คณิตศาสตร์และคอมพิวเตอร์ในชีวิตประจำวัน

Cyber Security
ความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์

1. อะไรคือความมั่นคงปลอดภัยไซเบอร์
2. การคุกคามทางไซเบอร์
3. มัลแวร์
4. การโจมตีเครือข่าย
5. ความมั่นคงปลอดภัยไซเบอร์สำหรับบุคคลทั่วไป

1. อะไรคือความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) **คือ**

- **กระบวนการ**หรือมาตรการ ที่ทำให้คนหรือองค์กร**ปราศจากความเสี่ยง**ที่มีผลต่อความปลอดภัยของข้อมูล รวมถึง
- **การระวังป้องกัน**ต่ออาชญากรรม การโจมตี การทำลาย และการจารกรรม โดย
- คำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูลเป็นหลักหรือ CIA 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

หน่วยงานในไทย

- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)
- ศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (G-CERT)

ประเภทภัยคุกคามทางไซเบอร์ (แบ่งโดย ThaiCERT)

1. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)
2. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)
3. **การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)**
4. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)
5. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)
6. **ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)**
7. **การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)**
8. โปรแกรมไม่พึงประสงค์ (Malicious Code)
9. ภัยคุกคามอื่นๆ (Other)

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	0	1	0	0	0	0	0	0	0	0	**1**
Availability	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Fraud	78	73	84	60	82	84	86	87	61	94	66	74	**929**
Information gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information security	0	2	1	2	1	0	0	5	0	2	2	3	**18**
Intrusion Attempts	74	100	59	57	64	103	111	114	100	76	126	118	**1102**
Intrusions	56	43	33	48	25	19	30	16	32	15	15	3	**335**
Malicious code	13	8	12	3	19	10	14	7	11	4	15	11	**127**
Other	0	0	0	0	0	1	0	6	0	1	0	0	**8**
รวม	**221**	**226**	**189**	**171**	**191**	**217**	**241**	**235**	**204**	**192**	**224**	**209**	**2520**

ตารางแสดงตัวอย่างภัยคุกคามทางไซเบอร์ในประเทศไทย (2561)

https://www.thaicert.or.th/statistics/statistics.html

2. การคุกคามทางไซเบอร์

การคุกคามทางไซเบอร์ (Cyber Security)

- **ภัยคุกคาม/ผู้โจมตี** (Threat) :
  - **คือ** อันตรายที่เป็นไปได้ต่อทรัพย์สิน (ข้อมูลหรือเครือข่าย)
- **ช่องโหว่/ความอ่อนแอ** (Vulnerability) :
  - **คือ** ส่วนที่ผู้บุกรุกสามารถเข้าไปยังระบบและสามารถขโมย หรือทำลายข้อมูลได้ เช่น ระบบปฏิบัติการ (OS) ไม่มีการติดตั้ง Anti virus หรือ การอัปเดต Security Patches
  - **มีสาเหตุจาก** ระบบ/ซอฟต์แวร์ ถูกออกแบบมาไม่ดีพอต่อการโจมตีของภัยคุกคาม
- **การโจมตี** (Exploit)
  - **คือ** กลไกที่ประสงค์ร้ายต่อทรัพย์สินโดยใช้ช่องโหว่ของระบบที่มีอยู่
  - **แบ่งเป็น** (1) การโจมตีทางไกล (Remote) เช่น การโจมตีผ่านเครือข่ายอินเทอร์เน็ต และ (2) การโจมตีท้องถิ่น (Local) เช่น การโจมตีคอมพิวเตอร์โดยตรง (ไวรัสที่ติดมากับ Trump drive)
- **ความเสี่ยง** (Risk) :
  - **คือ** ความเป็นไปได้ที่ภัยคุกคามจะโจมตีระบบผ่านทางช่องโหว่ของระบบ

ผู้คุกคามและแฮกเกอร์

1. แฮกเกอร์ (Hacker) แบ่งเป็น :

- **แฮกเกอร์หมวกขาว** (White Hat Hackers)
  - ใช้เครื่องมือ/ความสามารถ ในการตรวจหาช่องโหว่ของระบบต่างๆ
  - เมื่อตรวจเจอจะ**ทำการแก้ไขหรือแจ้งไปยังผู้เกี่ยวข้อง** โดยจะไม่นำช่องโหว่นั้นไปใช้ประโยชน์
- **แฮกเกอร์หมวกเทา** (Grey Hat Hackers)
  - ใช้เครื่องมือ หรือ ความสามารถ ในการตรวจหาช่องโหว่ของระบบต่างๆ
  - เมื่อตรวจเจอจะ**แจ้งไปยังผู้เกี่ยวข้อง หรือนำช่องโหว่นั้นไปใช้ประโยชน์หรือไม่ก็ได้**
- **แฮกเกอร์หมวกดำ** (Black Hat Hackers)
  - ใช้เครื่องมือ หรือ ความสามารถ ในการตรวจหาช่องโหว่ของระบบต่าง ๆ
  - เมื่อตรวจเจอจะนำช่องโหว่นั้นไป**โจมตีหรือทำการคุกคามเพื่อผลประโยชน์ของตัวเอง**

2. ผู้คุกคาม (Threat Actors) :

ผู้คุกคาม **คือ** Grey **หรือ** Black hat hackers.

3. มัลแวร์

ของมัลแวร์ (Malware)

- คำว่า “มัลแวร์” มาจาก มาลิเชียสซอฟต์แวร์ (Malicious Software)
- มัลแวร์ คือ ซอฟแวร์หรือโคดโปรแกรมที่มีจุดประสงค์ร้ายต่อระบบคอมพิวเตอร์
- มัลแวร์ออกแบบมาตามจุดประสงค์ต่างกัน เช่น สร้างความเสียหาย หยุดการทำงาน ขโมย และแฝงตัว ฯลฯ
- ตัวอย่างมัลแวร์ เช่น ไวรัส (Virus), เวอร์ม (Worm), โทรจัน (Trojan) ฯลฯ

ประเภทของมัลแวร์

- ไวรัส (Virus) : มุ่งทำลายข้อมูลหรือระบบคอมพิวเตอร์
- เวอร์ม (Worms) : แพร่กระจายด้วยตัวเองได้
- ม้าโทรจัน (Trojan Horses) : เปิดช่องโหว่ให้ผู้บุกรุกอื่นเข้ามา
- สปายแวร์ (Spyware) : สอดแนมข้อมูลที่สำคัญแล้วขโมย
- แอดแวร์ (Adware) : โฆษณารบกวน
- แรนซัมแวร์ (Ransomware) : เข้ารหัสข้อมูลแล้วเรียกค่าไถ่เพื่อถอดรหัสข้อมูล

ไวรัส (Virus)

- **มุ่งการทำลาย**ข้อมูลหรือระบบคอมพิวเตอร์
- **ไม่สามารถอยู่ได้ด้วยตัวเอง** ต้องแฝงตัวอยู่ในไฟล์หรือซอฟต์แวร์อื่น
- **ต้องการพาหะ** (ไฟล์หรือซอฟต์แวร์) ในการแพร่กระจาย ส่วนใหญ่ผู้ใช้งานระบบคอมฯ จะเป็นผู้นำพาเข้ามา ผ่านช่องทาง เช่น Flash Drive, e-mail ฯลฯ

