็นไฟล์มัลแวร์โดยตรง หรือพาไปยังเว็บไซต์หลอกลวงเช่น Phishing ต่อไปในอนาคต เพราะเป็นฟังก์ชันการทำงานที่สามารถทำได้อยู่แล้ว

เนื่องจาก Google Adsense เป็นระบบโฆษณาที่สร้างรายได้ให้กับผู้พัฒนาเว็บไซต์ จึงทำให้มีเว็บไซต์หลายแห่งนำ Adsense ไปติดในเว็บไซต์ของตนเองเพื่อที่จะมีรายได้จากจำนวนผู้เข้าเยี่ยมชม ดังนั้นถึงแม้ว่าผู้ใช้งานระบบปฏิบัติการ Android จะไม่ได้เข้าไปยังเว็บไซต์ที่มีความเสี่ยง เช่น เว็บไซต์ลามก หรือเว็บไซต์ใต้ดิน เพียงแค่เข้าเยี่ยมชมเว็บไซต์ทั่ว ๆ ไปก็มีโอกาสเสี่ยงที่จะถูกโจมตีด้วยวิธีนี้ได้

สิ่งที่ไทยเซิร์ตได้ดำเนินการ

ทางไทยเซิร์ตได้แจ้งข้อมูลปัญหาที่พบไปยังทีมงาน Google Adsense เพื่อขอให้ช่วยตรวจสอบยืนยันแล้ว แต่ในขณะนี้ยังไม่มีข้อมูลที่ชัดเจนว่ามีผู้ลงโฆษณารายอื่นที่ใช้วิธีแบบเดียวกันนี้ในการหลอกลวงผู้ใช้หรือไม่

ข้อแนะนำในการป้องกันตนเอง

1. ไทยเซิร์ตขอแนะนำให้ผู้พัฒนาเว็บไซต์ที่ใช้งาน Google Adsense ควรหมั่นตรวจสอบเว็บไซต์ของท่านโดยทดลองเข้าใช้งานผ่านอุปกรณ์ที่ใช้งานระบบปฏิบัติการ Android/iOS หรือตั้งค่าเบราว์เซอร์แสดง User-Agent เป็นโทรศัพท์มือถือ/แท็บเล็ต เพื่อหาความผิดปกติ **[6]**

2. สำหรับผู้ใช้ทั่วไป หากพบ Popup ลักษณะนี้ และมีไฟล์ .apk ให้ดาวน์โหลด ไม่ควรดาวน์โหลดหรือติดตั้งแอปพลิเคชันนั้น ควรติดตั้งแอปพลิเคชันจาก Play Store เท่านั้น และนอกจากนี้ไม่ควรเปิดให้มีการอนุญาตติดตั้งแอปพลิเคชันจากแหล่งที่มาที่ไม่รู้จัก (Unknown Source)

3. หากพบว่าภายหลังจากเข้าใช้งานเว็บไซต์แล้วมีการนำไปยังหน้าเว็บไซต์ที่ให้กรอกข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ ฯลฯ ควรระมัดระวังตรวจสอบข้อความที่ปรากฏในหน้าเว็บไซต์เหล่านั้นก่อนกรอกข้อมูล เช่น เป็นการสมัครสมาชิกรับข่าวสารผ่าน SMS หรือเป็นบริการที่ต้องเสียเงินหรือไม่

อ้างอิง

1. https://www.virustotal.com/en/file/c24efe41af8f59758b278a5c2d682da9a-8459245b44e78c1feff5929332bf8d7/analysis/
2. http://pastebin.com/Qi1ZcumE
3. http://pastebin.com/6Kj9Kcxp
4. http://pastebin.com/ba2MiVH2
5. http://samsclass.info/126/proj/revmagdalen.htm
6. https://developer.chrome.com/devtools/docs/mobile-emulation

ภาพหลุดดารา กับปัญหาความมั่นคงปลอดภัย ในการใช้งาน iCloud

ผู้เขียน : เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่ : 5 กันยายน 2557
ปรับปรุงล่าสุด : 5 กันยายน 2557

ข่าวใหญ่ในช่วงสัปดาห์นี้คงหนีไม่พ้นเรื่องของภาพหลุดดาราฮอลลีวูดชื่อดังจำนวนมาก บทความนี้จะนำเสนอที่มาที่ไปและประเด็นความเสี่ยงด้านความมั่นคงปลอดภัยที่เกิดขึ้นจากการใช้อุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS ควบคู่กับระบบ iCloud เพื่อให้ผู้อ่านได้มีความตระหนักและสามารถป้องกันตัวจากการตกเป็นเหยื่อได้

ภาพหลุดในข่าวนี้มีการเผยแพร่กันมาตั้งแต่วันที่ 1 กันยายน 2557 ซึ่งหลายภาพเป็นภาพถ่ายส่วนตัวที่มีลักษณะโป๊เปลือย ถึงแม้ว่าเบื้องต้นจะมีการสันนิษฐานว่าสาเหตุของภาพหลุดน่าจะเกิดจากช่องโหว่ของระบบ Find My iPhone แต่ทาง Apple ก็ได้ออกมาปฏิเสธแล้วว่าไม่เป็นความจริงแต่อย่างใด แต่เกิดจากการที่ผู้ใช้ตั้งรหัสผ่านและคำถามความมั่นคงปลอดภัย (Security Question) ที่คาดเดาได้ง่ายเอง ทาง Apple แนะนำให้ผู้ใช้ตั้งรหัสผ่านที่คาดเดาได้ยาก และเปิดใช้งานระบบการตรวจสอบการยืนยันตัวตนแบบ 2 ขั้นตอน (2-Step Verification)

เหตุการณ์กลับไม่จบแค่นั้น เพราะกลุ่มคนที่อ้างว่าเป็นผู้ที่นำภาพออกมาเผยแพร่ บอกว่าสามารถใช้เครื่องมือพิเศษในการดึงภาพออกมาจากระบบ iCloud ได้โดยตรง และจากการตรวจสอบโดยผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยก็พบว่าระบบรักษาความมั่นคงปลอดภัยของ Apple นั้นยังมีจุดอ่อนอยู่ ที่ทำให้ถึงแม้จะเปิดใช้งานระบบการตรวจสอบการยืนยันตัวตนแบบ 2 ขั้นตอนแล้วก็ตาม แต่ก็ไม่สามารถช่วยป้องกันไม่ให้ข้อมูลถูกขโมยออกมาได้ แต่ก่อนจะไปถึงขั้นนั้น ขอพาไปทำความรู้จักกับระบบ iCloud กันก่อน

ระบบ iCloud คืออะไร

iCloud เป็นบริการของ Apple ที่ใช้สำหรับการแชร์ข้อมูลระหว่างอุปกรณ์ที่ใช้งาน Apple ID เดียวกัน **[1]** โดยสามารถแชร์เพลง รูปภาพ เอกสาร รหัสผ่าน ข้ามระหว่างอุปกรณ์ รวมถึงสำรองข้อมูลการตั้งค่าแอปพลิเคชันต่าง ๆ ไปเก็บไว้บน iCloud เพื่อที่เวลาเปลี่ยนเครื่องใหม่แล้วล็อกอินเข้า Apple ID เดิม จะสามารถดึงข้อมูลการตั้งค่าจากอุปกรณ์เครื่องเก่ามายังเครื่องใหม่ได้โดยอัตโนมัติ **[2]** โลโก้ของบริการ iCloud เป็นดังรูปที่ 1

รูปที่ 1 โลโก้ของบริการ iCloud

ผู้ที่ใช้งานระบบปฏิบัติการ iOS หรือ OS X สามารถเข้าใช้งาน iCloud ได้โดยตรงผ่านหน้าจอ Settings ส่วนผู้ที่ใช้งานระบบปฏิบัติการ Windows สามารถติดตั้งโปรแกรม iCloud Control Panel **[3]** เพื่อเข้าถึงอีเมล ปฏิทิน หรือ รูปถ่าย และจัดการข้อมูลอื่น ๆ ที่เก็บอยู่ใน iCloud ได้ หน้าจอโปรแกรม iCloud Control Panel เป็นดังรูปที่ 2

รูปที่ 2 ตัวอย่างหน้าจอโปรแกรม
iCloud Control Panel

นอกจากนี้ iCloud ยังสามารถใช้ร่วมกับระบบ Find My iPhone **[4]** เพื่อใช้ตามหาอุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS เช่น iPhone, iPod, iPad ที่หายหรือถูกขโมยไป รวมถึงใช้สั่งล็อกหรือทำลายข้อมูลในเครื่อง (Factory Reset) จากระยะไกลได้อีกด้วย

Find My iPhone เป็นระบบที่ใช้ค้นหาและระบุตำแหน่งของอุปกรณ์ของ Apple เช่น iPhone, iPad, Mac โดยสามารถเข้าใช้งานได้จากเว็บไซต์ http://www.icloud.com/#find หรือเข้าผ่านแอปพลิเคชัน Find My iPhone **[5]** โดยต้องล็อกอินโดยใช้ Apple ID เดียวกันกับที่ใช้ลงทะเบียนอุปกรณ์นั้น **[6]** ตัวอย่างหน้าจอแอปพลิเคชัน Find My iPhone เป็นดังรูปที่ 3

รูปที่ 3 ตัวอย่างหน้าจอแอปพลิเคชัน
Find My iPhone

และก่อนหน้าที่ทาง Apple จะออกแถลงการณ์ ก็มีการคาดเดากันว่า สาเหตุหนึ่งที่ทำให้ภาพหลุดออกมา เป็นเพราะผู้ไม่หวังดีนำภาพออกมาจาก iCloud ผ่านช่องโหว่ของ Find My iPhone

ช่องโหว่ของ Find My iPhone

ก่อนหน้าที่จะเกิดเหตุการณ์ภาพหลุด เมื่อช่วงปลายเดือนพฤษภาคม 2557 มีผู้ไม่หวังดีใช้วิธีการบางอย่างเข้าถึง Apple ID ของเหยื่อแล้วสั่งล็อกเครื่องเพื่อเรียกค่าไถ่ โดยใช้ Find My iPhone หลังจากที่มีการสืบสวนและจับกุมตัวผู้กระทำผิดได้ ทาง Apple ได้ออกมาชี้แจงว่าระบบ Find My iPhone ไม่ได้มีปัญหา **[7] [8]** แต่ก็ไม่ได้มีคำชี้แจงออกมาว่าผู้ไม่หวังดีสามารถเข้าถึง Apple ID ของเหยื่อและเข้าไปสั่งล็อกเครื่องผ่านระบบ Find My iPhone ได้ด้วยวิธีใด

วันที่ 31 สิงหาคม 2557 นักวิจัยด้านความมั่นคงปลอดภัยได้ค้นพบว่าระบบ Find My iPhone มีช่องโหว่ที่ไม่ว่าผู้ใช้จะใส่รหัสผ่านผิดไปกี่ครั้งก็ยังไม่ถูกบล็อก จึงทำให้ผู้ไม่หวังดีที่รู้แค่ Apple ID ของเหยื่อสามารถสุ่มเดารหัสผ่านได้แบบไม่จำกัดจำนวนครั้ง **[9]** นักวิจัยได้ทดลองเขียนสคริปต์ขึ้นมาชื่อ iBrute ตัวสคริปต์ดังกล่าวนี้จะใช้วิธีการเดารหัสผ่าน iCloud แบบ Brute Force ซึ่งเป็นการสุ่มเดารหัสผ่านทุกค่าที่เป็นไปได้ และเผยแพร่สคริปต์ดังกล่าวนี้ให้คนทั่วไปสามารถดาวน์โหลดได้จากอินเทอร์เน็ต **[10]**

วันที่ 1 กันยายน มีภาพหลุดดาราฮอลลีวูดจำนวนมากถูกเผยแพร่อยู่บนอินเทอร์เน็ต โดยลักษณะของภาพถ่ายบางภาพเป็นเหมือนภาพที่ถ่ายเล่นส่วนตัวโดยถ่ายจากโทรศัพท์มือถือ **[11]** เนื่องจากเหตุการณ์ที่เกิดขึ้นนี้ประจวบเหมาะกับข่าวช่องโหว่ของ Find My iPhone พอดี หลายคนจึงพุ่งเป้าไปที่ภาพหลุดจากบริการ iCloud ซึ่งหลังจากที่ Apple ทราบข่าว ก็ได้แก้ไขช่องโหว่การเดารหัสผ่านแบบ Brute Force ในทันที **[12]**

อย่างไรก็ตาม เมื่อวันที่ 3 กันยายน 2557 ทาง Apple ได้ออกมาปฏิเสธว่าสาเหตุของภาพหลุดจำนวนมากนั้นไม่ได้เกิดจากการเจาะระบบ iCloud หรือ Find My iPhone โดยให้ข้อมูลเพียงแค่ว่าผู้ไม่หวังดีสามารถเข้าถึง Apple ID ของเหยื่อได้โดยการเดาจากคำถามความมั่นคงปลอดภัยที่ใช้สำหรับกู้คืนรหัสผ่าน **[13]** แต่ทาง Apple ก็ไม่ได้ให้ข้อมูลทางเทคนิคอะไรมากกว่านี้ อีกทั้งในแถลงการณ์ดังกล่าวก็ไม่ได้มีการกล่าวถึงช่องโหว่ของ Find My iPhone ที่เพิ่งแก้ไขไปหลังจากที่เกิดปัญหาภาพหลุดแต่อย่างใด

ภาพหลุดออกมาได้อย่างไร

ท่ามกลางความสงสัยและการคาดเดาต่าง ๆ นานาว่าภาพลับส่วนตัวนั้นหลุดออกมาได้อย่างไร ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยหลายแห่งก็คาดการณ์ว่าน่าจะเกิดจากการ Brute Force รหัสผ่าน Apple ID ผ่านระบบ Find My iPhone ซึ่งมีความเป็นไปได้ว่าอาจจะเป็นช่องโหว่เดียวกันกับที่เคยเกิดเหตุการณ์ผู้ไม่หวังดีสั่งล็อกเครื่องของเหยื่อเพื่อเรียกค่าไถ่เมื่อตอนปลายเดือนพฤษภาคมที่ผ่านมา

ในเวลาไม่นานนัก ช่วงก่อนหน้าที่ Apple จะออกแถลงการณ์ปฏิเสธว่าเหตุการณ์ภาพหลุดที่เกิดขึ้นไม่ได้เกิดจากช่องโหว่ของ iCloud หรือ Find My iPhone กลุ่มแฮกเกอร์ที่อ้างว่าเป็นคนปล่อยภาพหลุดดังกล่าวได้ออกมาให้ข้อมูลในเว็บบอร์ดแห่งหนึ่ง ยืนยันว่าได้นำภาพดังกล่าวออกมาจากระบบ iCloud จริง โดยทำผ่านเครื่องมือที่ใช้สำหรับการสืบสวนสอบสวนของตำรวจชื่อ Elcomsoft Phone Password Breaker (ต่อไปนี้ขอเรียกชื่อย่อว่า EPPB) **[14]**

EPPB เป็นโปรแกรมที่ใช้ในการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensic) ความสามารถอย่างหนึ่งของโปรแกรมนี้คือจำลองตัวเองเป็นอุปกรณ์ของ Apple เพื่อดึงข้อมูล iCloud Backup ออกมาจากเซิร์ฟเวอร์ของ Apple ได้ ตัวอย่างหน้าจอโปรแกรม EPPB ตอนดาวน์โหลดของข้อมูล iCloud Backup เป็นดังรูปที่ 4

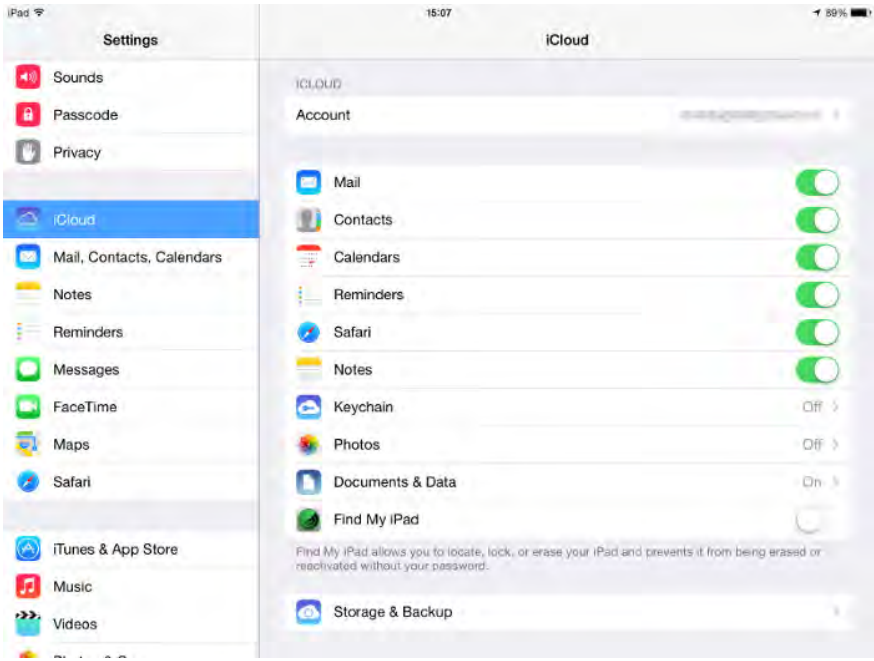
รูปที่ 4 ตัวอย่างหน้าจอโปรแกรม EPPB
ตอนดาวน์โหลดข้อมูล iCloud Backup

ถึงแม้ว่าโปรแกรม EPPB จะขายให้เฉพาะหน่วยงานของรัฐและหน่วยงานด้านกฎหมาย แต่โปรแกรมเวอร์ชันเถื่อนก็มีเผยแพร่อยู่ในอินเทอร์เน็ต เมื่อใช้โปรแกรมนี้ร่วมกับรหัสผ่านที่ได้จากการใช้สคริปต์เดารหัสผ่าน iCloud การจะดึงรูปภาพหรือข้อมูลอื่น ๆ ออกมาจาก iCloud ก็ไม่ใช่เรื่องยากอีกต่อไป **[15]**

อย่างไรก็ตาม ยังไม่สามารถยืนยันได้ว่าภาพหลุดของดาราหลุดออกมาตามวิธีการที่คนกลุ่มนี้กล่าวอ้างหรือไม่ แต่ผู้เชี่ยวชาญหลายคนเชื่อว่าวิธีการนี้สามารถเป็นไปได้ **[16]**

มีอะไรอยู่ใน iCloud Backup

เมื่อผู้ใช้ลงทะเบียน iCloud จะได้พื้นที่ 5GB ไว้สำหรับเก็บข้อมูล ซึ่งสามารถใช้ในการสำรองและกู้คืนข้อมูลได้ในกรณีที่ย้ายไปใช้อุปกรณ์เครื่องใหม่ **[17]** ตัวอย่างข้อมูลที่เก็บอยู่ใน iCloud เช่น ภาพถ่ายและคลิปวิดีโอ SMS รหัสผ่าน การตั้งค่าอุปกรณ์ และข้อมูลในแอปพลิเคชันต่าง ๆ เป็นต้น **[18]** ผู้ใช้งานระบบปฏิบัติการ iOS สามารถตรวจสอบข้อมูลที่เก็บอยู่ใน iCloud ได้ด้วยการเข้าไปที่ Settings เลือกแท็บ iCloud ดังรูปที่ 5



รูปที่ 5 หน้าจอการตั้งค่า iCloud Backup

แน่นอนว่าหากผู้ไม่หวังดีสามารถดาวน์โหลดข้อมูล iCloud Backup ออกมาจากเซิร์ฟเวอร์ของ Apple ได้แล้ว ไม่ใช่แค่ภาพถ่ายหรือคลิปวิดีโอเท่านั้น แต่ข้อมูลอื่น ๆ ที่เป็นความลับก็อาจจะหลุดออกมาด้วย

ยิ่งไปกว่านั้น ถึงแม้ว่าผู้ใช้จะลบภาพที่ถ่ายไว้ออกไปจาก iCloud แล้วก็ตาม แต่ภาพที่ถูกลบไปแล้วก็ยังสามารถกู้กลับคืนมาได้อยู่ดี เพราะนักวิจัยจากบริษัท Check Point Software ได้วิเคราะห์ข้อมูลที่อยู่ใน iCloud Backup แล้วพบว่า ทุก ๆ อุปกรณ์ที่มีการส่งข้อมูลขึ้น iCloud จะเก็บข้อมูลสำรองไว้ 3 ชุด คือชุดล่าสุด 1 ชุด และชุดข้อมูลย้อนหลังอีก 2 ชุด ดังนั้นจึงทำให้ถึงแม้จะมีการลบภาพที่ถ่ายไว้ออกไปนานมากแล้ว แต่หากมีคนที่สามารถนำข้อมูลเก่าออกมาจาก iCloud Backup ได้ ก็จะสามารถกู้คืนไฟล์ที่ถูกลบไปแล้วได้ **[19]**

ถึงแม้ว่าทาง Apple จะตรวจสอบสาเหตุที่ภาพหลุดและยืนยันว่า iCloud กับ Find My iPhone ไม่ได้มีช่องโหว่ แต่ก็ได้แนะนำให้ผู้ใช้ตั้งรหัสผ่านให้คาดเดาได้ยาก และเปิดใช้งานระบบการยืนยันตัวตนแบบ 2 ขั้นตอน เพื่อเพิ่มความมั่นคงปลอดภัยในการล็อกอิน แต่ก็มีผู้กล่าวว่าต่อให้เปิดใช้งานระบบดังกล่าวนี้ ก็ไม่ได้ช่วยป้องกันข้อมูลที่เก็บอยู่ใน iCloud ได้แต่อย่างใด

การยืนยันตัวตนแบบ 2 ขั้นตอนคืออะไร

การยืนยันตัวตนแบบ 2 ขั้นตอน เป็นระบบที่ Apple พัฒนาขึ้นมาเพื่อเพิ่มความมั่นคงปลอดภัยให้กับการใช้งาน Apple ID โดยเมื่อเปิดใช้งานระบบนี้ ทุกครั้งที่ผู้ใช้ซื้อสินค้าจาก App Store หรือ iTunes จะมีการส่ง SMS เป็นตัวเลข 4 หลักมายังหมายเลขโทรศัพท์ที่ลงทะเบียนไว้ เพื่อใช้ในการยืนยันการจ่ายเงินอีกครั้งหนึ่ง **[20]**

อย่างไรก็ตาม ระบบการยืนยันตัวตนแบบ 2 ขั้นตอนนี้ ทาง Apple ไม่ได้เปิดใช้งานให้กับทุกบริการ มีเพียงแค่ 3 กรณีเท่านั้นที่ต้องใช้รหัสยืนยันจาก SMS คือ

- ล็อกอินเข้าจัดการข้อมูลใน My Apple ID **[21]**
- ซื้อสินค้าใน App Store, iTunes Store หรือ iBook Store จากอุปกรณ์เครื่องใหม่
- ติดต่อ Apple Support เพื่อขอความช่วยเหลือเรื่อง Apple ID

นอกเหนือจาก 3 กรณีข้างต้นนี้ ต่อให้ผู้ใช้งานตั้งค่าการยืนยันตัวตนแบบ 2 ขั้นตอนไว้ ก็ไม่ได้ถูกเรียกใช้งานอยู่ดี ยังสามารถใช้แค่รหัสผ่านก็เข้าถึงข้อมูลได้

ระบบสำคัญที่ Apple ไม่เปิดให้ใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอนคือการจัดการข้อมูลใน iCloud และ Find My Phone ซึ่งทำให้ผู้ไม่หวังดีที่แค่รู้ Apple ID และรหัสผ่านก็สามารถเข้าไปดาวน์โหลดรูปภาพหรือข้อมูลจาก iCloud ออกมาได้ **[22] [23]**

การใช้งาน iCloud มีความมั่นคงปลอดภัยมากน้อยแค่ไหน

คำถามของความมั่นคงปลอดภัยในการใช้งาน iCloud คือ ผู้ใช้จะแน่ใจได้อย่างไรว่าข้อมูลที่เก็บอยู่ใน iCloud นั้นมั่นคงปลอดภัยจริง และจะมีวิธีการใดบ้างในการป้องกันไม่ให้เกิดปัญหาแบบนี้ขึ้นกับตัวเอง

แม้ทาง Apple จะปฏิเสธว่าเหตุการณ์ภาพหลุดที่เกิดขึ้นนั้นไม่ได้เกิดจากช่องโหว่ของ iCloud หรือ Find My iPhone แต่ก็ปฏิเสธไม่ได้ว่าก่อนหน้านี้ระบบ Find My iPhone มีช่องโหว่ที่ทำให้ผู้ไม่หวังดีสามารถ Brute force รหัสผ่านได้จริง

ถึงแม้ในตอนนี้ Apple จะแก้ไขไม่ให้สามารถ Brute Force รหัสผ่าน iCloud ผ่าน Find My iPhone ไปแล้วก็ตาม แต่ก็ยังไม่สามารถยืนยันได้ว่าก่อนที่จะพบว่าระบบมีปัญหาและทำการแก้ไข มีผู้โชคร้ายคนไหนบ้างที่ถูกเดารหัสผ่านและสูญเสียข้อมูลไปแล้ว

อีกทั้งระบบการยืนยันตัวตนแบบ 2 ขั้นตอน ที่เปิดให้ใช้งานได้แค่เฉพาะบางบริการก็ทำให้เกิดคำถามว่าทำไม Apple ถึงไม่ทำให้เปิดใช้งานได้ทั้งหมด และกับบริการสำคัญอย่าง iCloud Backup หรือ Find My iPhone ที่ผู้ไม่หวังดีสามารถเข้าไปขโมยข้อมูลหรือสั่งทำลายข้อมูลในเครื่องของเหยื่อได้ ทำไม Apple ถึงไม่เปิดระบบการยืนยันตัวตนแบบ 2 ขั้นตอนให้กับบริการเหล่านี้ด้วย

คำแนะนำและข้อควรระวัง

ตั้งรหัสผ่านที่ยาวและคาดเดาได้ยาก

สำหรับผู้ที่ไม่แน่ใจว่ารหัสผ่าน iCloud ของตัวเองถูกขโมยไปหรือยัง ควรรีบเปลี่ยนรหัสผ่านใหม่โดยเร็วที่สุด การตั้งรหัสผ่านที่ยาวและคาดเดาได้ยาก จะช่วยให้การ Brute Force รหัสผ่านทำได้ยากขึ้น เพราะต้องใช้เวลานานกว่าจะเดารหัสผ่านได้ถูก รหัสผ่านที่ดีควรมีความยาวมากกว่า 8 ตัวอักษรขึ้นไป ไม่ควรใช้คำทั่วไปที่มีอยู่ในดิกชันนารีและควรใส่อักขระพิเศษหรือตัวเลขเพิ่มเข้าไปด้วย

ระวังในการใช้บริการเก็บข้อมูลบนอินเทอร์เน็ต

ปัจจุบันมีผู้ให้บริการหลายรายที่เปิดให้ผู้ใช้งานเก็บข้อมูลส่วนตัวไว้บนอินเทอร์เน็ต ไม่ว่าจะเป็นภาพถ่าย คลิปวิดีโอ หรือข้อมูลอื่น ๆ สิ่งหลัก ๆ ที่ควรระวังในการใช้งานบริการเหล่านี้คือ เมื่อเราปล่อยให้ข้อมูลออกไปอยู่นอกตัวเครื่อง สิ่งที่เป็นความลับก็จะไม่เป็นความลับอีกต่อไป วิธีป้องกันที่ง่ายที่สุดที่อาจฟังดูเหมือนกำปั้นทุบดินไปหน่อย คืออย่าถ่ายรูปลับ หรือนำสิ่งที่เป็นความลับไปเก็บไว้บนอินเทอร์เน็ต

ในบางกรณีเราก็อาจจะเผลอปล่อยรูปพวกนี้ขึ้นไปบนอินเทอร์เน็ตโดยไม่ตั้งใจ เพราะเกิดจากการตั้งค่าให้โปรแกรมอัปโหลดรูปขึ้นไปเก็บบนอินเทอร์เน็ตโดยอัตโนมัติ อีกทั้งการลบรูปในโทรศัพท์มือถือก็ไม่ได้หมายความว่ารูปที่เก็บอยู่ในอินเทอร์เน็ตจะมีการลบไปด้วยเสมอไป ในบางบริการ ถึงแม้จะลบรูปออกจากเครื่องไปแล้ว แต่ภาพในเซิร์ฟเวอร์ยังอยู่ หรือในบางบริการยังสามารถกู้คืนไฟล์ที่ถูกลบไปแล้วได้

ไม่เชื่อมต่อ WiFi ที่ไม่น่าเชื่อถือ

ไม่ควรเชื่อมต่อ WiFi ฟรี หรือ WiFi ที่ไม่แน่ใจเรื่องความมั่นคงปลอดภัย เพราะอาจมีผู้ไม่หวังดีเปิดโปรแกรมรอดักรับข้อมูลอยู่ได้

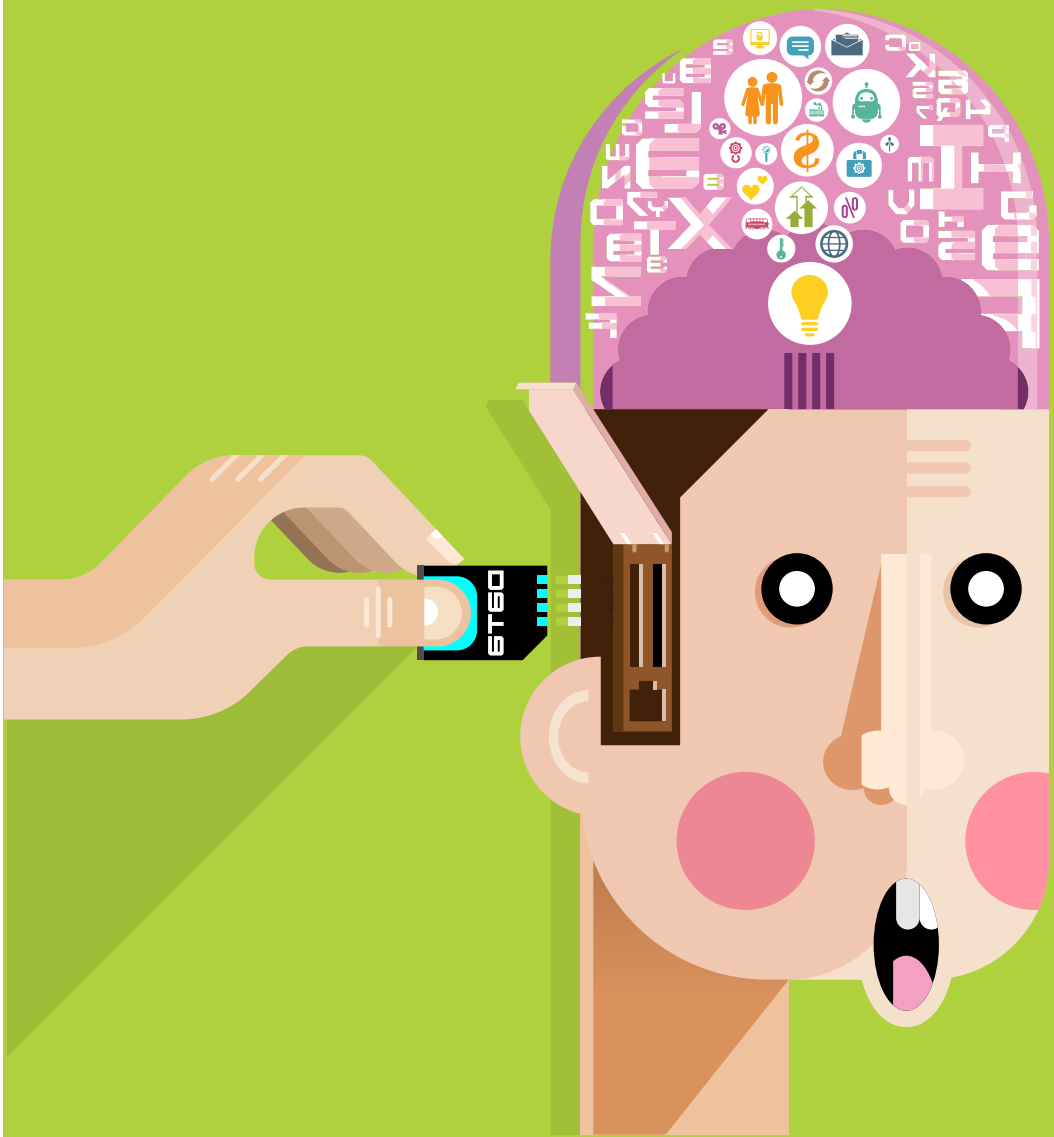
เปิดใช้การยืนยันตัวตนแบบ 2 ขั้นตอน

ถึงแม้ปัจจุบันนี้ทาง Apple ยังไม่เปิดใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอนให้กับระบบ iCloud แต่ก็ได้แจ้งว่าจะปรับปรุงความมั่นคงปลอดภัยของบริการ iCloud เช่น เปิดใช้งานระบบการยืนยันตัวตนแบบ 2 ขั้นตอน การแจ้งเตือนเมื่อมีการล็อกอินจากอุปกรณ์ใหม่ รวมทั้งการกู้คืนข้อมูลจาก iCloud Backup ด้วย โดยน่าจะปรับปรุงระบบแล้วเสร็จภายในเดือนกันยายนนี้ **[24]** ดังนั้นการเปิดใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอนก็เป็นสิ่งที่ควรทำไว้เพื่อที่จะได้พร้อมใช้งานในทันทีที่ Apple เปิดให้บริการ

หากยังไม่มั่นใจในการเก็บภาพไว้บน iCloud สามารถเปลี่ยนไปใช้ผู้ให้บริการรายอื่นที่มีระบบการยืนยันตัวตนแบบแบบ 2 ขั้นตอนได้ เช่น Google Drive, Dropbox, OneDrive เป็นต้น

อ้างอิง

1. https://www.apple.com/th/icloud/
2. http://support.apple.com/kb/PH2608?viewlocale=th_TH&locale=en_US
3. http://support.apple.com/kb/DL1455
4. http://support.apple.com/kb/PH2696?viewlocale=th_TH
5. http://itunes.apple.com/th/app/find-my-iphone/id376101648?mt=8
6. https://www.apple.com/th/icloud/find-my-iphone.html
7. http://www.theinquirer.net/inquirer/news/2346670/hackers-hijack-find-my-iphone-to-hold-ios-and-mac-users-to-ransom
8. http://threatpost.com/alleged-oleg-pliss-iphone-hackers-arrested-in-russia
9. http://www.engadget.com/2014/09/01/find-my-iphone-exploit/
10. https://github.com/hackappcom/ibrute
11. http://mashable.com/2014/08/31/celebrity-nude-photo-hack/
12. http://www.techworm.net/2014/09/apple-patches-icloud-security-gap-after.html
13. http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html
14. http://www.elcomsoft.com/eppb.html
15. http://www.wired.com/2014/09/eppb-icloud/
16. http://www.bbc.com/news/technology-29045789
17. https://www.apple.com/th/support/icloud/backup/
18. http://support.apple.com/kb/PH12519?viewlocale=th_TH&locale=th_TH
19. http://www.csoonline.com/article/2602386/data-protection/apple-icloud-backup-quirk-could-have-allowed-hackers-to-access-deleted-files.html
20. http://support.apple.com/kb/HT5570?viewlocale=th_TH
21. https://appleid.apple.com/th/account/home
22. http://techcrunch.com/2014/09/02/apples-two-factor-authentication-doesnt-protect-icloud-backups-or-photo-streams/
23. http://www.tuaw.com/2014/09/02/think-iclouds-two-factor-authentication-protects-your-privacy/
24. http://www.macrumors.com/2014/09/04/cook-security-alerts-icloud/


GT60

บทความเชิงเทคนิค

ข้อควรระวังในการใช้เครื่องมือตรวจพิสูจน์ **พยานหลักฐานดิจิทัลในการค้นหาคำหรือข้อความภาษาไทย**

ผู้เขียน : เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่ : 29 มีนาคม 2557
ปรับปรุงล่าสุด : 29 มีนาคม 2557

ในการตรวจพิสูจน์พยานหลักฐานดิจิทัล มีปัจจัยสำคัญหลายอย่างที่ต้องคำนึงและต้องคอยระมัดระวังเพื่อไม่ให้เกิดความผิดพลาด โดยเฉพาะอย่างยิ่ง การเลือกเครื่องมือที่เหมาะสมกับงาน การทำความเข้าใจถึงวิธีการใช้เครื่องมือที่ถูกต้อง การตรวจสอบความสามารถและข้อจำกัดของเครื่องมือ รวมถึงการตรวจทานเพิ่มเติมอีกครั้งเพื่อยืนยันว่าผลลัพธ์ที่ได้จากการใช้เครื่องมือนั้นถูกต้องจริง ๆ และนอกจากนี้หากจำเป็นต้องเลือกใช้เครื่องมือที่ผลิตจากต่างประเทศก็ต้องตรวจสอบว่าสามารถใช้งานร่วมกับระบบที่เป็นภาษาไทย ซึ่งอาจมีรูปแบบการทำงานที่เป็นลักษณะเฉพาะ ซึ่งหากเครื่องมือที่ใช้นั้นไม่รองรับการทำงานร่วมกับภาษาไทยอย่างเต็มที่หรือมีข้อจำกัดในบางกรณี ก็อาจทำให้ผลการตรวจพิสูจน์นั้นไม่ถูกต้องหรือไม่ครอบคลุมในสิ่งที่ต้องการค้นหาได้

ปัญหาอย่างหนึ่งของการใช้เครื่องมือตรวจพิสูจน์พยานหลักฐานดิจิทัลในการค้นหาคำหรือข้อความที่เป็นภาษาไทย คือเรื่องของ Character Set เนื่องจากมาตรฐานการเก็บข้อมูลอักขระภาษาไทยนั้นมีอยู่ด้วยกันหลายรูปแบบ ในกรณีที่ต้องการตรวจสอบว่ามีข้อความภาษาไทยที่เราต้องการค้นหาอยู่ในไฟล์ที่กำหนดหรือไม่ ถ้าหากเลือก Character Set ผิด ผลการค้นหาก็อาจกลายเป็นว่าไม่พบข้อความที่ต้องการอยู่ในไฟล์ดังกล่าวได้ทั้งที่จริง ๆ แล้วข้อความนั้นมีอยู่

Character Set คืออะไร

ก่อนจะไปพูดถึง Character Set ขอเล่าถึงที่มาและรูปแบบการเก็บข้อมูลในคอมพิวเตอร์กันสักนิด เราคงทราบกันดีกว่าคอมพิวเตอร์เก็บข้อมูลในรูปแบบดิจิทัลโดยใช้แค่ตัวเลข 0 กับ 1 ตัวเลขหนึ่งตัวเรียกว่า 1 bit ถ้ามีตัวเลขแปดตัว (8 bit) เรียกว่า 1 byte

เนื่องจากว่าการรับส่งข้อมูลในคอมพิวเตอร์โดยแท้จริงแล้วเป็นแค่การรับส่งตัวเลข 0 กับ 1 ดังนั้นถ้าจะส่งข้อมูลที่เป็นตัวอักษร ก็จำเป็นต้องมีการสร้างรหัสขึ้นมาเพื่อใช้อ้างอิงว่าตัวเลขชุดนี้แทนตัวอักษรอะไร ซึ่งถ้าหากจะเปรียบเทียบให้เห็นภาพในสิ่งที่คล้าย ๆ กันก็ลองเปรียบเทียบกับรหัสมอร์สที่ใช้การเคาะจังหวะสั้นกับยาวเพื่อใช้ในการส่งข้อความ

ASCII เป็นรหัสที่ทางอเมริกากำหนดขึ้นมาเพื่อใช้ในการแลกเปลี่ยนข้อมูล โดยในรหัส ASCII ประกอบด้วย ตัวอักษรภาษาอังกฤษ (แบบ Latin) ตัวเลขอารบิก เครื่องหมาย วรรคตอน และสัญลักษณ์ต่าง ๆ โดยมีตารางแอสกี (ASCII table) หรือชุดอักขระแอสกี (ASCII character set) มาใช้ในการอ้างอิงว่ารหัสนี้แทนตัวอักษรอะไร เช่น ตัว A ในภาษาอังกฤษ แทนด้วย 65 ในเลขฐานสิบ (Decimal) หรือ 41 ในเลขฐานสิบหก (Hexadecimal) เป็นต้น **[1]** ตัวอย่างตารางแอสกีเป็นดังรูปที่ 1

