




Security Trends 2017 By ActiveMedia (Thailand)



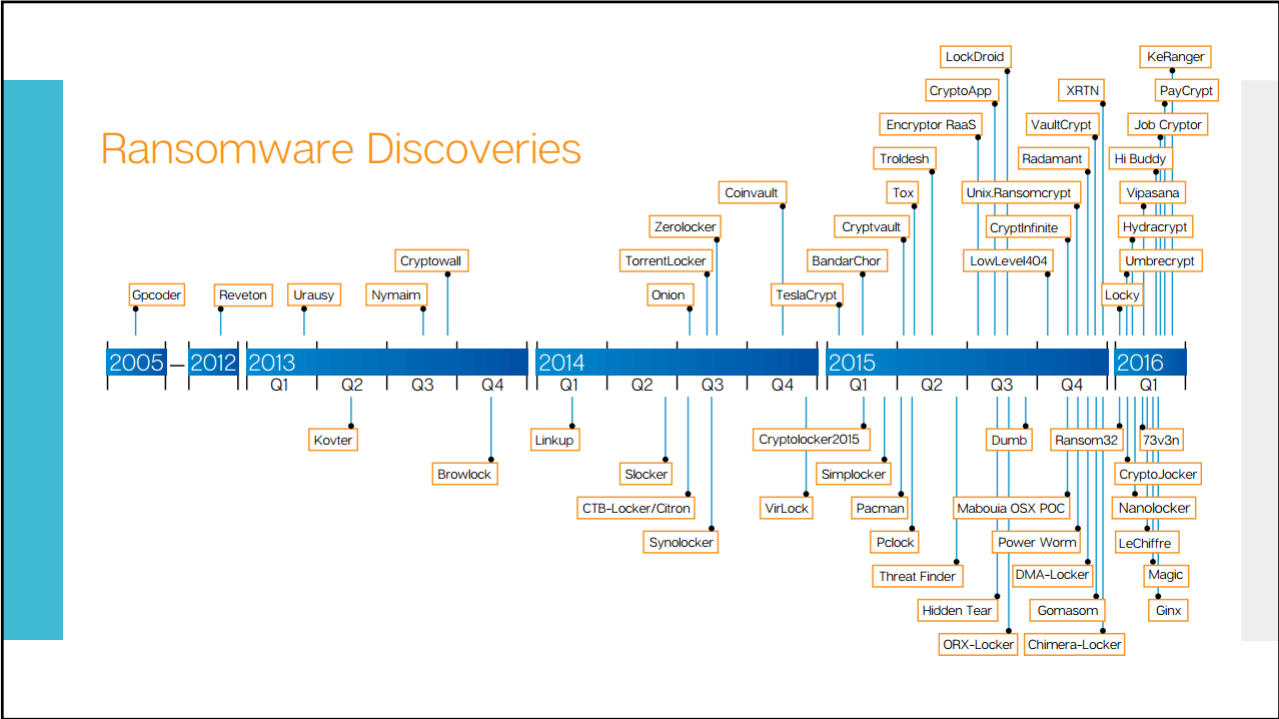
- Ransomware Knowledge
- Ransomware of Things (RoT)
- Security education and social responsibility
- Mobile Security
- Vulnerability
- Healthcare challenges
- Gaming platforms

Ransomware Knowledge



- ❖ พยายามแพร่กระจายผ่านเว็บไซต์ต่าง ๆ, แนบไฟล์ไปใน email
- ❖ สร้าง service และฝังการทำงานของ service ไปยัง Registry ของเครื่อง เพื่อให้ทำงานทุกครั้งเมื่อมีการเปิดเครื่อง
- ❖ ติดต่อกลับไปยังเครื่อง C&C Server(Command and Control Server) ของ Hacker เพื่อ download key สำหรับการเข้ารหัสและ config ต่าง ๆ ของภายใน Ransomware พร้อมทั้งลงทะเบียนกับ C&C Server เพื่อระบุว่าเครื่องที่ติดอยู่ที่ใด
- ❖ นำ Key และ config ที่ได้รับจาก C&C Server มาเข้ารหัสเอกสารข้อมูลต่าง ๆ ภายในเครื่อง
- ❖ แสดงหน้าข่มขู่ผู้ใช้งานพร้อมกับบอก link สำหรับวิธีการโอน Bitcoin ไปให้กับ Hacker