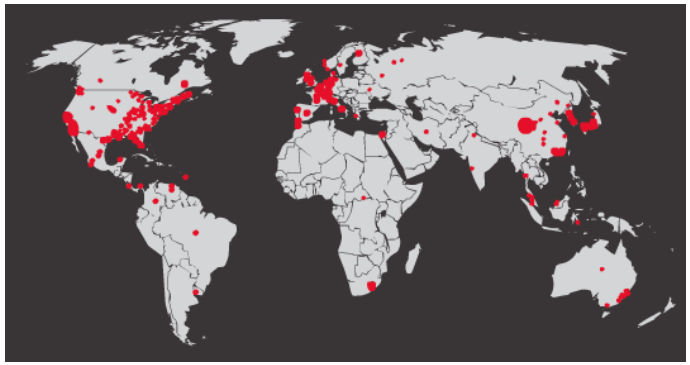
อาการของเครื่องที่ติดไวรัส

- ใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
- เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
- เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้อยู่
- แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ ๆ ก็หายไป
- เครื่องทำงานช้าลง
- เครื่องบูตตัวเองโดยไม่ได้สั่ง
- ระบบหยุดทำงานโดยไม่ทราบสาเหตุ
- อื่นๆ

เวอร์ม (Worms)

- มุ่งทำลายข้อมูลและระบบคอมพิวเตอร์ โดยเฉพาะระบบเครือข่าย
- **สามารถแพร่กระจายด้วยตัวเอง** (ไม่อาศัยพาหะ) ไปยังระบบคอมพิวเตอร์อื่น ๆ ในเครือข่ายเดียวกันได้

Initial Code Red Worm Infection – 658 servers



Code Red Worm Infection– 19 Hours Later
300,000 servers

ม้าโทรจัน (Trojan Horses)

- **มุ่งในการเปิดช่องโหว่**ให้มัลแวร์ชนิดอื่นหรือผู้ที่มุ่งร้าย เข้ามาในระบบคอมพิวเตอร์
- **มุ่งในการลักลอบขโมย**รหัสผ่านและข้อมูลส่วนบุคคล ขโมยข้อมูลธนาคาร เปิดเผยข้อมูลความลับ ฯลฯ
- ส่วนใหญ่ติดมาจากการใช้งานที่เกี่ยวกับอินเทอร์เน็ต เช่น การเข้าเว็บไซต์ที่อันตราย การโหลดเกมส์หรือซอฟแวร์เถื่อน ฯลฯ
- แทรกตัวเข้าไปในคอมพิวเตอร์ โดยการปลอมแปลงตัวเองให้เหมือนกับไฟล์หรือโปรแกรมที่เคยใช้งานในชีวิตประจำวัน

สปายแวร์ (Spyware)

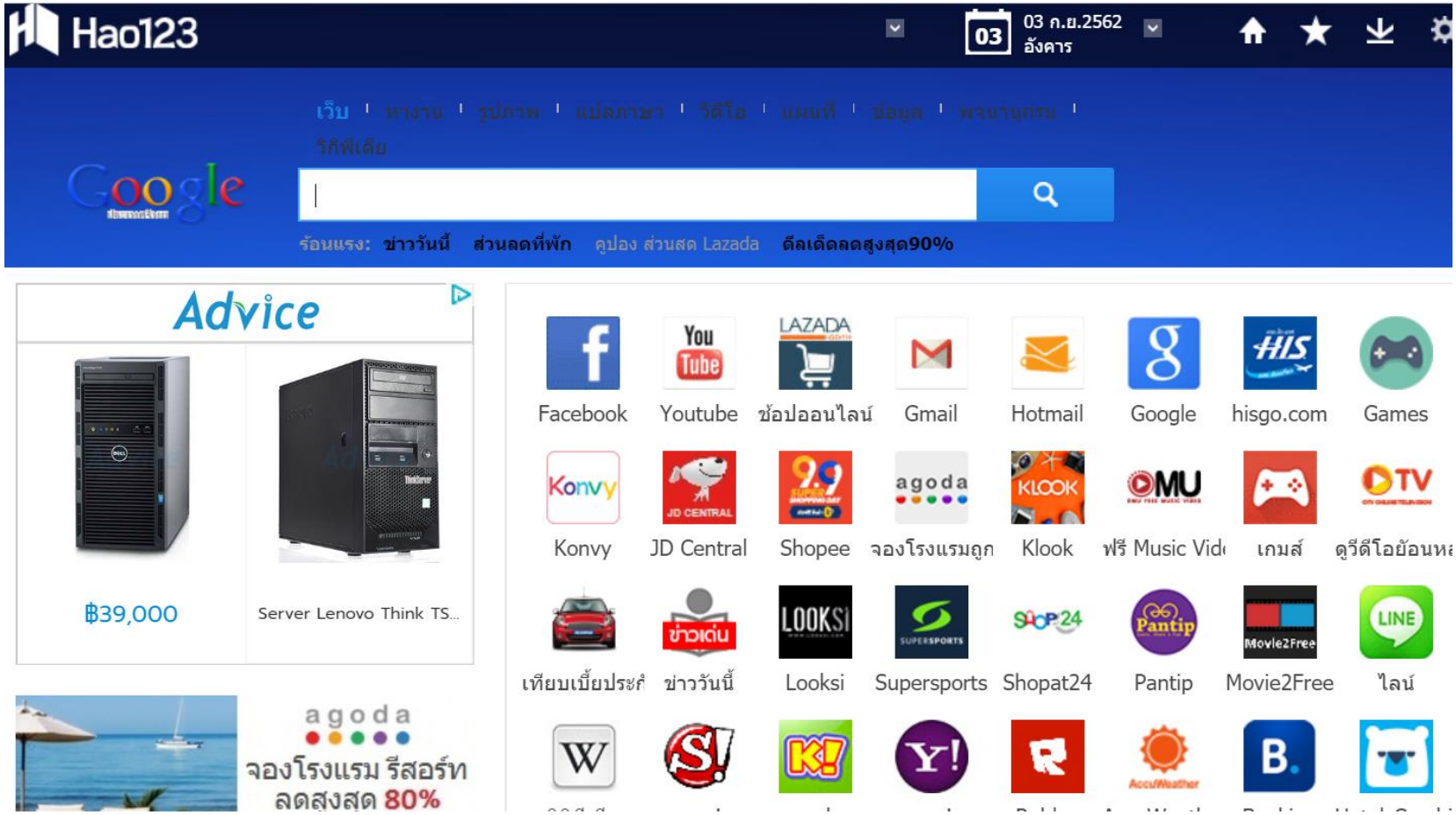
เป็นมัลแวร์ที่ใช้ในการ**สอดส่องและเก็บข้อมูลการใช้งาน**ของผู้ใช้ เช่น ข้อมูลส่วนตัว ที่อยู่ เบอร์โทร Email รวมถึงข้อมูลสำคัญ เช่น รหัสผ่านหรือข้อมูลบัตรเครดิต เป็นต้น

แอดแวร์ (Adware)