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

รูปที่ 1 ตัวอย่างตารางแอสกี (ที่มา: ASCII Set [2])

เนื่องจากอักขระ (Character) ในภาษาอังกฤษ (ตัวเลข+ตัวอักษร+เครื่องหมาย+อักขระพิเศษอื่น ๆ) รวมกันแล้วมีประมาณร้อยกว่าตัว จึงสามารถใช้รหัส ASCII แบบ 7 bit ที่สามารถเก็บข้อมูลได้ 128 รูปแบบ (2^7 = 128) มาใช้ในการเก็บตัวอักษรและอักขระพิเศษทั้งหมดได้ในรหัสตั้งแต่ 0 - 127

ต่อมาได้มีการปรับปรุงรหัส ASCII ให้เป็นแบบ 8 bit เพื่อให้เก็บอักขระภาษาอื่น ๆ เพิ่มได้อีก 128 ตัว (2^8 = 256) โดยอักขระของภาษาอื่น ๆ จะมีการเก็บอยู่ในส่วน 128 ช่องที่เพิ่มเข้ามา (รหัสตั้งแต่ 128-255) ส่วนที่เพิ่มขึ้นมานี้เรียกว่า Extended ASCII ดังตัวอย่างในรูปที่ 2

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	∑
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	ø
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	₧	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

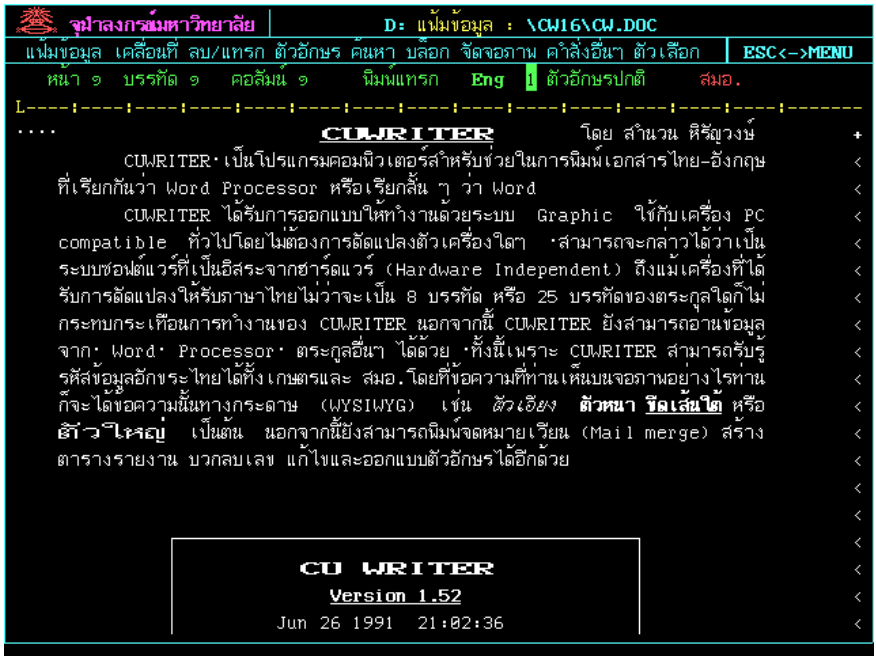
รูปที่ 2 ตัวอย่างตาราง Extended ASCII (ที่มา: ASCII Set [2])

ผังตาราง ASCII แบบ 8 bit จะแตกต่างกันไปตามแต่ละภาษา โดยในส่วน 128 bit แรก ส่วนใหญ่จะยังคงเป็นเหมือนกันหมด แต่ส่วน 128 bit หลังจะเพิ่มอักขระของภาษาตัวเองเข้ามา ผังตารางอักขระที่แตกต่างกันไปในแต่ละภาษานี้เรียกว่า Code Page (หรือ Character Encoding) **[3]** อย่างไรก็ตาม เนื่องจากในสมัยก่อน Code Page ของบางภาษายังไม่มีมาตรฐานที่ชัดเจน หรืออาจมีมาตรฐานอยู่แล้ว แต่ผู้ผลิตซอฟต์แวร์ไม่ยอมทำตาม ไปสร้าง Code Page ของตัวเองขึ้นมาใช้เอง ทำให้ในบางภาษามีหลาย Code Page ซึ่งอาจทำให้มีปัญหาเวลานำไปใช้อ้างอิง เพราะถ้าเลือก Code Page ผิด ข้อมูลที่อ่านได้จะไม่ตรงกัน **[4]**

ANSI เป็นรูปแบบหนึ่งของ Extended ASCII โดยทั่วไปใช้สำหรับอ้างอิงอักขระภาษาอังกฤษ อย่างไรก็ตาม การอ้างอิงรหัสอักขระในแบบ ANSI นั้นยังไม่มีมาตรฐานที่แน่นอน โดยหลัก ๆ แล้ว 128 bit แรกจะยังคงเหมือนกับตารางมาตรฐาน ASCII แต่ส่วน 128 bit หลังนั้นอาจแตกต่างกันไปตามแต่ละซอฟต์แวร์ ขึ้นอยู่กับว่าจะอ้างอิงมาตรฐานอะไร **[5]**

มาตรฐานรหัสภาษาไทย

ในสมัยก่อนคอมพิวเตอร์ยังไม่รองรับภาษาไทย และยังไม่มีการกำหนดมาตรฐานรหัสภาษาไทยอย่างเป็นทางการ ผู้ผลิตซอฟต์แวร์แต่ละเจ้าจึงทำมาตรฐานภาษาไทยของตัวเองขึ้นมาใช้ ซึ่งโดยหลัก ๆ ก็อ้างอิงพื้นฐานมาจากตาราง ASCII แบบ 7 bit โดยใช้พื้นที่ 128 ช่องที่เหลือในการเก็บอักขระภาษาไทย ตัวอย่างรหัสภาษาไทยที่เคยมีการใช้งานในสมัยก่อน เช่น รหัสเกษตรฯ **[6]** รหัส สมอ. **[7]** รหัส MacThai **[8]** เป็นต้น ตัวอย่างโปรแกรม CU Writer ที่ใช้มาตรฐานรหัสภาษาไทยสมัยเก่าเป็นดังรูปที่ 3



รูปที่ 3 ตัวอย่างโปรแกรม CU Writer
ที่ใช้มาตรฐานรหัสภาษาไทยสมัยเก่า (ที่มา: Wikipedia [9])

ในส่วนของรายละเอียดมาตรฐานรหัสภาษาไทยที่เคยมีการใช้งานในสมัยก่อน ปัจจุบันนี้อาจหาได้ยากเต็มที เพราะบางรหัสไม่มีการเปิดเผยข้อมูลทางเทคนิคออกสู่สาธารณะ หรือบางรหัสไม่ได้รับความนิยมและไม่มีการเก็บข้อมูลรายละเอียดในส่วนนี้เอาไว้

ภายหลังจากที่มีการพัฒนามาตรฐานรหัสภาษาไทยอย่างเป็นทางการขึ้นมา มาตรฐานรหัสภาษาไทยสมัยเก่าที่ผู้ผลิตซอฟต์แวร์พัฒนาขึ้นมาเองก็เริ่มเสื่อมความนิยมและไม่ได้รับการใช้งานในที่สุด ปัจจุบันมาตรฐานรหัสภาษาไทยที่ยังคงมีการใช้งานอยู่โดยหลัก ๆ มีอยู่ 3 แบบ คือ TIS-620, Windows-874 และ Unicode

TIS-620

รหัส มอก.620 หรือ รหัส สมอ. เป็นมาตรฐานรหัสตัวอักษรภาษาไทยที่กำหนดโดยสำนักงานมาตรฐานอุตสาหกรรม (สมอ.) โดยพัฒนาเพิ่มเติมจากมาตรฐาน ISO-646-1983 และ IBM GX20-1850-4 ซึ่งเป็นรหัสที่ใกล้เคียงกับ ASCII แบบ 7 bit **[10] [11]** มาตรฐาน TIS-620 ออกมาครั้งแรกในปี พ.ศ. 2529 และมีการปรับปรุงเพิ่มเติมอีกครั้งหนึ่งในปี พ.ศ. 2533 ตัวอย่างตาราง TIS-620 เป็นดังรูปที่ 4

HEX DIGITS 1ST → 2ND ↓	0-	1-	2-	3-	4-	5-	6-	7-	8-	9-	A-	B-	C-	D-	E-	F-
-0			๐	0	@	P	`	p				ฐ	ภ	ะ	เ	๐
-1			!	1	A	Q	a	q			ก	ฑ	ม	ั	แ	๑
-2			"	2	B	R	b	r			ข	ฒ	ย	า	โ	๒
-3			#	3	C	S	c	s			ฃ	ณ	ร	ำ	ใ	๓
-4			$	4	D	T	d	t			ค	ด	ฤ	ิ	ไ	๔
-5			%	5	E	U	e	u			ฅ	ต	ล	ี	ๅ	๕
-6			&	6	F	V	f	v			ฆ	ถ	ฦ	ึ	ๆ	๖
-7			'	7	G	W	g	w			ง	ท	ว	ื	็	๗
-8			(	8	H	X	h	x			จ	ธ	ศ	ุ	่	๘
-9			)	9	I	Y	i	y			ฉ	น	ษ	ู	้	๙
-A			*	:	J	Z	j	z			ช	บ	ส	ฺ	๊	ฯ
-B			+	;	K	[	k	{			ซ	ป	ห		๋	๏
-C			,	<	L	\	l	|		ฌ	ผ	ฬ		์	
-D			-	=	M	]	m	}			ญ	ฝ	อ		ํ	
-E			.	>	N	^	n	~			ฎ	พ	ฮ		๎	
-F			/	?	O	_	o				ฏ	ฟ	ฯ	๏	๏	

รูปที่ 4 ตัวอย่างตาราง TIS-620 (ที่มา: IBM [12])

ต่อมามีการพัฒนามาตรฐาน TIS-620 เพิ่มเติมเพื่อให้ได้รับการยอมรับในระดับสากล จนได้รับการประกาศให้เป็นมาตรฐาน ISO-8859-11 ในปี พ.ศ. 2544 โดยรูปแบบแล้ว Character Set ของ TIS-620 กับ ISO-8859-11 มีความใกล้เคียงกันมาก มีความแตกต่างกันอยู่บ้างในบางจุดเท่านั้น **[13] [14] [15]**

Windows-874

Microsoft นำเอามาตรฐาน TIS-620 มาพัฒนาต่อ เพื่อใช้เป็นรูปแบบตัวอักษรภาษาไทยสำหรับการแลกเปลี่ยนข้อมูลในระบบปฏิบัติการ Windows เนื่องจากตัวมาตรฐาน Windows-874 นั้นได้รับการพัฒนาขึ้นมาโดยใช้พื้นฐานจาก TIS-620 จึงทำให้มีความเข้ากันได้กับไฟล์ที่บันทึกมาในมาตรฐาน TIS-620 แต่เนื่องจากว่าใน Windows-874 นั้นมีอักขระบางอย่างที่ใส่เพิ่มขึ้นมาภายหลังซึ่งไม่มีใน TIS-620 จึงอาจก่อให้เกิดปัญหาในกรณีที่บันทึกไฟล์โดยใช้มาตรฐาน Windows-874 แต่ไปเปิดอ่านโดยใช้มาตรฐาน TIS-620 **[16]**

Windows-874 มีชื่ออื่น ๆ ว่า CP874, MS874, x-windows-874 และ x-IBM874 อย่างไรก็ตาม เนื่องจากว่า Windows-874 นั้นไม่ได้รับการยอมรับให้เป็นมาตรฐานสากล จึงทำให้บางโปรแกรมหรือบางระบบปฏิบัติการไม่รองรับมาตรฐานนี้ ตัวอย่างตาราง Windows-874 เป็นดังรูปที่ 5

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	NUL 0000	STX 0001	SOT 0002	ETX 0003	EOT 0004	ENQ 0005	ACK 0006	BEL 0007	BS 0008	HT 0009	LF 000A	VT 000B	FF 000C	CR 000D	SO 000E	SI 000F
10	DLE 0010	DC1 0011	DC2 0012	DC3 0013	DC4 0014	NAK 0015	SYN 0016	ETB 0017	CAN 0018	EM 0019	SUB 001A	ESC 001B	FS 001C	GS 001D	RS 001E	US 001F
20	SP 0020	! 0021	" 0022	# 0023	$ 0024	% 0025	& 0026	' 0027	(0028	) 0029	* 002A	+ 002B	, 002C	- 002D	. 002E	/ 002F
30	0 0030	1 0031	2 0032	3 0033	4 0034	5 0035	6 0036	7 0037	8 0038	9 0039	: 003A	; 003B	< 003C	= 003D	> 003E	? 003F
40	@ 0040	A 0041	B 0042	C 0043	D 0044	E 0045	F 0046	G 0047	H 0048	I 0049	J 004A	K 004B	L 004C	M 004D	N 004E	O 004F
50	P 0050	Q 0051	R 0052	S 0053	T 0054	U 0055	V 0056	W 0057	X 0058	Y 0059	Z 005A	[005B	\ 005C	] 005D	^ 005E	_ 005F
60	` 0060	a 0061	b 0062	c 0063	d 0064	e 0065	f 0066	g 0067	h 0068	i 0069	j 006A	k 006B	l 006C	m 006D	n 006E	o 006F
70	p 0070	q 0071	r 0072	s 0073	t 0074	u 0075	v 0076	w 0077	x 0078	y 0079	z 007A	{ 007B	| 007C	} 007D	~ 007E	DEL 007F
80	€ 20AC					… 2026										
90		' 2018	' 2019	" 201C	" 201D	• 2022	– 2013	— 2014								
A0	NBSP 00A0	ก 0E01	ข 0E02	ฃ 0E03	ค 0E04	ฅ 0E05	ฆ 0E06	ง 0E07	จ 0E08	ฉ 0E09	ช 0E0A	ซ 0E0B	ฌ 0E0C	ญ 0E0D	ฎ 0E0E	ฏ 0E0F
B0	ฐ 0E10	ฑ 0E11	ฒ 0E12	ณ 0E13	ด 0E14	ต 0E15	ถ 0E16	ท 0E17	ธ 0E18	น 0E19	บ 0E1A	ป 0E1B	ผ 0E1C	ฝ 0E1D	พ 0E1E	ฟ 0E1F
C0	ภ 0E20	ม 0E21	ย 0E22	ร 0E23	ฤ 0E24	ล 0E25	ฦ 0E26	ว 0E27	ศ 0E28	ษ 0E29	ส 0E2A	ห 0E2B	ฬ 0E2C	อ 0E2D	ฮ 0E2E	ฯ 0E2F
D0	ะ 0E30	ั 0E31	า 0E32	ำ 0E33	ิ 0E34	ี 0E35	ึ 0E36	ื 0E37	ุ 0E38	ู 0E39	ฺ 0E3A					฿ 0E3F
E0	เ 0E40	แ 0E41	โ 0E42	ใ 0E43	ไ 0E44	ๅ 0E45	ๆ 0E46	็ 0E47	่ 0E48	้ 0E49	๊ 0E4A	๋ 0E4B	์ 0E4C	ํ 0E4D	๎ 0E4E	๏ 0E4F
F0	๐ 0E50	๑ 0E51	๒ 0E52	๓ 0E53	๔ 0E54	๕ 0E55	๖ 0E56	๗ 0E57	๘ 0E58	๙ 0E59	๚ 0E5A	๛ 0E5B				

รูปที่ 5 ตัวอย่างตาราง Windows-874
(ที่มา: Microsoft [17])

Unicode

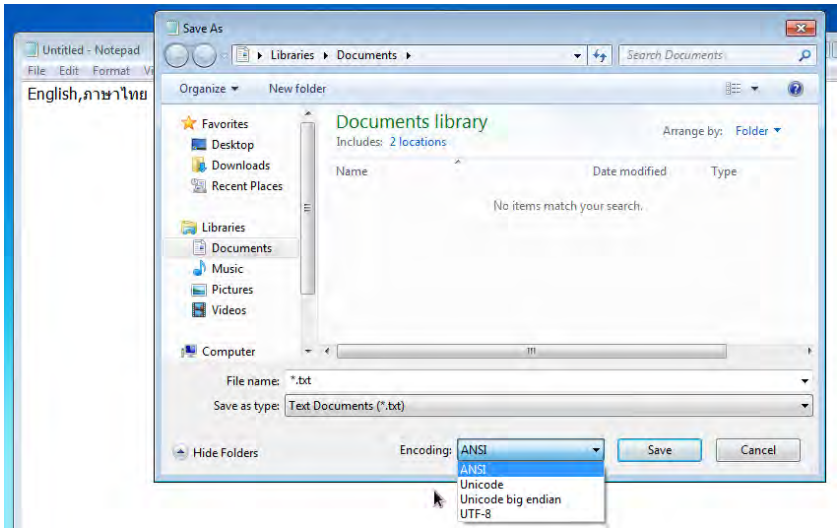
เนื่องจากว่า Character Set ของ ASCII แบบ 8 bit ใช้ 1 byte ต่อ 1 ตัวอักษร ทั้งภาษาอังกฤษและภาษาอื่น ๆ และสามารถเก็บอักขระได้สูงสุดแค่ 256 ตัว การเก็บข้อมูลในลักษณะนี้จึงทำให้หนึ่ง Character Set เก็บได้มากสุดแค่ 2 ภาษา (128 bit แรกเป็นภาษาอังกฤษ 128 bit หลังเป็นภาษาอื่น ๆ) เนื่องจากข้อจำกัดของการอ้างอิง Character Set ด้วยวิธีนี้ จึงทำให้ไม่สามารถใช้งานกับระบบที่ต้องรองรับหลาย ๆ ภาษาพร้อมกันได้

จากปัญหาดังกล่าว จึงได้มีการพัฒนามาตรฐาน Unicode ขึ้นมา เพื่อกำหนดให้เป็นรหัสภาษาที่ใช้ได้ครอบคลุมภาษาส่วนใหญ่บนโลก โดยสร้างตารางที่รวบรวมอักขระของแต่ละภาษา และกำหนดหมายเลขเฉพาะให้กับอักขระนั้น ๆ **[18]** ทำให้โปรแกรมเดียวสามารถแสดงผลหลาย ๆ ภาษาพร้อมกันได้ ปัจจุบันระบบปฏิบัติการ เบราว์เซอร์ ซอฟต์แวร์สมัยใหม่ รวมถึงการแลกเปลี่ยนข้อมูลผ่านอินเทอร์เน็ต ต่างก็รองรับมาตรฐาน Unicode ด้วยกันทั้งสิ้น

มาตรฐาน Unicode เวอร์ชัน 1.0.0 ออกมาในปี พ.ศ. 2534 รองรับ 24 Character Set ครอบคลุมอักขระทั้งหมด 7,161 รูปแบบ ภายหลังได้รับการปรับปรุงเพิ่มเติมเรื่อย ๆ จนกระทั่งเวอร์ชันล่าสุดคือ 6.3.0 ที่ออกมาในปี พ.ศ. 2556 รองรับ 93 Character Set ครอบคลุมอักขระทั้งหมด 110,187 รูปแบบ **[19] [20]** และในอนาคต มาตรฐาน Unicode 7.0.0 ที่จะออกในช่วงกลางปี พ.ศ. 2557 ก็จะรองรับอักขระต่าง ๆ เพิ่มขึ้นอีกกว่า 3,000 รูปแบบ **[21]** Unicode มีวิธีการ Encode รหัสตัวอักษรอยู่ 2 แบบคือ Unicode Transformation Format (UTF) และ Universal Character Set (UCS) แต่ในปัจจุบันนิยมใช้กันอยู่หลักๆ 2 รูปแบบคือ UTF-8 และ UTF-16

UTF-8 เป็น Encoding ที่นิยมใช้มากที่สุด โดยเฉพาะอย่างยิ่งการใช้เป็น Character Encoding ในการรับส่งข้อมูลผ่านอินเทอร์เน็ต โดยส่วนใหญ่เว็บไซต์หรือโปรแกรมรับส่งอีเมลในปัจจุบันต่างก็ใช้ UTF-8 เป็นค่าเริ่มต้น **[22]** ระบบปฏิบัติการตระกูล Unix หรือ Linux เวอร์ชันใหม่ ๆ ส่วนใหญ่ใช้ UTF-8 ในการรับส่งข้อมูลระหว่างโปรแกรม ตั้งชื่อไฟล์ หรือใช้เก็บข้อมูลการตั้งค่าการทำงานอื่น ๆ **[23]** การเก็บข้อมูลในรูปแบบ UTF-8 ในส่วนที่เป็นภาษาอังกฤษยังคงใช้ 8 bit เหมือนกับ ASCII แต่สำหรับอักขระในภาษาอื่น ๆ นั้นอาจเป็นไปได้ตั้งแต่ 16 bit ถึง 32 bit อักขระภาษาไทยใน UTF-8 ใช้ 24 bit **[24]**

UTF-16 เป็น Encoding หลักที่ใช้ใน Windows (ตั้งแต่ Windows 2000 เป็นต้นไป) โปรแกรมต่าง ๆ ที่ทำงานบน Windows เมื่อบันทึกข้อมูลเป็น Unicode จะใช้ Encoding แบบ UTF-16 **[25]** การเก็บข้อมูลในรูปแบบ UTF-16 จะใช้ 16 bit ต่อการเก็บข้อมูล 1 อักขระ (ในบางภาษาอาจใช้ 32 bit ในการเก็บ 1 อักขระ) อักขระภาษาไทยใน UTF-16 ใช้ 16 bit **[26]** ตัวอย่าง Encoding ที่โปรแกรม Notepad รองรับ เป็นดังรูปที่ 6



รูปที่ 6 ตัวอย่าง Encoding ที่โปรแกรม Notepad รองรับ

Unicode ต่างจาก ASCII ตรงที่ไม่ได้มีการกำหนดจำนวน bit ตายตัวว่าแต่ละอักขระจะใช้พื้นที่เท่าไหร่ในการเก็บข้อมูล แต่จะดูที่ค่า Hexadecimal ว่าอักขระนี้ใช้พื้นที่กี่ byte เช่น ใน UTF-8 ถ้าโค้ดที่มีค่า Hex ระหว่าง 000000 ถึง 00007F จะใช้ 1 byte แต่ถ้ามีค่า Hex ระหว่าง 000800 ถึง 003FFF จะใช้ 3 byte ในการเก็บข้อมูล ดังรูปที่ 7

<table>
<tr><th>Code range (hexadecimal)</th><th>UTF-8</th><th>UTF-16</th><th>UTF-32</th><th>UTF-EBCDIC</th><th>GB 18030</th></tr>
<tr><td>000000 – 00007F</td><td>1</td><td rowspan="6">2</td><td rowspan="8">4</td><td rowspan="2">1</td><td>1</td></tr>
<tr><td>000080 – 00009F</td><td rowspan="3">2</td><td rowspan="5">2 for characters inherited from GB 2312/GBK (e.g. most Chinese characters) 4 for everything else.</td></tr>
<tr><td>0000A0 – 0003FF</td><td>2</td></tr>
<tr><td>000400 – 0007FF</td><td rowspan="2">3</td><td rowspan="2">3</td></tr>
<tr><td>000800 – 003FFF</td></tr>
<tr><td>004000 – 00FFFF</td><td rowspan="2">4</td></tr>
<tr><td>010000 – 03FFFF</td><td rowspan="2">4</td><td rowspan="2">4</td><td rowspan="2">4</td></tr>
<tr><td>040000 – 10FFFF</td><td>5</td></tr>
</table>

รูปที่ 7 จำนวน byte ต่อโค้ดที่ใช้ในการเก็บข้อมูลในรูปแบบ Unicode (ที่มา: Wikipedia [27])

ปัญหา Character Encoding กับข้อความภาษาไทย

เนื่องจากมาตรฐาน Character Encoding ภาษาไทยนั้นมีอยู่หลายแบบ อีกทั้งระบบปฏิบัติการ หรือโปรแกรมแต่ละตัวก็อาจใช้ Character Encoding ที่แตกต่างกัน ทำให้เมื่อนำไฟล์ที่บันทึกโดยใช้ Character Encoding ที่โปรแกรมปลายทางไม่รองรับมาเปิดดูข้อมูล ก็จะพบว่าเป็นข้อมูลที่อ่านไม่ออก หรือที่เราเรียกกันว่าเป็นตัวหนังสือภาษาต่างดาว

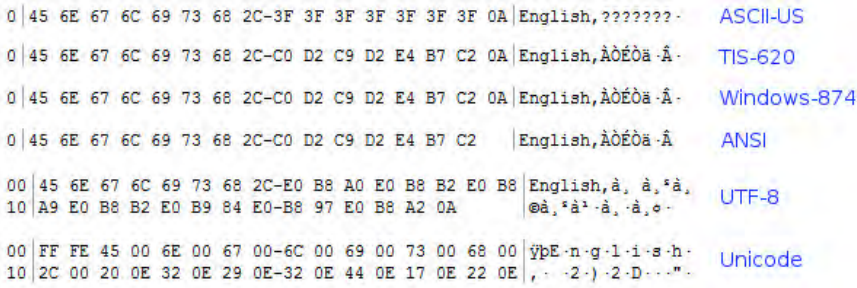
เนื่องจาก Character Encoding ภาษาไทยที่ใช้ในสมัยก่อน บางรูปแบบไม่ได้รับความนิยมแล้ว ทำให้โปรแกรมสมัยใหม่หลายตัวไม่รองรับ ส่วน Character Encoding ภาษาไทยที่ยังมีการใช้งานอยู่ สามารถใช้ไลบรารี libiconv ของ GNU [28] แปลงไปมาระหว่าง ISO-8859-11, TIS-620, CP874, MacThai และ Unicode ได้ อย่างไรก็ตาม ปัจจุบันพบว่าโปรแกรมสมัยใหม่หลายตัวไม่รองรับ Character Encoding แบบอื่นแล้วนอกจาก Unicode

การตรวจพิสูจน์พยานหลักฐานดิจิทัลกับการค้นหาข้อความภาษาไทย

ในกรณีที่ต้องตรวจพิสูจน์พยานหลักฐานดิจิทัลเพื่อค้นหาว่ามีไฟล์ที่มีข้อความภาษาไทยตาม Keyword ที่ต้องการอยู่ในพยานหลักฐานหรือเปล่า การเลือก Code Page ให้ถูกต้องเป็นสิ่งที่จำเป็น เพราะหากเลือก Code Page ผิด อาจทำให้ผลการค้นหาไม่เจอไฟล์ที่มีเนื้อหาตรงกับ Keyword ทั้งที่จริง ๆ แล้วมีไฟล์ดังกล่าวอยู่ในพยานหลักฐาน

สำหรับไฟล์ที่มีรูปแบบแน่นอนว่าใช้ Code Page แบบไหน ก็ไม่น่าจะมีปัญหาในการค้นหาข้อความที่เป็นภาษาไทยที่อยู่ข้างในไฟล์นั้น แต่หากเป็นไฟล์ที่ไม่มีการกำหนด Code Page (เช่น ไฟล์ข้อความ) เครื่องมือตรวจพิสูจน์พยานหลักฐานอาจไม่สามารถตัดสินใจได้ว่าไฟล์นั้นใช้ Code Page แบบไหน จึงอาจเลือกอ่านไฟล์ดังกล่าวโดยใช้ Code Page มาตรฐาน (เช่น UTF-8) ซึ่งนั่นอาจทำให้ไฟล์ข้อความที่มีการ Encode โดยใช้รูปแบบรหัสภาษาไทยแบบเก่า เช่น TIS-620 หรือ Windows-874 ไม่สามารถอ่านออกเป็นข้อความภาษาไทยได้ และทำให้ค้นหาข้อความที่ต้องการในไฟล์ไม่เจอ

การทดสอบสร้างไฟล์ข้อความที่มีคำว่า “English,ภาษาไทย” บันทึกโดยใช้ Encoding ที่แตกต่างกันคือ ASCII (US), ANSI, TIS-620, Windows-874, UTF-8 และ Unicode เมื่อนำไฟล์ที่ได้มาเปิดดูข้อมูลในรูปแบบ Hexadecimal จะเห็นข้อมูลดังรูปที่ 8

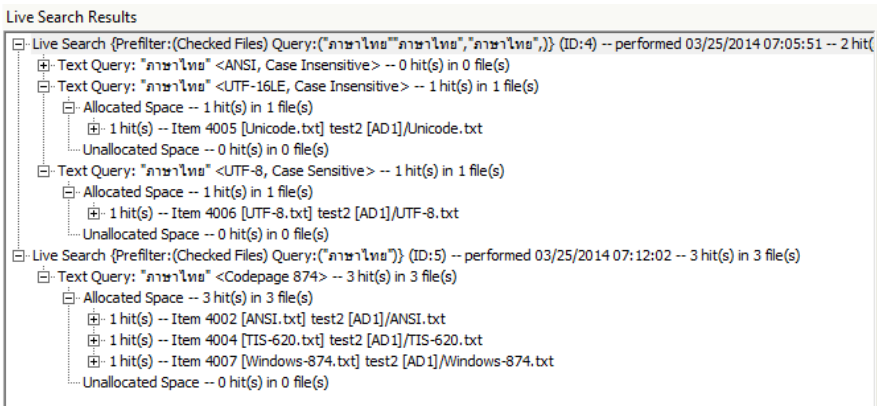


รูปที่ 8 เปรียบเทียบผลลัพธ์ที่ได้จากการ Encode ข้อความภาษาไทย โดยใช้ Character Set แบบต่างๆ

จากรูปจะเห็นว่าส่วนที่เป็นอักขระภาษาอังกฤษ ทั้ง ASCII (US), TIS-620, Windows-874, ANSI และ UTF-8 จะใช้ค่าเดียวกัน ส่วน Unicode แบบ UTF-16 byte แต่ byte ที่สองจะเป็น 00 เนื่องจาก UTF-16 ใช้ 2 byte (16 bit) ต่อการเก็บอักขระหนึ่งตัว (หมายเหตุ: ค่า FFFE ที่เห็นในส่วน Header ของ Unicode เป็นตัวบอกว่าเก็บข้อมูลแบบ Big-endian หรือ Litttle-endian ถ้าเป็น FFFE คือ Little-endian)

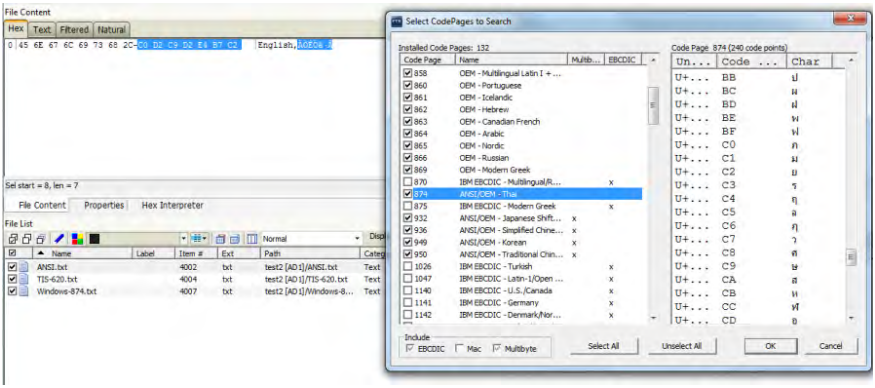
ส่วนการเก็บอักขระที่เป็นภาษาไทย เนื่องจาก ASCII (US) ไม่รองรับภาษาไทย เมื่อบันทึกข้อมูลโดยใช้ Encoding แบบนี้จึงเป็นอักขระที่อ่านไม่ได้ และจากรูปจะเห็นว่า Encoding อักขระภาษาไทยของ TIS-620, Windows-874 และ ANSI เป็นค่าเดียวกัน (หมายเหตุ: ค่า 0A เป็นอักขระจบบรรทัด ซึ่งอาจมีหรือไม่มีก็ได้) ส่วน Encoding แบบ UTF-8 และ UTF-16 เก็บข้อมูลอักขระภาษาไทยเป็นคนละค่ากัน

การทดลองใช้โปรแกรม FTK ค้นหาข้อความภาษาไทยโดยเลือกวิธีการค้นหาแบบ Live Search ซึ่งเป็นการค้นหา String ที่มีข้อความตรงกับ Keyword ที่กำหนดในคำว่า “ภาษาไทย” โดยเลือกรูปแบบข้อความเป็น ANSI, Unicode (UTF-8 และ UTF-16 little-endian) ผลลัพธ์ที่ได้คือพบไฟล์ที่มีข้อความตรงกับ Keyword ทั้งหมด 2 ไฟล์ คือ ไฟล์ที่ Encode แบบ UTF-8 และ UTF-16 ในขณะที่ไฟล์ที่ Encode โดยใช้ ANSI กลับไม่อยู่ในรายชื่อไฟล์ที่มีข้อความตรงกับ Keyword ในขณะที่เมื่อเปลี่ยนไปค้นหาโดยใช้ Encoding แบบ TIS-620 และ Windows-874 ผลที่ได้คือไฟล์ที่ Encode แบบ TIS-620, Windows-874 และ ANSI โดยไฟล์ที่ Encode แบบ UTF-8 และ UTF-16 ไม่ปรากฏในหน้าผลลัพธ์การค้นหา ดังรูปที่ 9



รูปที่ 9 ผลการค้นหาแบบ Live Search

เนื่องจากการ Search ของโปรแกรม FTK จะใช้วิธีนำ Keyword ไป Encoding ตาม Character Set ที่เราเลือก เช่น เมื่อนำคำว่า “ภาษาไทย” ไป Encode โดยใช้ Character Set แบบ Windows-874 จะได้ค่า Hexadecimal คือ C0D2C9D2E4B7C2 ซึ่งหลังจากนั้นโปรแกรมจะนำค่าที่ได้ไปเปรียบเทียบกับข้อมูลที่อยู่ในพยานหลักฐานอีกทีหนึ่ง ดังตัวอย่างในรูปที่ 10



รูปที่ 10 ตัวอย่างการค้นหาคำว่า “ภาษาไทย” ในไฟล์ที่ Encode โดยใช้ Character Set แบบ Windows-874

อีกหนึ่งปัญหาที่พบ คือถึงแม้จะเลือกให้ค้นหาข้อความที่ Encode แบบ ANSI แล้วก็ตาม แต่ผลการค้นหากลับไม่พบข้อความในไฟล์ดังกล่าว สาเหตุหลัก ๆ ของปัญหานี้เกิดจากการที่ Encoding แบบ ANSI นั้นไม่มีมาตรฐานที่ชัดเจน ทำให้บางครั้งการบันทึกไฟล์แบบ ANSI จะไปอ้างอิง Code Page จากข้อมูลการตั้งค่า Region ของระบบปฏิบัติการ **[29]** แต่เมื่อ Search กลับไปอ้างอิง Code Page อื่น จึงทำให้อ่านข้อมูลไม่ถูกต้อง ซึ่งจากการทดลองพบว่าเมื่อบันทึกไฟล์โดยใช้ Encoding แบบ ANSI ระบบจะบันทึกโดยใช้ Encoding รหัส 874 แต่โปรแกรม FTK ค้นหาข้อความโดยใช้ Encoding รหัสอื่น (โดยปกติ Microsoft เลือกใช้ Code Page 1252 เป็นค่าเริ่มต้นของ ANSI ใน Windows **[30]**) จึงทำให้ค้นหาข้อมูลไม่พบ

สรุป

เนื่องจากมาตรฐานการเข้ารหัสข้อความอักขระภาษาไทยนั้นมีอยู่หลายรูปแบบ ดังนั้นในการตรวจพิสูจน์พยานหลักฐานที่ต้องการใช้เครื่องมือค้นหาคำหรือข้อความที่เป็นภาษาไทย จำเป็นต้องตรวจสอบการตั้งค่า Code Page ที่สอดคล้องกันด้วย เพราะว่าหากเลือกการตั้งค่าผิด ก็อาจทำให้เกิดข้อผิดพลาดในผลการตรวจสอบพิสูจน์ได้

อ้างอิง

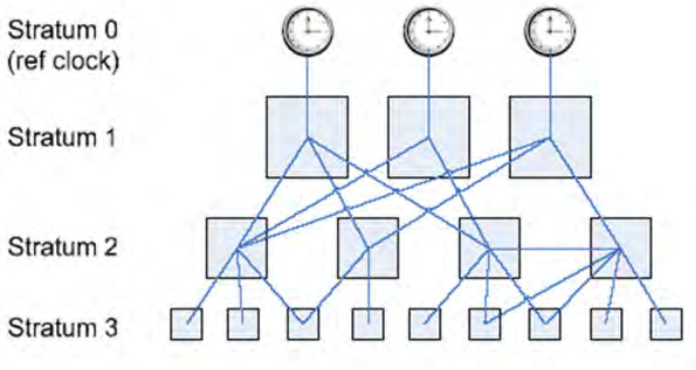
1. http://www.wps.com/projects/codes/index.html
2. http://asciiset.com/
3. http://en.wikipedia.org/wiki/Code_page
4. http://linux.thai.net/pub/ThaiLinux/cvs/docs/tis-620/
5. http://stackoverflow.com/questions/701882/what-is-ansi-format
6. http://www.ku.ac.th/timeline/query.php?year=1981
7. http://www.narisa.com/forums/index.php?showtopic=6943
8. http://www.kreativekorp.com/charset/encoding.php?file=macthai.kte
9. http://th.wikipedia.org/wiki/CU_Writer
10. http://th.wikipedia.org/wiki/TIS-620
11. http://www.nectec.or.th/it-standards/thaistd.pdf
12. http://publib.boulder.ibm.com/infocenter/aix/v7r1/index.jsp?topic=%2Fcom.ibm.aix.nls%2Fdoc%2Fnlsgdrf%2Ftis-620.htm
13. http://linux.thai.net/pub/thailinux/cvs/docs/thai-howto2/Thai-HOWTO/Thai-HOWTO-2.html
14. http://www.nectec.or.th/it-standards/std620/std620.htm
15. http://www.kreativekorp.com/charset/encoding.php?file=iso-8859-11.kte
16. http://www.kreativekorp.com/charset/encoding.php?file=cp874.kte
17. http://msdn.microsoft.com/en-us/goglobal/cc305142.aspx
18. http://www.unicode.org/standard/translations/thai.html
19. http://www.unicode.org/versions/Unicode6.3.0/
20. http://en.wikipedia.org/wiki/Unicode
21. http://babelstone.blogspot.com/2013/10/whats-new-in-unicode-70.html
22. http://googleblog.blogspot.com/2008/05/moving-to-unicode-51.html
23. http://www.cl.cam.ac.uk/~mgk25/unicode.html#linux
24. http://www.utf8-chartable.de/unicode-utf8-table.pl?start=3584&number=128&utf8=0x
25. http://msdn.microsoft.com/en-us/library/dd374081.aspx
26. http://www.unicode.org/charts/PDF/U0E00.pdf
27. http://en.wikipedia.org/wiki/Comparison_of_Unicode_encodings
28. http://www.gnu.org/software/libiconv/
29. http://msdn.microsoft.com/en-us/library/dd317756%28VS.85%29.aspx
30. http://msdn.microsoft.com/en-us/library/windows/desktop/dd317752%28v=vs.85%29.aspx

NTP Reflection DDoS attack

ผู้เขียน : พรพรหม ประภากิตติกุล
วันที่เผยแพร่ : 31 มีนาคม 2557
ปรับปรุงล่าสุด : 31 มีนาคม 2557