คำถามที่พบบ่อย ๆ

- ถ้าเราขโมยไวรัสได้แล้วไฟล์เราจะกลับมาได้หรือเปล่า?
- มี Anti-Virus อยู่ในเครื่องแล้วมันไม่ช่วยเลยหรือ?
- เราจะป้องกันตัวจากแรนซัมแวร์ได้อย่างไร?

ข้อเสนอแนะในการป้องกันความเสียหายจากภัย Ransomware

<p>ดำเนินการทันทีเพื่อรักษาความพร้อมใช้งานของข้อมูล</p>	 <p>สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ</p>	 <p>ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ</p>
<p>สร้างความตระหนักในการใช้อีเมลและเปิดเว็บไซต์</p>	 <p>ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย</p>	 <p>ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น</p>
<p>ในกรณีที่เกิดเป็นเหยื่อ</p>	 <p>ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่</p>	 <p>ให้ติดต่อกับเจ้าหน้าที่ IT ของหน่วยงานในทันที</p>

 [etda.thailand](https://www.facebook.com/etda.thailand)
 [ThaiCERT](https://twitter.com/ThaiCERT)
 thaicert.or.th



ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA



ETDA
RWSG
www.etda.or.th



ICT
Smart Thailand

Ransomware of Things (RoT)

แนวโน้มของ Internet of Things



IBM model for the Internet of Things

The diagram illustrates a funnel-shaped model with five layers:

- Things:** Includes icons for a TV, car, factory, power grid, and heart. Description: "Things" can be remotely controlled or viewed, and they can send telemetry for analysis.
- Local network:** Includes icons for a house, car, and factory. Description: This may be a controller area network (CAN) in connected cars, a local network in homes, etc.
- Global network:** Includes a globe icon. Description: Most "things" connect to the Internet, except for power grids or classified government systems.
- Cloud service:** Includes a cloud icon. Description: Cloud services provide the repository and access control between the "thing" and its controller.
- Controlling device:** Includes a smartphone icon. Description: Smartphones, tablets and other smart devices can control all types of "things."

Graphic 1. IBM model for the Internet of Things
Source: IBM X-Force® Research and Development

Internet of Thing

ในยุคหลังปี 2000 โลกมีอุปกรณ์อิเล็กทรอนิกส์ออกมาเป็นจำนวนมากและมีการใช้คำว่า Smart ซึ่งในที่นี้คือ smart device, smart grid, smart home, smart network, smart intelligent transportation