มุ่งในการโฆษณาเป็นหลัก เมื่อเครื่องคอมพิวเตอร์ติดแล้วจะมีอาการดังนี้

- หน้าแรกของ Web Browser จะถูกแก้ไขเป็นหน้าโฆษนา
- ขณะท่องอินเทอร์เน็ต ก็จะพบ Pop-Up หน้าโฆษนา เช่น โฆษนา Baidu, hao123

http://th.hao123.com/



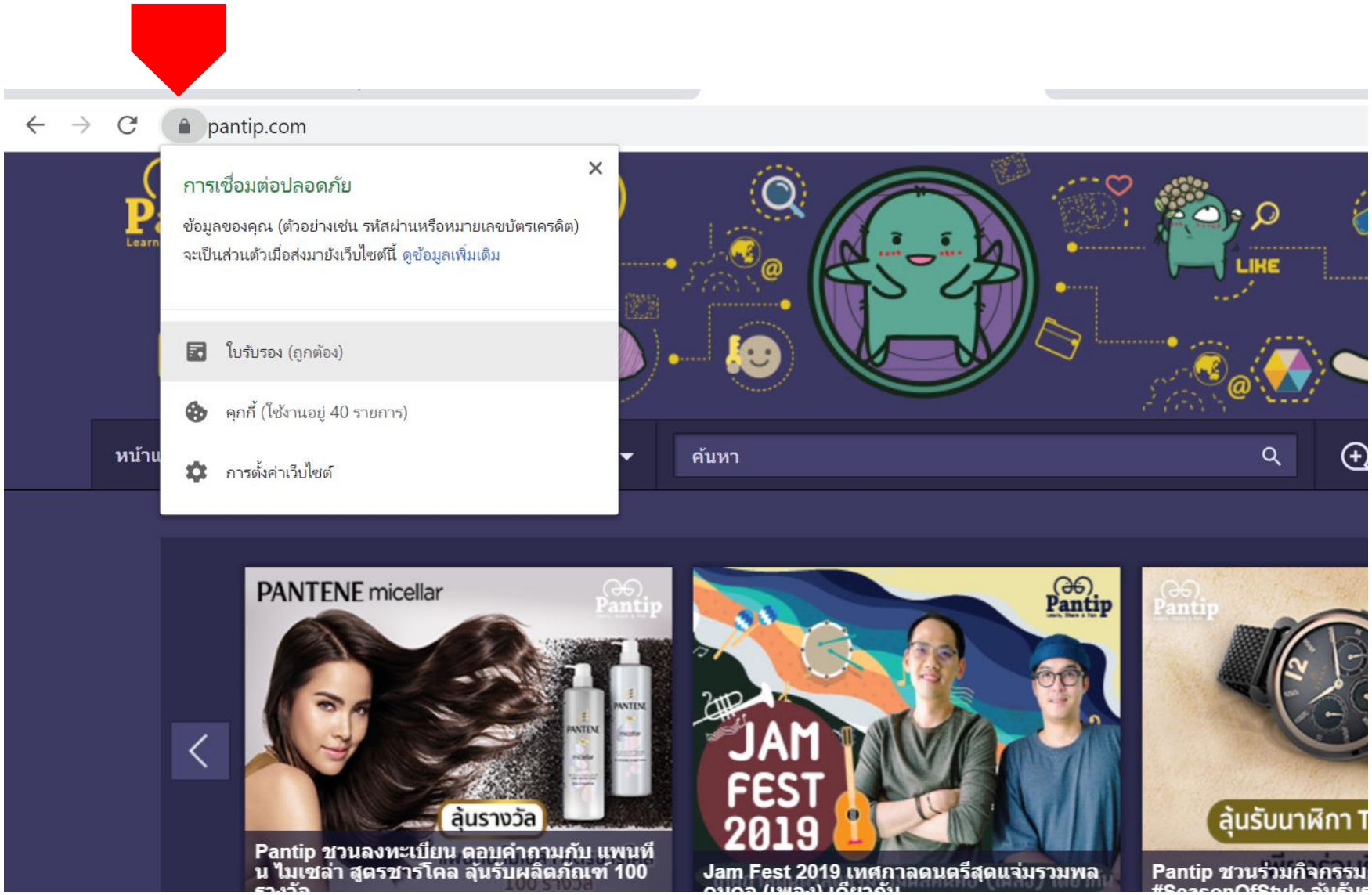
แรนซัมแวร์ (Ransomware)

- **มุ่งทำการเข้ารหัสข้อมูลและเรียกค่าไถ่**
- ทำให้ผู้ใช้ไม่สามารถใช้งานไฟล์ที่สำคัญได้ หรือไม่สามารถใช้งานโปรแกรมได้
- ถ้าหากอยากถอดรหัสไฟล์นั้น ๆ ให้กลับมาเหมือนเดิม ต้องจ่ายเงินให้กับแฮคเกอร์เพื่อทำการถอดรหัส

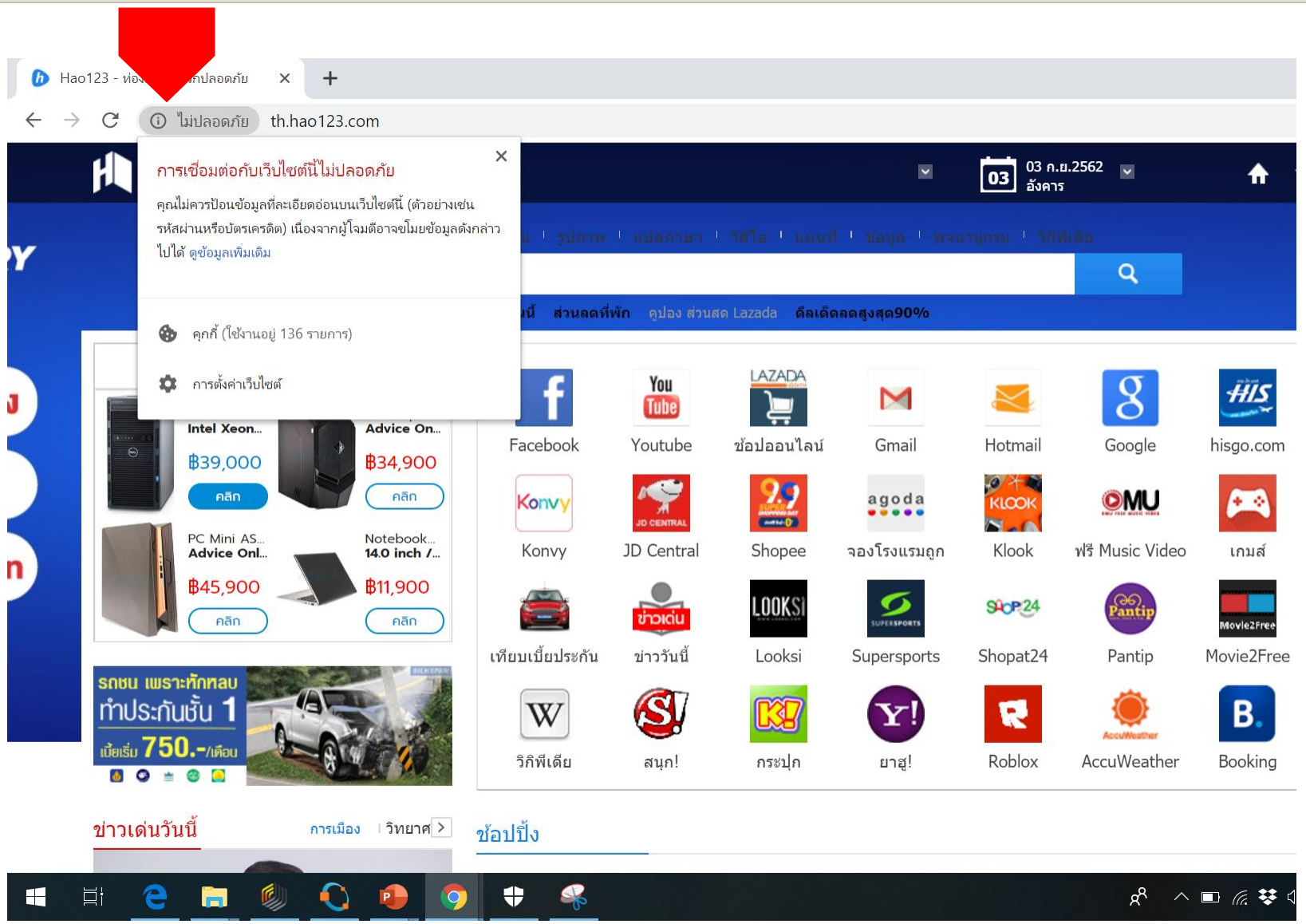
- WannaCry หรือ WannaCrypt เป็นข่าวโด่งดังไปทั่วโลกมีระบบคอมพิวเตอร์โดนโจมตีและเรียกค่าไถ่เป็นจำนวนมาก
- เกิดจากช่องโหว่ของ Windows รุ่นเก่าที่ไม่อับเดทมานาน