หลายคนคงคุ้นหูกับศัพท์คำว่า NTP หรือที่ย่อมาจากคำว่า Network Time Protocol เป็นโพรโทคอลสำหรับการเทียบเวลามาตรฐานและตั้งค่าเวลาบนเครื่องคอมพิวเตอร์นั้น ๆ ผ่านระบบเครือข่าย ส่วนใหญ่มีการนำมาใช้ในองค์กรเพื่อช่วยให้เวลาในเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายมีค่าตรงกัน โดยรูปแบบการทำงานนั้นแบ่งเป็น 2 ส่วนหลัก ๆ คืออุปกรณ์ที่ให้บริการเทียบเวลา (NTP Server) กับเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ต้องการเทียบเวลา (NTP Client) โดยโพรโทคอล NTP นั้นเชื่อมต่อผ่านทางระบบเครือข่ายด้วยโพรโทคอล UDP ผ่านพอร์ต 123 (โพรโทคอล UDP มีความรวดเร็วในการรับส่งข้อมูล แต่ก็มีข้อเสียตรงที่โพรโทคอล UDP ไม่มีการตรวจสอบความถูกต้องของข้อมูลที่รับส่งกันอยู่เหมือน TCP)

NTP เป็นโพรโทคอลที่ได้รับความนิยมมาช้านานตั้งแต่ปี 2528 มีการพัฒนาโดยทีม NTP Project (R&D) **[1]** สำหรับซอฟต์แวร์ที่ทำงานเป็น NTP Server บนระบบปฏิบัติการ Unix ปัจจุบันได้พัฒนาออกมาถึงเวอร์ชัน 4.2.6 และกำลังอยู่ในระหว่างการทดสอบสำหรับเวอร์ชัน 4.2.7 (ในระบบปฏิบัติการอื่น ๆ เช่น Windows ก็มีผู้พัฒนานำซอร์สโค้ดที่อยู่บนเว็บ NTP ไปพัฒนาต่อยอดสำหรับใช้งานเป็น NTP Server บน Windows ด้วย) รวมถึงในปัจจุบันยังมีอีกหลายบริษัทที่พัฒนาอุปกรณ์ประเภท NTP Appliance มาจำหน่าย ซึ่งอุปกรณ์ดังกล่าวสามารถรับสัญญาณจากดาวเทียม GPS ได้โดยตรงส่งผลให้ทำงานในลักษณะที่มีความเที่ยงตรงสูงมาก โดยลักษณะการให้บริการเทียบเวลาของโพรโทคอล NTP แบ่งออกเป็นลำดับชั้น (Clock Strata) และมีการใช้ชื่อเรียกในแต่ละลำดับว่า Stratum เช่น Stratum 0 เป็นต้น ลำดับชั้นที่ยอมรับว่ายังมีความเที่ยงตรงที่สุด คือ Stratum 0-4 หากลำดับชั้นสูงกว่านี้ถือว่าไม่ได้รับการยอมรับตามมาตรฐานที่กำหนดขึ้นโดยมาจากหน่ายงาน ANSI (American National Standards Institute)



รูปที่ 1 แสดงแผนผังรูปภาพการเชื่อมต่อของโพรโทคอล NTP

จากรูปที่ 1 พบว่ามีการแบ่งระดับชั้นของ Stratum ออกเป็นหลายส่วน โดยสามารถอธิบายความแตกต่างของแต่ละ Stratum ดังนี้

Stratum 0 คืออุปกรณ์เทียบเวลาที่ใช้สัญญาณนาฬิกาเป็นตัวอ้างอิง เช่น GPS เป็นต้น

Stratum 1 คืออุปกรณ์เทียบเวลาที่เชื่อมต่อกับ NTP Server ที่ทำงานใน Stratum 0 มีค่าความคลาดเคลื่อนไม่เกิน 1 มิลลิวินาที

Stratum 2 คืออุปกรณ์เทียบเวลาที่เชื่อมต่อกับ NTP Server ที่ทำงานใน Stratum 1 มีค่าความคลาดเคลื่อนประมาณ 10-100 มิลลิวินาที

Stratum 3 คืออุปกรณ์เทียบเวลาที่เชื่อมต่อกับ NTP Server ที่ทำงานใน Stratum 2

Stratum 4 คืออุปกรณ์เทียบเวลาที่เชื่อมต่อกับ NTP Server ที่ทำงานใน Stratum 3

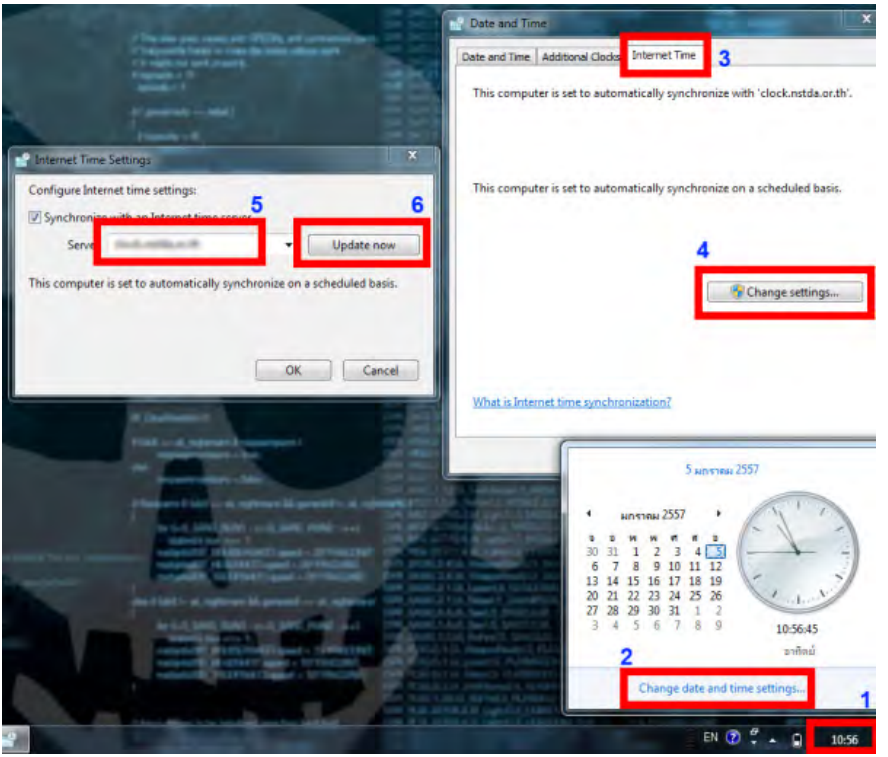
ในประเทศไทยเอง พบว่ามีผู้ให้บริการเทียบเวลาในระดับ Stratum 1 อยู่หลายหน่วยงาน เช่น สถาบันมาตรวิทยาแห่งชาติ และ กรมอุทกศาสตร์กองทัพเรือ เป็นต้น

ลักษณะการใช้งาน NTP แบ่งเป็น 2 ลักษณะใหญ่ ๆ ดังนี้

1. ใช้เพื่อเทียบเวลา

รูปแบบนี้มักเกิดขึ้นกับผู้ใช้งานหรือผู้ดูแลระบบทั่วไปที่ไม่ต้องการความเข้าใจที่มากนักเกี่ยวกับ NTP Server ว่ามีรายละเอียดการทำงานอย่างไร รู้เพียงแค่วิธีการตั้งค่าเทียบเวลาของอุปกรณ์คอมพิวเตอร์ที่ใช้งานอยู่กับ NTP Server หรือเรียกอีกอย่างว่ารู้วิธีการใช้งาน NTP Client กับรู้รายการ NTP Server ที่ต้องการใช้งานเทียบเวลา ซึ่งโดยปกติข้อมูลรายการ NTP Server เป็นข้อมูลที่สามารถค้นหาผ่านระบบ Search Engine ได้ไม่ยาก ในประเทศไทยมี NTP Server ที่มีความน่าเชื่อถือในระดับ Stratum 1 หลายหน่วยงาน เช่น สำนักมาตรวิทยาแห่งชาติ (NTP Server ชื่อ time1.nimt.or.th) โดยเมื่อ

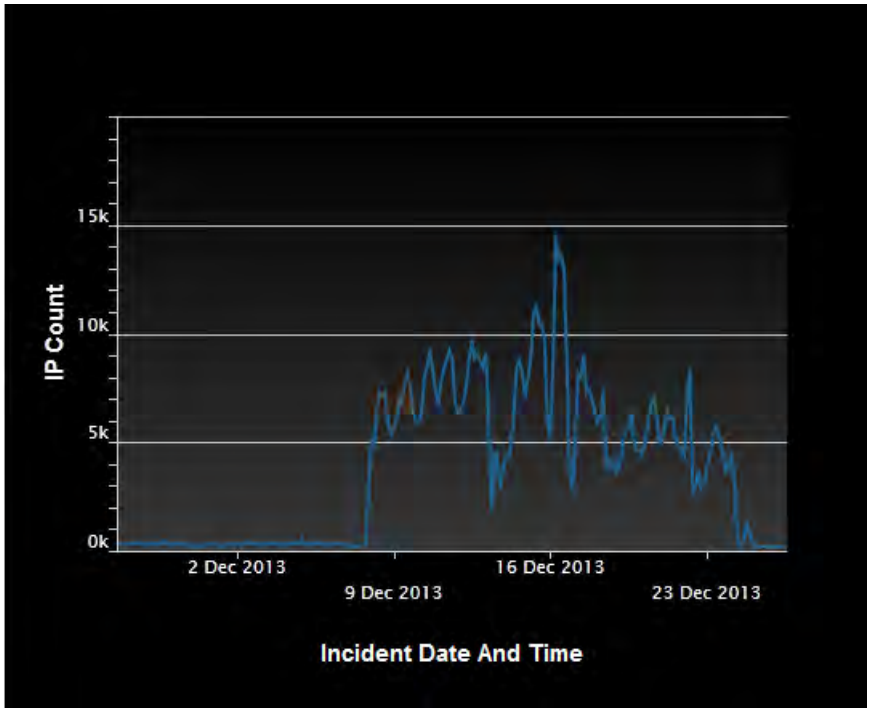
รู้ข้อมูลครบทั้ง 2 ส่วนแล้วก็สามารถเทียบและตั้งค่าเวลาในเครื่องคอมพิวเตอร์หรือเครื่องเซิร์ฟเวอร์ที่ใช้งานได้ทันที ตัวอย่าง NTP Client ที่เห็นได้ชัดเช่น Windows Time Server ซึ่งเป็นโมดูลมาตรฐานที่มีการติดตั้งมาตั้งแต่ Windows 2000 และ Windows XP สามารถดูตัวอย่างได้จากรูปที่ 2



รูปที่ 2 แสดงตัวอย่างการตั้งค่า NTP Client บนระบบปฏิบัติการ Windows 7

ถึงแม้โพรโทคอล NTP จะได้รับการคิดค้นและใช้งานมานาน รวมทั้งมีการใช้งานอย่างแพร่หลาย แต่เมื่อปลายเดือนธันวาคม 2556 ที่ผ่านมานี้ บริษัท Symantec ได้พบข้อมูลที่น่าสนใจเกี่ยวกับปริมาณการรับส่งข้อมูลที่เพิ่มมากขึ้นจนผิดปกติของการใช้งานโพรโทคอล NTP ซึ่งปริมาณการรับส่งข้อมูลด้วยโพรโทคอลที่เพิ่มสูงขึ้นอย่างผิดปกติคาดการณ์ว่าน่าจะเกิดจากการกระทำการบางอย่างที่ผิดปกติหรืออาจหมายถึงการโจมตีรูปแบบใหม่ก็เป็นได้ โดยจากรูปที่ 2 Symantec ได้เปิดเผยสถิติที่บ่งชี้ว่าช่วงกลางเดือนธันวาคม 2556 มีการใช้ NTP Server ประมาณ 15,000 เครื่อง ซึ่งพบว่ามีความพยายามส่งข้อมูลมหาศาลไปยังระบบต่าง ๆ และเมื่อทำการวิเคราะห์ลงในเชิงลึกแล้ว ก็ยืนยันได้ว่าเป็นลักษณะของการโจมตีจริง โดยรูปแบบเทคนิคการโจมตีดังกล่าวอาศัยประโยชน์จาก NTP Server ที่ตั้งค่าไม่เหมาะสมหรือต่อไปจะเรียกว่า NTP Server

ที่มีช่องโหว่ ซึ่งมีการนำมาใช้เป็นส่วนหนึ่งของการโจมตีในลักษณะ DDoS หรือ Distribute Denial Of Service โดยมีจุดประสงค์ของการโจมตีเพื่อจะหยุดยั้งการให้บริการของเครื่องที่ถูกโจมตี ทำให้ไม่สามารถให้บริการหรือทำงานต่อได้ โดยสามารถอธิบายตามตัวอย่างได้ดังรูปที่ 4



รูปที่ 3 บริษัท Symantec ได้เปิดเผยสถิติที่บ่งชี้ว่าช่วงกลางเดือนธันวาคม 2556 มีการใช้ NTP Server ประมาณ 15,000 เครื่องในการโจมตีระบบต่าง ๆ

รูปที่ 4 แสดงรูปแบบการโจมตีระบบ
โดยเทคนิค Reflection DDoS Attack

จากรูปที่ 4 แสดงให้เห็นว่าผู้ไม่หวังดีสามารถโจมตีเครื่องให้บริการเว็บไซต์แห่งหนึ่ง หรือเรียกว่าเครื่องเป้าหมายในลักษณะ DDoS และเป็นที่น่าสังเกตมากคือเทคนิคดังกล่าวสร้างความเสียหายแก่เป้าหมายอย่างรุนแรง โดยสามารถทำสิ่งที่เรียกว่าการขยายปริมาณข้อมูลที่โจมตี (Amplification Attack) โดยการส่งแพ็กเก็ตเล็ก ๆ (ปริมาณแพ็กเก็ต ละ 8 ไบต์) ต่อจำนวนหนึ่งไปยังเครื่อง NTP Server ต่าง ๆ ที่มีช่องโหว่ จากนั้นเครื่อง NTP Server เหล่านั้นจะส่งข้อมูลกลับไปยังเครื่องเป้าหมายในปริมาณมหาศาล ส่งผลให้เครื่องเป้าหมายที่ถูกโจมตีต้องรับภาระในการประมวลผลข้อมูลมหาศาล จนสุดท้ายไม่สามารถให้บริการต่อไปได้ โดยการโจมตีเชิงลึกจะกล่าวถึงในรายละเอียดต่อไป

รวมถึงเมื่อวันที่ 13 มกราคม 2557 ได้มีการเผยแพร่ข้อมูลการโจมตีระบบของเกมออนไลน์ชื่อดังหลายแห่ง เช่น Battle.net, EA.com ถูกโจมตีด้วยเทคนิค Reflection DDoS Attack เป็นผลให้ระบบต่าง ๆ ต้องหยุดให้บริการในทันที **[2]** ข้อมูลเพิ่มเติมแจ้งว่าผู้โจมตีใช้ประโยชน์จากเครื่อง NTP ที่มีช่องโหว่ประมาณ 100 เครื่องเพื่อโจมตีระบบของเกมออนไลน์ต่าง ๆ และพบว่าปริมาณ Bandwidth สูงสุดที่โจมตีในครั้งนี้สูงถึง 100 Gbps ส่วน Bandwidth การโจมตีเฉลี่ยอยู่ที่ 7.3 Gbps และล่าสุดที่พบเกี่ยวกับรูปแบบการโจมตีที่เผยแพร่โดยบริษัท Cloudfare (บริษัทที่ดูแลเครือข่ายใหญ่ที่สุดแห่งหนึ่งของโลก) เกี่ยวกับการโจมตีเครือข่ายในยุโรปที่มีปริมาณการโจมตีสูงสุดถึง 400 Gbps ซึ่งนับว่าเป็นการโจมตีที่สูงที่สุดครั้งหนึ่งของโลก มากกว่าครั้งที่มีการใช้เทคนิค DNS Amplification Attack **[3]**

ผลกระทบ

เครื่อง NTP Server ที่เปิดให้มีการเรียกใช้งานฟังก์ชัน “monlist” สามารถใช้เป็นส่วนหนึ่งของการกระทำความผิดในการโจมตีเครื่องให้บริการอื่น ๆ ในลักษณะ Amplification Attack ทันที

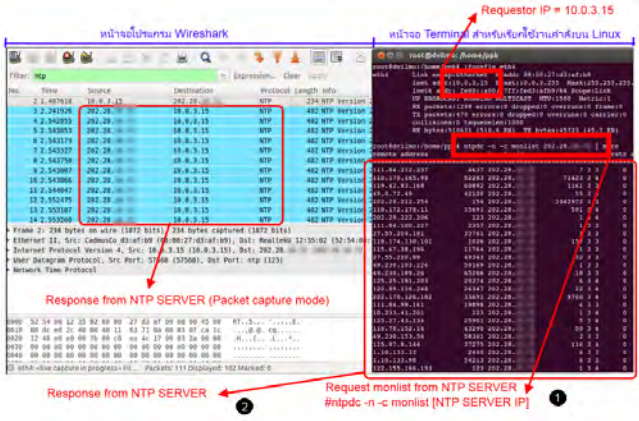
วิเคราะห์ NTP Server กับโหมดการทำงานอันตราย

NTP มีโหมดการทำงานที่พัฒนามาสำหรับผู้ดูแลระบบในการตรวจสอบการเข้าใช้งาน NTP Server ชื่อโมดูลว่า Monitor โดยมีวัตถุประสงค์เพื่อแสดงข้อมูลรายการ NTP Client ที่เชื่อมต่อเข้ามาล่าสุด โมดูลดังกล่าวสามารถแสดงรายการ NTP Client ที่เชื่อมต่อได้สูงสุดถึง 600 รายการไอพีแอดเดรส และตั้งแต่ NTP เวอร์ชันเวอร์ชัน 4.2.6 ลงมา และมีการตั้งค่าให้โมดูลดังกล่าวทำงานตั้งแต่ต้นได้อยู่แล้ว

การใช้งานโมดูล Monitor ของ NTP Server นั้นสามารถทำได้หลายรูปแบบ ปัจจุบันมีโปรแกรมที่มีโมดูลตรวจสอบข้อมูลในส่วนนี้หลายโปรแกรม เช่น NTPDC, NMAP หรือ Metasploit เป็นต้น โดยในเอกสารฉบับนี้จะใช้โปรแกรม ntpdc รวมถึง Script ที่พัฒนาขึ้นสำหรับทดสอบ เพื่อให้เห็นรูปแบบการทำงานของการโจมตี

ทดสอบการเรียก Query กับ NTP Server

ด้วยการส่งคำสั่งเรียกใช้งานฟังก์ชัน monlist ซึ่งเป็นโมดูลสำหรับการมอนิเตอร์รายละเอียดของ NTP Server เกี่ยวกับรายการที่ NTP Server นั้น ๆ เคยมีการเชื่อมต่อในลักษณะคล้ายเป็น History ตามด้านล่าง จะพบผลลัพธ์ตามรูปที่ 5



รูปที่ 5 ตัวอย่างการใช้ฟังก์ชัน monlist

จากรูปที่ 5 แสดงให้เห็นว่าการใช้งานฟังก์ชัน monlist นั้นสามารถนำมาใช้ในการโจมตีในลักษณะ Amplification Attack ได้เป็นอย่างดี สังเกตจาก Response ที่ส่งกลับมาเป็นจำนวนมากเมื่อเทียบกับปริมาณข้อมูล Request ที่ส่งออกไปเพียงนิดเดียว ซึ่งจากรูปแบบดังกล่าวทำให้ผู้ไม่หวังดีนำมาใช้เป็นช่องทางการโจมตีโดยการสร้างการเชื่อมต่อลักษณะที่มีการปลอมแปลงแหล่งที่มาหรือที่เรียกกันว่า Spoofing IP เพื่อปลอมเป็นหมายเลขไอพีที่ต้องการโจมตี จากนั้นใช้หมายเลขไอพีดังกล่าวส่งคำร้องไปยังเครื่อง NTP Server ที่มีช่องโหว่ เพื่อให้ NTP Server ดังกล่าวตอบกลับมาด้วยปริมาณข้อมูลมากเป็นหลายเท่าตัว

ข้อแนะนำ

ซอฟต์แวร์ NTP Server เวอร์ชัน 4.2.7 (ปัจจุบันยังคงเป็นเวอร์ชันที่กำลังพัฒนาเปิดให้ดาวน์โหลดในลักษณะ Beta) ได้มีการถอนฟังก์ชันการทำงานของ ‘monlist” เพื่อแก้ไขปัญหาดังกล่าวด้วย อย่างไรก็ตามสำหรับผู้ดูแลระบบที่ไม่สามารถทำการอัปเดตซอฟต์แวร์ในเวอร์ชันดังกล่าวได้ สามารถใช้วิธีการตั้งค่าตามรายละเอียดด้านล่างเพื่อลดผลกระทบจากการโจมตีช่องโหว่ดังกล่าว ในไฟล์การตั้งค่าของ NTP Server (ไฟล์ชื่อ ntp.conf) โดยสามารถเลือกทำข้อใดข้อหนึ่งก็ได้ตามข้อมูลดังต่อไปนี้

1. ตั้งค่าเพื่อปิดการทำงานของฟังก์ชัน monlist

#เพิ่ม

disable monitor

2. ตั้งค่าเพื่อปิดการเรียกใช้งานฟังก์ชันการอ่านค่าต่าง ๆ ของ NTP Server

#เพิ่ม

restrict -4 default nomodify nopeer noquery notrap

restrict -6 default nomodify nopeer noquery notrap

จากนั้นให้ทำการ Restart บริการของ NTP Server เพื่อให้ระบบใช้งานการตั้งค่าใหม่และทดสอบเรียกใช้งานฟังก์ชัน monlist ดูอีกครั้ง จะพบว่าไม่สามารถเรียกใช้งานได้อีกต่อไป

อ้างอิง
1. http://www.ntp.org
2. http://thehackernews.com/2014/01/ddos-attack-NTP-server-reflection-protection.html
3. http://thehackernews.com/2014/02/NTP-Distributed-Denial-of-Service-DDoS-attack.html

WireLurker และ Masque Attack : ผู้ใช้ iOS ติดมัลแวร์ได้แม้ไม่ Jailbreak

ผู้เขียน : เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่ : 24 พฤศจิกายน 2557
ปรับปรุงล่าสุด : 24 พฤศจิกายน 2557

ปัญหามัลแวร์ในระบบปฏิบัติการบนอุปกรณ์พกพาอย่าง iOS หรือ Android นั้น กำลังเริ่มมีมากขึ้นเรื่อย ๆ ส่วนหนึ่งเป็นเพราะความนิยมใช้งานโทรศัพท์มือถือและแท็บเล็ตเพื่อช่วยอำนวยความสะดวกในชีวิตประจำวัน ไม่ว่าจะเกี่ยวกับการทำงานหรือเรื่องส่วนตัว จึงมีโอกาสสูงที่จะมีข้อมูลสำคัญและเป็นเป้าหมายของผู้ไม่หวังดีเก็บอยู่ในอุปกรณ์เหล่านั้น ดังนั้นจึงไม่น่าแปลกใจหากปัจจุบันเราจะพบว่านักพัฒนามัลแวร์หันมาเน้นโจมตีผู้ใช้งานระบบปฏิบัติการมือถือเป็นหลัก โดยเฉพาะระบบปฏิบัติการ Android ที่ในตอนนี้ตกเป็นเป้าหมายหลักของการโจมตี โดยผลการสำรวจพบว่าบรรดามัลแวร์ในมือถือเป็นมัลแวร์ที่โจมตีระบบปฏิบัติการ Android มากถึง 97% **[1]** ส่วนระบบปฏิบัติการคู่แข่งอย่าง iOS นั้นเนื่องจากมีการออกแบบระบบให้เน้นเรื่องความมั่นคงปลอดภัยมากกว่า Android มาตั้งแต่ต้น ดังนั้นจึงมีปริมาณมัลแวร์น้อยกว่า แต่ก็ไม่ได้หมายความว่าผู้ใช้ระบบปฏิบัติการ iOS จะปลอดภัยจากมัลแวร์ไปเสียทีเดียว เพราะล่าสุดได้ค้นพบมัลแวร์ตัวใหม่ที่สามารถโจมตีอุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS ได้แทบจะทุกเครื่องที่เปิดใช้งานอยู่ในปัจจุบัน

ก่อนหน้านี้เราเคยมีความเชื่อกันว่าระบบปฏิบัติการ iOS นั้นมั่นคงปลอดภัยจากมัลแวร์มากกว่าระบบปฏิบัติการ Android สาเหตุหลัก ๆ ก็เนื่องจากตัวระบบปฏิบัติการ iOS เองได้รับการออกแบบให้เน้นเรื่องความมั่นคงปลอดภัยมากกว่า Android ตั้งแต่แรก ตัวอย่างมาตรการการรักษาความมั่นคงปลอดภัยของอุปกรณ์ iOS เช่น

- การติดตั้งแอปพลิเคชันที่โดยปกติแล้ว ผู้ใช้ทั่วไปจะไม่สามารถดาวน์โหลดแอปพลิเคชันจากแหล่งภายนอกมาติดตั้งเองได้ ต้องดาวน์โหลดจาก App Store เท่านั้น ซึ่งต่างจากระบบปฏิบัติการ Android ที่ยอมให้ผู้ใช้สามารถติดตั้งแอปพลิเคชันจากไฟล์ที่ดาวน์โหลดมาเองได้

- กระบวนการตรวจสอบแอปพลิเคชันที่ขึ้น App Store เป็นการตรวจสอบโดยมนุษย์ **[2]** ซึ่งมีการตรวจสอบทั้งคุณภาพของแอปพลิเคชันและความมั่นคงปลอดภัยในการใช้งาน ดังนั้นจึงมีโอกาสน้อยที่แอปพลิเคชันอันตรายจะหลุดขึ้นมาอยู่บน App Store ได้ เหมือนกับที่เคยเกิดขึ้นใน Play Store ของ Android ที่ใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบ **[3]**

- ความเข้มงวดในการจำกัดสิทธิการเข้าถึงข้อมูลสำคัญของผู้ใช้ แอปพลิเคชันที่ต้องการเข้าถึงข้อมูลสำคัญหรือต้องการใช้ความสามารถที่อาจละเมิดความเป็นส่วนตัว เช่น เปิดใช้งานกล้องถ่ายรูป อัดเสียง ดูภาพที่ถ่าย ดูข้อมูลปฏิทิน ดูตำแหน่ง GPS จำเป็นต้องได้รับการอนุญาตจากผู้ใช้ก่อนเสมอ โดยจะมีหน้าต่างแจ้งเตือนการ

ขออนุญาตแสดงขึ้นมาในครั้งแรกที่ผู้ใช้เรียกใช้งานความสามารถนั้น ๆ ซึ่งจะต่างจากระบบปฏิบัติการ Android ที่แอปพลิเคชันจะต้องขอสิทธิทุกอย่างมาตั้งแต่แรก และหากผู้ใช้จะติดตั้งแอปพลิเคชันจะต้องยอมมอบสิทธิ์ทั้งหมดที่แอปพลิเคชันนั้นร้องขอ โดยไม่สามารถเลือกว่าจะอนุญาตให้แอปพลิเคชันมีสิทธิแค่อย่างใดอย่างหนึ่งได้

• แอปพลิเคชันที่ติดตั้งอยู่ในเครื่องไม่สามารถเข้าถึงข้อมูลของแอปพลิเคชันอื่น ๆ ได้ นอกจากผู้ใช้จะเป็นคนกำหนดข้อมูลที่ต้องการแชร์ระหว่างแอปพลิเคชันต่าง ๆ เอง

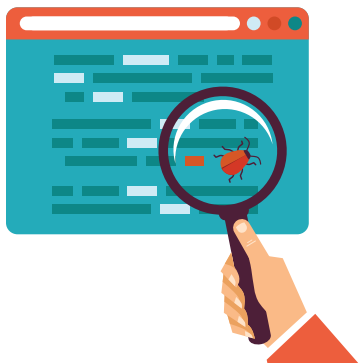
• ระบบการจัดการแอปพลิเคชันของ iOS แอปพลิเคชันที่รันเป็น Background (ไม่ถูกเรียกขึ้นมาแสดงผล) จะมีการจำกัดความสามารถในการทำงาน ไม่สามารถใช้ทรัพยากรของระบบได้มากเท่า Android เช่น แอปพลิเคชันของ iOS ที่รันเป็น Background จะสามารถรับข้อความแจ้งเตือนเพื่อมาแสดงผลได้เท่านั้น ไม่สามารถอัดเสียงหรือประมวลผลงานอื่นที่ทำค้างอยู่ได้ **[4] [5]**

จากรายละเอียดทั้ง 5 ข้อนี้ก็เพียงพอที่จะทำให้การใช้งานระบบปฏิบัติการ iOS ในแบบผู้ใช้ทั่วไปนั้นมีความมั่นคงปลอดภัยมากกว่าการใช้งานระบบปฏิบัติการ Android อยู่มากพอสมควร ยกเว้นเสียแต่ว่ากระบวนการบางอย่างทำงานผิดพลาด อย่างเช่นการตรวจสอบแอปพลิเคชันก่อนส่งขึ้น App Store ซึ่งหากคนที่ตรวจสอบไม่มีความรัดกุมพอก็อาจเผลอปล่อยแอปพลิเคชันที่เป็นมัลแวร์หลุดออกมาได้ ซึ่งเหตุการณ์เช่นนี้เคยเกิดขึ้นมาแล้ว

เมื่อปี 2011 นักวิจัยชื่อ Charlie Miller ได้ทดลองส่งแอปพลิเคชันขึ้น App Store โดยลักษณะภายนอกเป็นแอปพลิเคชันธรรมดาแต่ตั้งค่าไว้ว่าเมื่อผู้ใช้ติดตั้งแอปพลิเคชันนี้ลงในเครื่องแล้วจะแอบไปดาวน์โหลดโค้ดของมัลแวร์มาทำงานทีหลัง แอปพลิเคชันตัวนี้สามารถผ่านการตรวจสอบจาก Apple และหลุดขึ้นมาอยู่บน App Store ได้ **[6]** ต่อมาในปี 2013 ทีมนักวิจัยจาก Georgia Tech ได้ใช้เทคนิคใหม่ที่ทำให้ส่งแอปพลิเคชันที่เป็นมัลแวร์ขึ้นไปอยู่บน App Store ได้อีกครั้ง **[7]** เหตุการณ์เหล่านี้ก็เป็นเครื่องพิสูจน์ที่ดีว่าถึงแม้จะใช้คนตรวจแล้วก็ตาม แต่ก็ไม่อาจไว้ใจเรื่องความมั่นคงปลอดภัยได้ 100% อยู่ดี

มัลแวร์ใน iOS

มัลแวร์ใน iOS ตัวแรกมีการค้นพบเมื่อปี 2009 เป็นมัลแวร์ที่แอบส่ง SMS ไปยังบุคคลอื่น หลังจากนั้นก็เริ่มมีการะค้นพบมัลแวร์ใน iOS อยู่เรื่อย ๆ โดยมีทั้งแบบที่เป็น Spyware หรือมัลแวร์ขโมยข้อมูลธนาคารออนไลน์ แต่เกือบทั้งหมดสามารถแพร่ระบาดได้เฉพาะเครื่องที่ถูก Jailbreak แล้วเท่านั้น ดังรูปที่ 1 (อ้างอิง: Fortinet **[8]**)



Name	Discovery date	Presumed origin	Devices	Type
iOS/Trapsms.Altr.spy	June 2009	Russia?	Jailbroken	SMS Forwarder
Spy/MobileSpy/iPhoneOS	Aug 2009	USA	Jailbroken	Spyware
iOS/Eeki.A!worm	Nov 2009	Australia (Ashley Towns)	Jailbroken	Worm Proof of Concept
iOS/Eeki.B!worm	Nov 2009	The Netherlands	Jailbroken	Mobile banking malware
iOS/Toires.Altr.spy	Nov 2009	Switzerland (Nicolas Seriot)	Any (jailbroken or not)	Rogue application - Proof Of Concept
Adware/LBTM!iOS	Sep 2010	France	Any (jailbroken or not) - Was found (and removed) in the official AppStore	Call premium phone number
Spy/iKeyGuard!iPhoneOS	Apr 2011	Czech Rep.	Jailbroken	Keylogger
iOS/FindCall.Altr.spy	July 2012	Russia?	Any (jailbroken or not) - Was found (and removed) in the official AppStore	Privacy trojan
Riskware/Kill!mobliOS	July 2013	USA	Jailbroken	Spyware
iOS/AdThief.Altr	Mar 2014	China	Jailbroken	Ad revenue hijacking
iOS/SSLCreds.Altr.pws	Apr 2014	China	Jailbroken	Password stealer

รูปที่ 1 รายชื่อมัลแวร์ใน iOS ทั้งหมดที่ค้นพบตั้งแต่เดือนมิถุนายน 2009 ถึงเมษายน 2014

ที่ผ่านมา มีเพียงแค่ 2 ครั้งเท่านั้นที่พบว่ามัลแวร์ใน iOS (ตัวที่ไม่ใช่นักวิจัยทดลองทำ) สามารถหลุดขึ้นไปอยู่บน App Store และมีผู้ใช้ได้รับความเสียหาย โดยในปี 2010 พบมัลแวร์ตัวแรกปรากฏอยู่บน App Store เป็นมัลแวร์ที่โทรศัพท์ไปยังหมายเลขปลายทางที่คิดค่าบริการในราคาแพง **[9]** และอีกครั้งในปี 2012 เป็นมัลแวร์ที่ส่งรายชื่อคนใน Contact List ออกไปทาง SMS **[10]** มัลแวร์ทั้งสองตัวนี้หลังจากที่ได้รับการค้นพบก็มีการลบออกจาก App Store ในเวลาอันรวดเร็ว

ตลอดหลายปี นอกจากกรณีของมัลแวร์ 2 ตัวข้างต้นที่สามารถหลุดขึ้นไปอยู่บน App Store ได้แล้ว เกือบทั้งหมดของมัลแวร์ที่พบใน iOS นั้นสามารถติดได้เฉพาะในเครื่องที่ถูก Jailbreak แล้วเท่านั้น นั่นเป็นเหตุผลที่ทำให้ Apple กล้าบอกกับผู้ใช้ได้อย่างอย่างมั่นใจว่าถ้าเครื่องที่ใช้งานปกติ ไม่ได้ถูก Jailbreak ก็แทบจะไม่มีทางติดมัลแวร์ได้อย่างแน่นอน นอกจากนี้ทาง Apple ยังมีระบบ Kill Switch ที่สามารถสั่งลบแอปพลิเคชันใด ๆ ก็ตามออกจากเครื่องของผู้ใช้ในกรณีที่ Apple ตรวจพบในภายหลังว่าแอปพลิเคชันนั้นเป็นอันตรายได้อีกด้วย **[11]**

อย่างไรก็ตาม ถึงแม้ว่าโดยปกติแล้วระบบปฏิบัติการ iOS จะไม่อนุญาตให้ผู้ใช้ติดตั้งแอปพลิเคชันจากแหล่งอื่นที่ไม่ใช่ App Store แต่ Apple ก็ได้เปิดช่องทางให้ผู้พัฒนาแอปพลิเคชันหรือองค์กรต่าง ๆ สามารถแจกจ่ายหรือติดตั้งแอปพลิเคชันที่พัฒนาขึ้นมาเองลงในอุปกรณ์ของตัวเองได้โดยไม่ผ่านช่องทาง App Store ซึ่งโดยส่วนใหญ่จะเป็นแอปพลิเคชันที่พัฒนาขึ้นมาสำหรับทดสอบหรือเพื่อใช้งานเฉพาะภายในองค์กรเป็นหลัก

ในการจะทำแบบนี้ได้ นักพัฒนาต้องนำหมายเลข UDID ซึ่งเป็นหมายเลขเฉพาะที่ใช้ระบุตัวตนของอุปกรณ์เครื่องนั้นมาลงทะเบียนกับทาง Apple เพื่อบอกให้รู้ว่าเป็นเครื่องสำหรับนักพัฒนา และต้องมีการสร้าง Provisioning Profiles ขึ้นมาในอุปกรณ์ iOS เพื่อให้สามารถติดตั้งแอปพลิเคชันจากนักพัฒนาได้ การติดตั้งแอปพลิเคชันด้วยวิธีนี้ทำได้

ทั้งจากการเชื่อมต่ออุปกรณ์ iOS เข้ากับ iTunes หรือกดติดตั้งแอปพลิเคชันด้วยการเปิดเข้าเว็บไซต์ที่ใช้สำหรับเผยแพร่แอปพลิเคชันนั้น [12]

วิธีการติดตั้งแอปพลิเคชันในรูปแบบนี้ก็เป็นสิ่งที่รู้กันดีกว่ามีความมั่นคงปลอดภัยน้อยกว่าการติดตั้งแอปพลิเคชันจาก App Store ตามปกติ เพราะแอปพลิเคชันที่จะนำมาติดตั้งนั้นไม่ได้ผ่านการตรวจสอบจากทีม Apple และอาจมีปัญหาด้านความมั่นคงปลอดภัยได้ ซึ่งในงาน Black Hat USA 2013 กลุ่มนักวิจัยจาก Georgia Institute of Technology ได้เผยแพร่งานวิจัยที่ใช้ช่องโหว่ของระบบปฏิบัติการ iOS ร่วมกับการติดตั้งแอปพลิเคชันแบบองค์กร (Enterprise Deployment) ที่กล่าวมานี้ มาใช้ในการสร้างเครื่องมือที่สามารถทำให้อุปกรณ์ iOS ใด ๆ ก็ตามสามารถติดมัลแวร์ได้หากนำมาเชื่อมต่อ ซึ่งอุปกรณ์ iOS ที่ว่านั้นไม่จำเป็นต้องถูก Jailbreak แต่อย่างใด [13] หลังจากที่นักวิจัยนำเสนอเทคนิคนี้ กว่าหนึ่งปีผ่านไปก็ยังไม่พบการแพร่ระบาดของมัลแวร์ที่โจมตีด้วยวิธีนี้ ดังนั้นผู้ใช้งานอุปกรณ์ iOS ที่ไม่ได้ Jailbreak ก็ยังคงมั่นใจว่าตัวเองจะมั่นคงปลอดภัยจากมัลแวร์ จนกระทั่งการปรากฏตัวของมัลแวร์ที่มีชื่อว่า WireLurker

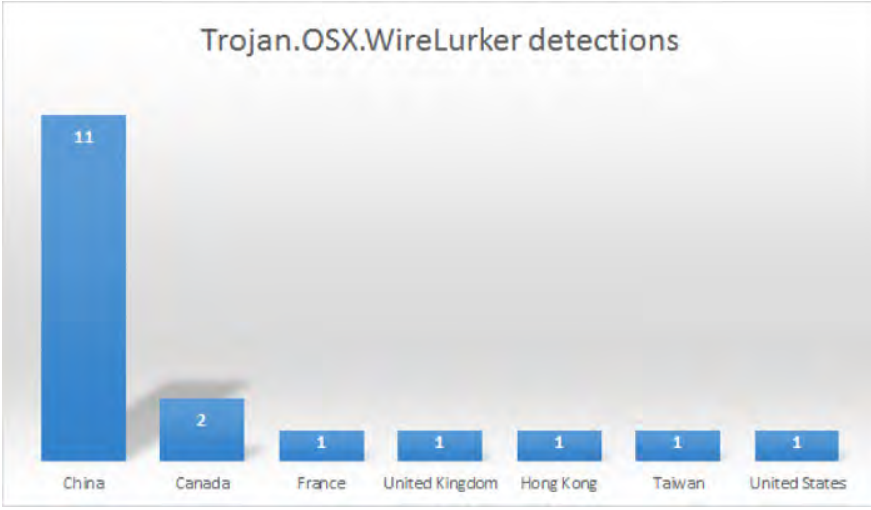
WireLurker

เมื่อต้นเดือนพฤศจิกายน 2014 นักวิจัยจาก Palo Alto Network ได้เผยแพร่รายงานการค้นพบมัลแวร์ตัวแรกที่ใช้ช่องโหว่การติดตั้งแอปพลิเคชันแบบองค์กรมาใช้สร้างความเสียหาย โดยมัลแวร์ตัวนี้นอกจากจะติดในเครื่อง iOS ที่ไม่ Jailbreak ได้แล้ว ยังสามารถติดในเครื่องที่ใช้งาน Mac OS X และ Windows ได้อีกด้วย