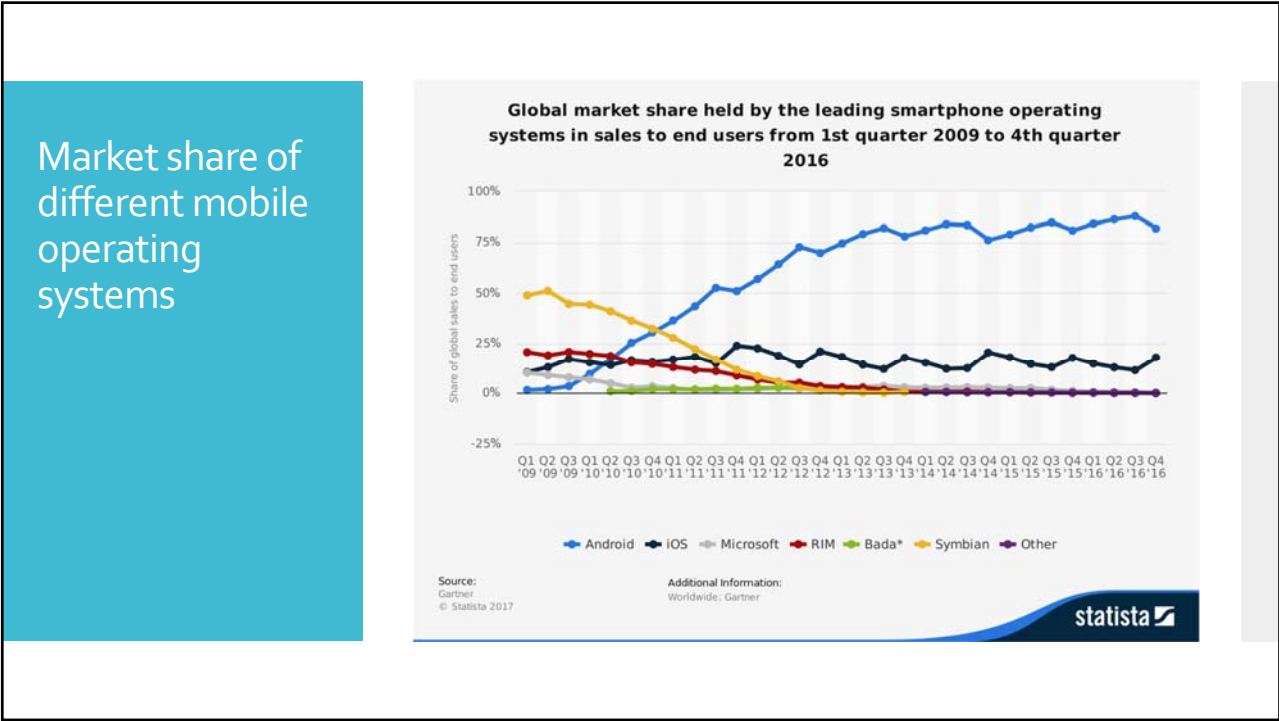
สิ่งต่าง ๆ เหล่านี้ล้วนมีโครงสร้างพื้นฐานที่สามารถเชื่อมต่อกับโลกอินเทอร์เน็ตได้ ซึ่งการเชื่อมต่อเหล่านั้นเองก็เลยมาเป็นแนวคิดที่ว่าอุปกรณ์เหล่านั้นก็ย่อมสามารถสื่อสารกันได้ด้วยเช่นกันโดยอาศัยตัว Sensor ในการสื่อสารถึงกัน

Security education and social responsibility

การเรียนรู้เกี่ยวกับการรักษาความปลอดภัยและความรับผิดชอบต่อสังคม

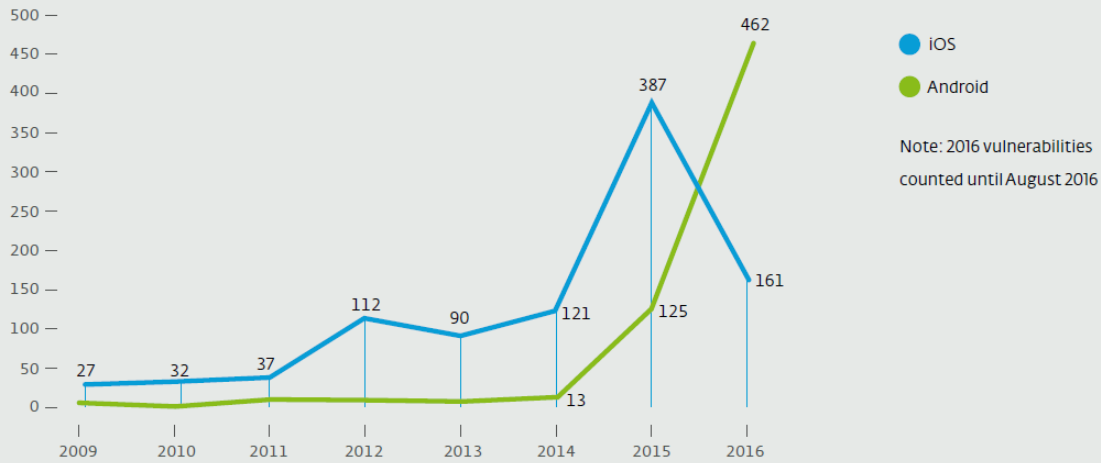


Mobile Security



Market share of different mobile operating systems

Annual number of vulnerabilities in Android and iOS since 2009



PHISHING GEAR: WHAT'S IN A PHISHING ATTACK?