แนวทางป้องกันมัลแวร์

- อัปเดต Antivirus อยู่เสมอ ๆ
- อัปเดตระบบปฏิบัติการ (OS) อยู่เสมอ ๆ
- **ไม่**ติดตั้งซอฟต์แวร์เถื่อน
- **ไม่**เปิดอ่านอีเมลหรือดาวน์โหลดไฟล์จากอีเมลของคนที่ไม่รู้จัก
- **ไม่**นำ Trump Drive เข้าสู่เครื่องคอมฯ หากยังไม่ทำการ Scan Trump Drive หรือไม่แน่ใจว่า Trump Drive มีมัลแวร์หรือไม่
- **ไม่**เข้าเว็บไซต์ที่มีความน่าเชื่อถือ (สังเกตรูปแม่กุญแจตรงช่อง URL ของ Web Browser)



รูปแสดงตัวอย่างของเว็บที่น่าจะปลอดภัย



รูปแสดงตัวอย่างของเว็บที่อาจจะไม่ปลอดภัย

4. การโจมตีเครือข่าย

การโจมตีเครือข่าย (Network Attacks) แบ่งออกเป็น 3 ประเภท

1. การโจมตีแบบลาดตระเวณ (Reconnaissance Attacks)
2. ความพยายามเข้าใช้ระบบ (Access Attacks)
3. การทำให้ระบบไม่สามารถใช้การได้ (Deny of Service Attacks)

1. การโจมตีแบบลาดตระเวณ (Reconnaissance Attacks)

- **เป็นการค้นหา (Scan) ช่องโหว่**ของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ ที่ไม่มีระบบรักษาความปลอดภัยที่ดี แล้ว
- **เก็บรวบรวมข้อมูลของช่องโหว่**นั้นไว้ จากนั้นจะ
- **กลับมาทำการโจมตีผ่านทางช่องโหว่นั้น** ด้วยกระบวนการ Access Attack หรือ DOS Attack

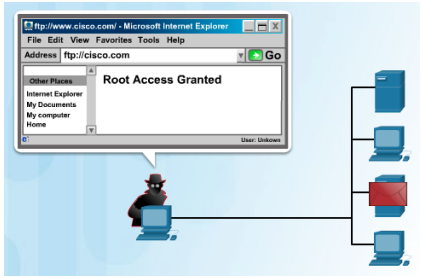
2. ความพยายามเข้าใช้ระบบ (Access Attacks)

เป็นความพยายามเข้าถึงเครือข่ายหรือระบบคอมพิวเตอร์ที่ต้องการโดย**ไม่ได้รับอนุญาต**โดยสามารถเข้าถึงได้สองแบบหลัก ๆ คือ

(1) **ผ่านทางช่องโหว่**ของระบบคอมพิวเตอร์ เช่น ระบบปฏิบัติการ (OS) ที่ไม่มีการอัปเดท หรือ Web Browser รุ่นเก่า

(2) **ผ่านการหลอกลวง** เพื่อให้ได้ Password ในการเข้าถึงระบบคอมพิวเตอร์ ซึ่งเป็นวิธีที่นิยมมากในปัจจุบัน

- เมื่อเข้าถึงได้แล้วจะค้นหาและขโมยข้อมูลออกไป
- ให้สิทธิ์ตัวเองเป็นผู้ดูแลระบบที่สามารถถึงระบบอื่น ๆ ได้ด้วย



การโจมตีแบบวิศวกรรมสังคม (Social Engineering Attacks)

- เป็นรูปแบบหนึ่งของ **ความพยายามเข้าใช้ระบบ**
- เป็น**การหลอกลวง** โดยอาศัยจุดอ่อน ความไม่รู้ หรือความประมาทเลินเล่อ
- เป็นวิธีที่ได้รับความ**นิยมมากและได้รับผลดีมาก**ในปัจจุบัน

วิธีการหลอกลวง

- ปลอมเป็นผู้อื่นที่มีความสำคัญมากๆ เช่น CEO ของบริษัท เพื่อสนิท หรือคนในครอบ แล้วทำส่ง Email หาเยื่อ
- ในเนื้อความ กล่าวถึงเหตุการณ์หรือสถานการณ์ในปัจจุบันเพื่อให้ดูสมจริง (เช่น เสนอผลตอบแทนหรือโปรโมชันเพื่อสร้างแรงจูงใจ)
- อำพราง URL อันตรายให้เหมือนกับ URL ทั่วๆ ไป

เมื่อวันที่ 5 ก.ย. ที่ผ่านมาตำรวจกองปราบบุกจับ คนร้ายแฮคเฟชบุ้ค ก่อนใช้บัญชีเฟซฯ ของเหยื่อที่ขโมยมาได้ ขอยืมเงินเพื่อนๆ เข้ากระเป๋าตัวเอง โดยใช้ข้อมูลจาก Social media เพียงไม่กี่อย่าง ก็เข้าถึงบัญชีเป้าหมายได้!!!

ในรายงานดังกล่าวนั้น ระบุว่า คนร้ายชื่อ นายมหาราช จันทร์ศรี อายุ 22 ปี เป็นผู้ต้องหาตามหมายศาลในข้อหาฉ้อโกง ซึ่งผู้ต้องหาจะใช้วิธีการแฮคเข้าไปยังเฟซบุ๊คของเหยื่อ โดนเน้นที่มีข้อมูลน่าเชื่อถือ มีเพื่อนฝูงที่มีหน้ามีตา ฯลฯ ก่อนจะปลอมเป็นเจ้าของเฟซฯ ทำการแชท-พูดคุยกับเหยื่อที่เป็นเพื่อน เพื่อขอยืมเงิน และให้เหยื่อโอนเงินเข้าบัญชีของคนร้าย

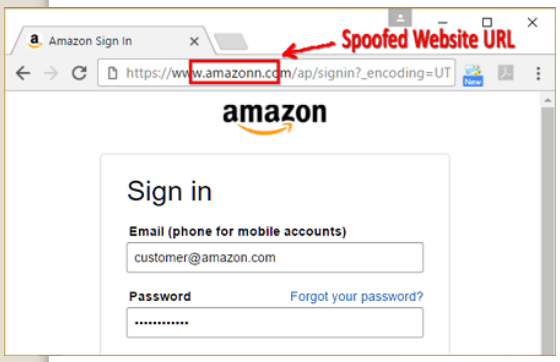
ซึ่งในคดีนี้ เป็นเพียงคดี ในอีกจำนวนมากที่เกิดขึ้นบนโลกออนไลน์ในทุกวันนี้ ซึ่งหลายคนใช้อยู่โดยไม่ได้ระมัดระวังเป็นเหตุให้ คนร้ายสามารถใช้-เข้าถึงบัญชีโลกโซเชียลมีเดียของคุณได้