หลักการทำงานคือ ตัวมัลแวร์จะติดในเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Mac OS X หรือ Windows ก่อน และจะเฝ้ารอให้ผู้ใช้นำอุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS มาเชื่อมต่อกับเครื่องผ่านพอร์ต USB แล้วจึงแอบติดตั้งแอปพลิเคชัน iOS อันตรายลงไปในเครื่องเหยื่อเพื่อขโมยข้อมูล นอกจากนี้ยังมีความสามารถเชื่อมต่อไปยังเซิร์ฟเวอร์ของผู้สั่งการมัลแวร์เพื่ออัปเดตความสามารถใหม่ ๆ เพิ่มเติมขึ้นได้อีกด้วย เนื่องจากมัลแวร์ตัวนี้แพร่กระจายผ่านการเสียบสายเคเบิลจึงได้รับตั้งชื่อว่า WireLurker [14]

ในตอนแรก ทางนักวิจัยพบว่ามัลแวร์ WireLurker แพร่กระจายผ่านเว็บไซต์แห่งหนึ่งในประเทศจีนที่แจกโปรแกรมเถื่อนของ Mac OS X โดยมีโปรแกรมทั้งหมด 467 ตัวที่ถูกฝังมัลแวร์นี้ไว้ และมียอดดาวน์โหลดไปแล้วมากกว่า 350,000 ครั้ง โดยเบื้องต้นมีการประเมินว่าผู้เสียหายจากมัลแวร์ตัวนี้น่าจะมีมากกว่าหมื่นราย ในเวลาต่อมา นักวิจัยจาก AlienVault Labs ได้ค้นพบว่ามีเว็บไซต์จีนอีกแห่งหนึ่งที่แพร่กระจายมัลแวร์ตัวนี้ด้วย และเป็นมัลแวร์ WireLurker เวอร์ชันที่ทำงานบนระบบปฏิบัติการ Windows โดยมีโปรแกรมทั้งหมด 247 ตัวที่เป็นมัลแวร์ และมีการดาวน์โหลดไปแล้วมากกว่า 65,000 ครั้ง จากการวิเคราะห์พบว่ามัลแวร์เวอร์ชัน Windows ที่พบนี้เป็นตัวที่เก่ากว่ามัลแวร์เวอร์ชัน Mac OS X ตัวที่พบตอนแรก [15]

ทางศูนย์วิจัยของ Kaspersky พบว่ามัลแวร์ WireLurker นอกจากจะแพร่ระบาดในประเทศจีนแล้วยังมีการแพร่กระจายไปในประเทศอื่น ๆ เช่น แคนาดา ไต้หวัน ฮ่องกง อีกด้วย ดังรูปที่ 2 แต่บริเวณที่ระบาดหนักสุดคือประเทศจีน [16]



รูปที่ 2 การแพร่กระจายของมัลแวร์ WireLurker ในประเทศต่างๆ

แอปพลิเคชันอันตรายที่มัลแวร์ WireLurker ติดตั้งลงในเครื่อง iOS นั้นมีทั้งแอปพลิเคชันปลอมและแอปพลิเคชันจริงที่ถูกแคร็กแล้ว นอกจากนี้มัลแวร์ยังสามารถคัดลอกแอปพลิเคชันที่ผู้ใช้ติดตั้งอยู่ในเครื่องเพื่อนำมาดัดแปลงใส่โค้ดอันตรายแล้วติดตั้งลงไปใหม่ทับแอปพลิเคชันเดิมในเครื่องได้ด้วย **[17]** สาเหตุที่มัลแวร์สามารถติดตั้งแอปพลิเคชันอันตรายลงไปทับแอปพลิเคชันเดิมในเครื่องได้ เพราะใช้ช่องโหว่ในฟีเจอร์ Enterprise/Ad-hoc provisioning ของ iOS ซึ่งทางนักวิจัยจาก FireEye ได้เรียกชื่อช่องโหว่นี้ว่า Masque Attack

Masque Attack

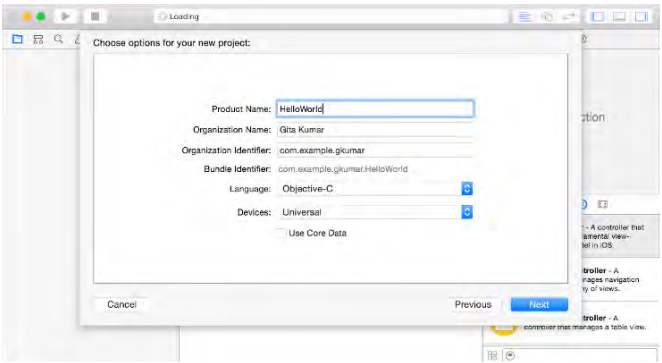
ก่อนจะไปดูว่า Masque Attack คืออะไร ขออธิบายที่มาที่ไปสักนิด เนื่องจากว่าทาง Apple ได้ออกแบบระบบปฏิบัติการ iOS ให้รองรับการใช้งานภายในองค์กรโดยสร้างฟีเจอร์ชื่อ iOS Enterprise Deployment ขึ้นมาเพื่อให้ผู้ดูแลระบบสามารถพัฒนาแอปพลิเคชันสำหรับใช้งานภายในองค์กรและติดตั้งแอปพลิเคชันในอุปกรณ์ iOS ขององค์กรได้โดยไม่จำเป็นต้องอัปโหลดขึ้น App Store **[18]** ในการจะใช้ความสามารถนี้ได้ ผู้พัฒนาแอปพลิเคชันจำเป็นต้องลงทะเบียนและสมัคร iOS Developer Enterprise Program ซึ่งจะมีค่าใช้จ่าย $299 ต่อปี **[19]** แอปพลิเคชันที่พัฒนาขึ้นมาโดยนักพัฒนาที่ลงทะเบียนแบบ Enterprise สามารถนำไปติดตั้งลงในเครื่องปลายทางได้ “ไม่จำกัดจำนวน” ซึ่งต่างจากแอปพลิเคชันที่พัฒนาโดยนักพัฒนาทั่วไปที่มีข้อจำกัดว่าสามารถติดตั้งลงในเครื่องเพื่อทดสอบได้แค่ประมาณ 100 เครื่องเท่านั้น **[20]**

ภายหลังจากที่มีข่าวการแพร่ระบาดของมัลแวร์ WireLurker ได้เพียงไม่กี่วัน นักวิจัยจากบริษัท FireEye ได้เผยแพร่รายงานช่องโหว่ของระบบ iOS Enterprise

Deployment ซึ่งผู้ไม่หวังดีสามารถใช้ช่องโหว่นี้สร้างมัลแวร์ให้ติดตั้งแอปพลิเคชันอันตรายทับแอปพลิเคชันที่ผู้ใช้ดาวน์โหลดมาติดตั้งอยู่ในเครื่องได้ ซึ่งช่องโหว่นี้เป็นเทคนิคเดียวกับที่มัลแวร์ WireLurker ใช้ในการแพร่กระจายมัลแวร์ลงในเครื่อง iOS ที่ไม่ได้ Jailbreak **[21]** ช่องโหว่ดังกล่าวนี้มีผลกระทบกับ iOS 7.1.1, 7.1.2, 8.0, 8.1 รวมถึง 8.1.1

สาเหตุของช่องโหว่นี้ เกิดจากการที่ iOS ไม่ตรวจสอบใบรับรอง (Certificate) ของแอปพลิเคชันที่สร้างโดยนัก Enterprise Program โดยทาง FireEye ได้พบว่าเมื่อมีการติดตั้งแอปพลิเคชันที่มีชื่อ Bundle Identifier ซ้ำกับแอปพลิเคชันเดิมที่เคยมีอยู่ในเครื่อง หากแอปพลิเคชันนั้นมีใบรับรองของนักพัฒนาแบบ Enterprise ระบบปฏิบัติการ iOS จะยอมให้ติดตั้งแอปพลิเคชันตัวใหม่ทับของเดิมได้ทันทีโดยไม่มีการแจ้งว่าใบรับรองของผู้พัฒนาแอปพลิเคชันเดิมกับแอปพลิเคชันใหม่ไม่ตรงกัน

นั่นหมายความว่านักพัฒนาที่มีสิทธิพัฒนาแอปพลิเคชันแบบ Enterprise (หรือใครก็ตามที่สามารถสมัคร Enterprise Program สำเร็จ) ก็สามารถสร้างแอปพลิเคชันปลอมของแอปพลิเคชันใด ๆ ที่ผู้ใช้สามารถดาวน์โหลดมาติดตั้งได้โดยไม่ผ่าน App Store เพียงแค่ตั้งชื่อ Bundle Identifier ให้เป็นชื่อเดียวกับแอปพลิเคชันเดิมที่อยู่ในเครื่องของผู้ใช้ ดังรูปที่ 3 ซึ่งการที่จะหาว่าแอปพลิเคชันต้นทางที่ต้องการติดตั้งทับนั้นใช้ Bundle Identifier ว่าอะไรไม่ใช่เรื่องยาก เพราะสามารถเปิดเข้าไปดูได้จาก iTunes Library **[22]**



รูปที่ 3 ตัวอย่างการตั้งชื่อ Bundle Identifier
ของแอปพลิเคชัน (ที่มา: Apple [23])

เนื่องจากการเผยแพร่แอปพลิเคชันด้วยวิธี Enterprise Deployment นั้นสามารถเผยแพร่ผ่านเว็บไซต์ได้ โดยเมื่อผู้ใช้ใช้เบราว์เซอร์ของ iOS (เช่น Safari) เปิดเข้าใช้งานเว็บไซต์ที่ใช้สำหรับกระจายแอปพลิเคชัน ก็จะปรากฏหน้าจอขึ้นมาเพื่อถามว่าผู้ใช้ต้องการติดตั้งแอปพลิเคชันนั้นหรือไม่ ดังรูปที่ 4 หากผู้ใช้กด Install ก็จะเป็นการดาวน์โหลดแอปพลิเคชันนั้นมาติดตั้งในเครื่องทันที โดยไม่จำเป็นต้องตั้งค่าอะไรในเครื่องแต่อย่างใด

รูปที่ 4 ตัวอย่างหน้าจอสอบถามการติดตั้งแอปพลิเคชันแบบ Enterprise

ยิ่งกว่านั้น ผู้ไม่หวังดียังสามารถตั้งชื่อแอปพลิเคชันเป็นชื่ออื่นเพื่อหลอกล่อให้ผู้ใช้เข้าใจผิดแล้วกดติดตั้งได้ โดยทาง FireEye ได้ทำคลิปขึ้นมาเพื่อสาธิตการโจมตีผ่านช่องโหว่นี้

จากในคลิปตัวอย่าง (https://www.youtube.com/watch?v=3VEQ-bJUhPw&feature=player_embedded) เมื่อผู้ใช้เปิดเข้าเว็บไซต์ จะพบหน้าจอถามว่า

ต้องการติดตั้งแอปพลิเคชันชื่อ New Flappy Bird หรือไม่ แต่เมื่อผู้ใช้กดปุ่ม Install กลับกลายเป็นว่าแอปพลิเคชันใหม่นั้นมีการติดตั้งทับแอปพลิเคชัน Gmail เดิมที่อยู่ในเครื่อง (ตั้งชื่อ Bundle Identifier ว่า com.google.Gmail เพื่อให้ติดตั้งทับแอปพลิเคชัน Gmail ของจริง)

หลังจากที่แอปพลิเคชันใหม่มีการติดตั้งทับแอปพลิเคชันเดิมแล้ว มันสามารถเข้าถึงข้อมูลที่แอปพลิเคชันเดิมเก็บอยู่ได้ เช่น แอปพลิเคชัน Gmail ปลอมที่มีการติดตั้งทับเข้าไป สามารถเข้าถึงบัญชีผู้ใช้และอ่านอีเมลทั้งหมดที่เก็บอยู่ในเครื่องได้ ซึ่งในกรณีนี้หากเป็นแอปพลิเคชันอื่น เช่น eBay, Paypal ผู้ใช้ก็อาจถูกสวมรอยหรือถูกขโมยเงินในบัญชีออกไปได้ง่าย ๆ

อีกจุดหนึ่งที่สำคัญของช่องโหว่นี้คือ ใครก็ตามสามารถนำเอาแอปพลิเคชันที่ผู้ใช้ติดตั้งอยู่ในเครื่องไปแก้ไขให้มีโค้ดอันตรายฝังอยู่ แล้วใส่กลับเข้ามาทับแอปพลิเคชันเดิมได้ (เป็นวิธีที่มัลแวร์ WireLurker ใช้) ซึ่งวิธีนี้ผู้ใช้จะสังเกตความผิดปกติได้ลำบากเพราะหน้าจอแอปพลิเคชันที่ใส่ทับเข้ามานั้นจะดูเหมือนเดิมทุกอย่าง

อย่างไรก็ตาม ช่องโหว่ของระบบ iOS Enterprise Deployment นี้ยังจำกัดอยู่แค่สามารถติดตั้งแอปพลิเคชันปลอมทับแอปพลิเคชันที่ผู้ใช้ดาวน์โหลดมาติดตั้งเองได้เท่านั้น สำหรับแอปพลิเคชันที่ติดตั้งมาพร้อมกับเครื่อง เช่น Mail, Safari นั้นไม่สามารถติดตั้งทับด้วยวิธีนี้ได้

ความอันตรายของ WireLurker และ Masque Attack

มัลแวร์ WireLurker และช่องโหว่ Masque Attack เป็นการนำระบบ Enterprise Deployment มาใช้ในทางที่ไม่ถูกต้อง บวกกับอาศัยความไม่รู้ของผู้ใช้ที่ยังเข้าใจว่าระบบปฏิบัติการ iOS ที่ไม่ได้ Jailbreak นั้นมีความมั่นคงปลอดภัยเนื่องจากสามารถติดตั้งแอปพลิเคชันจาก App Store ได้อย่างเดียว การติดตั้งแอปพลิเคชันจากแหล่งอื่นนั้นไม่สามารถทำได้ ดังนั้นเมื่อผู้ใช้เห็นข้อความบนจอที่บอกให้ติดตั้งโปรแกรมก็อาจกด Install ไปเลยโดยไม่ได้ระวังอะไร ซึ่งกลายเป็นว่าหากผู้ไม่หวังดีต้องการเผยแพร่มัลแวร์ใน iOS ผ่านหน้าเว็บไซต์ (แบบที่เคยเกิดขึ้นกับ Android **[24]**) จะมีโอกาสโจมตีได้สำเร็จสูงกว่าการเผยแพร่มัลแวร์ Android มาก เพราะผู้ใช้ iOS กดปุ่ม Install แค่ปุ่มเดียวแอปพลิเคชันอันตรายก็จะเข้าไปอยู่ในเครื่องได้ทันที

จุดอ่อนอีกอย่างหนึ่งใน iOS ที่ทำให้ Masque Attack ประสบความสำเร็จนั่นคือการติดตั้งแอปพลิเคชันนอก App Store ทำได้ง่ายมาก เพียงแค่เปิดเว็บไซต์แล้วกด Install โดยที่ข้อความที่ขึ้นมาบอกว่าจะติดตั้งแอปพลิเคชันอะไรนั้นก็ไม่มีการบอกรายละเอียดให้ชัดเจน แสดงเพียงแค่ชื่อแอปพลิเคชันเท่านั้น (ซึ่งสามารถปลอมเป็นชื่ออะไรก็ได้) ในจุดนี้กลับกลายเป็นว่าระบบปฏิบัติการ Android นั้นมีความมั่นคงปลอดภัยมากกว่าเพราะไม่ได้เปิดให้สามารถติดตั้งแอปพลิเคชันจากแหล่งที่มาภายนอกได้ตั้งแต่แรก และหากผู้ใช้ Android ยืนยันต้องการติดตั้งแอปพลิเคชันจากแหล่งภายนอกที่ไม่ใช่ Play Store ก็จำเป็นต้องเข้าไปเปิดตัวเลือกให้สามารถติดตั้งแอปพลิเคชันจากแหล่งที่มาที่ไม่รู้จัก (Unknown Source) และถึงแม้ผู้ใช้ Android จะเข้าเว็บไซต์ที่ปล่อยมัลแวร์ ก็ยังไม่สามารถติดตั้งแอปพลิเคชันโดยตรงจากหน้าเว็บไซต์ได้ จำเป็นต้องดาวน์โหลดไฟล์

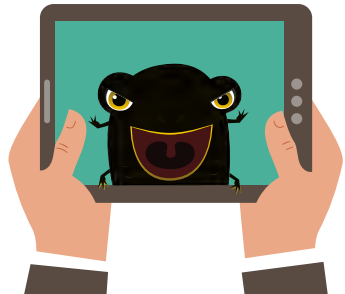
.apk มาแล้วสั่งติดตั้งเอง ซึ่งก่อนจะติดตั้ง Android ก็ยังมีหน้าต่างแสดงรายละเอียดชื่อโปรแกรมและสิทธิการเข้าถึงที่แอปพลิเคชันนั้นร้องขอมาให้ผู้ใช้ทราบก่อนอยู่ดี ในส่วนนี้จึงสามารถช่วยให้ผู้ใช้สังเกตเห็นความผิดปกติของแอปพลิเคชันก่อนที่จะติดตั้งได้ นอกจากนี้ใน Android ยังมีการตรวจสอบใบรับรองของแอปพลิเคชันที่มีชื่อซ้ำกับแอปพลิเคชันตัวที่เคยติดตั้งอยู่แล้วในระบบ ซึ่งหากพบว่าใบรับรองของแอปพลิเคชันเก่าและใหม่ไม่ตรงกันจะไม่ยอมให้ติดตั้ง

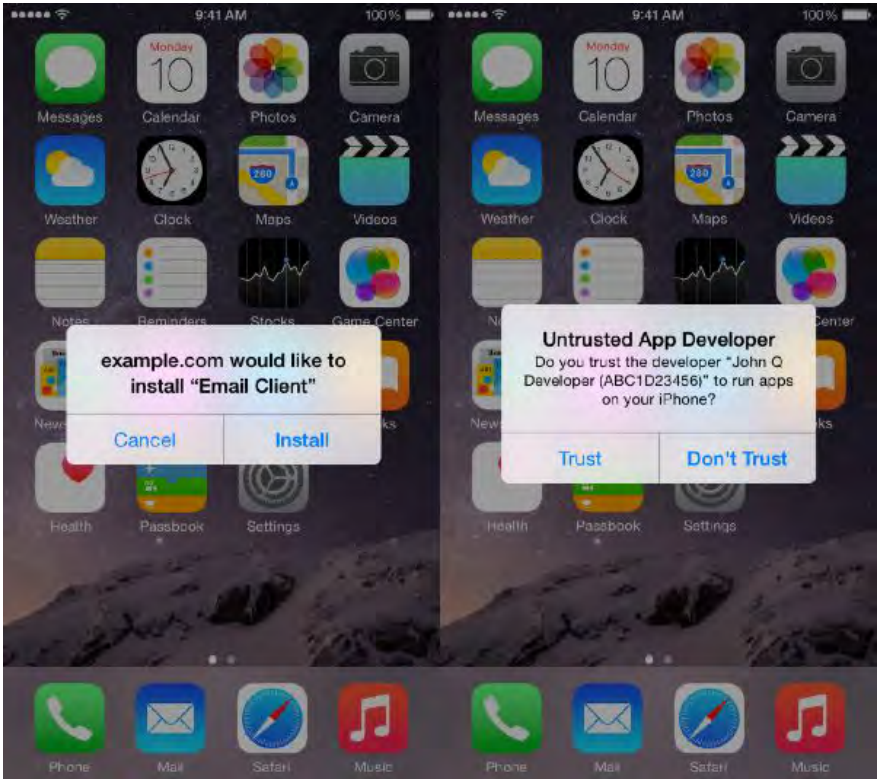
นอกจากนี้ จุดที่น่าเป็นห่วงอีกอย่างหนึ่งคือวิธีการโจมตีและแพร่กระจายมัลแวร์ ในกรณีของ WireLurker ที่แพร่กระจายโดยการติดไปกับโปรแกรมเถื่อนนั้น เป็นที่รู้กันดีกว่าการติดตั้งโปรแกรมเถื่อนนั้นมีอันตรายมากแค่ไหน และคนที่ชอบติดตั้งโปรแกรมเถื่อนก็ควรต้องรับทราบความเสี่ยงในจุดนี้อยู่แล้ว ส่วนที่น่าจะต้องระวังคงเป็นวิธีการหลอกลวงให้ผู้ใช้ทั่วไปดาวน์โหลดมัลแวร์ไปติดตั้งผ่านช่องโหว่ Masque Attack ซึ่งผู้ไม่หวังดีก็อาจไม่ต้องใช้วิธีสลับซับซ้อนอะไรมาก เพราะเป็นเพียงแค่การหลอกให้เหยื่อเปิดหน้าเว็บไซต์ ดังนั้นแค่การส่งลิงก์ไปทางอีเมลหรือทาง SMS แล้วบอกว่าเป็นโปรแกรมสำคัญต้องการให้ติดตั้ง ก็น่าจะมีผู้หลงเชื่อและเปิดเข้าเว็บไซต์เพื่อไปติดตั้งโปรแกรมอยู่แล้ว ซึ่งถ้าจะอ้างอิงจากเหตุการณ์การแพร่กระจายของมัลแวร์ใน Android เมื่อก่อนหน้านี้ก็สามารถยืนยันได้อย่างดีกว่าวิธีการนี้ยังได้ผล **[25]**

Apple ไม่แก้ไข ผู้ใช้ต้องระวังเอง

ถึงแม้จะมีการแพร่ระบาดของมัลแวร์ WireLurker รวมถึงมีนักวิจัยส่งข้อมูลเรื่องปัญหาของระบบ iOS Enterprise Deployment ไปให้กับทาง Apple หลายครั้งแล้วก็ตาม (วิธีการโจมตีแบบที่ WireLurker ใช้ มีการเผยแพร่ตั้งแต่เดือนสิงหาคม 2013 ส่วนทาง FireEye ก็แจ้งช่องโหว่ Masque Attack ไปให้ทาง Apple ตั้งแต่เดือนมิถุนายน 2014) แต่ทาง Apple ก็ได้ปฏิเสธที่จะแก้ไขปัญหานี้ โดยบอกว่ายังไม่พบว่ามีลูกค้าของ Apple ที่ประสบปัญหา และอีกอย่างระบบของ iOS และ OS X ก็ออกแบบมาเพื่อแจ้งเตือนให้ผู้ใช้ทราบในกรณีที่ผู้ใช้ติดตั้งแอปพลิเคชันที่อาจจะเป็นอันตรายอยู่แล้ว ดังนั้นหากผู้ใช้ติดตั้งแอปพลิเคชันนอกเหนือจากแหล่งที่มาที่ Apple กำหนดไว้ ก็ต้องระมัดระวังเอง **[26]**

Apple ได้เปิดหน้าเว็บไซต์ Support ขึ้นมาเพื่อบอกให้ผู้ใช้ระมัดระวังในการติดตั้งแอปพลิเคชันผ่านช่องทาง Enterprise Program **[27]** โดยหากผู้ใช้ไม่ต้องการจะติดตั้งแอปพลิเคชันที่พัฒนาขึ้นมาสำหรับเพื่อใช้งานในองค์กร แต่พบหน้าจอถามการติดตั้งโปรแกรมดังรูปที่ 5 ปรากฏขึ้นมา ก็ไม่ควรกดปุ่ม Install แต่หากกดไปแล้ว ในครั้งแรกที่ผู้ใช้กดเข้าไปใช้งานแอปพลิเคชันนั้น จะมีการแสดงชื่อของผู้พัฒนาแอปพลิเคชันขึ้นว่าและถามว่าผู้ใช้เชื่อถือนักพัฒนาคนนี้หรือไม่ หากผู้ใช้ไม่เชื่อถือหรือไม่แน่ใจก็ไม่ควรกดปุ่ม Trust และลบแอปพลิเคชันนี้ออกจากเครื่องโดยเร็ว





รูปที่ 5 การแจ้งเตือนด้านความมั่นคงปลอดภัยเมื่อผู้ใช้จะติดตั้งหรือเปิดใช้งานแอปพลิเคชันที่พัฒนาขึ้นมาเพื่อใช้งานในองค์กร

ข้อควรระวัง วิธีการตรวจสอบและแก้ไข

เนื่องจากตอนนี้รายงานจากศูนย์วิจัยด้านความมั่นคงปลอดภัยหลายแห่งมีความเห็นตรงกันว่าเป้าหมายของมัลแวร์ WireLurker มุ่งเน้นไปที่ผู้ใช้งานในประเทศจีนเป็นหลัก และการแพร่ระบาดของมัลแวร์ที่ใช้ช่องโหว่ Masque Attack นั้นปัจจุบันก็ยังไม่พบ ดังนั้นผู้ใช้ทั่วไปที่ไม่ได้มีการติดตั้งโปรแกรมเถื่อนหรือมีพฤติกรรมเสี่ยงอันตรายก็อาจจะไม่ต้องตื่นตระหนกกับปัญหานี้มากนัก แต่ก็ควรระมัดระวังและตระหนักถึงปัญหาที่อาจจะเกิดขึ้นได้

ในการป้องกันปัญหามัลแวร์ WireLurker การโจมตีผ่านช่องโหว่ Masque Attack หรือภัยคุกคามรูปแบบอื่นที่อาจใช้เทคนิคที่ใกล้เคียงกัน ผู้ใช้หรือองค์กรที่มีการใช้งานอุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS, Mac OS X และ Windows ควรมีความระมัดระวังดังนี้ [28]

• ติดตั้งโปรแกรมแอนติไวรัสในระบบปฏิบัติการ Windows และ Mac OS X พร้อมอัปเดตฐานข้อมูลให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

• ไม่ติดตั้งโปรแกรมที่ไม่ทราบแหล่งที่มาที่ชัดเจน หรือมาจากนักพัฒนาที่ไม่น่าเชื่อถือ โดยเฉพาะโปรแกรมเถื่อน

• อัปเดตระบบปฏิบัติการ iOS และแอปพลิเคชันที่ติดตั้งอยู่ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

• ขณะที่ใช้งานระบบปฏิบัติการ iOS หากพบหน้าจอสอบถามการติดตั้งแอปพลิเคชันแบบ Enterprise ถ้าไม่แน่ใจว่าเป็นแอปพลิเคชันที่ต้องการใช้งานจริง ๆ ก็ไม่ควรกดติดตั้ง

• หากเปิดใช้งานแอปพลิเคชันบนระบบปฏิบัติการ iOS แล้วระบบขึ้นแจ้งเตือนว่าแอปพลิเคชันนี้มาจากนักพัฒนาที่ไม่รู้จัก ถ้าไม่แน่ใจว่าแอปพลิเคชันนั้นมาจากนักพัฒนาที่เชื่อถือได้จริง ๆ ก็ไม่ควรกดเปิดใช้งาน และควรลบออกจากเครื่องโดยเร็วที่สุด

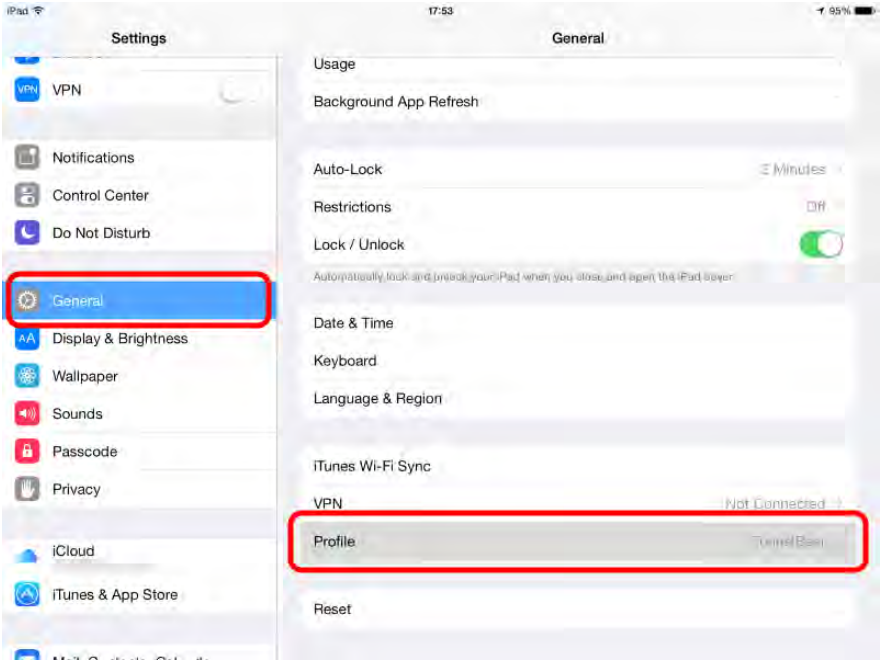
• ควรเสียบชาร์จอุปกรณ์ iOS จากปลั๊กไฟโดยตรงเท่านั้น ไม่ควรเสียบชาร์จจากอุปกรณ์อื่นหรือเสียบชาร์จจากเครื่องคอมพิวเตอร์ที่ไม่แน่ใจเรื่องความมั่นคงปลอดภัย

• ไม่ควรเชื่อมต่ออุปกรณ์ iOS เข้ากับเครื่องคอมพิวเตอร์ที่ไม่รู้จักหรือไม่แน่ใจเรื่องความมั่นคงปลอดภัย

• ไม่ควร Jailbreak อุปกรณ์ iOS หรือหาก Jailbreak แล้วก็ควรติดตั้งแอปพลิเคชันจากแหล่งที่มาที่น่าเชื่อถือเท่านั้น

สำหรับการตรวจสอบว่าเครื่อง Windows หรือ Mac OS X ที่ใช้งานอยู่นั้นติดมัลแวร์ WireLurker หรือไม่ สามารถตรวจสอบได้โดยใช้โปรแกรมแอนติไวรัสหรือใช้โปรแกรม WireLurker Detector ที่ทาง Palo Alto Networks เป็นผู้พัฒนาขึ้น **[29]** ส่วนการกำจัดมัลแวร์ WireLurker ออกจากเครื่องที่ใช้ Windows หรือ Mac OS X นั้น ปัจจุบันโปรแกรมแอนติไวรัสที่อัปเดตฐานข้อมูลเป็นเวอร์ชันล่าสุดสามารถกำจัดได้แล้ว

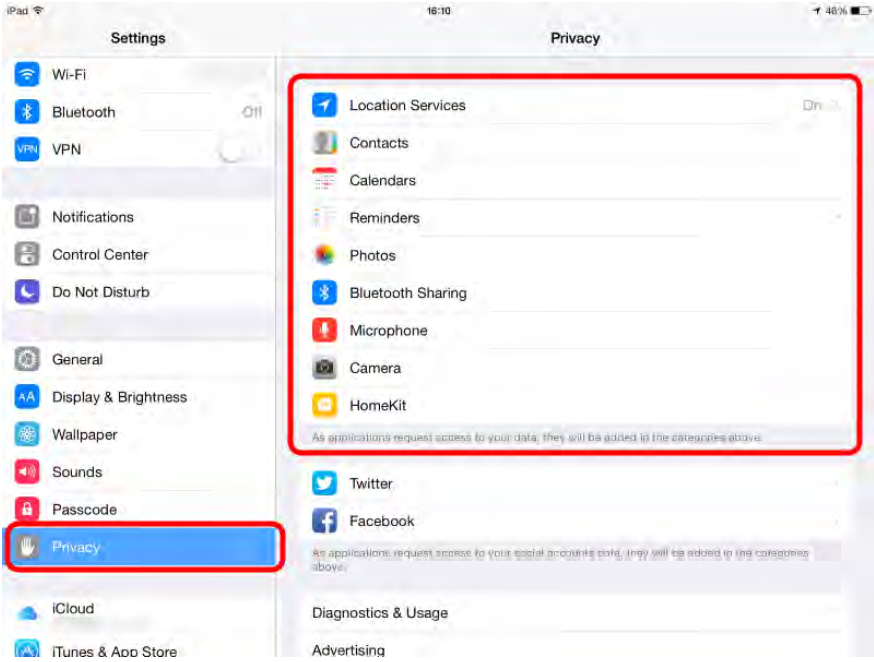
สำหรับการตรวจสอบว่าเครื่อง iOS ที่ใช้งานอยู่นั้นติดมัลแวร์ WireLurker หรือมีการติดตั้งแอปพลิเคชันแบบ Enterprise หรือไม่ สามารถตรวจสอบได้จากข้อมูล Profile ที่อยู่ในเครื่อง ซึ่งทำได้โดยการเข้าไปที่ Settings เลือกเมนู General แล้วไปที่ Profile ดังรูปที่ 6 โดยปกติแล้วผู้ใช้ทั่วไปที่ไม่ได้ติดตั้งแอปพลิเคชันขององค์กรไม่ควรมี Profile อื่นอยู่ หากพบ Profile ที่ไม่รู้จักให้ลบออกทันที



รูปที่ 6 ตัวอย่างอุปกรณ์ iOS ที่มี Profile ชื่อ TunnelBear
ติดตั้งอยู่ในเครื่อง

นอกจากนี้ยังอาจสังเกตได้จากการเปิดใช้งานแอปพลิเคชันที่ติดตั้งอยู่ในเครื่อง โดยแอปพลิเคชันปลอมที่ถูกติดตั้งเข้าไปทับ เมื่อเปิดใช้งานครั้งแรกจะปรากฏหน้าจอสอบถามว่าต้องการเปิดใช้งานแอปพลิเคชันที่มาจากนักพัฒนาภายนอกหรือไม่ ซึ่งหากพบความผิดปกติลักษณะนี้ไม่ควรกดใช้งานต่อและรีบลบแอปพลิเคชันนี้ออกจากเครื่องทันที

หากพบว่าเครื่อง iOS ติดมัลแวร์ WireLurker หรือถูกติดตั้งแอปพลิเคชันแบบ Enterprise โดยที่ผู้ใช้ไม่ได้เป็นคนทำ วิธีการแก้ปัญหาคือลบแอปพลิเคชันอันตรายออกจากเครื่อง ตรวจสอบและลบ Profile แปลกปลอม รวมทั้งตรวจสอบการอนุญาตให้แอปพลิเคชันเข้าถึงเข้ามูลส่วนบุคคล ซึ่งสามารถทำได้โดยเข้าไปที่ Settings เลือกหัวข้อ Privacy และตรวจสอบสิทธิการเข้าถึงของแอปพลิเคชันในหมวดต่าง ๆ เช่น Contact, Photos, Microphone, Camera ดังรูปที่ 7 ซึ่งหากพบแอปพลิเคชันใดที่ไม่ต้องการให้เข้าถึงความสามารถในส่วนนี้สามารถปิดเฉพาะแอปพลิเคชันนั้นได้ **[30]** แต่หากยังไม่มั่นใจว่าจะแก้ปัญหาทั้งหมดได้ อาจพิจารณาการทำ Factory Reset เพื่อล้างข้อมูลในเครื่องทั้งหมด



รูปที่ 7 การตรวจสอบสิทธิการเข้าถึง Privacy
ของแอปพลิเคชันต่าง ๆ ใน iOS

สรุป

ถึงแม้ว่าปัญหามัลแวร์ใน iOS ที่สามารถติดในเครื่องที่ไม่ถูก Jailbreak ได้จะไม่ใช่เรื่องใหม่ แต่การแพร่ระบาดของมัลแวร์ WireLurker ก็ถือเป็นสัญญาณหนึ่งที่บ่งบอกได้ว่านักพัฒนามัลแวร์เริ่มเล็งเป้ามาที่การโจมตีอุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS แล้ว

ส่วนปัญหา Masque Attack นั้นเนื่องจากทาง Apple บอกแล้วว่าไม่ได้สนใจที่จะแก้ไข ดังนั้นเป็นหน้าที่ของผู้ใช้เองที่ต้องตรวจสอบและระวังตัว ไม่ติดตั้งแอปพลิเคชันที่ไม่ทราบแหล่งที่มาชัดเจน และหากยืนยันจะติดตั้งแอปพลิเคชันก็ควรอ่านคำเตือนที่ปรากฏขึ้นมาบนหน้าจอทุกครั้งก่อนที่จะดำเนินการต่อ ส่วนในอนาคตจะมีการแพร่ระบาดของมัลแวร์ที่โจมตีโดยใช้ช่องโหว่นี้หรือไม่นั้นก็คงเป็นเรื่องที่ต้องติดตามกันต่อไป

อ้างอิง

1. http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/
2. https://developer.apple.com/app-store/review/guidelines/
3. http://www.ibtimes.com/google-play-store-gets-built-malware-scanner-alerts-users-against-possible-threats-download-stage
4. http://support.apple.com/en-us/HT202070
5. http://android-developers.blogspot.com/2010/04/multitasking-android-way.html
6. http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/
7. http://www.cnet.com/news/researchers-slip-malware-onto-apples-app-store-again/
8. https://blog.fortinet.com/post/ios-malware-does-exist
9. http://www.fortiguard.com/encyclopedia/virus/#id=2102975
10. http://securelist.com/blog/incidents/33544/find-and-call-leak-and-spam-57/
11. http://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html
12. http://3qilabs.com/how-to-ad-hoc-distribute-your-ios-app-via-a-website-and-ota/
13. https://www.thaicert.or.th/papers/general/2013/pa2013ge007.html
14. http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/
15. http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-windows/
16. http://securelist.com/blog/67457/ios-trojan-wirelurker-statistics-and-new-information/
17. http://blog.kaspersky.com/wirelurker-ios-osx-malware/
18. https://www.apple.com/ipad/business/docs/iOS_Enterprise_Deployment_Overview_EN_Feb14.pdf
19. https://developer.apple.com/programs/ios/enterprise/
20. http://stackoverflow.com/questions/22745946/is-there-any-limitation-to-distribution-of-apps-in-ios-enterprise-program
21. http://www.fireeye.com/blog/technical/cyber-exploits/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html
22. https://kb.acronis.com/content/39368
23. https://developer.apple.com/library/ios/documentation/IDEs/Conceptual/AppDistributionGuide/ConfiguringYourApp/ConfiguringYourApp.html
24. https://thaicert.or.th/papers/general/2014/pa2014ge004.html
25. https://thaicert.or.th/alerts/user/2014/al2014us017.html
26. http://www.imore.com/apple-comments-masque-attack
27. http://support.apple.com/en-us/HT6584
28. https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
29. https://github.com/PaloAltoNetworks-BD/WireLurkerDetector
30. http://blog.trendmicro.com/trendlabs-security-intelligence/removing-wirelurker-from-your-ios-or-osx-device/


!
NEWS

ข่าวสั้น

หลอดไฟก็โดนแฮกได้

ในยุค Smart Home ที่อุปกรณ์ไฟฟ้าต่าง ๆ เช่น ทีวี ตู้เย็น ควบคุมการทำงานผ่านอินเทอร์เน็ตหรือ WiFi จากอุปกรณ์ต่าง ๆ อย่างสมาร์ตโฟนได้ นักวิจัยพบช่องโหว่ในอุปกรณ์เหล่านี้ ล่าสุดบริษัทด้านความมั่นคงปลอดภัย Contextis ได้ค้นพบช่องโหว่ในหลอดไฟอัจฉริยะ LIFX ที่ทำให้ผู้ไม่หวังดีสามารถควบคุมการเปิดปิดหรือเปลี่ยนสีของหลอดไฟได้

วันที่: 2014-07-16 | ที่มา: Contextis <http://thcert.co/kY2fPT>

พบช่องโหว่ที่ทำให้ข้อมูลไฟล์บน Google Drive รั่วไหล

โดยปกติเมื่อคลิกลิงก์เอกสารบน Google Drive จะมีการนำผู้ใช้ไปยังเว็บไซต์ตามลิงก์ แต่ช่องโหว่นี้ทำให้เจ้าของเว็บไซต์ สามารถดูหัวข้อของข้อมูล รวมถึงอาจอ่านเอกสารนั้นได้ ซึ่งช่องโหว่นี้ไม่ได้เกิดขึ้นกับทุกเอกสาร ขณะนี้ Google ได้หาทางปิดช่องโหว่นี้ไม่ให้เกิดขึ้นกับเอกสารที่สร้างใหม่แล้ว ส่วนเงื่อนไขของเอกสารที่ได้รับผลกระทบและวิธีแก้ไขสามารถอ่านได้ที่ https://nakedsecurity.sophos.com/2014/07/10/google-drive-security-hole-leaks-users-files/

วันที่: 2014-07-16 | ที่มา: Naked Security <http://thcert.co/7107j3>

อัปเดต Java ปิดช่องโหว่

เมื่อวันที่ 14 กรกฎาคม Oracle ได้ปล่อยอัปเดตปิด 20 ช่องโหว่ใน Java ซึ่งมีอยู่ 8 ช่องโหว่ที่เป็นช่องโหว่ร้ายแรงซึ่งเปิดโอกาสให้ผู้ไม่หวังดีสามารถโจมตีจากระยะไกลโดยไม่จำเป็นต้องยืนยันตัวตน (Authentication) กรณีที่ใช้ Java 7 แนะนำให้อัปเดตเป็น Java 7 Update 65 ส่วนที่ใช้ Java 8 ให้อัปเดตเป็น Java 8 Update 11 ใครที่สงสัยว่าเครื่องคอมพิวเตอร์ตัวเองมี Java หรือเปล่า หรือเป็นเวอร์ชันเก่าหรือไม่ ก็สามารถตรวจสอบได้ที่ https://www.java.com/en/download/installed.jsp

วันที่: 2014-07-17 | ที่มา: Oracle <http://thcert.co/680eK1>

ผู้ใช้ Facebook ตกเป็นเป้าอันดับหนึ่งของผู้ใช้โซเชียลมีเดียที่ถูกโจมตีด้วย Phishing

Kaspersky เตือนผู้ใช้ Facebook ตกเป็นเป้าอันดับหนึ่งของผู้ใช้โซเชียลมีเดียที่ถูกโจมตีด้วยวิธี Phishing โดยพบการตรวจจับหน้าล็อกอินปลอมของ Facebook ถึง 11% จากการตรวจจับหน้าเว็บล็อกอินปลอมทั้งหมดจากแอนติไวรัสบนเครื่องผู้ใช้

วันที่: 2014-07-20 | ที่มา: Kaspersky <http://thcert.co/m5S922>

เว็บข่าว CNET โดนเจาะ แฮกเกอร์ได้ข้อมูลผู้ใช้ 1 ล้านคน

เว็บข่าวเทคโนโลยีอย่าง CNET ตกเป็นเหยื่อของการโจมตีทางไซเบอร์ของแฮกเกอร์ที่ใช้นามแฝง Twitter ว่า rev_priv8 โดยเขาได้โจมตีผ่านช่องโหว่ของ Symfony PHP Framework ซึ่งข้อมูลที่ถูกขโมยไปได้แก่ อีเมล ไอดี และรหัสผ่านที่มีการเข้ารหัสลับของผู้ใช้ 1 ล้านคน ใครที่เป็นสมาชิกของเว็บไซต์ CNET ขอแนะนำให้เปลี่ยนรหัสผ่านของบัญชีผู้ใช้บนเว็บไซต์ CNET รวมทั้งบัญชีผู้ใช้อื่น ๆ ที่ใช้รหัสผ่านเดียวกัน

วันที่: 2014-07-21 | ที่มา: Naked Security <http://thcert.co/I6iKc9>

Password Manager เก็บรหัสผ่านอย่างมั่นคงปลอดภัยจริงหรือ?