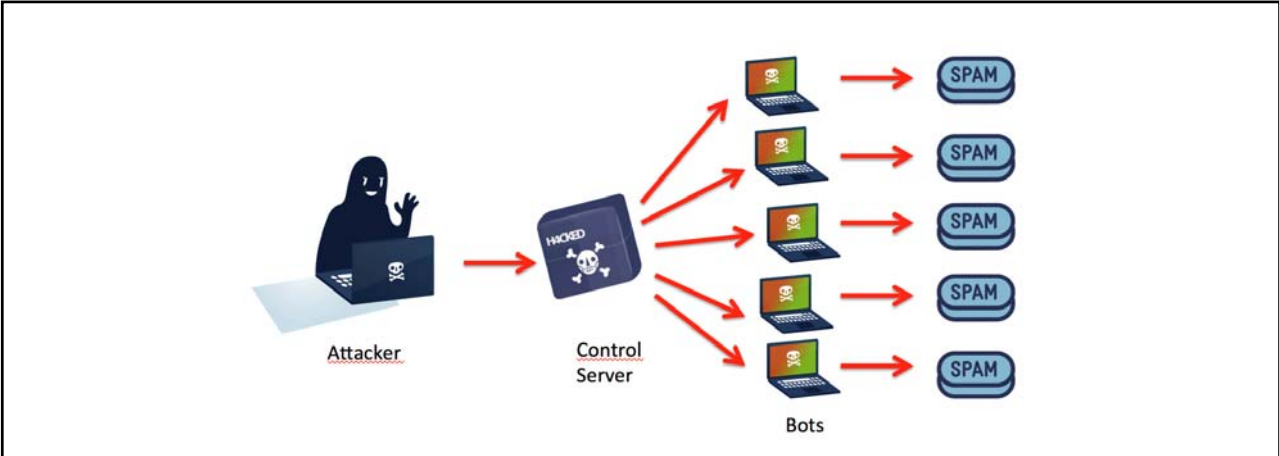


Mobile Phishing

และการเรียกค่าไถ่

- Social Engineering ผ่านแอปพลิเคชันบนมือถือและ SMS
- หลอกผู้ใช้งานให้ทำตามความต้องการของตน
- ส่งผลให้ระบบเครือข่ายรวมทั้ง PC ของผู้ใช้งานต้องติดมัลแวร์ไปด้วยเช่นกัน
- ไม่สามารถเปิดไฟล์งานได้ จนกว่าจะจ่ายเงิน

รูปประกอบจาก The Guardian | <http://www.theguardian.com/media-network/media-network-blog/2013/jul/12/cyber-threats-trends-spear-phishing>



ใช้ช่องโหว่ของอุปกรณ์ **Mobile** ในการโจมตีอุปกรณ์ใกล้เคียง

Vulnerability

ช่องโหว่ ถือเป็นช่องทางหลักของแฮกเกอร์ที่จะใช้แทรกซึมเข้ามาในระบบ

แต่ข่าวดีก็คือเหตุการณ์โจมตีช่องโหว่เริ่มลดลง อาจจะเป็นเพราะคนเข้าใจเทคโนโลยีมากขึ้น และผู้ผลิตมีมาตรการในการรับมือได้ดียิ่งขึ้น





Healthcare challenges

สถานพยาบาลกำลังตกเป็นเป้าหมายในการโจมตี



Gaming platforms

ในขณะที่แทบทุกสิ่งจะถูกย้ายขึ้นมาทำบนโทรศัพท์มือถือ เกมส์ก็เช่นเดียวกัน หลายคนถึงจอขนาดยักษ์และจอยสติค มานั่งเล่นเกมสบนโทรศัพท์มือถือแทน

ด้วยเหตุผลของความสะดวกสบายในการพกพาและสามารถเล่นได้ในทุก ๆ ที่