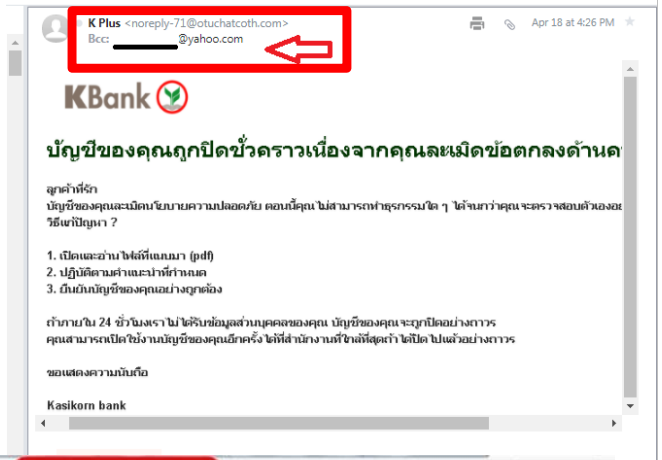
การโจมตีแบบฟิชชิ่ง (Phishing Attacks)

ฟิชชิ่ง คือรูปแบบของ Social Engineering แบบหนึ่งโดยใช้การส่งข้อมูลหลอกลวง ข้อมูลปลอม Email ปลอม หรือเว็บไซน์ปลอม ฯลฯ ไปหาเหยื่อเพื่อให้เหยื่อกดลิ้งที่ในนั้น หรือกรอกข้อมูลที่ต้องการลงไป วิธี Phishing ยอดนิยม เช่น

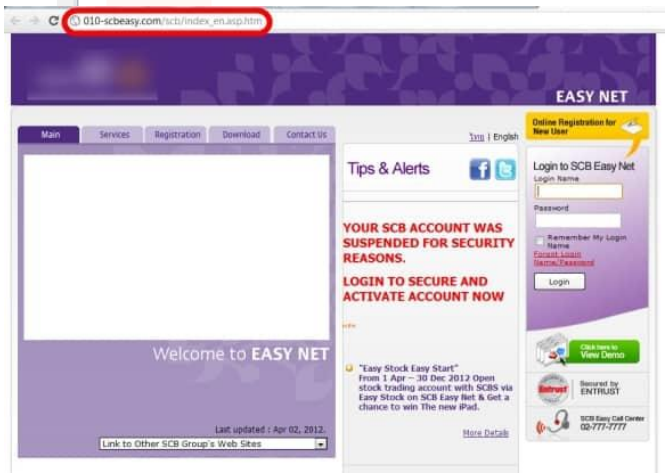
- Deceptive Phishing – อีเมลจากบริษัทหรือหน่วยงานชื่อดัง เช่น Facebook, ธนาคาร เพื่อหลอกขโมยข้อมูล เช่น ให้ยืนยัน Account, กรอกข้อมูลส่วนตัว, ชำระเงินออนไลน์
- Spear Phishing – เหมือนแบบแรก แต่จะเจาะจงเป้าหมายมาที่เหยื่อเพียงคนเดียว แฮ็คเกอร์จะรวบรวมข้อมูลของเหยื่อแล้วพยายามหลอกล่อให้แนบเนียนที่สุด เพื่อให้ได้ข้อมูลที่ตัวเองต้องการ
- CEO Fraud – แฮ็คเกอร์ปลอมอีเมลให้คล้ายคลึงกับอีเมลของผู้บริหารระดับสูง เพื่อหลอกให้พนักงานที่ไม่ใส่ใจ โอนเงินหรือส่งข้อมูลความลับให้
- Pharming – แฮ็คเกอร์ทำการไฮแจ็คชื่อโดเมนของเว็บไซต์ เมื่อเหยื่อเผลอเข้าเว็บไซต์ดังกล่าวก็จะถูก Redirect ไปยังเว็บไซต์ปลอมของแฮ็คเกอร์แทน (Weakest Link)

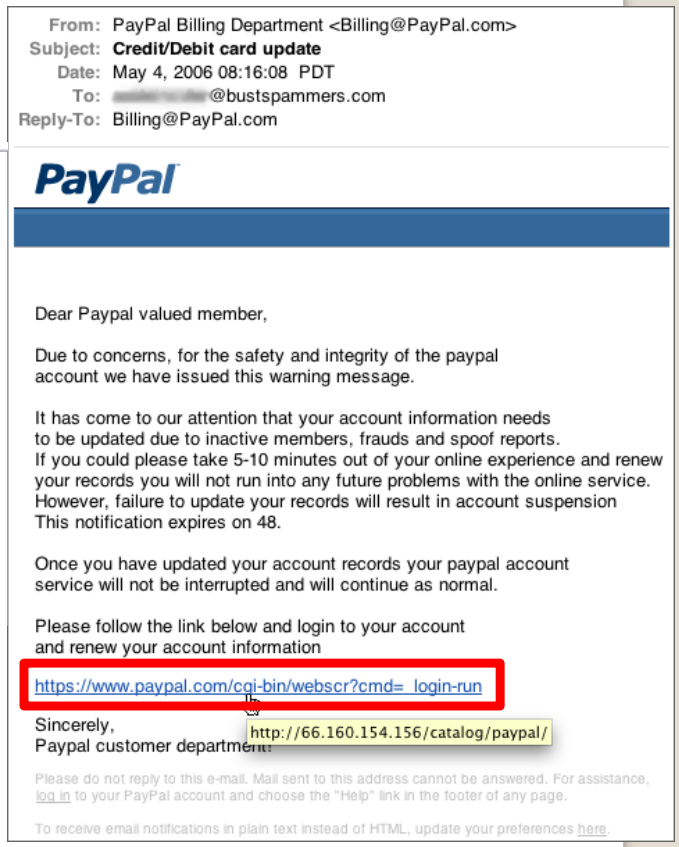
https://www.onespan.com/blog/social-engineering-win-battle-trust-infographic


Amazon Sign In
Spoofed Website URL
https://www.amazonn.com/ap/signin?_encoding=UT
amazon
Sign in
Email (phone for mobile accounts)
customer@amazon.com
Password
Forgot your password?


K Plus <noreply-71@otuchatcoth.com>
Bcc: @yahoo.com
Apr 18 at 4:26 PM
KBank
บัญชีของคุณถูกปิดชั่วคราวเนื่องจากคุณละเมิดข้อตกลงด้านค
ลูกค้าที่รัก
บัญชีของคุณละเมิดนโยบายความปลอดภัย ดอนนี้คุณไม่สามารถทำธุรกรรมใด ๆ ได้จนกว่าคุณจะตรวจสอบตัวของ
วิธีแก้ปัญหา ?
1. เปิดและอ่านไฟล์ที่แนบมา (pdf)
2. ปฏิบัติตามคำแนะนำที่กำหนด
3. ยืนยันบัญชีของคุณอย่างถูกต้อง
ถ้าภายใน 24 ชั่วโมงเราไม่ได้รับข้อมูลส่วนบุคคลของคุณ บัญชีของคุณจะถูกปิดอย่างถาวร
คุณสามารถเปิดใช้งานบัญชีของคุณอีกครั้งได้ที่สำนักงานที่ใกล้ที่สุดถ้าได้ปิดไปแล้วอย่างถาวร
ขอแสดงความนับถือ
Kasikorn bank


23% 23:59
imagenesr23.no
facebook
เว็บปลอม
เข้าสู่ระบบ
สร้างบัญชีผู้ใช้ใหม่


010-scbeasy.com/scb/index_en.asp.htm
EASY NET
Main
Services
Registration
Download
Contact Us
Tips & Alerts
YOUR SCB ACCOUNT WAS SUSPENDED FOR SECURITY REASONS.
LOGIN TO SECURE AND ACTIVATE ACCOUNT NOW
Welcome to EASY NET
Login to SCB Easy Net
Login
Last updated : Apr 02, 2012.
Link to Other SCB Group's Web Sites


From: PayPal Billing Department <Billing@PayPal.com>
Subject: Credit/Debit card update
Date: May 4, 2006 08:16:08 PDT
To: @bustspammers.com
Reply-To: Billing@PayPal.com
PayPal
Dear Paypal valued member,
Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.
It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.
Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.
Please follow the link below and login to your account and renew your account information
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run
http://66.160.154.156/catalog/paypal/
Sincerely,
Paypal customer department
Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.
To receive email notifications in plain text instead of HTML, update your preferences here.