นักวิจัยพบช่องโหว่ของบริการที่ใช้เก็บรหัสผ่าน (Password Manager) อย่าง LastPass และอีก 4 Password Manager โดยสามารถขโมยรหัสผ่านที่เก็บไว้ได้ แต่โอกาสที่จะนำช่องโหว่นี้ไปโจมตีได้จริงค่อนข้างต่ำ

วันที่: 2014-07-22 | ที่มา: Arstechnica <http://thcert.co/6MshY9>

ผลสำรวจประเทศใดส่งสแปมมากที่สุดจาก Sophos

Sophos ได้ทำการสำรวจถึงปริมาณการส่งสแปมของประเทศต่าง ๆ ในช่วงไตรมาสที่ 2 พบว่า 3 อันดับแรกคือ สหรัฐฯ ฝรั่งเศส และ จีน โดยปริมาณการส่งสแปมของสหรัฐฯ คิดเป็น 25% ของทั้งหมด แต่หากคำนวณองค์ประกอบตามสัดส่วนประชากรของแต่ละประเทศ พบว่า 3 อันดับแรกคือ บัลแกเรีย เบลารุส และ สวิตเซอร์แลนด์

วันที่: 2014-07-23 | ที่มา: Naked Security <http://goo.gl/RCmt7y>

เว็บเพจที่ Google ต้องลืม แต่ “Hidden From Google” รวมไว้ให้จำ

หลัง Google ได้รับคำสั่งศาลยุโรปให้ถอนบางเว็บเพจที่ส่งผลกระทบด้านลบต่อชีวิตส่วนบุคคลออกจากผลลัพธ์ในบริการค้นหา ตามคำร้องขอของบุคคลต่าง ๆ เช่น หน้าเว็บเพจข่าวเกี่ยวกับการประมูลขายบ้านเพราะร้อนเงินของนาย Costeja González เพราะถือว่าเป็นการคุ้มครองข้อมูลส่วนบุคคล ซึ่ง Google มองว่ามีผลกระทบต่อเสรีภาพการรับรู้ข้อมูลข่าวสารของประชาชน เหตุการณ์นี้ทำให้ผู้คนนับหมื่นร้องขอ Google ในลักษณะคล้ายกัน ล่าสุดเว็บไซต์ Hidden From Google ได้รวบรวมเว็บเพจที่ได้รับการถอดออกจากการค้นหาของ Google ใครสนใจเข้าไปดูได้ที่ http://hiddenfromgoogle.afaqtariq.com/

วันที่: 2014-07-24 | ที่มา: Naked Security <http://thcert.co/5S5bz8>

ญี่ปุ่นเตรียมพร้อมต้านภัยไซเบอร์

ในอีก 1 เดือนข้างหน้า คาดการณ์ว่ารัฐบาลญี่ปุ่นจะสามารถผ่านกฎหมายที่เสริมสร้างความมั่นคงปลอดภัยให้กับประเทศ ซึ่งกฎหมายนี้จะทำให้หน่วยงาน NISC (National Information Security Center) มีอำนาจทางกฎหมายที่ช่วยในการรับมือและจัดการภัยคุกคาม รวมถึงเสริมสร้างความร่วมมือจากหน่วยงานโครงสร้างพื้นฐานด้านการเงิน การคมนาคม และการไฟฟ้า นอกจากนี้กฎหมายยังบังคับให้หน่วยงานภาคเอกชนที่โดนโจมตีต้องรายงานการโจมตีโดยไม่ปิดบังอีกด้วย

วันที่: 2014-07-25 | ที่มา: Bloomberg <http://thcert.co/61Mfp3>

ศาลตัดสิน รัฐบาลเนเธอร์แลนด์ใช้ข้อมูลที่สอดแนมมาแบบผิดกฎหมายได้

ศาลสูงสุดของประเทศเนเธอร์แลนด์เพิ่งตัดสินให้รัฐบาลเนเธอร์แลนด์มีสิทธิใช้ข้อมูลสอดแนมที่ได้มาจากหน่วยงานต่างประเทศ อย่างเช่น NSA ถึงแม้ว่าการสอดแนมนั้นจะมาด้วยวิธีที่ผิดกฎหมาย ตามกฎหมายของประเทศเนเธอร์แลนด์ รัฐบาลสามารถสอดแนมข้อมูลแบบมีเป้าหมายเฉพาะเท่านั้น ไม่สามารถดักข้อมูลที่วิ่งผ่านเครือข่ายโดยไม่เฉพาะเจาะจง (Untargeted Interception) เหมือนอย่างหน่วยงานในรัฐบาลอเมริกา ซึ่งรัฐบาลกำลังร่างข้อเสนอเปลี่ยนกฎหมายให้สามารถสอดแนมได้ลักษณะนี้ นี่อาจเป็นเหตุผลหนึ่งที่รัฐบาลยังต้องการข้อมูลสอดแนมจากหน่วยงานต่างประเทศอยู่ และถึงแม้รัฐบาลจะชนะในชั้นศาล รัฐบาลก็ถูกบังคับให้เปิดเผยว่า มีส่วนร่วมกับ NSA ในการดักฟัง 1.8 ล้านการสนทนาทางโทรศัพท์

วันที่: 2014-07-28 | ที่มา: ZDnet <http://thcert.co/t0iByB>

Googlebot ปลอม ถูกใช้เพื่อโจมตี DDoS

บริษัท Incapsula พบว่าทุก ๆ 25 Googlebot ที่มาเยี่ยมเว็บไซต์ 1 ในนั้นเป็น Googlebot ปลอมที่มีจุดประสงค์ร้าย และประมาณ 1 ใน 4 ของ Googlebot ปลอม ถูกใช้ในการโจมตีประเภท DDoS

วันที่: 2014-07-28 | ที่มา: Threatpost <http://thcert.co/99672t>

Intel เปิดตัวฮาร์ดดิสก์ SSD รุ่นใหม่ มีชิปเข้ารหัสลับข้อมูลในตัว

Intel เปิดตัวฮาร์ดดิสก์แบบ SSD สำหรับใช้ในหน่วยงานที่ต้องการเก็บรักษาความลับของข้อมูล ในชื่อรุ่น Intel SSD 2500 Pro ฮาร์ดดิสก์รุ่นนี้ติดตั้งชิปสำหรับเข้ารหัสลับข้อมูลแบบ 256-bit มาให้ในตัว เพื่อประหยัดการใช้พลังงานไฟฟ้าและไม่ให้กระทบกับประสิทธิภาพการทำงานของระบบ

วันที่: 2014-07-29 | ที่มา: The Hacker News <http://thcert.co/K1qKHh>

Debian ปล่อยแพตช์ปิดช่องโหว่ Modsecurity ของ Apache

จากช่องโหว่ของ Modsecurity หมายเลข CVE-2013-5705 ซึ่งส่งผลให้ผู้ไม่หวังดีสามารถ Bypass การป้องกันของ Modsecurity ของ Apache ในการโจมตีเว็บไซต์ได้ ล่าสุดมีการปล่อยแพตช์สำหรับ Debian แล้ว สามารถดูรายละเอียดได้ที่ http://thcert.co/qq7876

วันที่: 2014-07-29 | ที่มา: Debian <http://thcert.co/qq7876>

ผู้ใช้ในยุโรปเสี่ยงสูง เพราะ Browser Plugin เก่า

จากข้อมูลของบริษัท Cyscon พบว่ามีผู้ใช้ฝั่งยุโรปจำนวนมากไม่ได้อัปเดต Browser Plugin ซึ่งทำให้เสี่ยงต่อการถูกโจมตี หากดูในสถิติตามเว็บ thcert.co/EUDg39 พบว่าประเทศไทยมี 74 % ที่ใช้เบราว์เซอร์เวอร์ชันเก่า นอกจากนี้ผู้สนใจสามารถเข้าไปตรวจสอบเบราว์เซอร์ และ Browser Plugin ของตัวเองว่าเก่าหรือไม่ ได้ที่ thcert.co/48M5Ga

วันที่: 2014-07-30 | ที่มา: Softpedia <http://thcert.co/Nd7R36>

ข้อมูลเทคโนโลยีระบบป้องกันขีปนาวุธอิสราเอล Iron Dome ถูกขโมย

รายงานข่าวจากเว็บ KrebsonSecurity ระบุว่า มีการโจมตีทางไซเบอร์เพื่อขโมยข้อมูลเทคโนโลยีระบบป้องกันขีปนาวุธอิสราเอลที่ชื่อ Iron Dome ระหว่างปี 2554-2555 จาก 3 บริษัทผู้รับจ้างพัฒนาระบบนี้ ซึ่งผลตรวจสอบของบริษัท CyberESI พบว่าเป็นกลุ่มแฮกเกอร์จากฝ่ายทหารของประเทศจีน รัฐบาลอิสราเอลได้ให้เครดิตกับ Iron Dome ว่าเป็นระบบที่ช่วยป้องกันจรวดที่ยิงจากกองกำลังปาเลสไตน์กว่า 2,000 ลูก และรัฐบาลสหรัฐฯ กำลังพิจารณาลงทุนเพิ่มอีก 350 ล้าน รวมเป็น 1 พันล้านดอลลาร์สำหรับการผลิต Iron Dome ในช่วงกว่า 5 ปี

วันที่: 2014-07-30 | ที่มา: Krebsonsecurity <http://thcert.co/y71IkT>

นักวิจัยพบวิธีโจมตีอุปกรณ์ Android ผ่านลำโพงของตัวเครื่อง

นักวิจัยค้นพบวิธีในการโจมตีอุปกรณ์ที่ใช้งานระบบปฏิบัติการ Android เพื่อให้ส่งข้อความ ส่งอีเมล หรือเข้าถึงข้อมูลสำคัญที่เก็บอยู่ในเครื่องได้โดยใช้แอปพลิเคชันที่ไม่จำเป็นต้องมีการร้องขอสิทธิ (Permission) แต่อย่างใด นักวิจัยเรียกวิธีการโจมตีดังกล่าวว่า GVS-Attack GVS ย่อมาจาก Google Voice Search ซึ่งเป็นฟังก์ชันที่มาพร้อมอุปกรณ์ที่ใช้งานระบบ Android ทุกเครื่องอยู่แล้ว โดยจะรับคำสั่งจากเสียงของผู้ใช้แล้วนำมาทำงาน ทำให้นักวิจัยสามารถอัดเสียงคำสั่งต่าง ๆ เช่น โทรศัพท์ออกไปยังหมายเลขปลายทางหรือส่งข้อความ จากนั้นเรียกใช้งาน Google Voice Search แล้วให้แอปพลิเคชันที่ติดตั้งในเครื่อง เล่นเสียงที่อัดไว้ออกทางลำโพง ก็สามารถสั่งงานเครื่องให้ทำตามคำสั่งที่ต้องการได้

วันที่: 2014-07-30 | ที่มา: Net-security <http://thcert.co/7p3B85>

ทดสอบแฮกบัญชีผู้ใช้ IG ผ่าน WiFi

นาย Mazin Ahmed ได้สาธิตการแฮกเพื่อเข้าบัญชีผู้ใช้ Instagram โดยไม่ได้รับอนุญาต ด้วยการดักจับข้อมูลระหว่างแอปพลิเคชันและเซิร์ฟเวอร์ผ่าน WiFi เนื่องจากข้อมูลไม่ได้มีการเข้ารหัสระหว่างการรับส่ง ทำให้สามารถใช้ข้อมูลที่ขโมยเพื่อเข้าถึงบัญชีผู้ใช้ได้ ซึ่งทาง Facebook ได้รับรายงานข้อมูลดังกล่าวแล้ว แต่ยังไม่ได้ชี้แจงการดำเนินการแก้ไขจุดอ่อนดังกล่าว

วันที่: 2014-07-30 | ที่มา: Arstechnica <http://thcert.co/cx3K8S>

นักวิจัยพบ 70% ของ Internet of Things มีช่องโหว่

Internet of Things คืออุปกรณ์อัจฉริยะต่าง ๆ ที่สามารถแลกเปลี่ยนข้อมูลกับอุปกรณ์อื่นและเชื่อมต่อกับอินเทอร์เน็ตได้ ซึ่งอาจเป็นอุปกรณ์ที่เราใช้ในชีวิตประจำวัน เช่น ทีวี ตู้เย็น แว่นตา ฯลฯ

จากการศึกษาโดย Hewlett-Packard security unit Fortify พบว่า 70% ของอุปกรณ์เหล่านี้มีช่องโหว่ เนื่องจากไม่มีการเข้ารหัสลับข้อมูลหรือการจำกัดการเข้าถึงข้อมูลที่เพียงพอ และพบเฉลี่ย 25 ช่องโหว่ต่ออุปกรณ์

วันที่: 2014-07-31 | ที่มา: Phys <http://thcert.co/3Y62DV>

USB อันเดียวก็เสียวได้

จากเหตุการณ์โจมตีโรงงานนิวเคลียร์ด้วยมัลแวร์ชื่อดังอย่าง Stuxnet ที่แพร่จาก USB Stick อุปกรณ์หนึ่งที่นิยมใช้แพร่มัลแวร์ ล่าสุดนักวิจัยด้านความมั่นคงปลอดภัยได้ออกมาเปิดเผยเทคนิคชื่อ BadUSB ที่สามารถเปลี่ยนอุปกรณ์ที่เชื่อมต่อด้วย USB เช่น Keyboard, Web Cam หรือสมาร์ตโฟนมือถือ Andriod ให้กลายเป็นอุปกรณ์วายร้ายที่ควบคุมเครื่องคอมพิวเตอร์ หรือหลอกให้เข้าเว็บปลอม อย่าง Google, Facebook เพื่อขโมยไอดี/รหัสผ่านของผู้ใช้

ทั้งนี้การตรวจสอบอุปกรณ์เชื่อมต่อผ่าน USB ว่ามีการดัดแปลงให้สามารถโจมตีด้วยเทคนิคนี้หรือไม่นั้นทำได้ยาก และแอนติไวรัสก็ไม่สามารถตรวจจับได้ ซึ่งลักษณะการโจมตีเป็นการดัดแปลงในส่วนของเฟิร์มแวร์ เพื่อเพิ่มความสามารถต่าง ๆ ในการโจมตี

วันที่: 2014-08-01 | ที่มา: Arstechnica <http://thcert.co/5x5XxF>

หน้าเว็บปลอม Facebook หลอกเอามากกว่า ไอดี/รหัสผ่าน

หนึ่งในวิธีนิยมที่แฮกเกอร์ชอบใช้คือการสร้างหน้าล็อกอินปลอมเพื่อหลอกให้เหยื่อใส่ไอดี/รหัสผ่าน แต่นักวิจัยจาก Malwarebytes ค้นพบการหลอกลวงอีกแบบที่กำลังแพร่หลายโดยมีลักษณะแจ้งว่าบัญชีโดนล็อก และให้ใส่ข้อมูลต่าง ๆ เพื่อยืนยันตัวตน เช่น ไอดี/รหัสผ่าน อีเมลที่ใช้สมัคร หมายเลขบัตรเครดิต คำถามคำตอบเพื่อยืนยันตัวตน (Security Question)

วันที่: 2014-08-01 | ที่มา: Malwarebytes <http://thcert.co/yAay92>

ฝ่ายต่อต้านรัฐบาลแฮกทีวีโปรแกรมจีน

เมื่อวันที่ 11 สิงหาคมที่ผ่านมา แฮกเกอร์กลุ่มต่อต้านรัฐบาลคอมมิวนิสต์จีนได้ทำการเจาะระบบเครือข่ายเคเบิลทีวีที่มีผู้ชม 4 ล้านคน เผยแพร่ข้อความโจมตีรัฐบาลนาน 10 นาที

วันที่: 2014-08-04 | ที่มา: Internation Business Times <http://thcert.co/761rMs>

มัลแวร์ระบาดบนเครื่องรูดบัตรเครดิต

หน่วยงานด้านความมั่นคงปลอดภัยสหรัฐฯ US-CERT เตือนการระบาดของมัลแวร์ชื่อ “Backoff” ตามเครื่องรับชำระเงินผ่านบัตรเครดิต (PoS-Point of Sale) ต่าง ๆ ซึ่งมัลแวร์ที่ว่าสามารถขโมยข้อมูลบัตรเครดิตที่ทำการรูดบน PoS ที่ติดมัลแวร์นี้ เนื่องจาก PoS เหล่านี้ได้รับการติดตั้ง Remote Desktop Application เช่น Microsoft Remote Desktop, Apple Remote Desktop หรือ LogMeIn ซึ่งมีการตั้งรหัสที่เดาได้ง่ายหรือรหัสผ่านเดียวกัน ทำให้แฮกเกอร์สามารถเข้าถึง PoS เหล่านี้และเผยแพร่มัลแวร์ได้

วันที่: 2014-08-04 | ที่มา: US-CERT <http://thcert.co/2R78Uo>

EMET 5.0 ออกแล้ว

EMET เป็นเครื่องมือที่ใช้เสริมความมั่นคงปลอดภัยให้กับซอฟต์แวร์ต่าง ๆ ที่ติดตั้งอยู่ในระบบปฏิบัติการ Windows ล่าสุดทาง Microsoft ได้ออก EMET รุ่น 5.0 ซึ่งเพิ่มความสามารถเด่น ๆ อย่าง “Attack Surface Reduction (ASR) tool” ที่ช่วยเพิ่มทางเลือกในการป้องกันการโจมตีผ่านทางปลั๊กอินต่าง ๆ เช่น การบล็อกเว็บไซต์จากอินเทอร์เน็ตไม่ให้ใช้ Java แต่อนุญาตให้เว็บไซต์จากอินทราเน็ตใช้ได้ หรือการบล็อกไม่ให้ Microsoft Word เรียกใช้ Adobe Flash ที่ฝังไว้ในไฟล์เอกสาร ใครสนใจทดลองดาวน์โหลดได้ที่เว็บไซต์ของ Microsoft

วันที่: 2014-08-05 | ที่มา: Technet <http://thcert.co/69pvzU>

Symantec

ช่องโหว่ Privilege Escalation ใน Symantec Endpoint Protection

Offensive-security พบช่องโหว่ใน Symantec Endpoint Protection ซึ่งเป็นผลิตภัณฑ์รักษาความมั่นคงปลอดภัยเครื่องคอมพิวเตอร์ของ Symantec ช่องโหว่ดังกล่าวทำให้ Local User ได้รับสิทธิการทำงานเกินปกติ (Privilege Escalation)

วันที่: 2014-08-05 | ที่มา: Security Tracker <http://thcert.co/XN5koa>

มัลแวร์ IcoScript ใช้อีเมล Yahoo รับคำสั่งแฮกเกอร์

นักวิจัยได้ค้นพบมัลแวร์ชื่อ "IcoScript" ที่ใช้บริการอีเมล Yahoo เป็นช่องทางติดต่อสื่อสารกับแฮกเกอร์เพื่อรับคำสั่ง และมัลแวร์ดังกล่าวหลุดรอดการตรวจจับตั้งแต่ปี 2012 ความโดดเด่นของเจ้ามัลแวร์นี้อยู่ที่ความสามารถในการเชื่อมต่อกับเว็บไซต์ Yahoo ผ่านโปรแกรม Internet Explorer และที่สำคัญแฮกเกอร์สามารถตั้งค่าให้มัลแวร์เชื่อมต่อกับระบบอื่น ๆ อย่าง เช่น Gmail, Facebook หรือ LinkedIn ได้ง่ายดาย การใช้บริการยอดนิยมเหล่านี้เป็นช่องทางในการติดต่อ ทำให้ไม่สามารถ Blacklist URL เพื่อบล็อกการเชื่อมต่อ อีกทั้งยังทำให้ตรวจจับมัลแวร์จากการเชื่อมต่อได้ยากขึ้น

วันที่: 2014-08-06 | ที่มา: Softpedia <http://thcert.co/X7G8N1>

แก๊ง CyberVor ขโมย 1.2 พันล้านไอดี/รหัสผ่าน

บริษัทด้านความมั่นคงปลอดภัย Hold Security ค้นพบแก๊งอาชญากรไซเบอร์ชาวรัสเซียที่ขโมย 4.5 พันล้านข้อมูล ซึ่งเป็นไอดี/รหัสผ่านอยู่ 1.2 พันล้านข้อมูล ถือได้ว่าเป็นหนึ่งในการขโมยข้อมูลที่มีจำนวนมากที่สุดเลยทีเดียว โดยแก๊งดังกล่าวได้รับการตั้งชื่อว่า CyberVor

การขโมยข้อมูลของแก๊งนี้เริ่มจากการควบคุมกลุ่มคอมพิวเตอร์ที่ติดมัลแวร์ (Botnet) จำนวนหนึ่ง เพื่อใช้หาช่องโหว่ประเภท SQL Injection ในเว็บไซต์ต่าง ๆ จากนั้นจึงทำการแฮกเว็บไซต์ที่มีช่องโหว่มากกว่า 400,000 เว็บเพื่อขโมยข้อมูลที่เก็บไว้ในเว็บไซต์

ทั้งนี้ Hold Security ได้เปิดให้บริการแจ้งเตือนเจ้าของเว็บไซต์เมื่อพบว่าถูกแฮกโดยมีค่าใช้จ่าย และเตรียมให้บริการฟรีแจ้งเตือนแก่ผู้ใช้ทั่วไปว่าไอดี/รหัสผ่านของตนถูกขโมยหรือไม่ ในเร็ว ๆ นี้

วันที่: 2014-08-07 | ที่มา: Hold Security <http://thcert.co/0S866M>

Google ลด Ranking เว็บที่ไม่ใช้การเชื่อมต่อแบบเข้ารหัสลับ (HTTPS)

Google ยักษ์ใหญ่แห่งวงการ Search Engine ได้ตัดสินใจนำปัจจัยที่ว่า เว็บไซต์ใช้ HTTPS หรือไม่ มาคิดคำนวณในการจัดอันดับเว็บไซต์ (Ranking) เพื่อส่งเสริมการใช้ HTTPS เข้ารหัสลับข้อมูลที่รับส่งระหว่างผู้เข้าเว็บและเว็บเซิร์ฟเวอร์ นับเป็นอีกสัญญาณที่แสดงว่า Google ให้ความสำคัญกับความมั่นคงปลอดภัย ถึงแม้ปัจจัยนี้จะยังมีผลน้อยต่อการคำนวณในการจัดอันดับ โดยส่งผลกระทบต่อการค้นหาเพียง 1% ของการค้นหาทั่วโลก แต่ทาง Google ก็อาจจะเพิ่มความสำคัญของปัจจัยนี้ในอนาคต

วันที่: 2014-08-08 | ที่มา: Google Online Security <http://thcert.co/m75uU2>

ระวัง แมว อาจเข้ามาแอบเก็บข้อมูลรหัสผ่าน WiFi ที่บ้านท่าน

นักวิจัยด้านความมั่นคงปลอดภัยได้ทดลองใช้แมวเดินเก็บข้อมูล WiFi ของเพื่อนบ้าน โดยได้ทำปลอกคอแมวที่มีแผงวงจรติดชิป WiFi, GPS, ชิปวิเคราะห์ข้อมูล WiFi และแบตเตอรี่ จากนั้นปล่อยให้แมวเดินไปทั่วหมู่บ้านเพื่อสแกนข้อมูล WiFi ที่แต่ละบ้านปล่อยออกมา แล้วนำข้อมูลมาพล็อตลงในแผนที่

จากการปล่อยให้แมวเดินสำรวจหมู่บ้านเป็นเวลา 3 ชั่วโมง พบการปล่อย WiFi ทั้งหมด 23 จุด มี 4 จุดที่ใช้เฟิร์มแวร์ของเราเตอร์เป็นเวอร์ชันเก่าและสามารถเจาะรหัสผ่านได้ และอีก 4 จุดไม่มีการตั้งค่าความมั่นคงปลอดภัยในการเชื่อมต่อเลย

นักวิจัยเรียกวิธีการนี้ว่า “Warkitteh” โดยล้อเลียนมาจากคำว่า Wardriving ซึ่งเป็นการที่ผู้ไม่หวังดีขับรถไปตามหมู่บ้านเพื่อสแกนข้อมูล WiFi ที่แต่ละบ้านเปิดอยู่

วันที่: 2014-08-13 | ที่มา: The Hacker News <http://thcert.co/50p8R8>

แอป Foursquare เวอร์ชันใหม่ แอบติดตามตำแหน่งผู้ใช้ตลอดเวลาที่เครื่องเปิดอยู่

แอปพลิเคชัน Foursquare ออกอัปเดตเวอร์ชันใหม่ไปเมื่อช่วงสัปดาห์ที่ผ่านมา โดยความสามารถใหม่ที่เพิ่มขึ้นมาคือการแจ้งเตือนให้ผู้ใช้ Check-in เวลาไปยังสถานที่สำคัญ นักวิจัยพบว่าความสามารถนี้กลายเป็นการติดตามตำแหน่งของผู้ใช้และแจ้งพิกัดไปยัง Foursquare อยู่ตลอดเวลา ถึงแม้ว่าผู้ใช้จะไม่ได้เปิดใช้งานแอป Foursquare เลยก็ตาม

ระบบการติดตามตำแหน่งนี้ทาง Foursquare ใช้ทั้ง GPS, WiFi และข้อมูลการเชื่อมต่อเสาสัญญาณโทรศัพท์ เพื่อให้ได้ข้อมูลที่ละเอียดที่สุด ซึ่งนักวิจัยมองว่าการทำเช่นนี้มีความเสี่ยงด้านความมั่นคงปลอดภัยและละเมิดความเป็นส่วนตัว ถึงแม้ตอนที่ติดตั้งแอปพลิเคชันจะมีข้อความแจ้งให้ผู้ใช้ทราบว่ามีการทำงานของระบบนี้ แต่ก็ไม่ได้มีข้อความที่ระบุชัดเจนว่าความสามารถนี้จะเปิดใช้งานอยู่ตลอดเวลา

ผู้ใช้งานแอปพลิเคชัน Foursquare สามารถปิดการทำงานของระบบติดตามตำแหน่งได้โดยเปิดแอปพลิเคชัน Foursquare ไปที่การตั้งค่า Profile (ไอคอนมุมขวาล่าง) เลือก Settings ไปที่เมนู Location Settings และเอาตัวเลือก Location Services ออก

วันที่: 2014-08-13 | ที่มา: Naked Security <http://thcert.co/c1nW0g>

นักวิจัยพบโทรศัพท์มือถือกว่าสองพันล้านเครื่องสามารถถูกโจมตีได้ผ่าน OTA Update

นักวิจัยพบช่องโหว่ในกระบวนการอัปเดตเฟิร์มแวร์ของโทรศัพท์มือถือผ่านระบบ Over-the-air (OTA) โดยสามารถโจมตีกลไกการทำงานของระบบดังกล่าวเพื่อใส่โค้ดสำหรับสั่งการให้โทรศัพท์มือถือทำงานตามที่ต้องการได้

กระบวนการอัปเดตแบบ OTA เป็นวิธีการที่ผู้ผลิตโทรศัพท์มือถือปล่อยเฟิร์มแวร์เวอร์ชันใหม่ไว้บนเซิร์ฟเวอร์เพื่อให้ผู้ใช้งานเชื่อมต่อเข้ามาผ่านระบบอินเทอร์เน็ตเพื่อดาวน์โหลดไปติดตั้ง

สาเหตุของช่องโหว่ดังกล่าวนี้อยู่ในโพรโทคอล Open Mobile Alliance Device Management (OMA-DM) ที่ผู้ผลิตโทรศัพท์มือถือส่วนใหญ่นิยมใช้เป็นช่องทางในการเผยแพร่อัปเดต โดยนักวิจัยได้ทดลองส่งโค้ดเจลเบรก iOS ผ่านช่องทางดังกล่าว และให้โทรศัพท์มือถือ iPhone 5c ที่มาจากโรงงานเชื่อมต่อเข้ามาดาวน์โหลดอัปเดต ผลลัพธ์คือสามารถเจลเบรก iPhone 5c ได้สำเร็จ

วิธีการโจมตีในรูปแบบนี้ นักวิจัยแจ้งว่าในระบบปฏิบัติการ Android และ BlackBerry สามารถทำได้ง่ายกว่า iOS

วันที่: 2014-08-13 | ที่มา: Softpedia <http://thcert.co/4b660C>

Adobe ออกอัปเดตปิดช่องโหว่ Adobe Reader, Acrobat และ Adobe Flash Player

เมื่อวันที่ 12 สิงหาคม ที่ผ่านมา Adobe ได้ปล่อยอัปเดตปิดช่องโหว่ใน Adobe Reader, Acrobat และ Adobe Flash Player ซึ่งเป็นช่องโหว่ที่อาจเปิดโอกาสให้แฮกเกอร์เข้ามาโจมตีควบคุมเครื่องคอมพิวเตอร์ของเหยื่อและขโมยข้อมูลในเครื่องได้ โดยปัจจุบันพบการโจมตีโดยใช้ช่องโหว่ใน Adobe Reader และ Acrobat แล้ว

ผู้ที่ใช้ซอฟต์แวร์ที่มีช่องโหว่ดังกล่าวควรอัปเดตให้เป็นเวอร์ชันล่าสุด รายละเอียดเวอร์ชันของซอฟต์แวร์ที่มีช่องโหว่และเวอร์ชันที่ปิดช่องโหว่แล้ว สามารถอ่านได้ที่เว็บไซต์ของ Adobe (http://thcert.co/K955S7, http://thcert.co/v6LRuz)

วันที่: 2014-08-14 | ที่มา: Adobe <http://thcert.co/K955S7>

งานเข้า! บัญชี Twitter นายกฯ รัสเซียโดนแฮก โพสต์ลาออกไปเป็นช่างภาพ

เมื่อวันที่ 14 สิงหาคม บัญชี Twitter ของนายกฯ รัสเซียโดนแฮก โดยแฮกเกอร์ได้แอบโพสต์ข้อความว่า ผมขอลาออกจากตำแหน่งไปประกอบอาชีพช่างถ่ายภาพอิสระแทน ซึ่งกลุ่มแฮกเกอร์ผู้ต้องสงสัยอันดับต้น ๆ Shaltay-Boltay ได้ออกมาปฏิเสธผ่านสำนักข่าวออนไลน์ Gazeta ว่าไม่ใช่การกระทำของกลุ่ม แต่อาจเกิดจากการกระทำของสมาชิกในกลุ่ม

วันที่: 2014-08-15 | ที่มา: The Moscow Times <http://thcert.co/qA4RDS>

แข่งแฮกงาน DefCon พบ 15 ช่องโหว่ในเราเตอร์ยอดนิยม

จากการแข่งขันท้าให้แฮกเราเตอร์ ในงานประชุมเชิงวิชาการด้านความมั่นคงปลอดภัย DefCon ที่จัดขึ้นในสหรัฐฯ แฮกเกอร์ได้ใช้ความสามารถเพื่อหาช่องโหว่ในเราเตอร์ยอดนิยมต่าง ๆ เช่น Linksys EA6500, ASUS RT-AC66U,TP-Link TL-WR1043ND, D-Link DIR-865L ทำให้แฮกเกอร์พบช่องโหว่ในการแข่งขันครั้งนี้ถึง 15 ช่องโหว่

อย่างไรก็ตามในบรรดา 15 ช่องโหว่ที่พบ มีเพียง 4 ช่องโหว่ที่ไม่เคยพบมาก่อน ส่วนช่องโหว่ที่เหลือเคยพบใน Model อื่นและมีการอัปเดตปิดช่องโหว่ไปแล้ว แต่เพิ่งจะมาพบในเราเตอร์ Model ที่ใช้ในการแข่งขันครั้งนี้ ซึ่งสาเหตุอาจจะมาจากผู้ผลิตที่รับรายงานช่องโหว่ในเราเตอร์ Model รุ่นหนึ่ง แต่ไม่ได้ทดสอบช่องโหว่ที่ได้พบกับ Model รุ่นอื่น เพียงแต่ออกอัปเดตปิดช่องโหว่ใน Model ที่ได้รับรายงานเท่านั้น

วันที่: 2014-08-15 | ที่มา: CIO <http://thcert.co/p4iX08>

นักวิจัยพบว่า Gyroscope ในโทรศัพท์มือถือสามารถใช้แอบอัดเสียงได้

Gyroscope เป็นเซ็นเซอร์ที่ใช้วัดระดับความเอียงของเครื่อง เพื่อใช้เปลี่ยนรูปแบบการแสดงผลบนหน้าจอเวลาที่ผู้ใช้เอียงเครื่อง โดยปกติโทรศัพท์มือถือสมัยใหม่มักจะมี Gyroscope ติดตั้งมาให้พร้อมอยู่แล้ว นักวิจัยจากมหาวิทยาลัย Stanford และกลุ่มนักวิจัยเพื่อป้องกันอิสราเอลได้ค้นพบว่า Gyroscope มีความไวเพียงพอที่จะใช้จับข้อมูลการสั่นไหวของอาการเพื่อใช้ในการแอบอัดเสียงคนพูดได้

อย่างไรก็ตาม ในการแอบอัดเสียงนั้นจำเป็นต้องใช้เทคนิคการวิเคราะห์รูปแบบการสั่นของอากาศเพื่อประมวลผลออกมาเป็นคำพูดทีละคำ ไม่สามารถอัดเสียงต่อเนื่องนาน ๆ เหมือนกับไมโครโฟนได้ โดยในปัจจุบันนักวิจัยสามารถใช้ Gyroscope ในการวิเคราะห์คำพูดหรือวิเคราะห์เพศของผู้พูดได้ในระดับความแม่นยำ 65 - 80% เลยทีเดียว

ในโทรศัพท์มือถือ Android และ iOS โปรแกรมเว็บเบราว์เซอร์สามารถอ่านข้อมูล Gyroscope ทำให้ผู้ใช้ที่เข้าไปยังเว็บไซต์ที่มีสคริปต์สำหรับอ่านข้อมูลจาก Gyroscope ก็อาจถูกแอบอัดเสียงได้ โดยไม่จำเป็นต้องติดตั้งโปรแกรมอันตรายใด ๆ ลงในเครื่องเลย

วันที่: 2014-08-18 | ที่มา: wired <http://thcert.co/R8gU06>

Yahoo Ad Networks ถูกใช้เผยแพร่มัลแวร์ CryptoWall

นักวิจัยจาก Blue Coat System รายงานการโจมตี Yahoo Ad Networks ซึ่งเป็นระบบที่ใช้แสดงผลโฆษณาในหน้าเว็บไซต์ โดยได้พบว่ามีผู้ไม่หวังดีลงโฆษณาที่มีจุดประสงค์เพื่อหลอกให้ผู้ใช้คลิกเข้าไปยังเว็บไซต์เผยแพร่มัลแวร์ชื่อ CryptoWall ซึ่งเป็นโปรแกรมประเภท Ransomware เข้ารหัสลับข้อมูลไฟล์ในเครื่องเพื่อเรียกค่าไถ่

นักวิจัยกล่าวว่า การโจมตีระบบที่ใช้แสดงผลโฆษณาในหน้าเว็บไซต์มักจะได้ผลดี เพราะผู้ใช้เห็นว่าเป็นการคลิกลิงก์จากเว็บไซต์ที่สามารถเชื่อถือได้ จึงอาจติดตั้งโปรแกรมที่เว็บไซต์ดังกล่าวแจ้งให้ดาวน์โหลดโดยไม่ได้สงสัยอะไร

วันที่: 2014-08-18 | ที่มา: Softpedia <http://thcert.co/000q98>

มัลแวร์ AdThief ติดในอุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS ที่ถูก Jailbreak กว่า 75,000 เครื่อง

นักวิจัยด้านความมั่นคงปลอดภัยได้ค้นพบการแพร่ระบาดของมัลแวร์ชื่อ AdThief ซึ่งเป็นมัลแวร์ที่เอาโฆษณาของตัวเองไปใส่แทนที่โฆษณาของคนอื่น เมื่อแอปพลิเคชันใด ๆ แสดงโฆษณาขึ้นมาบนหน้าจอแล้วผู้ใช้กดคลิกโฆษณาดังกล่าว ทางผู้พัฒนามัลแวร์จะได้เงินค่าโฆษณาไปแทน

มัลแวร์ที่พบนี้แพร่กระจายผ่านช่องทาง Cydia Substrate ซึ่งเป็นแหล่งดาวน์โหลดแอปพลิเคชันที่อยู่นอก App Store ซึ่งทำงานได้บนเครื่องที่ใช้งานระบบปฏิบัติการ iOS ที่ถูก Jailbreak แล้วเท่านั้น

อย่างไรก็ตาม ในขณะนี้ยังไม่พบว่ามัลแวร์ดังกล่าวแพร่กระจายผ่าน Cydia Substrate ได้อย่างไร ผู้ที่ใช้งานอุปกรณ์ iOS ที่ Jailbreak แล้ว ควรระมัดระวังในการติดตั้งแอปพลิเคชันที่ไม่ทราบแหล่งที่มาชัดเจนและไม่ควรติดตั้งแอปพลิเคชันละเมิดลิขสิทธิ์เพราะอาจเป็นแหล่งที่มาของมัลแวร์

วันที่: 2014-08-19 | ที่มา: iDownloadBlog <http://thcert.co/NvwZ16>

คิดใหม่... หากเข้าใจว่า การเข้ารหัสลับจะช่วยให้รอดการสอดแนมการใช้ Facebook

โดยปกติแล้วข้อมูลการใช้งาน Facebook หรือ Twitter ที่มีการรับส่งจากอุปกรณ์ต่าง ๆ จะได้รับการเข้ารหัสลับไว้ แฮกเกอร์จะต้องถอดรหัสลับก่อนจึงจะอ่านข้อมูลได้ อย่างไรก็ตามนักวิจัยได้ค้นพบวิธีที่จะระบุว่าข้อมูลที่ได้รับการเข้ารหัสลับเป็นการใช้งานอะไรบ้าง เช่น การโพสต์ข้อความ หรือ การเข้าไปดูโปรไฟล์เพื่อนในโซเชียลมีเดียอย่าง Twitter หรือ Facebook รวมถึงการส่งอีเมล

สำหรับวิธีนั้น นักวิจัยได้คิดค้นเทคนิควิเคราะห์ข้อมูลที่ได้รับการเข้ารหัสลับ มีการเปรียบเทียบกับลักษณะข้อมูลที่เป็นการใช้งานโซเชียลมีเดียหรือการส่งอีเมล โดยดูจากองค์ประกอบต่าง ๆ เช่น ขนาดข้อมูล ทิศทางการส่งข้อมูล ว่าเหมือนกันหรือไม่ ซึ่งได้ทำการทดลองและพบว่าได้ผลแม่นยำ 90-100% เลยทีเดียว

นอกจากนี้ หน่วยงานระดับรัฐบาลที่แอบสอดแนมข้อมูลบนเครือข่ายอินเทอร์เน็ต ก็อาจนำเทคนิคนี้ไปใช้เพื่อสืบหาบุคคลที่โพสต์ข้อความในโซเชียลมีเดียได้

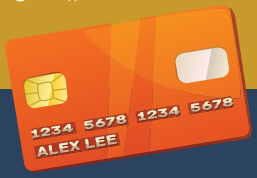
วันที่: 2014-08-20 | ที่มา: The Register <http://thcert.co/BOvJ5X>

คณะกรรมการกำกับดูแลด้านนิวเคลียร์สหรัฐฯ เผยถูกแฮกแล้ว 2 ครั้งใน 3 ปี

จากการสืบสวนภายในองค์กร พบว่า คณะกรรมการกำกับดูแลด้านนิวเคลียร์ของสหรัฐอเมริกา (US Nuclear Regulator Commission) ถูกแฮกถึง 2 ครั้งในช่วง 3 ปีที่ผ่านมา ทำให้ถูกขโมยข้อมูลภายในองค์กร

วิธีการแฮกทั้ง 2 ครั้งนั้น แฮกเกอร์ได้ส่งอีเมลหลอกลวงเพื่อขโมยข้อมูลจากพนักงานขององค์กร รูปแบบแรกเป็นลักษณะส่งอีเมลแนบลิงก์ที่พาไปยังหน้า Google Spreadsheet เพื่อให้ใส่ไอดี/รหัสผ่าน และรูปแบบที่สองเป็นลักษณะส่งอีเมลแนบลิงก์ที่พาไปยังมัลแวร์ที่อยู่บน Microsoft Skydrive ซึ่งเป็นบริการพื้นที่เก็บข้อมูลของ Microsoft และทำการโจมตีต่อหลังจากที่สามารถเข้าถึงบัญชีอีเมลของพนักงานองค์กร โดยส่งอีเมลแนบไฟล์ PDF ที่มีมัลแวร์แฝงอยู่ไปยังพนักงานคนอื่น การโจมตีโดยใช้อีเมลหลอกลวงเป็นหนึ่งในวิธีที่แฮกเกอร์นิยมใช้ในการขโมยข้อมูลขององค์กรเพราะป้องกันได้ยาก ซึ่งภาระส่วนหนึ่งตกอยู่ที่ตัวผู้ใช้ที่ควรตระหนักรู้และเข้าใจในเรื่องความมั่นคงปลอดภัยไซเบอร์

วันที่: 2014-08-21 | ที่มา: Nextgov <http://thcert.co/g95qpi>



แอบให้เนียน ATM Skimmer บางเท่ามีดโกน

เว็บบล็อก KrebsonSecurity ได้แจ้งเตือนเกี่ยวกับการพบอุปกรณ์ขโมยข้อมูลบัตรเครดิตหรือบัตร ATM (ATM Skimmer) ขนาดบางเท่ามีดโกนที่ได้รับการติดตั้งในช่องเสียบบัตร ATM ตู้หนึ่งทางฝั่งใต้ของยุโรปเมื่อสัปดาห์ที่แล้ว

ในการป้องกัน ATM Skimmer ทางฝั่งยุโรปพยายามบังคับให้ใช้บัตรรูปแบบใหม่ที่ใช้เทคโนโลยี EMV ซึ่งเก็บข้อมูลบัตรใน Chip ที่อยู่ในบัตรแทนการเก็บข้อมูลในแถบแม่เหล็ก ทำให้ค่าใช้จ่ายทำบัตรปลอมสูงขึ้นมากจนอาจไม่คุ้มกับการก่ออาชญากรรม

อย่างไรก็ตาม บางแห่งยังคงออกบัตรที่ใช้ EMV ที่มีแถบแม่เหล็กด้วย เนื่องจากตู้ ATM ในต่างประเทศส่วนหนึ่งไม่รองรับ EMV เป็นจุดอ่อนให้เหล่ามิจฉาชีพใช้เป็นช่องทางสร้างบัตรปลอมที่ใช้แถบแม่เหล็กแล้วนำไปถอนเงินในตู้ ATM ในสหรัฐฯ ซึ่งทางธนาคารได้พยายามป้องกันโดยออกมาตรการให้บัตรสามารถใช้ได้ภายในประเทศหรือดินแดนที่กำหนดไว้

จากข้อมูลของ EAST เกี่ยวกับความสูญเสียจาก ATM Skimming ในประเทศต่าง ๆ พบว่าประเทศไทยอยู่ในอันดับที่สองรองจากสหรัฐฯ

วันที่: 2014-08-22 | ที่มา: Krebs on Security <http://thcert.co/44649s>

ข้ออ้างยอดนิยม 4 ข้อ ละเลย Security

1. “ไม่มีใครสนใจตัวเล็ก ๆ อย่างฉันหรอก แฮกเกอร์น่าจะไปโจมตีองค์กรใหญ่เพื่อขโมยเงินหรือข้อมูลที่สำคัญกว่า”

นอกจากการโจมตีที่มุ่งเป้าไปยังองค์กรขนาดใหญ่ ก็พบการโจมตีที่มุ่งเป้าไปยังระดับองค์กรขนาดเล็กและบุคคล เช่น การเผยแพร่มัลแวร์ CryptoLocker ที่เข้ารหัสลับข้อมูลของเหยื่อทำให้เปิดใช้งานไม่ได้เพื่อเรียกค่าไถ่ 300 ดอลลาร์ต่อราย ซึ่งมีผู้ติดมัลแวร์มากกว่า 100,000 คน

2. “อัปเดตแล้วใช้พรินเตอร์ไม่ได้”

อัปเดตซอฟต์แวร์ที่ควบคุมฮาร์ดแวร์รุ่นเก่าแล้วทำให้ฮาร์ดแวร์ใช้งานไม่ได้ เลยไม่อัปเดต เช่น การใช้งานซอฟต์แวร์ควบคุมระบบการผลิตในโรงงาน บนระบบปฏิบัติการเก่าอย่าง Windows XP ที่ไม่ได้รับอัปเดตปิดช่องโหว่แล้ว ซึ่งการทำให้ซอฟต์แวร์ที่ควบคุมระบบขนาดใหญ่สามารถใช้งานได้บนระบบปฏิบัติการอื่นอาจมีค่าใช้จ่ายสูง แต่สำหรับผู้ใช้งานทั่วไปควรพิจารณาเปลี่ยนไปใช้ระบบปฏิบัติการอื่นเพราะมีความเสี่ยงสูง

3. “ผมใช้ Mac มั่นคงปลอดภัยแน่นอน”

ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์แบบไหน หากเครื่องโดนขโมยก็สามารถถูกขโมยข้อมูลในเครื่องได้เหมือนกัน ถึงแม้ว่าข้อมูลของคุณคนเดียวดูเหมือนจะมีไม่มีค่า แต่ผู้ไม่หวังดีสามารถรวบรวมข้อมูลของหลาย ๆ คนรวมกันแล้วนำไปขายในตลาดมืดต่อ

4. “การรักษาความมั่นคงปลอดภัยทำให้เครื่องช้า”

การเข้ารหัสลับข้อมูลในฮาร์ดดิสก์ทั้งลูก (Full Disk Encryption) เพื่อป้องกันการขโมยข้อมูล ที่ต้องถอดรหัสลับข้อมูลทุกครั้งที่จะใช้งาน ดูเหมือนจะทำให้เครื่องช้า แต่ด้วยความสามารถของ CPU ที่เพิ่มขึ้นและเทคโนโลยีซอฟต์แวร์เข้ารหัสลับในปัจจุบัน อย่าง BitLocker บน Windows หรือ FileVault บน OSX ทำให้การเข้ารหัสลับไม่ได้ทำให้เครื่องช้าอย่างที่เข้าใจกัน

แอนติไวรัสที่ว่าทำให้เครื่องช้านั้น บ่อยครั้งพบว่าเกิดจากการเปิดใช้งานฟังก์ชันที่ไม่จำเป็น และการเพิ่มความมั่นคงปลอดภัยด้วยการเปิดใช้งานการตรวจสอบยืนยันแบบ 2 ขั้นตอน (2-Step Verification) ก็คุ้มค่ากับการปกป้องบัญชีที่สำคัญของเรา

วันที่: 2014-08-25 | ที่มา: Sophos <http://thcert.co/P7zT52>

แนวโน้มการใช้จ่ายด้านความมั่นคงปลอดภัยทั่วโลกที่เพิ่มขึ้นในปี 2014

Gartner คาดการณ์แนวโน้มการใช้จ่ายด้านความมั่นคงปลอดภัยทั่วโลกที่เพิ่มขึ้นว่า

- การใช้จ่ายด้านความมั่นคงปลอดภัยทั่วโลกในปี 2014 จะสูงถึง 71,000 ล้านดอลลาร์ (เพิ่ม 7.9% จากปีที่แล้ว) โดยใช้จ่ายเพื่อป้องกันการขโมยข้อมูลหรือข้อมูลรั่วไหลเพิ่มขึ้น 18.9%

- การลงทุนด้านความมั่นคงปลอดภัยในปี 2015 จะสูงถึง 76,900 ล้านดอลลาร์

- 10% ของความสามารถโดยรวมของอุปกรณ์ต่าง ๆ เพื่อรักษาความมั่นคงปลอดภัยให้องค์กร จะอยู่ในรูปแบบ Cloud

- 30% ของผลิตภัณฑ์เพื่อรักษาความมั่นคงปลอดภัยองค์กรจะถูกขายในรูปแบบของแพ็กเกจที่รวมหลายผลิตภัณฑ์ เช่น ระบบรักษาความความมั่นคงปลอดภัยของคอมพิวเตอร์ของพนักงาน (Endpoint Protection Platform) ระบบรักษาความมั่นคงปลอดภัยของมือถือของพนักงาน การตรวจสอบช่องโหว่

- ภายในปี 2018 มากกว่าครึ่งหนึ่งของจำนวนองค์กรจะใช้บริการจากองค์กรที่เชี่ยวชาญในเรื่องของการปกป้องข้อมูล (Data Protection) การจัดการเรื่องความเสี่ยง (Risk Management) การรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานขององค์กร (Security Infrastructure Management)

- ผู้ใช้งานจะให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยข้อมูลในมือถือ (Mobile Security) มากขึ้นตั้งแต่ปี 2017

วันที่: 2014-08-26 | ที่มา: Gartner <http://thcert.co/kmdDb1>

แนะนำฟีเจอร์น่าสนใจ เพิ่มความมั่นคงปลอดภัยใน Twitter

- Login Verification เพิ่มความมั่นคงปลอดภัยในการล็อกอิน ด้วยการใส่รหัสผ่านที่ 2 นอกจากใส่รหัสผ่านที่มีอยู่แล้ว โดยสามารถเลือกที่จะรับรหัสผ่านที่ 2 ผ่าน SMS หรือแอปพลิเคชัน Twitter บนสมาร์ตโฟน

- Password Reset รีเซ็ตรหัสผ่านใหม่ในกรณีที่ลืมรหัสผ่านเดิมหรือไม่สามารถล็อกอินด้วยรหัสผ่านที่มี ซึ่งปกติจะต้องใส่ Username ที่ต้องการจะรีเซ็ต หากเปิดใช้งาน “Require personal information to reset my password” ก็จะเพิ่มความมั่นคงปลอดภัยขึ้น

วันที่: 2014-08-27 | ที่มา: Sophos <http://thcert.co/lt1IZV>

เว็บไซต์ชื่อดังหลายแห่งเช่น Java, Photobucket, deviantART ถูกโจมตีผ่านมัลแวร์ในโฆษณา

ในช่วงวันที่ 19 - 22 สิงหาคมที่ผ่านมา มีรายงานว่าเว็บไซต์ชื่อดังหลายแห่ง เช่น Java.com, Photobucket.com, deviantART.com ถูกโจมตีผ่านมัลแวร์ที่ฝังมาในโฆษณา โดยผู้ใช้ที่ติดตั้งปลั๊กอิน Java, Adobe Flash Player หรือ Microsoft Silverlight เวอร์ชันเก่า จะติดมัลแวร์ทันทีที่เข้าไปยังเว็บไซต์ดังกล่าว

ปัญหาของการโจมตีด้วยการฝังมัลแวร์ในโฆษณาคือผู้ใช้จะไม่สามารถรู้ตัวได้เลยว่าเครื่องติดมัลแวร์ไปแล้วหรือไม่ เพราะโค้ดของมัลแวร์ที่ถูกฝังอยู่ในเว็บไซต์สามารถทำงานได้ทันทีที่มีการโหลดหน้าเว็บ โดยที่ผู้ใช้ไม่จำเป็นต้องคลิกที่ตัวโฆษณาหรือกดดาวน์โหลดโปรแกรมใด ๆ มาติดตั้งเลย และที่สำคัญ การแสดงผลโฆษณาจะปรากฏขึ้นมาเป็นแบบสุ่ม โดยอ้างอิงข้อมูลตำแหน่งของผู้ใช้ เบราว์เซอร์ที่ใช้ และประวัติการเข้าชมเว็บไซต์ จึงทำให้ผู้ดูแลระบบตรวจสอบความผิดปกติได้ลำบาก

สำหรับการป้องกัน ผู้ใช้งานควรตั้งค่าเบราว์เซอร์ หรือติดตั้งส่วนเสริมที่บล็อกการทำงานของปลั๊กอินต่าง ๆ เช่น Java, Flash, Silverlight ไว้โดยอัตโนมัติ ไม่ให้ทำงานจนกว่าผู้ใช้จะเป็นคนคลิกเข้าไปดูเอง รวมถึงควรหมั่นอัปเดตระบบปฏิบัติการและซอฟต์แวร์ที่ใช้งานอยู่อย่างสม่ำเสมอ

วันที่: 2014-08-28 | ที่มา: Softpedia <http://thcert.co/HdQ46d>

แฮกเกอร์เผย ดูดภาพลับของเหล่าดาราผ่านช่องโหว่ iCloud โดยใช้เครื่องมือที่ออกแบบมาสำหรับตำรวจ

หลังจากที่เมื่อวันที่ 1 สิงหาคมที่ผ่านมา มีข่าวภาพหลุดของดาราชื่อดังจำนวนมากถูกเผยแพร่ผ่านทางอินเทอร์เน็ต ถึงแม้ว่าทาง Apple จะบอกว่าไม่ใช่การเจาะระบบ iCloud แต่แฮกเกอร์ผู้ที่นำภาพเหล่านั้นออกมาก็บอกว่านำภาพออกมาจาก iCloud จริง โดยทำผ่านเครื่องมือที่ออกแบบมาเพื่อให้ตำรวจใช้ในการสืบสวน

ผู้ใช้รายหนึ่งได้โพสต์ในเว็บบอร์ดใต้ดินว่านำภาพหลุดของดาราออกมาโดยใช้โปรแกรมชื่อ Elcomsoft Phone Password Breaker ซึ่งเป็นโปรแกรมที่ออกแบบมาสำหรับการสืบสวน โปรแกรมดังกล่าวมีความสามารถในการเดารหัสผ่านของผู้ใช้งาน iCloud และจำลองตัวเองเป็นเครื่องมือจัดการบัญชีผู้ใช้ เพื่อให้สามารถดึงข้อมูล iCloud Backup ซึ่งเป็นข้อมูลทั้งหมดที่ผู้ใช้ส่งขึ้น iCloud ออกมาจากระบบได้

เนื่องจากเมื่อวันที่ 30 กันยายนที่ผ่านมา มีผู้พบช่องโหว่ของระบบ Find my iPhone ที่สามารถเดารหัสผ่านบริการ iCloud ได้แบบ Brute Force จึงมีผู้พัฒนาโปรแกรมชื่อ iBrute ขึ้นมาเพื่อใช้ในการโจมตี และโปรแกรม Elcomsoft Phone Password Breaker ก็มีความสามารถนี้ บรรดาแฮกเกอร์จึงสามารถนำมาใช้ในการดึงภาพลับของเหล่าดาราออกมาจาก iCloud ได้

วันที่: 2014-09-03 | ที่มา: Wired <http://thcert.co/c4l18L>

แนะนำฟีเจอร์น่าสนใจ เพิ่มความเป็นส่วนตัว (Privacy) ใน Twitter

- Photo Tagging : เราสามารถตั้งค่าได้ หากไม่ต้องการให้คนที่ไม่รู้จักแท็กเราในรูปโดยเลือก “Do not allow anyone to tag me in photos” หรือหากยอมให้เฉพาะคนที่เรา Follow เท่านั้นที่แท็กได้ ก็ให้เลือก “Only allow people I follow to tag me in photos”

- Tweet Privacy : เราสามารถจำกัดบุคคลที่สามารถอ่าน Tweet ของเรา โดยเลือก “Protect my tweet” เป็นการตั้งค่าป้องกันให้คนที่ต้องการ Follow เราต้องขออนุญาตเราก่อน และหลังจากเป็น Follower จึงจะสามารถอ่าน Tweet ของเรา

- Tweet Location : การเปิดใช้งาน “Add a location to my Tweets” จะเป็นการใส่ตำแหน่งที่เราอยู่ลงในทวีตด้วย ซึ่งค่าตั้งต้นไม่ได้เปิดใช้งานในส่วนนี้อยู่แล้ว

- Discoverability : โดยปกติคนอื่นสามารถค้นหาหน้า Profile ของเราโดยระบุชื่อ Twitter ของเรา แต่การเปิดใช้งาน “Let others find me by my email address” จะทำให้สามารถค้นหาจากที่อยู่อีเมล ซึ่งหากไม่มีความจำเป็นก็สามารถปิดการใช้งานนี้

- Personalization : โดยปกติหากเราเข้าเว็บไซต์ต่าง ๆ ที่มีปุ่ม Twitter ในเว็บไซต์ เช่น ปุ่มแชร์ลิงก์และเราล็อกอินอยู่ เว็บไซต์จะส่งข้อมูลว่าเราเยี่ยมชมเว็บไซต์นี้ให้กับ Twitter โดยข้อมูลนี้จะลบไปภายใน 10 วัน

- การตั้งค่า “Tailor Twitter based on my recent website visits” เป็นการนำข้อมูลจากที่การเข้าเว็บไซต์ต่าง ๆ ของเรา มาวิเคราะห์ความสนใจของเราและเสนอแนะคนที่เราอาจจะต้องการ Follow หากไม่ต้องการใช้งานในส่วนนี้ก็สามารถปิดการใช้งานได้

- Twitter จะนำข้อมูลดังกล่าวจากบริษัทโฆษณา เพื่อแสดงโฆษณาที่เราสนใจใน Twitter ซึ่งเราสามารถหยุดไม่ให้ Twitter นำข้อมูลมาวิเคราะห์ว่าเราสนใจอะไรโดยใช้การปิดการใช้งาน “Tailor ads based on information shared by ad partners”

วันที่: 2014-09-04 | ที่มา: Sophos <http://thcert.co/It1IZV>

มัลแวร์ Chrome Extension ระบาด ทะลุผ่านการป้องกันของ Chrome

ปกติ Chrome นั้นมีการป้องกันโดยจำกัดให้ติดตั้ง Extension ที่มาจาก Chrome Web Store เท่านั้น อย่างไรก็ตามนักวิจัยด้านความมั่นคงปลอดภัยพบการแพร่ระบาดของมัลแวร์ซึ่งเป็น Chrome Extension ที่สามารถติดตั้งใน Chrome โดยตรงจากเครื่องคอมพิวเตอร์

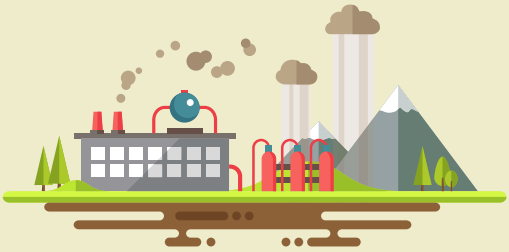
การแพร่ระบาดเริ่มจากการส่งข้อความ “Facebook Secrets” ใน Twitter และ Facebook โดยพบว่ามีการ Retweet ข้อความดังกล่าวมากกว่า 6,000 ครั้ง เพื่อหลอกให้คลิกลิงก์ดาวน์โหลดไฟล์ชื่อ download-video.exe ซึ่งจะไปดาวน์โหลดและติดตั้ง Chrome Extension ร้ายที่ปลอมเป็น Flash Player หลังจากนั้นหากเหยื่อเข้าเว็บ Facebook หรือ Twitter จะมีการนำไปยังเว็บไซต์ไม่พึงประสงค์โดยอัตโนมัติ (Redirect) นอกจากนี้ Chrome Extension ร้ายดังกล่าวยังสามารถสร้างให้มีความสามารถในการขโมยไอดี/รหัสผ่านของเว็บที่เราเข้าได้

วันที่: 2014-09-08 | ที่มา: The Hacker News <http://thcert.co/NmH3iA>

กลุ่มโจรไซเบอร์ดัดแปลงมัลแวร์บน Windows ให้ทำงานบน OS X

นักวิจัยด้านความมั่นคงปลอดภัยค้นพบมัลแวร์ซึ่งเคยทำงานบน Windows มาก่อน และได้รับการดัดแปลงให้ทำงานบน OS X โดยให้ชื่อว่า “XSLCmd” มัลแวร์นี้สามารถรับคำสั่งต่าง ๆ จากผู้โจมตี เช่น การดาวน์โหลดและติดตั้งมัลแวร์ตัวอื่น หรือการส่งข้อมูลกลับไปให้ผู้ไม่หวังดี โดยอาชญากรไซเบอร์ที่ตั้งชื่อกลุ่มว่า GREF ได้ใช้มัลแวร์นี้เพื่อโจมตีองค์กรต่าง ๆ เช่น US Defense Industrial Base รวมถึงบริษัทด้านอิเล็กทรอนิกส์และวิศวกรรมของสหรัฐฯ

วันที่: 2014-09-09 | ที่มา: SC Magazine.com <http://thcert.co/x4Mb79 >



5 สิ่งควรรู้ก่อนคลิกลิงก์ยกเลิกรับข่าวสารทางอีเมล

เราอาจเคยได้รับอีเมลที่ไม่ต้องการ เช่น อีเมลข่าวสารหรือชักชวนให้ซื้อของ ซึ่งด้านล่างมีลิงก์สำหรับยกเลิกการรับข่าวสารอยู่ (Unsubscribe Link) หรืออาจให้ส่งอีเมลกลับเพื่อยกเลิกข่าวสาร อย่างไรก็ตาม การกระทำดังกล่าวมีความเสี่ยงต่อการเปิดเผยข้อมูลหรือติดมัลแวร์ หากผู้ส่งมีจุดประสงค์ร้าย เพราะ

1. ทำให้รู้ว่า ที่อยู่อีเมลนี้มีคนใช้งานจริง จึงตกเป็นเป้าหมายได้รับ Spam มากขึ้น

2. ทำให้รู้ว่า คุณได้เปิดอ่านอีเมลและอาจสนใจเนื้อหา ซึ่งอาจเป็นเรื่องของเงิน หุ้น หรือยาเสริมสุขภาพ และอาจจะถูกนำไปใช้หลอกลวงต่อไป

3. การส่งอีเมลกลับ ทำให้ผู้ไม่หวังดีสามารถวิเคราะห์ตัวอีเมล และอาจทำให้รู้ว่าคุณใช้ซอฟต์แวร์อะไรสำหรับจัดการอีเมลอยู่

4. หากการคลิกลิงก์ นำไปสู่การเข้าเว็บไซต์ที่ผู้ไม่หวังดีเตรียมไว้ ก็อาจส่งผลให้ผู้ไม่หวังดีทราบตำแหน่งของคุณ หรือ เบราว์เซอร์ที่คุณใช้

5. และที่น่ากลัวที่สุดคือ การคลิกลิงก์อาจนำไปสู่การติดมัลแวร์โดยที่คุณไม่รู้ตัวเลยก็ได้

เพราะฉะนั้น อีเมลที่เราไม่ต้องการและคิดว่าเป็นอีเมลหลอกลวง ควรมาร์กให้เป็นสแปม เพื่อให้ระบบทำการบล็อกอีเมลแทน

วันที่: 2014-09-10 | ที่มา: Naked Security <http://thcert.co/P5hM72>

Google ประกาศเรื่อง 5 ล้านบัญชี Google รั่วไหล ล็อกอินได้จริง 2%

หลังจากที่มีข่าวเหตุการณ์รั่วไหลของบัญชี Google ที่มีการโพสต์ 5 ล้านไอดีของ Google และรหัสผ่านบนเว็บไซต์รัสเซียแห่งหนึ่ง Google ได้ออกมาประกาศว่าจากการจับคู่ไอดีกับรหัสผ่านมีการเผยแพร่มีเพียงแค่ 2% ที่สามารถใช้งานได้จริง นอกจากนี้ Google ยังมีระบบตรวจจับการล็อกอินที่น่าสงสัยว่ามาจากผู้ไม่หวังดี พร้อมแนะนำให้ใช้รหัสผ่านที่มีความมั่นคงปลอดภัยและเปิดการใช้งานการยืนยันแบบ 2 ขั้นตอน

วันที่: 2014-09-11 | ที่มา: Google Online Security <http://thcert.co/V61K7R>

Microsoft และ Adobe ปล่อยอัปเดตปิดช่องโหว่

เมื่อวันที่ 9 มิถุนายนที่ผ่านมา Microsoft ปล่อยอัปเดตประจำเดือนสำหรับระบบปฏิบัติการ Windows ที่ปิดช่องโหว่ใน Internet Explorer, .NET Framework, Windows Task Scheduler, Microsoft Lync Server ส่วน Adobe ก็ได้ปล่อยอัปเดตสำหรับ Flash Player, Adobe AIR ที่ปิดช่องโหว่ประเภทที่ส่งผลให้เครื่องคอมพิวเตอร์ของเหยื่อทำตามคำสั่งของผู้ไม่หวังดี (Remote Code Execution)

ทั้งนี้ Adobe ระบุว่าจะปล่อยอัปเดตปิดช่องโหว่สำหรับ Adobe Reader และ Acrobat ในสัปดาห์หน้า

วันที่: 2014-09-12 | ที่มา: Sophos <http://thcert.co/91T8BN>

พบช่องโหว่ในระบบควบคุมดาวเทียม NOAA ของสหรัฐฯ

จากการตรวจสอบความมั่นคงปลอดภัยของระบบ JPSS (Joint Polar Satellite System) ซึ่งเป็นระบบควบคุมและรับข้อมูลจากดาวเทียมสำหรับสำรวจสภาพอากาศขององค์กร NOAA (National Oceanic and Atmospheric Administration) ในประเทศสหรัฐฯ พบว่ามีช่องโหว่อยู่เป็นจำนวนมาก ซึ่งการโจมตีโดยใช้ช่องโหว่เหล่านี้สามารถส่งผลกระทบต่อการส่งข้อมูลจากดาวเทียมได้

การค้นพบครั้งนี้ถือเป็นเรื่องใหญ่เพราะบางช่องโหว่มีมาหลายปีแล้วและเครื่องมือสำหรับโจมตีผ่านช่องโหว่เหล่านี้ก็สามารถหาได้ในอินเทอร์เน็ต

วันที่: 2014-09-15 | ที่มา: The Hacker News <http://thcert.co/cWuP84>

นักวิจัยแฮกเอาเกม Doom ไปเล่นบนเครื่องพิมพ์ Canon Pixma

นักวิจัยด้านความมั่นคงปลอดภัยพบช่องโหว่ในส่วน Web Interface ของเครื่องพิมพ์ยี่ห้อ Canon ซึ่งอนุญาตให้ใครก็ตามสามารถเข้าไปจัดการระบบการทำงานของเครื่องพิมพ์ได้โดยไม่ต้องมีการตรวจสอบ รวมถึงพบช่องโหว่ในระบบ Firmware Update ซึ่งทำให้ผู้ไม่หวังดีสามารถดัดแปลงเฟิร์มแวร์ของเครื่องพิมพ์เพื่อใส่โค้ดสำหรับดักรับข้อมูลหรือดัดแปลงการทำงานให้ผิดปกติได้ โดยนักวิจัยได้สาธิตแก้ไขเฟิร์มแวร์ของเครื่องพิมพ์รุ่นดังกล่าวให้สามารถเล่นเกม Doom ซึ่งเป็นเกมเก่าบนเครื่องพีซีได้

เครื่องพิมพ์รุ่นที่มีช่องโหว่นี้ มีคุณสมบัติสามารถเชื่อมต่อ WiFi เพื่อรองรับการสั่งพิมพ์งานหรือจัดการการตั้งค่าจากระยะไกลได้ นักวิจัยได้ทดลองสแกนไอพีของเครื่องพิมพ์ที่เปิดเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต พบว่ามีเครื่องพิมพ์ประมาณ 2,000 เครื่องที่มีช่องโหว่นี้และเชื่อมต่อกับอินเทอร์เน็ตอยู่

นักวิจัยได้แจ้งช่องโหว่นี้ให้กับทาง Canon ทราบแล้ว และได้แนะนำให้ผู้ใช้หรือหน่วยงานที่มีเครื่องพิมพ์แบบเชื่อมต่อผ่าน WiFi ให้ตั้งค่าระบบเครือข่ายไม่ให้เครื่องพิมพ์นี้สามารถเข้าถึงได้จากอินเทอร์เน็ต

วันที่: 2014-09-16 | ที่มา: The Register <http://thcert.co/r5dRxU>

อัปเดตปิดช่องโหว่ Adobe Reader และ Acrobat ออกแล้ว

จากการเลื่อนปล่อยอัปเดตปิดช่องโหว่ใน Adobe Reader and Acrobat ในสัปดาห์ที่แล้ว เมื่อวันที่ 16 กันยายนที่ผ่านมา ทาง Adobe ได้ปล่อยอัปเดตของซอฟต์แวร์ทั้ง 2 เพื่อปิดช่องโหว่แล้ว จึงแนะนำให้อัปเดตเป็นเวอร์ชันล่าสุด

วันที่: 2014-09-17 | ที่มา: Adobe <https://thcert.co/0fShg0>

ระบบสอดแนมตำแหน่งผู้ใช้มือถือ เปิดขายทั่วโลก

ข่าวการสอดแนมประชาชนไม่ใช่เรื่องใหม่ในประเทศยักษ์ใหญ่อย่าง สหรัฐฯ อังกฤษ จีน เช่น การใช้ระบบสอดแนมตำแหน่งของผู้ใช้มือถือโดยหน่วยงาน NSA ของสหรัฐฯ หรือหน่วยงาน GCHQ ของอังกฤษ ซึ่งระบบดังกล่าวอาศัยหลักการที่ว่า มือถือจะต้องติดต่อกับเสาสัญญาณเพื่อรับส่งข้อมูล เมื่อรู้ว่ามือถือกำลังเชื่อมต่อกับเสาสัญญาณตรงบริเวณไหน ก็ทำให้ระบุตำแหน่งของผู้ใช้มือถือได้ไม่ยาก

อย่างไรก็ตาม ข่าวของ The Washington Post เผยว่า ปัจจุบันมีการขายระบบที่มีความสามารถดังกล่าวให้แก่รัฐบาลต่าง ๆ ที่ถึงแม้จะมีระบบเทคโนโลยีสารสนเทศด้อยกว่า ก็สามารถใช้งานได้ เพียงแค่ระบุเบอร์โทรศัพท์เข้าไปในระบบ ก็สามารถรู้ได้ว่า ผู้ใช้มือถืออยู่ที่ไหน ซึ่งหลายประเทศได้ซื้อระบบนี้มาใช้ในหลายปีที่ผ่านมา The Washington Post ยังได้ระบุถึงตัวอย่างระบบสอดแนม SkyLock พร้อมเอกสารที่มีภาพแสดงการสอดแนมในหลายประเทศ เช่น เม็กซิโก แอฟริกาใต้ บราซิล และคองโก

ความน่ากลัวของระบบสอดแนมอยู่ตรงที่ผู้ใช้งานทำอะไรไม่ได้มากนักในการตรวจสอบและการป้องกัน เพราะมันไม่ได้มาจากการหลอกให้ลงแอปพลิเคชันเพื่อสอดแนมในเครื่อง แต่มาจากการติดตั้งอุปกรณ์ใกล้เสาสัญญาณเพื่อขโมยข้อมูลหรืออาจขอความร่วมมือจากผู้ให้บริการโครงข่ายมือถือเพื่อขอข้อมูลโดยตรง

การนำระบบสอดแนมดังกล่าวมาใช้นั้น ไม่สามารถบอกได้ชัดเจนว่าเป็นเรื่องที่ถูกต้องหรือไม่ เพราะแม้ในบางประเทศจะมีกฎหมายคุ้มครองไม่ให้สอดแนมประชาชนของตน แต่ก็ไม่ได้ห้ามสำหรับคนต่างชาติ นอกจากนี้ยังมีประเด็นว่ามีหน่วยงานที่คอยควบคุมหรือตรวจสอบหน่วยงานที่สอดแนมเพื่อไม่ให้ใช้ในทางที่ผิดหรือไม่

วันที่: 2014-09-18 | ที่มา: The Washington Post <http://thcert.co/77u186>

ใช้เทคนิคใหม่ สังเกต URL ของหน้าเว็บปลอมยากกว่าเดิม

เว็บไซต์ SANS ได้โพสต์แจ้งเตือนการพบหน้าเว็บไซต์ปลอมที่ผู้ใช้งานสังเกต URL ได้ยากขึ้น โดยหน้าเว็บไซต์ดังกล่าวคือ url-bofa.support/BankOfAmerica.Com

เนื่องจากในอดีตมีการใช้ TLD ไม่กี่ตัว เช่น .com .net .org แต่ปัจจุบันหน่วยงาน ICANN ได้เปิดให้ใช้ TLD ตัวใหม่ ๆ อย่างเช่น .support ซึ่งทำให้เว็บไซต์ดูน่าเชื่อถือ และเว็บไซต์นี้ยังใช้ HTTPS ที่มาจากการรับรองฟรี 30 วันของบริษัท Comodo (Comodo Free SSL) ซึ่งทำให้คนมีโอกาสที่จะตกเป็นเหยื่อได้สูงขึ้น

วันที่: 2014-09-19 | ที่มา: SANS <http://thcert.co/alw6b8>

Apple เพิ่มความมั่นคงปลอดภัย iCloud ด้วยการยืนยันตัวตนแบบ 2 ขั้นตอน

ก่อนหน้านี้ผู้ใช้งาน Apple สามารถเพิ่มความมั่นคงปลอดภัยให้กับบัญชีด้วยการเปิดใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอน หากทำธุรกรรมสำคัญอย่างเช่น ซื้อของผ่าน App Store หรือเปลี่ยนรหัสผ่าน ระบบจะส่งรหัสผ่านที่ 2 (OTP) ทาง SMS เพื่อยืนยันตัวตน แต่ไม่นานมานี้ Apple ได้ขยายให้รองรับ iCloud ด้วย เพื่อป้องกันผู้ไม่หวังดีที่จะขโมยข้อมูลบน iCloud

ก่อนหน้านี้มีเหตุการณ์ภาพหลุดดาราจาก iCloud ซึ่งอาจเป็นปัจจัยให้ Apple ตัดสินใจเพิ่มความมั่นคงปลอดภัยให้กับ iCloud ด้วย ใครที่ต้องการเพิ่มความมั่นคงปลอดภัยก็สามารถเปิดการใช้งานได้ที่ Setting ในส่วนของรหัสผ่านและความปลอดภัย

วันที่: 2014-09-22 | ที่มา: Arstechnica <http://thcert.co/1slKJH8>

iOS 8.0.1 ทำพิษ Apple ถอดออกจากระบบอัปเดตแล้ว

จากเหตุการณ์ที่มีผู้ใช้งานลงอัปเดต iOS 8.0.1 แล้วเกิดปัญหาสัญญาณโทรศัพท์หายหรือ Touch ID ใช้ไม่ได้ ล่าสุด Apple ได้ถอดตัวอัปเดตเจ้าปัญหาออกจากระบบ และกำลังเตรียม 8.0.2 สำหรับแก้ปัญหาดังกล่าวแล้ว

สำหรับใครที่ลง 8.0.1 ไปแล้วมีปัญหา Apple แนะนำวิธีย้อนกลับไปติดตั้งรุ่น 8.0 ใครสนใจอ่านได้ที่ http://support.apple.com/kb/HT6487

วันที่: 2014-09-25 | ที่มา: Apple <http://thcert.co/OSd86h>

สิงห์นักบิตเสียว พบโฆษณาใน The Pirate Bay เผยแพร่มัลแวร์

The Pirate Bay เป็นเว็บไซต์บิตทอร์เรนต์ที่มีคนนิยมใช้ทั่วโลก เมื่อไม่นานมานี้ได้ค้นพบการแพร่ระบาดมัลแวร์จากเว็บไซต์ The Pirate Bay ซึ่งพบว่ามาจากในส่วนของโฆษณา โดยโจมตีผ่านช่องโหว่ของ Adobe Flash Player, Java หรือ Adobe Reader หากเหยื่อติดตั้งซอฟต์แวร์เหล่านี้ที่ไม่ได้อัปเดตแล้วเข้าเว็บไซต์ก็สามารถติดมัลแวร์ได้โดยอัตโนมัติ

มัลแวร์ที่แพร่ระบาดอยู่นี้อยู่ในตระกูล ZeroAccess ประเภท Rootkit ซึ่งมีความสามารถในการซ่อนตัวหลบหลีกการตรวจจับของแอนติไวรัสสูง และสามารถดาวน์โหลดมัลแวร์อื่นเพื่อใช้กระทำการต่าง ๆ เช่น ใช้ขุด Bitcoins ทำให้เครื่องกินไฟและช้า หรือแอบคลิกโฆษณาโดยที่ไม่ได้รับอนุญาต (Click Fraud)

วันที่: 2014-09-29 | ที่มา: Softpedia <http://thcert.co/S8266v>

สรุปสถานการณ์ ShellShock

จากเหตุการณ์พบช่องโหว่ในซอฟต์แวร์ Bash ที่มีการใช้อย่างแพร่หลายใน Linux, Unix และ OS X ช่องโหว่นี้เรียกว่า ShellShock ซึ่งแฮกเกอร์อาจใช้โจมตี เพื่อทำให้เครื่องคอมพิวเตอร์ประมวลผลตามคำสั่งของแฮกเกอร์จากระยะไกล (Remote Code Execution) และอาจส่งผลให้เครื่องคอมพิวเตอร์ถูกควบคุมและข้อมูลในเครื่องถูกขโมยได้ เว็บแอปพลิเคชันหรือบริการที่ใช้ Bash อย่าง CGI หรือ DHCP ก็พลอยได้รับผลกระทบด้วย