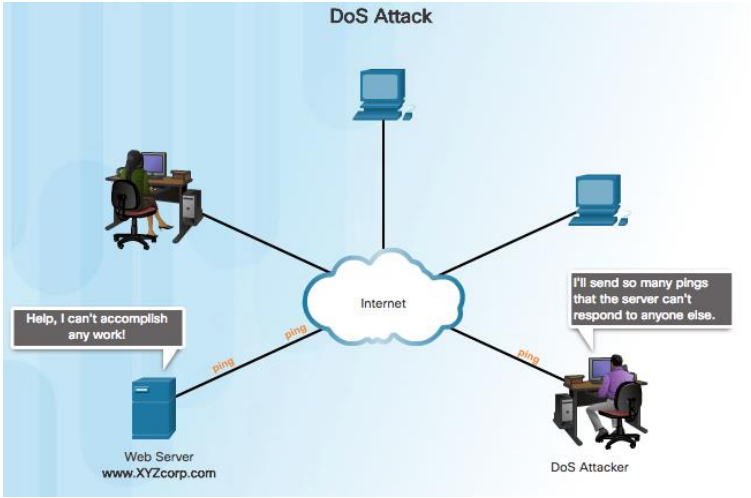
การค้นหาหรือได้มาของ password ด้วยวิธีอื่น ๆ

- การค้นหาด้วยดิกชันนารี
- การพยายามใส่พาสเวิดแบบแรนด้อมจนกว่าจะถูก
- การทำตัวเองเป็น man-in-the-middle เพื่อดัก Password เป็นเทคนิคที่คอยดักจับ Password เมื่อมีการส่งผ่าน Password ไปยัง Server เช่น การส่ง Password ไปยัง www.facebook.com

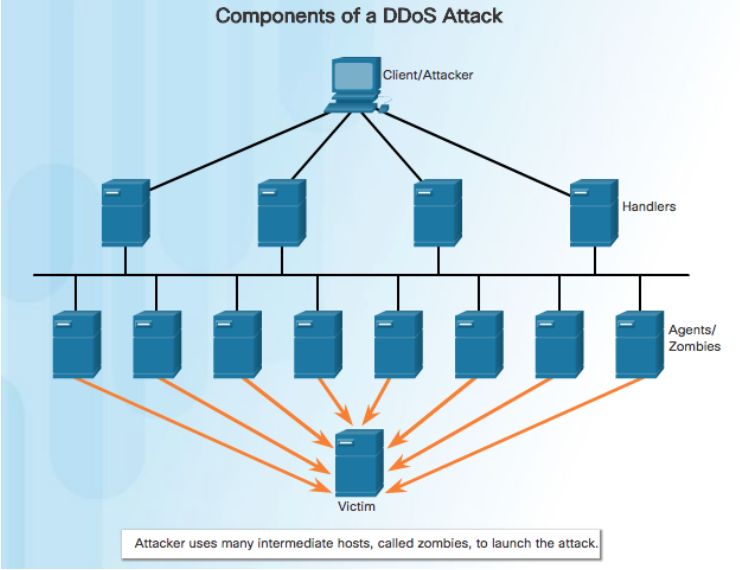
3. Denial of Service (DoS) Attacks

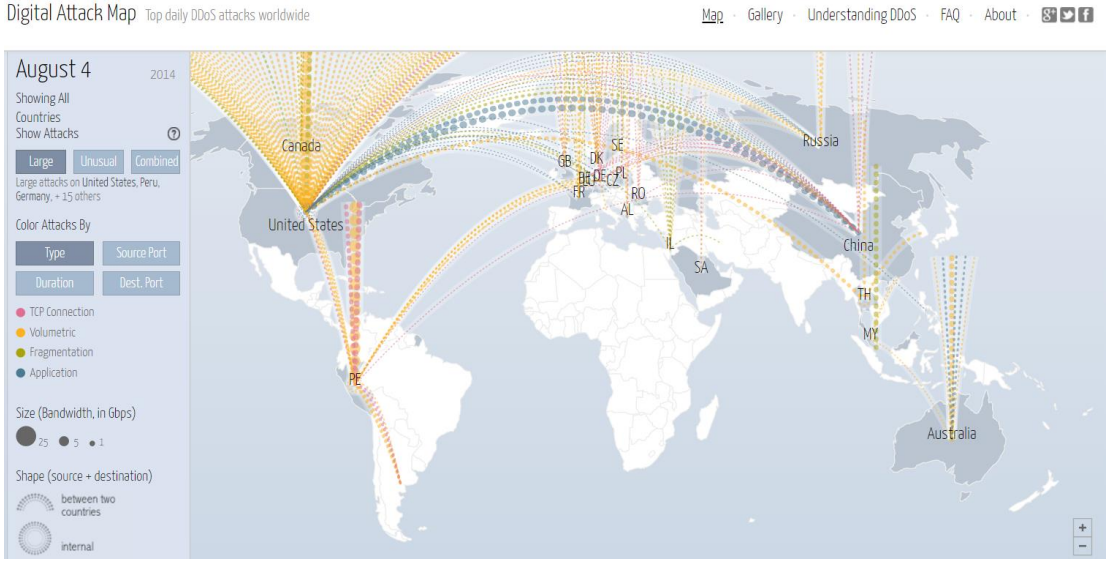
เป็นการโจมตีเพื่อจุดประสงค์ในการทำให้บริการหรือระบบคอมพิวเตอร์เป้าหมายไม่สามารถให้บริการได้อีกต่อไปด้วยวิธีการต่างๆ เช่น

- การฝัง Malware เอาไว้และสั่งให้ทำงาน
- โจมตีด้วยการ ส่งคำสั่งหลาย ๆ คำสั่งพร้อม ๆ กัน ไปยัง Server หรือ ระบบคอมพิวเตอร์ เพื่อให้หยุดทำงาน



- การโจมตีระบบคอมพิวเตอร์หรือบริการเป้าหมายโดยใช้งานผู้โจมตีมากกว่า 1 เครื่อง
- อาศัยเครื่องจำนวนมาก ๆ จากที่ Hacker เข้าไปยึดไว้ได้จากการติด Malware ที่ผู้ใช้เผลอติดโดยวิธีต่าง ๆ ที่กล่าวมาก่อนหน้านี้





เครือข่ายกล้องวงจรปิดที่ถูกแฮ็ก ถูกใช้ยิง DDoS ขนาดใหญ่เป็นประวัติการณ์ถึง 1Tbps

By: mk on 26 September 2016 - 08:09 Tags: DDoS Security Hosting Botnet

ต่อจากข่าว เว็บไซต์ KrebsOnSecurity ถูกถล่มด้วย DDoS ขนาดใหญ่ที่สุดในประวัติศาสตร์ สถิตินี้ก็ถูกทำลายอย่างรวดเร็ว เมื่อ OVH เว็บโฮสติ้งรายใหญ่จากฝรั่งเศส รายงานว่าถูกโจมตีด้วย DDoS ทราฟฟิกมหึมาถึง 1Tbps เลยทีเดียว (ของ Krebs คือ 665Gbps) โดยทราฟฟิกก้อนใหญ่ที่สุดที่ถูกยิงเข้ามามีขนาด 799Gbps

Octave Klaba ผู้ก่อตั้ง OVH เผยข้อมูลเรื่องนี้บน Twitter ของเขาเอง โดยระบุว่าตัว botnet ที่ใช้ยิง DDoS เป็นเครือข่ายกล้องวงจรปิดหรือเครื่องบันทึกวิดีโอ (DVR) ที่ติดมัลแวร์จำนวน 1.45 แสนเครื่อง ศักยภาพของมันสามารถยิงทราฟฟิกขนาดมากกว่า 1.5Tbps

Read more 24 comments

GitHub โดนยิง DDoS ด้วยทราฟิค 1.35 Tbps ใหญ่ที่สุดที่เคยมีมา

By: nismod on 2 March 2018 - 12:08 Tags: GitHub DDoS Cybersecurity Akamai

เมื่อวันพฤหัสที่ผ่านมาตามเวลาบ้านเรา GitHub ถูกโจมตีแบบ DDoS ด้วยทราฟิคมหาศาลที่สุดที่เคยมีมาถึง 1.35 Tbps และการโจมตีครั้งนี้ไม่ใช่ DDoS ที่ใช้บอตเน็ทแบบทั่วไป แต่เป็นการโจมตีด้วย Memcached

แฮกเกอร์ได้ปลอม IP ของ GitHub และยิง querie ไปที่เซิร์ฟเวอร์ memcached หลายๆ ตัว ประมาณ 10 querie ต่อวินาทีต่อเซิร์ฟเวอร์ ก่อน GitHub จะได้รับทราฟิคมหาศาลกลับเข้ามามากกว่าที่ querie ไปราว 51,000 เท่าจนเซิร์ฟเวอร์ GitHub รับไม่ไหวและต้องขอให้ทาง Akamai เข้ามาช่วยเหลือ

Read more 10 comments

กูเกิลเปิดตัว Cloud Armor บริการป้องกัน DDoS และการเจาะเว็บ

By: lew on 27 March 2018 - 11:01 Tags: Google Cloud Platform DDoS

กูเกิลเปิดบริการป้องกันการโจมตีแบบ DDoS ในชื่อ Cloud Armor โดยตอนแรกจะเปิดบริการสำหรับผู้ใช้ Global HTTP Load Balancer

บริการนี้เปิดจริงแล้ว โดยเปิดให้ผู้ใช้สร้างกฎง่ายๆ เช่น การทำ whitelist/blacklist หรือการใช้กฎป้องกันเพิ่มเติม แต่บางฟีเจอร์ เช่น การสร้างกฎอย่างซับซ้อน, การป้องกันตามภูมิประเทศ, การป้องกัน SQL Injection และ Cross-site Scripting ยังอยู่ในสถานะอัลฟ่า ทำให้ต้องขอใช้งานล่วงหน้า

ค่าบริการรายเดือนคิดตาม policy เดือนละ 5 ดอลลาร์ต่อ policy และจำนวนกฎ เดือนละ 1 ดอลลาร์ต่อกฎ เมื่อใช้งานจริงจะคิด 0.75 ดอลลาร์ต่อ 1 ล้านการเชื่อมต่อ HTTP

Read more

https://www.digitalattackmap.com/

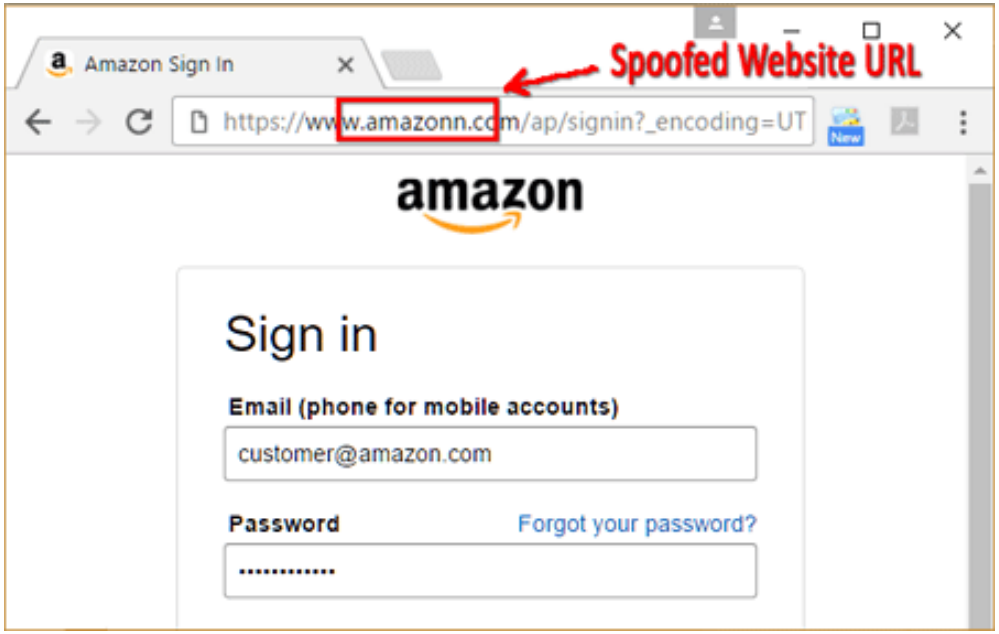
5. ความมั่นคงปลอดภัยไซเบอร์สำหรับบุคคลทั่วไป