ตั้งแต่เปิดเผยช่องโหว่ ก็พบความพยายามในการโจมตีผ่านช่องโหว่นี้ เมื่อสัปดาห์ที่แล้วบริษัทด้านความมั่นคงปลอดภัยอย่างบริษัท Incapsula ที่ปกป้องเว็บไซต์ต่าง ๆ ของลูกค้า เผยว่าใน 24 ชั่วโมงหลังการเปิดเผยช่องโหว่ พบการโจมตีมากกว่า 17,400 ครั้งในเว็บไซต์ต่าง ๆ จำนวนมากกว่า 1,800 เว็บไซต์ และพบการโจมตีมากขึ้นเรื่อย ๆ ในช่วงสุดสัปดาห์ที่ผ่านมา

ปัจจุบัน มีการค้นพบชุดช่องโหว่ใน Bash เป็นจำนวน 6 ช่องโหว่ (CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187) ผู้ที่ใช้งาน Unix, Linux รุ่นต่าง ๆ ควรเช็คว่ามีอัปเดตปิดช่องโหว่ทั้งหมดในระบบปฏิบัติการที่ใช้อยู่หรือยัง

จากการตรวจสอบ Linux หลายรุ่น หากอัปเดตเป็นเวอร์ชันล่าสุดก็จะปิดช่องโหว่ทั้งหมด เช่น Ubuntu, Redhat ส่วน OS X ได้ออกอัปเดตปิด 2 ช่องโหว่ (CVE-2014-6271 และ CVE-2014-7169) ส่วนผู้ใช้ Windows ไม่ได้รับผลกระทบโดยตรง แต่อาจได้รับผลกระทบทางอ้อม เช่น เว็บไซต์ที่ใช้งานอยู่ ถูกโจมตีผ่านช่องโหว่นี้ ทำให้ข้อมูลของผู้ใช้ที่ถูกเก็บในเว็บไซต์ถูกขโมย

วันที่: 2014-10-01 | ที่มา: Shellshocker < http://thcert.co/A4NBDy >

3 ข้อควรจำ เพื่อป้องกันก่อนถูกแฮก

Sophos ได้เผยแพร่คำแนะนำ 3 ข้อ สำหรับผู้ใช้งานคอมพิวเตอร์และอุปกรณ์สื่อสารต่าง ๆ เพื่อเพิ่มความมั่นคงปลอดภัย ดังนี้

1. เช็คอุปกรณ์ว่ามีมัลแวร์หรือไม่โดยใช้แอนติไวรัสที่ได้รับการอัปเดตแล้ว และนอกจากเครื่องคอมพิวเตอร์ที่ติดตั้ง Windows แล้ว อุปกรณ์อย่าง สมาร์ตโฟน, Mac, แท็บเล็ต ก็สามารถติดมัลแวร์ได้เช่นกัน ดังนั้นจึงควรติดตั้งแอนติไวรัสด้วย

2. ตั้งค่า WiFi ที่บ้าน โดยใช้ WPA หรือ WPA 2 แทน WEP เพราะ WEP มีช่องโหว่ที่ทำให้แฮกเกอร์สามารถขโมยข้อมูลที่รับส่งในเครือข่าย WiFi ได้ ผู้ที่สนใจสามารถศึกษาข้อแนะนำในการตั้งค่า WiFi ตามคลิป (http://www.youtube.com/watch?v=W-NNq9qoORw#t=89)

3. ตั้งรหัสผ่านให้ต่างกัน สำหรับแต่ละไอดีที่ใช้ในแต่ละเว็บไซต์ โดยอาจใช้ LastPass หรือ KeePass ซึ่งสามารถช่วยจำและเก็บรหัสผ่านแทนเรา รวมถึงตั้งรหัสผ่านที่คาดเดาได้ยาก

วันที่: 2014-10-03 | ที่มา: The Hacker News <http://thcert.co/9fRb9z>

พบมัลแวร์สายพันธุ์ใหม่บน Mac ติดอย่างน้อย 17,000 เครื่อง

เมื่อสัปดาห์ที่ผ่านเว็บไซต์ Dr.WEB ได้ประกาศว่าค้นพบมัลแวร์ใหม่บน Mac โดยมีชื่อสายพันธุ์ว่า Mac.BackDoor.iWorm เจ้ามัลแวร์นี้ทำหน้าที่รับคำสั่งต่าง ๆ จากเครื่องคอมพิวเตอร์ของแฮกเกอร์ ที่น่าสนใจคือมัลแวร์นี้จะดาวน์โหลดรายการที่อยู่ของเครื่องคอมพิวเตอร์ (หมายเลขไอพี) ของแฮกเกอร์จาก reddit.com ซึ่งเป็นเว็บที่มีบริการค้นหาคล้าย Google เมื่อมัลแวร์ใส่ค่าพิเศษในกล่องค้นหาของ Reddit ก็จะได้ผลลัพธ์คือรายการที่อยู่ของเครื่องคอมพิวเตอร์ของแฮกเกอร์ที่มัลแวร์สามารถเชื่อมต่อเพื่อรับคำสั่งต่าง ๆ เช่น คำสั่งดาวน์โหลดมัลแวร์อื่น ๆ ซึ่งอาจเป็นมัลแวร์ที่สามารถขโมยข้อมูลในเครื่องหรือมัลแวร์ที่สามารถเข้ารหัสลับข้อมูลเพื่อเรียกค่าไถ่

Mac.Backdoor.iWorm ระบาดไปยังเครื่องพิวเตอร์มากกว่า 17,000 เครื่อง ซึ่งเว็บ thesafemac (http://www.thesafemac.com/dr-web-announces-new-iworm-malware/) ได้ระบุว่าพบมัลแวร์จากซอฟต์แวร์เถื่อน Photoshop CC 2014 จากการดาวน์โหลดด้วยไฟล์บิตทอร์เรนต์ของ The Pirate Bay เหตุการณ์นี้เป็นอีกสัญญาณที่ย้ำให้เห็นถึงอันตรายของการดาวน์โหลดซอฟต์แวร์เถื่อน และเปลี่ยนความคิดที่ว่า “Mac OS X ไม่มีมัลแวร์หรอก” ผู้ใช้งานเครื่อง Mac จึงควรติดตั้งแอนติไวรัสด้วย

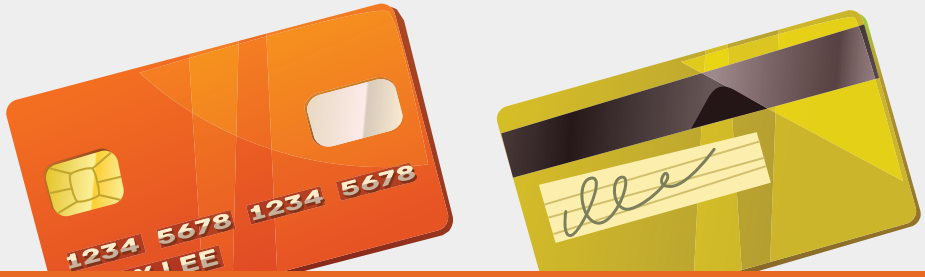
วันที่: 2014-10-06 | ที่มา: Dr.Web <http://thcert.co/GG08u9 >

Cisco ออกอัปเดต ปิดช่องโหว่ในซอฟต์แวร์บนอุปกรณ์ ASA

Cisco ได้ออกอัปเดต ปิดช่องโหว่ในซอฟต์แวร์บนอุปกรณ์ ASA (Cisco Adaptive Security Appliance) ซึ่งบางช่องโหว่ส่งผลกระทบต่อการให้บริการของอุปกรณ์ (Denial of Service)

สำหรับองค์กรใดที่ใช้อุปกรณ์นี้อยู่ แนะนำให้อ่านรายละเอียดตามที่มาซึ่งจะบอกว่าแต่ละช่องโหว่ส่งผลกระทบอะไรบ้าง และมีตารางบอกว่าซอฟต์แวร์เวอร์ชันอะไรได้รับผลกระทบจากช่องโหว่ใดบ้าง พร้อมระบุเวอร์ชันที่ปิดช่องโหว่แล้ว

วันที่: 2014-10-10 | ที่มา: Cisco <http://thcert.co/4YuBb9>



ขยายจากเม็กซิโก แฮกเกอร์ใช้มัลแวร์เจาะ ATM ขโมยเงินในหลายประเทศ

จากเหตุการณ์ก่อนหน้าที่แฮกเกอร์เคยเจาะระบบ ATM ใน Mexico เพื่อขโมยเงินในตู้ ปัจจุบันพบเหตุการณ์ในลักษณะเดียวกันทั่วโลกโดยเฉพาะในภูมิภาคเอเชียและประเทศรัสเซีย นอกจากนี้ยังพบตู้ ATM จำนวน 50 เครื่องในแถบยุโรปตะวันออกถูกโจมตีด้วย ซึ่งตำรวจอินเตอร์โปลกำลังดำเนินการสืบสวน

สำหรับวิธีการเจาะระบบของแฮกเกอร์นั้น มีดังนี้คือ

1. แฮกเกอร์แอบเชื่อมต่อมือถือที่มีมัลแวร์ชื่อ Ploutus กับ ATM ผ่าน USB แล้วตั้งมือถือทิ้งเอาไว้ในตู้ เมื่อ ATM ถูกเชื่อมต่อกับมือถือก็จะติดมัลแวร์และตกอยู่การควบคุมของแฮกเกอร์

2. แฮกเกอร์ส่งคำสั่งผ่าน SMS ไปยังมือถือที่เชื่อมต่อกับ ATM ให้ ATM ถอนเงินที่อยู่ในตู้ เพื่อให้แนบเนียนอาจให้คนหนึ่งแกล้งทำเป็นกดเงิน ในขณะที่อีกคนซึ่งอยู่ห่างออกไปส่ง SMS ทำให้สังเกตความผิดปกติได้ยาก

การโจมตีนี้เป็นการขโมยเงินในตู้โดยตรง ต่างจาก ATM Skimming ที่ขโมยเงินจากบัญชีของผู้ใช้งาน และสะดวกกว่าเพราะไม่ต้องขโมย PIN และข้อมูลเพื่อสร้างบัตรปลอม

วันที่: 2014-10-10 | ที่มา: Symantec <http://thcert.co/G07lo2>

ชื่อบัญชีและรหัสผ่านของผู้ใช้ Dropbox หลายร้อยรายถูกเผยแพร่ในอินเทอร์เน็ต รีบเปลี่ยนรหัสผ่านโดยด่วน

เมื่อวันที่ 13 ตุลาคมที่ผ่านมา มีผู้โพสต์รายชื่อบัญชีและรหัสผ่านของผู้ใช้บริการ Dropbox จำนวนหลายร้อยบัญชีลงในเว็บไซต์ Pastebin โดยอ้างว่าเป็นการแฮกระบบของ Dropbox และได้ข้อมูลไปมากกว่า 7,000,000 บัญชี

ผู้ใช้หลายรายรายงานว่ารหัสผ่านที่ถูกเผยแพร่ออกมานั้นสามารถใช้ล็อกอินได้จริง ล่าสุดทาง Dropbox ได้ส่งอีเมลชี้แจงให้ผู้ใช้งานเปลี่ยนรหัสผ่านของ Dropbox และแนะนำให้เปิดใช้งาน 2-Factor Authentication

ทาง Dropbox แจ้งว่าชื่อบัญชีและรหัสผ่านที่หลุดออกมานี้ไม่ได้มาจากการที่ระบบของ Dropbox แฮกตามที่ถูกกล่าวอ้าง แต่คาดว่าน่าจะหลุดจากระบบ 3rd Party ที่รองรับการเชื่อมต่อผ่าน Dropbox

วันที่: 2014-10-14 | ที่มา: Venturebeat <http://thcert.co/S9uQP0 >

เป็นเรื่อง! ภาพถ่ายและคลิปของ Snapchat หลุดมากกว่า 90,000 ไฟล์

Snapchat เป็นแอปพลิเคชันที่มีฟีเจอร์ส่งรูป โดยผู้ส่งสามารถตั้งค่าเวลาเพื่อให้รูปถูกลบออกจากเครื่องได้โดยอัตโนมัติ ซึ่งมีวัยรุ่นนิยมใช้แอปพลิเคชันนี้ส่งรูปนู้ด ซึ่งได้เกิดเหตุการณ์ภาพถ่ายและคลิปรวมมากกว่า 90,000 ไฟล์ ที่ไม่ได้มาจากทาง Snapchat โดยตรง หลุดจาก snapsaved.com ซึ่งปล่อยแอปพลิเคชันที่ช่วยเซฟภาพจาก Snapchat ไว้ในเครื่องอย่างถาวร โดยทาง SnapSaved ได้ออกมาเผยว่าถูกแฮก ทำให้ภาพถูกขโมย เพราะฉะนั้นผู้ที่ใช้งานเซฟภาพผ่านแอปพลิเคชันจาก SnapSaved อาจได้รับผลกระทบไปด้วย

กรณีนี้เป็นอีกตัวอย่างหนึ่งที่แสดงถึงความเสี่ยงในการให้แอปพลิเคชันใด ๆ เข้าถึงข้อมูลในอีกแอปพลิเคชันหนึ่ง โดยเฉพาะแอปพลิเคชันที่ไม่ได้มาจากแหล่งที่น่าเชื่อถืออย่าง Play Store หรือ App Store

วันที่: 2014-10-14 | ที่มา: Kenny Withers <http://thcert.co/80NHS8>

Adobe, Oracle และ Microsoft ปล่อยอัปเดตปิดช่องโหว่ พบการโจมตีผ่านช่องโหว่ Microsoft Office แล้ว

เมื่อวันที่ 14 ตุลาคม Adobe, Oracle และ Microsoft ปล่อยอัปเดตปิดช่องโหว่ใน Flash Player, Adobe AIR, Java, Microsoft Office, Internet Explorer, .NET และส่วนประกอบอื่น ของ Windows ในขณะที่ iSight บริษัทด้านความมั่นคงปลอดภัยระบุว่าพบการโจมตี NATO, หน่วยงานภาครัฐของประเทศยูเครนและประเทศฝั่งยุโรปตะวันตก รวมถึงบริษัทภาคพลังงาน ผ่านช่องโหว่ของ Microsoft Office ด้วยการส่งอีเมลหลอกลวงแนบไฟล์เอกสารของ Power Point หากเหยื่อเปิดไฟล์จะส่งผลให้เครื่องคอมพิวเตอร์ทำตามคำสั่งของผู้โจมตี

สำหรับผู้ที่ใช้งานซอฟต์แวร์ข้างต้นที่มีช่องโหว่ สามารถอัปเดตเป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่

วันที่: 2014-10-15 | ที่มา: Kreb On Security <http://thcert.co/uuyP50>

พบช่องโหว่ใน SSL 3.0 ผู้ไม่หวังดีสามารถอ่านข้อมูลที่มีการเข้ารหัสลับ

SSL เป็นเทคโนโลยีที่นิยมใช้ในการเข้ารหัสลับข้อมูลระหว่างรับส่ง ตัวอย่างการใช้ SSL ที่รู้จักกัน เช่น การเข้าเว็บไซต์ที่ใช้ HTTPS นั่นหมายความว่าข้อมูลที่ส่งจากเครื่องเราไปยังเว็บเซิร์ฟเวอร์ เช่น ไอดี/รหัสผ่าน จะมีการเข้ารหัสลับข้อมูลก่อนส่ง และข้อมูลที่ส่งจากเว็บเซิร์ฟเวอร์ก็จะมีการเข้ารหัสลับข้อมูลก่อนส่งมาหาเราเช่นกัน แฮกเกอร์ที่ดักขโมยข้อมูลระหว่างทางจะได้ข้อมูลที่อ่านไม่ออก ต้องทำการถอดรหัสลับข้อมูลก่อนซึ่งใช้เวลานานมากจนไม่คุ้มที่จะทำ

อย่างไรตาม Google ค้นพบช่องโหว่ใน SSL เวอร์ชัน 3.0 ซึ่งทำให้ผู้ไม่หวังดีถอดรหัสลับข้อมูลได้ง่ายขึ้น โดยให้ชื่อช่องโหว่ว่า POODLE ซึ่งส่งผลกระทบต่อบริการที่ใช้ SSL ทำให้แฮกเกอร์สามารถดักขโมยข้อมูลและถอดรหัสลับข้อมูลต่าง ๆ ได้ เช่น ไอดี/รหัสผ่านเมื่อเราล็อกอินเข้าเว็บที่ใช้ HTTPS รวมถึงอีเมลที่เราส่งหรือได้รับ

การป้องกันในส่วนของการใช้งาน HTTPS นั้น สามารถทำได้โดยการตั้งค่าเบราว์เซอร์หรือเซิร์ฟเวอร์ให้ไม่ใช้ SSL 3.0 (หากเบราว์เซอร์หรือเว็บเซิร์ฟเวอร์ไม่ยอมใช้ SSL 3.0 ในการรับส่งข้อมูล การโจมตีจะไม่สำเร็จ) ในขณะเดียวกันทาง Google และ Mozilla ได้บอกว่าจะอัปเดตให้ Chrome และ Firefox ปิดการใช้งาน SSL 3.0 โดยที่ผู้ใช้งานไม่ต้องตั้งค่าเองในเดือนหน้า

ผู้ที่ใช้เบราว์เซอร์ Firefox สามารถติดตั้ง Add-on ชื่อ SSL Version Control เพื่อปิดการใช้งาน SSL 3.0 และผู้ที่ใช้ IE, Chrome สามารถศึกษาการตั้งค่าเพื่อปิดการใช้งาน SSL 3.0 ได้ที่ https://zmap.io/sslv3

วันที่: 2014-10-15 | ที่มา: Zmap <http://thcert.co/53uc00>

Drupal ปล่อยอัปเดตปิดช่องโหว่ SQL Injection

Drupal ปล่อยอัปเดตเพื่อปิดช่องโหว่ SQL Injection ใน Drupal เวอร์ชัน 7.0 ถึงเวอร์ชันก่อนหน้า 7.32 แฮกเกอร์สามารถโจมตีผ่านช่องโหว่นี้โดยการส่งคำสั่ง SQL ที่ไม่พึงประสงค์เพื่อขโมยข้อมูลในฐานข้อมูลได้ ใครที่ใช้ Drupal สามารถอัปเดตเป็นเวอร์ชัน 7.32 เพื่อปิดช่องโหว่

วันที่: 2014-10-20 | ที่มา: Drupal <http://thcert.co/W85jh8>

Mozilla ปล่อยอัปเดตปิดชุดช่องโหว่ใน Firefox และ Thunderbird

Mozilla ได้ปล่อยอัปเดตปิดชุดช่องโหว่ใน Firefox และ Thunderbird ซึ่งบางช่องโหว่ส่งผลให้แฮกเกอร์สามารถขโมยข้อมูลหรือทำให้เครื่องคอมพิวเตอร์ของเหยื่อทำตามคำสั่งของแฮกเกอร์ได้ ใครที่ใช้ Firefox และ Thunderbird สามารถปิดช่องโหว่ได้ด้วยการอัปเดตเป็นเวอร์ชันล่าสุดคือ Firefox 33 และ Thunderbird 31.2

วันที่: 2014-12-08 | ที่มา: US-CERT <http://thcert.co/H4AbMS>

พบแนวโน้มการโจมตีตู้ ATM เก่าสูงขึ้น

เว็บ krebsonsecurity ได้เผยแพร่กราฟสถิติการแฮกตู้ ATM ตามประเทศต่าง ๆ เพื่อขโมยเงินในช่วงไตรมาสที่ 3 ที่ผ่านมา (http://krebsonsecurity.com/wp-content/uploads/2014/10/ncrmalware.png) พบว่าจำนวนการแฮกมีแนวโน้มสูงขึ้นเรื่อย ๆ

ล่าสุดเมื่อเดือนกันยายนที่ผ่านมา แก๊งอาชญากรไซเบอร์ได้ขโมยเงินรวมกว่า 1 ล้านดอลลาร์สหรัฐฯ จากตู้ ATM 18 ตู้ ในประเทศมาเลเซีย โดยพบว่าเป็นการแฮกโดยใช้มัลแวร์โจมตีผ่านช่องโหว่ในตู้ ATM ที่ใช้ Windows XP นอกจากนี้ยังเป็น ATM รุ่นเก่าที่ไม่แจ้งเตือนเมื่อมีการแงะตู้ ATM (แฮกเกอร์จำเป็นต้องเข้าถึงเครื่องคอมพิวเตอร์ในตู้ ATM เพื่อติดตั้งมัลแวร์)

วันที่: 2014-10-21 | ที่มา: Krebs On Security <http://thcert.co/026Ps2>

สร้างความอุ่นใจ ผู้ใช้ Windows 10 จะสามารถยืนยันตัวตนแบบ 2 ขั้นตอน (2-Step Verification)

ไมโครซอฟท์ได้เปิดเผยข้อมูลเกี่ยวกับ Windows 10 ที่จะเปิดตัวในปีหน้าว่าจะมีฟีเจอร์การยืนยันตัวตนแบบ 2 ขั้นตอน (2-Step Verification) โดยนอกจากการล็อกอินด้วยรหัสผ่านที่เราคุ้นเคย ก็สามารถเพิ่มการล็อกอินอีกขั้นโดยการใส่รหัสผ่านที่สองหรือลายนิ้วมือ

นอกจากนี้ Windows 10 ยังมีฟีเจอร์ด้านความมั่นคงปลอดภัยที่น่าสนใจอื่น ๆ เช่น สามารถล็อกอินโดยใช้มือถือเป็นเครื่องยืนยันตัวตนผ่าน WiFi, Bluetooth และสามารถจำกัดให้เครื่องคอมพิวเตอร์ของพนักงานในองค์กรสามารถติดตั้งซอฟต์แวร์ที่อยู่ใน Windows Store หรือซอฟต์แวร์ที่รับรองจากแหล่งที่น่าเชื่อถือ (Signed Application) แทนที่จะจำกัดไม่ให้ลงซอฟต์แวร์เลย

วันที่: 2014-10-24 | ที่มา: IT Pro Portal <http://thcert.co/sC73Zn>

Google รับรองความสามารถในการล็อกอินด้วยอุปกรณ์ USB แล้ว

Google ได้เพิ่มความสามารถในการล็อกอินชั้นที่สองนอกเหนือจากรหัสผ่านหลักที่เรามีอยู่แล้วด้วยอุปกรณ์ USB สำหรับล็อกอินที่รับรองเทคโนโลยี Universal 2nd Factor (U2F) Protocol

สำหรับการใช้งานต้องล็อกอินผ่าน Chrome (ปัจจุบันเบราว์เซอร์อื่น อย่าง Firefox, IE, Safari ยังไม่รองรับ U2F) ในขั้นแรกก่อน แล้วจึงเสียบอุปกรณ์ USB เพื่อยืนยันตัวตน

ก่อนหน้านี้เพื่อเพิ่มความมั่นคงปลอดภัย เราสามารถตั้งค่าใน Google เปิดใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอน (2-Step Verification) โดยในขั้นตอนที่ 2 จะใช้รหัสผ่านที่ได้รับจาก SMS หรือแอปพลิเคชันของ Google (Google Authenticator) บนมือถือ แต่ด้วยความสามารถใหม่ที่เพิ่มขึ้นมีข้อดีกว่าตรงที่ช่วยป้องกันการโจมตีประเภท Man In The Middle Attack และทำให้การล็อกอินขั้นที่ 2 ง่ายขึ้น ไม่ต้องพิมพ์รหัสผ่านถึง 2 ครั้ง

ในอนาคตเราคงจะได้เห็นเบราว์เซอร์และเว็บไซต์อื่น รองรับ U2F ให้เราได้ใช้อุปกรณ์ USB เพื่อล็อกอินในบริการออนไลน์ต่าง ๆ หลากหลายขึ้น

วันที่: 2014-10-24 | ที่มา: PC World <http://thcert.co/354v0j>

พบการโจมตีเซิร์ฟเวอร์ให้บริการส่งอีเมล (SMTP Server) ผ่านช่องโหว่ Shellshock

จากเหตุการณ์ค้นพบช่องโหว่ Shellshock ที่ส่งผลกระทบเป็นวงกว้าง ซึ่งบริการหรือซอฟต์แวร์ต่าง ๆ ที่เรียกใช้ Bash Shell และมีช่องโหว่นี้ก็อาจโดนโจมตีได้

ล่าสุดพบการโจมตีเซิร์ฟเวอร์ที่ให้บริการส่งอีเมล (SMTP Server) หลายแห่งผ่านช่องโหว่ดังกล่าวแล้ว โดยการโจมตีนี้มีจุดประสงค์เพื่อควบคุมเครื่องคอมพิวเตอร์ของเหยื่อ และใช้เป็นเครื่องมือในการโจมตีต่อเพื่อส่งผลกระทบต่อการทำงานหรือการให้บริการของเครื่องคอมพิวเตอร์อื่น ๆ

วันที่: 2014-10-28 | ที่มา: ZDnet <http://thcert.co/8gIF21>

พบช่องโหว่ NAT-PMP มีผลกระทบกับอุปกรณ์เราเตอร์มากกว่า 1.2 ล้านราย

NAT-PMP หรือ NAT Port Mapping Protocol เป็นโพรโทคอลที่ใช้ในการแมปหรือจับคู่ Port ระหว่างเครือข่ายภายนอกและเครือข่ายภายใน ให้มีความสัมพันธ์กันในอุปกรณ์เราเตอร์ เช่น การทำ Port Forwarding

อย่างไรก็ตามบริษัทด้านความมั่นคงปลอดภัย Rapid 7 ได้ค้นพบช่องโหว่ที่เกี่ยวข้องกับ NAT-PMP ซึ่งเกิดจากการตั้งค่าการทำงานที่ผิดพลาด (ไม่สอดคล้องกับ RFC 6886) ของ Vendor บนอุปกรณ์เราเตอร์ยี่ห้อต่าง ๆ ส่งผลให้ผู้ไม่หวังดีสามารถดักรับข้อมูลบนอุปกรณ์ดังกล่าว ทำให้สามารถขโมยข้อมูล ปลอมแปลงข้อมูล รวมถึงทำให้อุปกรณ์ดังกล่าวไม่สามารถให้บริการต่อได้

จากแหล่งข่าวอ้างอิง ได้แจ้งว่ามีผลกระทบกับเราเตอร์เป็นจำนวนมากกว่า 1.2 ล้านราย โดยมีข้อแนะนำให้ผู้ใช้งานติดต่อ Vendor ในการพัฒนาแก้ไขช่องโหว่ หรือหลีกเลี่ยงการใช้งานอุปกรณ์ดังกล่าวจนกว่าจะมีการแก้ไข โดยสามารถตรวจสอบรายชื่อ Vendor ที่มีผลกระทบได้จาก http://www.kb.cert.org/vuls/id/184540

วันที่: 2014-10-28 | ที่มา: CERT <http://thcert.co/ID5217>

แอปพลิเคชันไฟฉายยอดฮิต ขอสิทธิเกินความจำเป็น

บริษัทด้านความมั่นคงปลอดภัย Snoopwall ได้วิเคราะห์แอปพลิเคชันไฟฉายยอดฮิตทั้งหลายบน Play Store พบ 10 แอปพลิเคชันที่ขอสิทธิเกินความจำเป็น เช่น ขอสิทธิอ่าน Contact, GPS ซึ่งมีความเสี่ยงถ้าข้อมูลเหล่านี้ตกไปอยู่ในมือเหล่ามิจฉาชีพได้ เพื่อความมั่นคงปลอดภัย สำหรับผู้ใช้งานอาจดูสักนิดก่อนติดตั้งแอปพลิเคชันยอดฮิตทั้งหลายว่าขอสิทธิเกินความจำเป็นหรือไม่ และมีการบอกหรือไม่ว่านำไปใช้ทำอะไร

วันที่: 2014-10-29 | ที่มา: Snoopwall <http://thcert.co/V64zhy>

Apple ปล่อยอัปเดตปิดชุดช่องโหว่ใน QuickTime

Apple ได้ปล่อยอัปเดตปิดชุดช่องโหว่ใน QuickTime บน Windows ซึ่งแฮกเกอร์อาจโจมตีผ่านช่องโหว่นี้ ทำให้ QuickTime ทำงานผิดปกติหรือใช้การไม่ได้ (Denial of Service) หรือทำให้เครื่องคอมพิวเตอร์ทำตามคำสั่งของแฮกเกอร์จากระยะไกล (Remote Code Execution) ผู้ใช้งานสามารถปิดช่องโหว่โดยการอัปเดต QuickTime เป็นเวอร์ชัน 7.7.6

วันที่: 2014-10-30 | ที่มา: Apple <http://thcert.co/M8aj2J>

แฮกเกอร์เจาะระบบเครือข่ายคอมพิวเตอร์ของ White House

สำนักข่าว The Washington Post ได้เผยแพร่ข่าวเกี่ยวกับ การเจาะระบบเครือข่ายคอมพิวเตอร์ที่ใช้ใน White House ส่งผลให้บริการบางอย่างใช้การไม่ได้ อย่างไรก็ตาม ระบบเครือข่ายนี้ไม่ใช่เครือข่ายที่สำคัญ (Unclassified Network) และไม่พบการรั่วไหลของข้อมูลสำคัญ

วันที่: 2014-10-31 | ที่มา: The Washington Post <http://thcert.co/K644uL>

Drupal เตือนให้อัปเดตปิดช่องโหว่รอบสอง

จากที่ก่อนหน้านี้เมื่อวันที่ 15 ตุลาคม ทาง Drupal ได้ออกอัปเดตปิดช่องโหว่ SQL Injection ใน CMS ที่ส่งผลให้ผู้ไม่หวังดีสามารถขโมยข้อมูลออกจากฐานข้อมูลได้ เมื่อวัน 29 ตุลาคมที่ผ่านมา Drupal ได้ออกมาเตือนอีกครั้ง โดยแนะนำว่าหากไม่ได้อัปเดตช่วงที่ Drupal ประกาศเกี่ยวกับช่องโหว่วันที่ 15 ให้ตั้งสมมุติฐานว่าเว็บไซต์อาจถูกแฮกไปแล้ว ควรทำการกู้คืนจาก Back Up ก่อนหน้าวันที่ 15

วันที่: 2014-11-03 | ที่มา: Drupal <http://thcert.co/63T854>

ร้ายกาจกว่า Unit 61398 กลุ่มแฮกเกอร์จีนใช้เทคนิคซับซ้อน ขโมยข้อมูลองค์กร

ก่อนนี้เราอาจเคยได้ยินข่าวเกี่ยวกับกลุ่มแฮกเกอร์ชื่อ Unit 61398 ในกองทัพจีนที่ขโมยข้อมูลจากองค์กรต่าง ๆ ในสหรัฐฯ ล่าสุดกลุ่มนักวิจัยด้านความมั่นคงปลอดภัยจากหลายฝ่ายได้ร่วมมือกันค้นพบกลุ่มแฮกเกอร์จีนที่ใช้เทคนิคซับซ้อนยิ่งกว่า โดยตั้งชื่อให้ว่า Axiom ซึ่งมีความสามารถในการซ่อนร่องรอยการเจาะระบบดีกว่า

เมื่อดูจากลักษณะการโจมตี คาดว่ากลุ่มแฮกเกอร์นี้ได้รับการสนับสนุนจากรัฐบาลเพื่อขโมยความลับทางการค้า (Trade Secret) และมุ่งเป้าโจมตีหน่วยงานรัฐบาลและหน่วยงานที่สนับสนุนหรือคัดค้านระบอบประชาธิปไตย

Axiom ได้เผยแพร่มัลแวร์ไปยังคอมพิวเตอร์อย่างน้อย 43,000 เครื่องทั่วโลก มีทั้งเครื่องคอมพิวเตอร์ของหน่วยงานรัฐบาล นักข่าว บริษัทด้านพลังงานและการสื่อสารด้าน Telecommunication หน่วยงานสิทธิมนุษยชน และหน่วยงานสนับสนุนระบอบประชาธิปไตย

วันที่: 2014-11-04 | ที่มา: The Washington Post <http://thcert.co/F8Qlo4>

เพิ่มความเป็นส่วนตัว แก้ปัญหาเข้า Facebook ผ่าน Tor

โดยทั่วไป บุคคลหรือหน่วยงานที่สามารถดักรับข้อมูลระหว่างการรับส่ง เช่น ผู้ให้บริการอินเทอร์เน็ต (ISP) สามารถทราบได้ว่า หมายเลขไอพีไหนเข้าเว็บอะไรอยู่ ซึ่ง ISP นั้นอาจจะนำไปสืบต่อว่าเป็นเครื่องคอมพิวเตอร์ของบ้านไหนหรือหน่วยงานใดที่เข้าเว็บดังกล่าว ดังนั้น แทนที่จะเข้าเว็บตรง ผู้ใช้บางรายอาจเลือกที่จะป้องกันโดยการเข้าเว็บผ่านเครือข่ายที่เรียกว่า Tor ทำให้ ISP ที่เราเชื่อมต่ออยู่ไม่สามารถรู้ได้ว่าเรากำลังเข้าชมอะไร

อย่างไรก็ตาม ผู้ใช้งานอาจพบปัญหาในการใช้ Tor เข้าเว็บ Facebook เนื่องจาก Tor จะอำพรางโดยสุ่มเปลี่ยนหมายเลข IP ต้นทาง และดูเหมือนว่าเราเข้าเว็บจากสถานที่ต่าง ๆ ทั่วโลก ทำให้ Facebook อาจสับสนว่าบัญชีของเราถูกแฮกและกำลังถูกล็อกอินโดยเครื่องคอมพิวเตอร์ที่ถูกควบคุมโดยแฮกเกอร์

ในการแก้ปัญหาดังกล่าว Facebook ได้เพิ่มความสามารถสนับสนุน Tor โดยให้ผู้ที่ใช้ Tor สามารถเข้าเว็บไซต์ผ่านลิงก์ https://facebookcorewwwi.onion/(ต้องใช้ Tor ถึงจะเข้าได้) ซึ่งการเชื่อมต่อยังคงมีการเข้ารหัสลับข้อมูลเหมือนเข้าเว็บ Facebook เพื่อป้องกันไม่ให้แฮกเกอร์ที่ดักรับข้อมูลระหว่างทาง สามารถอ่านข้อมูลได้

วันที่: 2014-11-05 | ที่มา: Facebook <http://thcert.co/0Oaor8>

36 มัลแวร์ใหม่ผุด หยุดไม่อยู่ 20 ล้านสายพันธุ์ในรอบ 3 เดือน

แนวโน้มของจำนวนมัลแวร์สายพันธุ์ใหม่ดูเหมือนจะเพิ่มขึ้นอย่างหยุดไม่ได้ จากข้อมูลของบริษัทแอนติไวรัสชื่อ PandaLabs เผยสถิติช่วงไตรมาสที่ 3 พบว่ามีมัลแวร์ใหม่ 20 ล้านสายพันธุ์ หรือคิดเป็นอัตรา 227,747 สายพันธุ์ต่อวัน นอกจากนี้ PandaLabs ยังระบุอัตราการระบาดของมัลแวร์ทั่วโลกถึง 37.93% โดยพบส่วนใหญ่ในภูมิภาคเอเชียและประเทศในลาตินอเมริกัน ซึ่งประเทศที่มีอัตราการระบาดของมัลแวร์สูงเป็นอันดับหนึ่งคือประเทศจีน

วันที่: 2014-11-07 | ที่มา: Net-security <http://thcert.co/9R32Qn>

WireLurker เปิดยุคใหม่ของมัลแวร์บน OS X และ iOS

บริษัทด้านความมั่นคงปลอดภัย Palo Alto Networks เผยการค้นพบมัลแวร์สายพันธุ์ใหม่ WireLurker บนเครื่อง Mac ซึ่งมีความสามารถพิเศษคือสามารถเผยแพร่มัลแวร์ไปยังอุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS อย่าง iPhone หรือ iPad ที่มาเสียบเครื่องที่ติดมัลแวร์นี้ผ่าน USB (ถึงแม้ว่าไม่ได้ทำการ Jailbreak ก็ตาม) เพื่อขโมยข้อมูล

ทั้งนี้ มัลแวร์ดังกล่าวถูกเผยแพร่ในรูปแบบของ 467 แอปพลิเคชันบน App Store ชื่อ Maiyadi ซึ่งขายแอปพลิเคชันบน Mac สำหรับคนจีน และในช่วงที่ 6 เดือนที่ผ่านมามีคนดาวน์โหลดแอปพลิเคชันที่แฝงมัลแวร์เหล่านี้ถึง 356,104 ครั้ง

วันที่: 2014-11-07 | ที่มา: Palo Alto Networks <http://thcert.co/Hi60ar>

สำรวจ App. ส่ง Message ชื่อดัง มั่นคงปลอดภัยแค่ไหน

องค์กรไม่แสวงหากำไร EFF (Electronic Frontier Foundation) ได้วิเคราะห์แอปพลิเคชันต่าง ๆ สำหรับสื่อสารหรือส่งข้อความ ว่ามีความมั่นคงปลอดภัยมากน้อยแค่ไหน โดยประเมินในด้านต่าง ๆ เช่น ข้อมูลที่รับส่งมีการเข้ารหัสลับหรือไม่ ผู้ให้บริการสามารถอ่านข้อมูลของเราได้หรือไม่ หรือแค่ผู้รับและผู้ส่ง

แอปพลิเคชันที่เราคุ้นเคย เช่น Skype, WhatsApp, Snapchat, Facebook Chat, Google Hangouts ก็อยู่ในรายการที่ได้รับการวิเคราะห์ พบว่ามีการเข้ารหัสลับข้อมูลเพื่อป้องกันแฮกเกอร์แต่ผู้ให้บริการแอปพลิเคชันยังคงสามารถอ่านข้อมูลที่รับส่งได้ ในขณะที่แอปพลิเคชันที่ได้รับการประเมินว่ามีความสามารถด้านความมั่นคงปลอดภัยครบถ้วนทุกด้านตามเกณฑ์การประเมินคือ CryptoCat และ TextSecure ใครสนใจก็สามารถลองพิจารณาใช้ดูได้

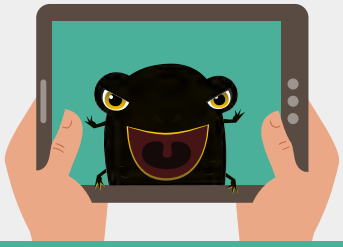
วันที่: 2014-11-11 | ที่มา: EFF <http://thcert.co/g368pQ>

มัลแวร์ WireLurker โจมตี Windows แล้ว

จากข่าวการแพร่ระบาดมัลแวร์ WireLurker บนเครื่อง Mac ไปสู่อุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS อย่าง iPhone, iPad ล่าสุดได้พบมัลแวร์นี้บน Windows แล้ว อย่างไรก็ตามมัลแวร์ที่พบเป็นเวอร์ชันที่เก่ากว่ามัลแวร์ที่พบบน Mac ซึ่งมีโอกาสโจมตีสำเร็จน้อยกว่า โดยมัลแวร์นี้ปลอมเป็น Installer สำหรับติดตั้งแอปพลิเคชันเถื่อนบน iOS

สำหรับ WireLurker บนเครื่อง MAC ปัจจุบัน Apple ได้ถอนใบรับรองดิจิทัลที่รับรองมัลแวร์นี้แล้ว หากผู้ใช้งานบังเอิญติดตั้งมัลแวร์ดังกล่าวก็จะได้รับการแจ้งเตือนว่าเป็นแอปพลิเคชันที่ไม่น่าเชื่อถือ

วันที่: 2014-11-11 | ที่มา: Palo Alto Networks <http://thcert.co/IL43s6>



เผยเทคนิคโจมตีใหม่แทนที่ App. แท้เพื่อล้วงข้อมูลใน iPhone, iPad

จากข่าวมัลแวร์ WireLurker ที่สามารถแพร่ระบาดจากคอมพิวเตอร์สู่เครื่อง iPad, iPhone ที่มาเชื่อมต่อผ่าน USB ถึงแม้อุปกรณ์จะไม่ได้ Jailbreak ก็ตาม ล่าสุดบริษัทด้านความมั่นคงปลอดภัย FireEye ออกมาเปิดเผยเทคนิคใหม่สำหรับเผยแพร่มัลแวร์ไปยัง iPad, iPhone โดยให้ชื่อว่า Masque Attack ซึ่ง WireLurker ก็ใช้ส่วนหนึ่งของเทคนิคที่ว่านี้ในการโจมตี

การโจมตีอาจเริ่มจากอีเมลหรือข้อความที่หลอกให้ผู้ใช้งานติดตั้งแอปพลิเคชันปลอมที่ไม่ได้อยู่ใน App Store ซึ่งหากผู้ใช้งานหลงกลกดยอมรับติดตั้ง มัลแวร์จะไปติดตั้งทับแอปพลิเคชันแท้ที่ติดตั้งอยู่ในเครื่องเพื่อขโมยข้อมูลต่าง ๆ ที่แอปพลิเคชันเข้าถึงได้ โดย FireEye ได้สาธิตติดตั้งมัลแวร์แทนแอปพลิเคชัน Gmail เพื่อที่จะขโมยไอดี/รหัสผ่าน รวมถึงอีเมลในคลิป (https://www.dropbox.com/s/v15d7jxd0fj2gtn/ios_demo_retake.mp4?dl=0)

ทั้งนี้ FireEye ได้แนะนำให้เลือกติดตั้งแอปพลิเคชันจาก App Store หรือจากองค์กรของผู้ใช้งานเพื่อหลีกเลี่ยงการโจมตี

วันที่: 2014-11-12 | ที่มา: The Register <http://thcert.co/3Ax8r0>

อัปเดตปิดช่องโหว่ใน Windows, Chrome และ Adobe Flash Player

ในสัปดาห์นี้มีการปล่อยอัปเดตมาปิดช่องโหว่ผลิตภัณฑ์ยอดนิยมหลายตัว เริ่มจาก Microsoft ที่ปล่อยอัปเดตประจำเดือนเพื่อปิดช่องโหว่ในส่วนประกอบต่าง ๆ เช่น IE, Windows OLE ซึ่งมีช่องโหว่ประเภท Remote Code Execution ที่ถูกนำไปใช้ในการโจมตี เพื่อทำให้เครื่องเหยื่อทำตามคำสั่งแฮกเกอร์

สำหรับ Chrome และ Adobe Flash Player ทาง Google และ Adobe ก็ปล่อยอัปเดตปิดช่องโหว่นี้เช่นกัน

ทั้งนี้หากผู้ใช้งานติดตั้ง Windows, Chrome และ Adobe Flash Player โดยใช้ค่าเริ่มต้น (Default Setting) ก็จะได้รับอัปเดตโดยอัตโนมัติ

วันที่: 2014-11-12 | ที่มา: Microsoft <http//thcert.co/8LFqkb>

iPhone 5s, Samsung Galaxy S5 และ Nexus 5 ถูกแฮกสำเร็จในงานแข่งขัน Pwn2Own

เมื่อสัปดาห์ที่แล้ว บริษัท HP ได้จัดงานแข่งขันรวมเหล่าผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยเพื่อประชันความสามารถโดยให้แฮกอุปกรณ์มือถือต่าง ๆ ภายใต้ชื่อ Mobile Pwn20wn 2014 ที่เมืองโตเกียว ประเทศญี่ปุ่น ซึ่งพบว่ามือถือยอดฮิตอย่าง iPhone 5s, Samsung Galaxy S5, Nexus 5, Amazon Fire Phone และ Nokia Lumia 1520 มีช่องโหว่และถูกแฮกสำเร็จ โดยพบช่องโหว่ต่าง ๆ เช่น ช่องโหว่ใน Safari บน iOS, ช่องโหว่เกี่ยวกับ NFC ใน Samsung Galaxy S5 และ Nexus 5 ซึ่งทางบริษัทเจ้าของอุปกรณ์จะนำข้อมูลมาสร้างอัปเดตเพื่อปิดช่องโหว่ต่อไป

วันที่: 2014-11-18 | ที่มา: 9to5mac <http://thcert.co/SLA94v>

อัปเดตปิดช่องโหว่ใน iOS, OS X Yosemite, and Apple TV

Apple ได้ปล่อยอัปเดตปิดช่องโหว่ในระบบปฏิบัติการของผลิตภัณฑ์ยอดนิยมหลายตัว ได้แก่ iPad/iPhone (iOS), Mac (OS X Yosemite) และ Apple TV ซึ่งเป็นช่องโหว่ประเภท Remote Code Execution ที่อาจส่งผลทำให้เครื่องของเหยื่อถูกขโมยข้อมูล และถูกควบคุมเพื่อใช้ในการโจมตีผู้อื่นได้ ผู้ใช้งานสามารถอัปเดตระบบปฏิบัติการเป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่

วันที่: 2014-11-18 | ที่มา: US-CERT <http://thcert.co/K5V3wA>

พบช่องโหว่ใน Windows Phone 8.1 มัลแวร์ได้สิทธิของแอปพลิเคชันอื่นที่ติดตั้งอยู่ในเครื่อง

นักวิจัยด้านความมั่นคงปลอดภัยพบช่องโหว่ในระบบปฏิบัติการ Windows Phone 8.1 บน Nokia Lumia ส่งผลให้มัลแวร์ที่ติดตั้งในเครื่องได้สิทธิเช่นเดียวกับแอปพลิเคชันอื่น โดยพบว่าหากติดตั้งมัลแวร์บนเครื่องและคัดลอกมัลแวร์แทนที่แอปพลิเคชันอื่นที่ถูกติดตั้งใน SD Card มัลแวร์นั้นก็จะได้สิทธิต่าง ๆ เช่น การเข้าถึงข้อมูล เหมือนกับแอปพลิเคชันที่ถูกแทนที่ ทั้งนี้ข้อมูลของช่องโหว่ดังกล่าวมีการรายงานไปยัง Microsoft เพื่อให้แก้ไขต่อไป

วันที่: 2014-11-19 | ที่มา: The Hacker News <http://thcert.co/W0T5C8>

Drupal ปล่อยอัปเดตปิดชุดช่องโหว่

Drupal ได้ออกอัปเดตปิดช่องโหว่ใน Drupal 6 และ Drupal 7 ที่เปิดโอกาสให้แฮกเกอร์สามารถสุ่มขโมย Session (Random Session Hijacking) และยังได้ออกอัปเดตปิดช่องโหว่ประเภท DoS ใน Drupal 7 ที่ส่งผลกระทบต่อการทำงานของระบบ

ผู้ที่ใช้งาน Drupal 6 และ 7 สามารถอัปเดตเป็นเวอร์ชัน 6.34 และ 7.34 เพื่อปิดช่องโหว่

วันที่: 2014-11-21 | ที่มา: Drupal <http://thcert.co/042280>

Microsoft

Microsoft ปล่อยอัปเดตปิดช่องโหว่ใน Windows Server

Microsoft ได้ออกอัปเดตเพื่อปิดช่องโหว่ใน Kerberos KDC ซึ่งเป็นส่วนประกอบของ Windows Server ช่องโหว่ดังกล่าวอาจส่งผลให้แฮกเกอร์ที่สามารถล็อกอินจากระบบ Active Domain สามารถเลื่อนสิทธิจากผู้ใช้งานทั่วไปเป็นผู้ดูแลระบบได้ (Privilege Escalation) ผู้ดูแลระบบที่ใช้ Windows Server สามารถอัปเดตเป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่

วันที่: 2014-11-21 | ที่มา: Microsoft <http://thcert.co/onPGT8>

พบช่องโหว่ในเครื่องอัดวิดีโอ Hikvision แฮกเกอร์สามารถเข้าควบคุมอุปกรณ์ได้

เมื่อเร็ว ๆ นี้ได้มีการค้นพบช่องโหว่ในเครื่องบันทึกวิดีโอจากกล้องวงจรปิด (Digital Video Recorders) ยี่ห้อ Hikvision ซึ่งจากการโจมตีผ่านช่องโหว่นี้ แฮกเกอร์สามารถลบวิดีโอที่มีการบันทึกไว้ หรือควบคุมอุปกรณ์เพื่อใช้เป็นฐานในการโจมตีอุปกรณ์อื่น ๆ ที่อยู่ในเครือข่ายเดียวกัน ทั้งนี้ นักวิจัยจากบริษัทด้านความมั่นคงปลอดภัย Rapid 7 ได้ระบุว่ามีอุปกรณ์นี้ 150,000 เครื่องที่สามารถเข้าถึงได้ผ่านอินเทอร์เน็ต ซึ่งอาจถูกโจมตีได้ และปัจจุบันยังไม่มีอัปเดตเพื่อปิดช่องโหว่

วันที่: 2014-11-25 | ที่มา: The Register <http://thcert.co/t6Cr0i>

Adobe ปล่อยอัปเดตปิดช่องโหว่ใน Adobe Flash Player

เมื่อวันที่ 25 พฤศจิกายนที่ผ่านมา Adobe ได้ออกอัปเดตเพื่อปิดช่องโหว่ใน Adobe Flash Player ซึ่งช่องโหว่นี้อาจเปิดโอกาสให้แฮกเกอร์สามารถควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้ และปัจจุบันมีนักวิจัยด้านความมั่นคงปลอดภัยระบุว่าพบการโจมตีโดยใช้ช่องโหว่นี้แล้ว

ผู้ใช้งานสามารถตรวจสอบเวอร์ชันของซอฟต์แวร์ที่ใช้ได้ที่ https://www.adobe.com/software/flash/about/ และสามารถอัปเดตเป็นเวอร์ชันล่าสุด (เวอร์ชัน 15.0.0.239 สำหรับ Windows และ Mac และเวอร์ชัน 13.0.0.258 สำหรับ Linux) เพื่อปิดช่องโหว่

วันที่: 2014-11-27 | ที่มา: Adobe <http://thcert.co/xm74R8>

Twitter ประกาศเริ่มเก็บข้อมูลว่าเครื่องมือถือลง App อะไรบ้าง

ทางบริษัทผู้พัฒนา Twitter ได้ประกาศว่า แอปพลิเคชัน Twitter บนสมาร์ตโฟนเริ่มเก็บข้อมูลว่าในเครื่องลงแอปพลิเคชันอะไรบ้าง เพื่อให้แสดงโฆษณาใน Twitter ตรงตามความสนใจของผู้ใช้มากขึ้น

ทั้งนี้หากผู้ใช้งานตั้งค่าเพื่อไม่ให้ Twitter แสดงโฆษณาตามความสนใจของผู้ใช้งาน Twitter ก็จะไม่เก็บข้อมูลว่าในเครื่องได้ลงแอปพลิเคชันอะไรบ้าง ผู้ใช้งานสามารถศึกษาวิธีการตั้งค่าได้จากเว็บไซต์ของ Twitter (https://support.twitter.com/articles/20172069)

วันที่: 2014-11-28 | ที่มา: Twitter <http://thcert.co/53ezM2>

หนังใหม่ Sony รั่วบนอินเทอร์เน็ต ก่อนเข้าโรง

บริษัทยักษ์ใหญ่ Sony ถูกโจมตีเมื่อสัปดาห์ที่แล้วจากแฮกเกอร์ที่ใช้ชื่อ GOP (The Guardians of Peace) โดยเริ่มจากคอมพิวเตอร์ของพนักงานในบริษัท ปรากฏข้อความว่าโดนแฮกโดย GOP พร้อมทั้งระบุชื่อไฟล์ของข้อมูลที่ได้ขโมยไปและบอกว่าหากไม่ทำตามคำเรียกร้องจะเผยแพร่ข้อมูลลับที่ได้มา นอกจากนี้แฮกเกอร์ยังได้ขโมยบัญชี Twitter สำหรับโปรโมตหนังและโพสต์ข้อความในเชิงลบอีกด้วย

ล่าสุดมีรายงานว่าพบหนังใหม่ของค่ายนี้ 5 เรื่องถูกเผยแพร่อยู่บนอินเทอร์เน็ต ซึ่ง 4 เรื่องยังไม่ได้ฉายในโรงภาพยนตร์ และข้อมูลที่ถูกขโมยอาจรวมไปถึงข้อมูลอื่น อย่างเช่น พาสปอร์ตของนักแสดง ข้อมูลเกี่ยวกับระบบ IT ของ Sony อย่างไรก็ตามยังไม่สามารถยืนยันได้ว่ามีความเกี่ยวข้องกับแฮกเกอร์ GOP

วันที่: 2014-12-01 | ที่มา: Torrent Freak <http://thcert.co/iQ1QoK>

พบ Backdoor ใหม่ แฝงมากับ Plug-in เถื่อนของ Joomla, WordPress และ Drupal

บริษัทด้านความมั่นคงปลอดภัย Fox-IT ได้เผยแพร่รายงานเกี่ยวกับ Backdoor ตัวใหม่ชื่อ CryptoPHP ซึ่งแอบแฝงมากับ Plug-in เถื่อนของ CMS ต่าง ๆ เช่น Joomla, WordPress และ Drupal

CryptoPHP จะแอบใส่ข้อความในหน้าเว็บไซต์ของเหยื่อที่ติดตั้ง Plug-in เถื่อน โดยมีจุดประสงค์เพื่อเพิ่ม Search Ranking ของเว็บไซต์ที่แฮกเกอร์ต้องการให้อยู่ในลำดับต้นของการค้นหา

ปัจจุบันพบว่า มัลแวร์ดังกล่าวอยู่บนเว็บเซิร์ฟเวอร์มากกว่า 23,000 เครื่องแล้ว การโจมตีในครั้งนี้ถือเป็นอีกตัวอย่างหนึ่งที่แสดงถึงอันตรายที่แฝงมากับ Plug-in เถื่อน ซึ่งอาจเกิดผลร้ายกับเครื่องคอมพิวเตอร์ของผู้ที่ติดตั้งโดยไม่รู้ตัว

วันที่: 2014-12-02 | ที่มา: PC World <http://thcert.co/z2s1I5>

FBI เตือนถึงการโจมตี ใช้มัลแวร์ลบข้อมูล

หลังเหตุการณ์ Sony ถูกโจมตี ซึ่งทำให้ข้อมูลขององค์กรรั่วไหล Sony ได้จ้างบริษัทด้านความมั่นคงปลอดภัย Mandiant เข้ามาช่วยรับมือและจัดการภัยคุกคามที่เกิดขึ้น และให้ทาง FBI เข้ามาสืบสวน

ล่าสุด FBI ออกมาเตือนภาคเอกชนเกี่ยวกับการโจมตี โดยแฮกเกอร์ได้ใช้มัลแวร์เพื่อลบข้อมูลในเครื่องคอมพิวเตอร์ด้วยวิธีที่ทำให้กู้คืนข้อมูลได้ยาก พร้อมแนะนำให้เพิ่มมาตรการในการป้องกันระบบสารสนเทศและจำกัดการเข้าถึงฐานข้อมูล อย่างไรก็ตาม FBI ปฏิเสธที่จะตอบคำถามว่าการโจมตีที่ได้แจ้งเตือนเป็นการโจมตี Sony หรือไม่

วันที่: 2014-12-03 | ที่มา: The Hacker News <http://thcert.co/iSn3J3>

Mozilla แจ้งอัปเดตปิดชุดช่องโหว่ใน Firefox, Thunderbird

Mozilla ได้ประกาศอัปเดตปิดชุดช่องโหว่ใน Firefox, Thunderbird ซึ่งแฮกเกอร์อาจสามารถอาศัยชุดช่องโหว่นี้ขโมยข้อมูล หรือทำให้ซอฟต์แวร์ทำงานผิดปกติได้ รวมถึงโจมตีด้วยช่องโหว่ประเภท Buffer Overflow

ผู้ที่ใช้ Firefox หรือ Thunderbird สามารถอัปเดตให้เป็นเวอร์ชันล่าสุด (Firefox เวอร์ชัน 34, Firefox ESR เวอร์ชัน 31.3 และ Thunderbird เวอร์ชัน 31.3) เพื่อปิดช่องโหว่นี้

วันที่: 2014-12-04 | ที่มา: US-CERT <http://thcert.co/YW1B93>

ภัยร้ายที่อาจแฝงมากับมือถือใหม่ของคุณ

ปัจจุบันผู้สร้างมัลแวร์ได้พัฒนาและปรับเปลี่ยนวิธีการใหม่ขึ้นมาเพื่อใช้จัดการเหยื่อในโลกไอที ล่าสุดมัลแวร์ประเภทโทรจันตัวใหม่ซึ่งได้รับการขนานนามว่า DeathRing ได้มีการตรวจพบโดยนักวิจัยทางด้านความมั่นคงปลอดภัย โดยมัลแวร์นี้จะถูกติดตั้งมาพร้อมกับสมาร์ตโฟนราคาประหยัดที่ใช้ระบบปฏิบัติการ Android และยิ่งไปกว่านั้นมัลแวร์ดังกล่าวยังไม่สามารถถูกถอนการติดตั้งได้โดยผู้ใช้งานหรือแอนติไวรัสอีกด้วย

DeathRing จะปลอมตัวเองเป็น Ringtone Application (แอปพลิเคชันสำหรับเสียงเรียกเข้า) เพื่อตบตาผู้ใช้สมาร์ตโฟน จากนั้นมัลแวร์นี้จะดาวน์โหลดข้อความ และข้อมูลต่าง ๆ จากเซิร์ฟเวอร์ที่ถูกควบคุมโดยผู้สร้างมัลแวร์ไปยังสมาร์ตโฟนของเหยื่อ โดยมีเนื้อหาเพื่อหลอกลวงเหยื่อ และล้วงเอาข้อมูลส่วนตัวที่สำคัญ รวมไปถึงหลอกล่อให้เหยื่อดาวน์โหลดมัลแวร์ตัวอื่นมาช่วยในการล้วงข้อมูล

ขณะนี้ DeathRing กำลังแพร่ระบาดในแอฟริกา เอเชีย และในอีกหลายประเทศที่กำลังพัฒนา ซึ่งรุ่นของสมาร์ตโฟนที่มีความเสี่ยงและเข้าข่ายในการถูกคุกคามมีดังนี้ Samsung GS4/Note II (ของเลียนแบบ), Samsung i9502+ (ของเลียนแบบ), Gionee Gpad G, Gionee GN708W, Gionee GN800, Polytron Rocket S2350, Hi-Tech Amaze Tab, Karbonn TA-FONE A34/A37, Jiayu G4S, Haier H7, รวมถึงอุปกรณ์รุ่นต่าง ๆ ของ TECNO

วันที่: 2014-12-08 | ที่มา: The Hacker News <http://thcert.co/nx6mvm>

ISC แจ้งอัปเดตปิดชุดช่องโหว่ใน BIND

ISC ได้แจ้งอัปเดตปิดชุดช่องโหว่ใน BIND ซึ่งมีช่องโหว่ที่อาจทำให้แฮกเกอร์สามารถโจมตีในลักษณะ DoS (Denial-of-Service) ส่งผลต่อการทำงานของซอฟต์แวร์ ผู้ที่ใช้ซอฟต์แวร์ดังกล่าวสามารถอัปเดตเป็น BIND 9.10.1-P1 เพื่อปิดช่องโหว่

วันที่: 2014-12-09 | ที่มา: ISC <http://thcert.co/3r5eb9>

อัปเดตปิดชุดช่องโหว่ใน vCenter Server, vCenter Server Appliance และ ESXi

VMware ประกาศอัปเดตปิดชุดช่องโหว่ใน vCenter Server, vCenter Server Applicance และ ESXi ซึ่งส่วนหนึ่งเป็นช่องโหว่ประเภท Cross-site Scripting และบางช่องโหว่อาจทำให้แฮกเกอร์สามารถโจมตีด้วยเทคนิค Man-in-the-Middle ผู้ที่ใช้งานซอฟต์แวร์ดังกล่าวสามารถอัปเดตเป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่

วันที่: 2014-12-09 | ที่มา: VMWare <http://thcert.co/0Pu3Yb>

อัปเดตการโจมตี Sony พบร่องรอยแฮกเกอร์ที่กรุงเทพฯ

จากเหตุการณ์โจมตีบริษัท Sony โดยแฮกเกอร์ที่เรียกตัวเองว่า GOP (Guardians of Peace) และเหตุการณ์การรั่วไหลของข้อมูล เช่น หนังก่อนเข้าโรง รวมถึงข้อมูลส่วนตัวของพนักงานและนักแสดง ซึ่งยังไม่มีการยืนยันว่าเป็นการกระทำของใคร โดย FBI ได้เข้าไปสืบสวนและในเวลาถัดมาได้ทำการแจ้งเตือนการโจมตีจากมัลแวร์ที่สามารถทำการลบข้อมูลในเครื่องคอมพิวเตอร์ ซึ่งมัลแวร์มีการติดต่อมายังหมายเลขไอพีในประเทศไทย (https://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/) อย่างไรก็ตามทาง FBI ไม่ได้ระบุชัดเจนว่า มัลแวร์นี้ถูกใช้ในการโจมตี Sony หรือไม่ ทั้งนี้บางรายงานให้ความเห็นว่าการโจมตีน่าจะมาจากเกาหลีเหนือ แต่ทางเกาหลีเหนือก็ออกมาปฏิเสธ

ทางสำนักข่าว Bloomberg รายงานว่า เหตุการณ์การรั่วไหลของข้อมูลมีจุดเริ่มต้นจากโรงแรม St. Regis ในกรุงเทพฯ ซึ่งเป็นไปได้ว่าแฮกเกอร์อาจจะพักในโรงแรม หรือเจาะระบบเข้ามาใช้เครือข่ายของโรงแรมในการเผยแพร่ข้อมูลส่วนตัวของพนักงานของ Sony และดาราราวม 47,000 คน

นอกจากนี้เมื่อวันที่ 8 ธันวาคมที่ผ่านมา ได้เกิดปัญหาการเข้าถึง Playstation Store เป็นเวลาหลายชั่วโมงโดยมีข้อความปรากฏว่า “Page Not Found! It’s not you. It’s the Internet’s fault” ซึ่งยังไม่มีรายงานว่าสาเหตุมาจากอะไร

วันที่: 2014-12-09 | ที่มา: Bloomberg <http://thcert.co/wd1li7>

Adobe ปล่อยอัปเดตปิดช่องโหว่ใน Adobe Flash Player , Adobe Reader และ ColdFusion

เมื่อวันที่ 9 พฤศจิกายน ที่ผ่านมา Adobe ได้ออกอัปเดตเพื่อปิดช่องโหว่ใน Adobe Flash Player, Adobe Reader และ ColdFusion ซึ่งช่องโหว่ดังกล่าวอาจเปิดโอกาสให้แฮกเกอร์สามารถควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้ ผู้ใช้งานสามารถอัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่

วันที่: 2014-12-11 | ที่มา: Adobe <http://thcert.co/iGrPv2>

Microsoft

Microsoft ปล่อยอัปเดตปิดช่องโหว่ประจำเดือนของ Windows

เมื่อวันที่ 9 ธันวาคม ที่ผ่านมา Microsoft ประกาศผ่านเว็บไซต์อัปเดตปิดชุดช่องโหว่ประจำเดือนของส่วนประกอบต่าง ๆ ของ Windows โดยเป็นช่องโหว่สำคัญใน Internet Explorer (MS14-080), Microsoft Word และ Microsoft Office Web Apps (MS14-081) และ Microsoft Exchange (MS14-084) ซึ่งช่องโหว่เหล่านี้อาจเปิดโอกาสให้แฮกเกอร์สามารถควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้ ผู้ใช้งานสามารถอัปเดต Windows เป็นเวอร์ชันล่าสุดเพื่อปิดช่องโหว่

วันที่: 2014-12-11 | ที่มา: Microsoft <http://thcert.co/zS5hYA>

กลับมาอีกครั้ง ซอฟต์แวร์หรืออุปกรณ์ที่มีการใช้ TLS สามารถถูกโจมตีด้วยเทคนิค POODLE ได้เช่นกัน

US-CERT แจ้งเตือนถึงช่องโหว่ใน TLS ซึ่งอาจส่งผลให้อุปกรณ์หรือซอฟต์แวร์บางตัวที่มีการใช้ TLS ถูกโจมตีด้วยเทคนิค POODLE ได้ ทำให้แฮกเกอร์สามารถถอดรหัสลับข้อมูลที่มีการรับส่ง และพบว่าจากบริการตรวจสอบเว็บไซต์ของ Qualys (https://www.ssllabs.com/ssltest/index.html) พบว่าบางเว็บไซต์ อย่าง Bank of America ก็มีช่องโหว่นี้ ผู้ที่ใช้อุปกรณ์หรือซอฟต์แวร์ที่มีการใช้งาน TLS ควรติดตามข่าวสารเกี่ยวกับอัปเดตปิดช่องโหว่จากบริษัทเจ้าของอุปกรณ์หรือซอฟต์แวร์

วันที่: 2014-12-12 | ที่มา: US-CERT <http://thcert.co/ma33O6>

อัปเดตปิดช่องโหว่ใน Docker

เมื่อวันที่ 11 ธันวาคมที่ผ่านมา เว็บไซต์ทางการของ Docker ประกาศอัปเดตซอฟต์แวร์ Docker เวอร์ชัน 1.4 และ 1.3.3 เพื่อปิดช่องโหว่ซึ่งอาจเปิดโอกาสให้แฮกเกอร์สามารถควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้ ผู้ที่ใช้งาน Docker สามารถอัปเดตเป็นเวอร์ชันดังกล่าวได้แล้ว

วันที่: 2014-12-15 | ที่มา: Docker <http://thcert.co/9081l3>

ไมโครซอฟท์ออกแพตช์ KB3024777 แก้ไขปัญหาติดตั้งแพตช์ KB3004394 แล้ว ติดตั้งแพตช์อื่นไม่ได้

หลังจากที่ไมโครซอฟท์ได้ปล่อยแพตช์หมายเลข KB3004394 ผ่านระบบ Windows Update ไปเมื่อช่วงวันอังคารที่ผ่านมา ก็มีรายงานจากผู้ใช้หลายรายแจ้งว่า ระบบมีปัญหาหลังจากที่ติดตั้งแพตช์ดังกล่าว ตัวอย่างปัญหาที่พบ เช่น Windows Defender ทำงานไม่ได้ เปิด VirtualBox ไม่ได้ มีปัญหากับไดรเวอร์การ์ดจอ ของ AMD หรือผู้ใช้บางรายถึงขั้นเข้า Windows Update เพื่อติดตั้งแพตช์อื่นไม่ได้ โดยปัญหานี้มีผลกระทบกับผู้ที่ใช้งานระบบปฏิบัติการ Windows 7 และ Windows Server 2008 R2 ทั้งเวอร์ชัน 32 บิตและ 64 บิต ซึ่งต่อมาทางไมโครซอฟท์ได้ถอดแพตช์ KB3004394 ออกจากระบบ Windows Update พร้อมแจ้งให้ผู้ใช้ที่ติดตั้งแพตช์ดังกล่าวนี้ลงในเครื่องให้ลบออกไปก่อน

และเมื่อวันที่ 12 ธันวาคมที่ผ่านมา ทางไมโครซอฟท์ได้ปล่อยแพตช์หมายเลข KB3024777 เพื่อแก้ไขปัญหาที่เกิดจากแพตช์ KB3004394 โดยเฉพาะปัญหาที่ผู้ใช้ไม่สามารถเข้าใช้งาน Windows Update ได้หลังจากที่ติดตั้งแพตช์ดังกล่าว ผู้ใช้สามารถดาวน์โหลดแพตช์หมายเลข KB3024777 ได้จาก Windows Update และเว็บไซต์ของไมโครซอฟท์

วันที่: 2014-12-15 | ที่มา: Microsoft <http://thcert.co/ORvnWd>

Smartwatch เสี่ยง! ถูกขโมยข้อมูล

นักวิจัยด้านความมั่นคงปลอดภัยจากบริษัท Bitdefender ค้นพบช่องโหว่ในการรับส่งข้อมูลระหว่าง Smartwatch กับ Smartphone ซึ่งอาจส่งผลให้แฮกเกอร์สามารถขโมยข้อมูล เช่น ข้อความสนทนาใน Google Hangout หรือ Facebook โดยช่องโหว่นี้อยู่ที่การเชื่อมต่อระหว่างอุปกรณ์ด้วย Bluetooth ซึ่งใช้รหัสผ่านเพียง 6 หลัก เปิดโอกาสให้แฮกเกอร์สามารถโจมตีด้วยวิธีการสุ่มรหัสผ่านได้ (Brute Force Attack)

นอกจากนี้ทางบริษัทได้เผยแพร่คลิปที่มีการทดลองดักรับข้อความสนทนาจาก Google Hangout ที่ส่งจาก Google Nexus 4 ไปยัง Samsung Gear Live Smartwatch (https://www.youtube.com/watch?v=utVnrq5uCuM#t=117)

วันที่: 2014-12-16 | ที่มา: The Hacker News <http://thcert.co/LRa0yb>

แฮกเกอร์อ้าง ขโมยฐานข้อมูลประชาชนทั้งหมดของเซอร์เบีย

จากเว็บสำนักข่าวออนไลน์ Inserbia ได้รายงานข่าวเกี่ยวกับกลุ่มแฮกเกอร์ที่อ้างว่าได้ขโมยฐานข้อมูลประชาชนทั้งหมดของเซอร์เบีย ได้แก่ หมายเลขประจำตัวประชาชน ที่อยู่ ที่ทำงาน และหมายเลขโทรศัพท์ ซึ่งหากเป็นจริงก็ถือเป็นเรื่องที่มีผลกระทบสูง เพราะข้อมูลอาจถูกนำไปใช้ในการสวมรอยเพื่อหลอกลวงหรือก่ออาชญากรรมอื่น ๆ

กลุ่มแฮกเกอร์ยังได้อ้างหลักฐานการโจมตีด้วยภาพที่แสดงรายชื่อคนและที่อยู่

พร้อมทั้งระบุสาเหตุการโจมตีเนื่องจากไม่พอใจที่ตำรวจเอาแต่ตามล่ากลุ่มแฮกเกอร์เชื้อชาติเซอร์เบีย โดยไม่สนใจกลุ่มแฮกเกอร์เชื้อชาติแอลเบเนีย และต้องการแสดงให้เห็นถึงความไม่มั่นคงปลอดภัยของระบบที่ต้องได้รับการแก้ไข

ก่อนหน้านี้ระบบจัดการหมายเลขประจำตัวประชาชนของเกาหลีก็ถูกโจมตี ทำให้ข้อมูลของประชาชน 80% ของประชากรทั้งหมดถูกขโมย ส่งผลให้ต้องแก้ไขระบบ ซึ่งใช้เงินไปกว่า 650 ล้านดอลลาร์สหรัฐฯ

วันที่: 2014-12-17 | ที่มา: Inserbia <http://thcert.co/E7WBe9>

มัลแวร์แฝงมาในสมาร์ตโฟน Coolpad แอบสอดแนมและขโมยข้อมูลในเครื่อง

บริษัทด้านความมั่นคงปลอดภัย Palo Alto Networks ได้รายงานการค้นพบมัลแวร์ประเภท Backdoor ที่แฝงมากับในสมาร์ตโฟนสัญชาติจีน Coolpad ในรุ่นต่าง ๆ รวม 24 รุ่น โดยพบมัลแวร์ในเครื่องตั้งแต่ผลิตจากโรงงาน มัลแวร์นี้สามารถสอดแนมตำแหน่งที่อยู่ปัจจุบันจาก GPS, ขโมยข้อมูลต่าง ๆ เช่น ข้อมูลเกี่ยวกับแอปพลิเคชันที่ติดตั้ง ประวัติการโทรศัพท์หรือการรับส่ง SMS รวมถึงสามารถแอบติดตั้งแอปพลิเคชันอื่น

นี่ไม่ใช่ครั้งแรกที่มีการค้นพบว่ามือถือจีนมีมัลแวร์มาตั้งแต่โรงงาน ก่อนหน้านี้พบว่ามือถือยี่ห้อ Star N9500 มีโทรจันฝังมาด้วยเหมือนกัน ในขณะที่มือถือของค่าย Xiaomi ยังไม่เคยพบว่ามีมัลแวร์ฝังมา แต่ก็พบว่ามีการแอบส่งข้อมูลกลับไปเซิร์ฟเวอร์ในจีน (ปัจจุบันแก้ไขแล้ว)

วันที่: 2014-12-18 | ที่มา: The Hacker News <http://thcert.co/C68hKQ>

FBI ระบุ เกาหลีเหนือแฮก Sony

FBI ได้ออกมาแถลงข้อมูลเกี่ยวกับกรณีสืบสวนการโจมตีบริษัท Sony Picture Entertainment ที่มีการขโมยและเผยแพร่ข้อมูลส่วนบุคคลของพนักงานและดารา รวมถึงหนังใหม่ที่ยังไม่เข้าโรงทางอินเทอร์เน็ต โดยทาง FBI ได้ระบุว่าเป็นฝีมือของรัฐบาลเกาหลีเหนือ เนื่องจาก

1. มัลแวร์ที่ใช้ในการโจมตีมีส่วนที่คล้ายคลึงกับมัลแวร์ที่ทางเกาหลีเหนือสร้าง

2. ในมัลแวร์ที่ใช้ในการโจมตีมีข้อมูลหมายเลขไอพี ซึ่งพบว่ามีการสื่อสารระหว่างหมายเลขไอพีนี้กับหมายเลขไอพีที่ถูกใช้งานโดยองค์กรในเกาหลีเหนือ

3. เครื่องมือที่ใช้การโจมตีมีส่วนคล้ายคลึงกับการโจมตีธนาคารและบริษัทสื่อเกาหลีใต้เมื่อเดือนมีนาคมปีที่แล้ว ซึ่งส่งผลให้ ATM ของหลายธนาคารใช้การไม่ได้เป็นช่วงระยะเวลาหนึ่ง

การระบุที่มาของการโจมตีในครั้งนี้สอดคล้องการคาดการณ์ว่าสาเหตุมาจากความไม่พอใจในหนังของ Sony เรื่อง The Interview ซึ่งเป็นหนังตลกมีเนื้อเรื่องของการสังหารผู้นำเกาหลีเหนือ โดยข่าวของ CNN ระบุว่าแฮกเกอร์ได้ส่งอีเมลไปยัง Sony

ชมเชยการหยุดการฉายหนังเรื่อง The Interview รวมถึงเรียกร้องให้หยุดเผยแพร่หนัง ในรูปแบบ DVD ด้วย

วันที่: 2014-12-22 | ที่มา: FBI <http://thcert.co/6VQQRA>

อัปเดตปิดช่องโหว่ใน NTPD

ทีมด้านความมั่นคงปลอดภัยของ Google ค้นพบชุดช่องโหว่ใน NTPD ซึ่งเป็นซอฟต์แวร์ที่ใช้ในการตั้งค่าเวลาของเครื่องให้ตรงตามมาตรฐานสากล โดยพบช่องโหว่ในรุ่น 4.2.7 และรุ่นก่อนหน้า ซึ่งอาจส่งผลให้แฮกเกอร์สามารถสั่งประมวลผลคำสั่งอันตรายบนเครื่องที่มีช่องโหว่จากระยะไกลได้ (Remote Code Execution)

ผู้ใช้งานสามารถอัปเดตเป็นรุ่น 4.2.8 เพื่อปิดช่องโหว่ดังกล่าว โดยสามารถดาวน์โหลดอัปเดตได้ที่ http://www.ntp.org/downloads.html

วันที่: 2014-12-23 | ที่มา: ICS-CERT <http://thcert.co/bT76XX>

พบช่องโหว่ Misfortune Cookie ในเราเตอร์กว่า 12 ล้านเครื่อง

นักวิจัยจากบริษัทด้านความมั่นคงปลอดภัย Check Point ค้นพบช่องโหว่ชื่อ Misfortune Cookie ในเราเตอร์ยี่ห้อต่าง ๆ เช่น D-Link, Edimax, Huawei, TP-Link, ZTE และ ZyXEL ซึ่งส่งผลให้แฮกเกอร์สามารถควบคุมเราเตอร์ และสามารถสอดแนมข้อมูลการใช้งานอินเทอร์เน็ตที่รับส่งผ่านเราเตอร์นั้นได้

ช่องโหว่นี้อยู่ในส่วนประกอบของเราเตอร์ที่เรียกว่า RomPager ซึ่งเป็น Web Server ทำหน้าที่ให้บริการหน้าเว็บสำหรับตั้งค่าต่าง ๆ ของเราเตอร์

ทั้งนี้ทาง Check Point ระบุว่าพบช่องโหว่ในอุปกรณ์ประมาณ 12 ล้านเครื่อง และระบุรายการยี่ห้อและ Model ที่เป็นไปได้ว่ามีช่องโหว่ดังกล่าว แต่ไม่ได้ระบุว่าเป็น Firmware รุ่นไหน โดยผู้ที่สนใจสามารถดูรายละเอียดได้ที่ http://mis.fortunecook.ie/misfortune-cookie-suspected-vulnerable.pdf

วันที่: 2014-12-23 | ที่มา: Misfortune Cookie <http://thcert.co/dQ87Xn>

เป็นเรื่อง! ข้อมูลของโรงงานนิวเคลียร์เกาหลีใต้รั่วไหล

แฮกเกอร์ได้ใช้ Twitter ภายใต้ชื่อ “president of anti-nuclear reactor group” เผยแพร่แบบแปลนและคู่มือของเครื่องปฏิกรณ์นิวเคลียร์ชื่อ Gori-2 และ Wolsong-1 รวมถึงแผนที่ชั้นต่าง ๆ ของโรงงานนิวเคลียร์ที่ดำเนินงานโดยบริษัท Korea Hydro and Nuclear Power Co. (KHNP)

อย่างไรก็ตามทาง KHNP ชี้แจงว่าข้อมูลที่รั่วไหลไม่ได้เกี่ยวข้องเทคโนโลยีหลักและไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยของเครื่องปฏิกรณ์นิวเคลียร์ ทั้งนี้แฮกเกอร์ได้กล่าวข่มขู่ว่าหากไม่ทำการปิดเครื่องปฏิกรณ์นิวเคลียร์จะเผยแพร่ข้อมูลทั้งหมดที่มีและทำการโจมตีอีกครั้ง

วันที่: 2014-12-26 | ที่มา: Yonhaps News Agency <http://thcert.co/xJ49Cn>

Apple ปล่อยอัปเดตปิดชุดช่องโหว่สำหรับ OS X

Apple ได้ปล่อยอัปเดตปิดชุดช่องโหว่ในส่วนประกอบ Network Time Protocol Daemon บนระบบปฏิบัติการ OS X Mountain Lion, Mavericks และ Yosemite แฮกเกอร์อาจสามารถโจมตีผ่านช่องโหว่ดังกล่าวเพื่อควบคุมเครื่องคอมพิวเตอร์ของเหยื่อจากระยะไกล ผู้ใช้งานสามารถปิดช่องโหว่โดยการอัปเดต OS X เป็นเวอร์ชันล่าสุด (OS X Mountain Lion v. 10.8.5, OS X Mavericks v. 10.9.5, OS X Yosemite v. 10.10.1)

วันที่: 2014-12-26 | ที่มา: Apple <http://thcert.co/Bc6XtW>

ระวัง! แฮกเกอร์ใช้ข่าวเครื่องบินสูญหาย หลอกผู้ใช้เข้าเว็บอันตรายเพื่อขโมยข้อมูล

เว็บไซต์ The Hacker News รายงานว่าพบการโจมตีด้วยการหลอกลวงผ่านโซเชียลมีเดียด้วยการโพสต์ข่าวการสูญหายของเครื่องบิน QZ 8501 ผ่านข้อความ “Missing AirAsia flight QZ850 has been found and that all its passengers are safe and alive” เพื่อให้คลิกเข้าเว็บไซต์ที่แฮกเกอร์เตรียมไว้ ซึ่งอาจมีจุดประสงค์เพื่อขโมยข้อมูลหรือเผยแพร่มัลแวร์ ผู้ใช้งานควรระมัดระวังในการคลิกลิงก์เกี่ยวกับข่าวดังกล่าวบนโซเชียลมีเดีย หากมี popup หรือพาไปยังหน้าเว็บไซต์ล็อกอิน หรือกรอกข้อมูลส่วนตัว ก็เป็นไปได้ว่าเป็นการหลอกลวง

วันที่: 2014-12-30 | ที่มา: The Hacker News <http://thcert.co/yY2Hai>

บทความ

บทความ CYBER THREATS 2014

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

ETDA สพธอ www.etda.or.th

Ministry of ICT Smart Thailand

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 21 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพมหานคร 10310

เว็บไซต์ไทยเซิร์ต www.thaicert.or.th
เว็บไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) www.etda.or.th
เว็บไซต์กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร www.mict.go.th

ISBN 978-616-7956-03-9