1. ระวังอันตรายเรื่องข้อมูลส่วนตัว

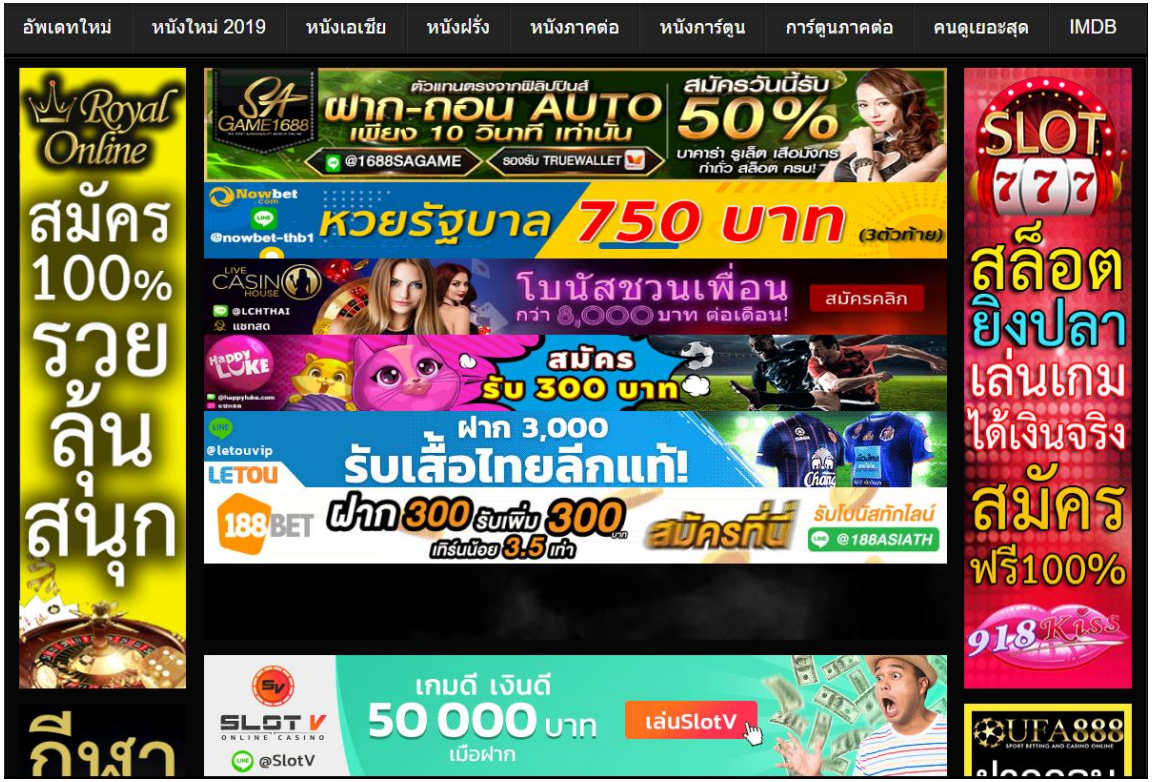
- ข้อมูลส่วนตัวควรเป็นความลับ
- เปิดเผยเรื่องส่วนตัวแค่พอดี
- ไม่กำหนดให้จำรหัสผ่านในเครื่องสาธารณะ และลบข้อมูลการใช้ Internet
- ยกเลิกการใช้งานแอคเคาท์ต่างๆ ที่ไม่ใช้
- เรียกดูเว็บอย่างปลอดภัยด้วย https เป็นหลัก
- อย่าใช้รหัสผ่านเดียวกันกับทุกบริการ
- ตั้งรหัสผ่านให้ปลอดภัยโดยใช้การผสมระหว่างตัวเลขและตัวอักษรทั้งตัวเล็กและใหญ่
- จ่ายเงินออนไลน์ต้องระวังตัวอย่างดี

2. ระวังอันตรายจากการหลอกลวงรูปแบบต่างๆ

- ระวังและป้องกันตัวจากหน้าเว็บหลอกลวง (Phishing)
  - ดู URL ของเว็บที่กำลังใช้งานให้ถูกต้องอยู่เสมอ
  - อย่าไว้ใจคลิกลิ้งที่มีคนส่งให้ทันที



- อย่ากดลิ้งที่หลอกลวงตามหน้าเว็บต่าง ๆ หรือโฆษณาในเว็บที่ไม่น่าเชื่อถืออาจได้ของแถมเป็น Malware ได้



- หลอกให้ดาวน์โหลดโปรแกรม/แอพ
  - อย่าติดตั้งโปรแกรมที่มีผู้แนะนำให้ติดตั้งจากเว็บหรือคนที่ไม่น่าเชื่อถือ
  - อย่าไว้ใจคลิกลิ้งที่มีคนส่งให้ทันที

- ซื้อสินค้าหรือทำธุรกรรมออนไลน์ให้ปลอดภัย
  - ก่อนกรอกข้อมูลบัตรเครดิตต่างๆ ก็อย่าลืมเช็คว่าหน้าเว็บนั้นเป็นระบบ https หรือไม่เพื่อป้องกันการดักจับข้อมูลจากแฮกเกอร์
  - ตรวจสอบประวัติของร้านหรือผู้ขาย โดยค้นหาข้อมูลร้านนั้นจากผู้ที่เคยซื้อหรือใช้บริการจาก Google
  - ตรวจสอบชื่อผู้รับเงินก่อนโอนให้ถูกต้องเสมอ
  - แม้ว่าจะเคยซื้อกับทางร้านนั้น ๆ มาก่อนแล้วก็อย่าเพิ่งไว้ใจ มีข่าวที่ผู้ขายหลอกให้ตายใจ ครั้งแรก ๆ ก็ซื้อขายกันตามปกติพอซื้อยอดสูง ๆ แล้วไม่ทำการส่งของให้

3. Chat, Comment, Like และ Share ให้ปลอดภัย

- ออนไลน์อย่างไรไม่ให้ผิด พ.ร.บ. คอมพิวเตอร์
  - ระวังการ**นำเข้าข้อมูลอันเป็นเท็จ**ก่อให้เกิดความเสียหายหรือเสื่อมเสียชื่อเสียงต่อผู้อื่น
  - โพสต์ข้อความเท็จเพื่อหลอกลวงผู้อ่านบนเว็บบอร์ดหรือสื่อสังคมออนไลน์
  - ตัดต่อภาพของผู้อื่น ทำให้ผู้อื่นเสียหาย
  - ระวังการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา บนอินเทอร์เน็ต
    - การเผยแพร่ข้อมูลละเมิดลิขสิทธิ์ เช่น อัพโหลดหนังหรือเพลงที่ละเมิดลิขสิทธิ์ขึ้นไปบนเว็บต่างๆ
    - ข้อความ ภาพถ่าย ภาพวาด วิดีโอ หนัง เพลง โปรแกรมคอมพิวเตอร์ งานวรรณกรรม เป็นต้น
    - นำภาพหรือข้อความของผู้อื่นไปใช้ควรให้เครดิต
- ระวัง! แอพที่ติดตั้งใน Social media
  - ตรวจสอบว่าแอพพวกนั้นขอข้อมูลส่วนตัวมากเกินไปหรือไม่ถ้าขอข้อมูลอะไรมากเกินไปที่ไม่จำเป็นไม่ควรติดตั้งเด็ดขาด

THE STANDARD

STAND UP FOR THE PEOPLE

HOME NEWS CULTURE LIFESTYLE OPINION VIDEO PODCAST MAGAZINE CONTACT

BUSINESS TECH

Facebook โดนปรับเป็นประวัติการณ์ 1.55 แสนล้านบาท ฐานบกพร่องปกป้องความเป็นส่วนตัวผู้ใช้ กรณี Cambridge Analytica

โดย ปณชัย อารีเพิ่มพร
25.07.2019

994

4. ระวังอันตรายจากการออนไลน์หรือใช้อุปกรณ์ไม่เหมาะสม

- ใช้ Wi-Fi สาธารณะฟรีอย่างระมัดระวัง
  - หลีกเลี่ยงการใช้ Wi-Fi สาธารณะที่ไม่น่าไว้ใจ เช่น Wi-Fi ชื่อแปลกๆ หรือเข้าได้ฟรี ๆ ไม่มี login
  - อย่าทำธุรกรรมหรือใช้บริการที่ต้องกรอกชื่อ, รหัสผ่าน รวมถึงข้อมูลส่วนตัว
  - ถ้าจำเป็นจริง ๆ ก็ควรเชื่อมต่ออินเทอร์เน็ตผ่าน 3G/4G แทน
- เช็ค Wi-Fi ที่ปลอดภัยก่อนเข้าใช้โดยใช้ Application เช่น SSLSTRIPGuard
- อัพเดท OS เป็นรุ่นล่าสุดเสมอ

แบบฝึกหัด

1. จงอธิบาย องค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล (CIA) 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และการรักษาความพร้อมใช้งานของข้อมูล (Availability) พอสังเขป
2. จงอธิบายความสัมพันธ์ระหว่าง ภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) และการโจมตี (Exploit)
3. จงอธิบายความแตกต่างของผู้คุกคาม (Threat Actors) และแฮกเกอร์ (Hackers)
4. จงอธิบายความแตกต่างระหว่างไวรัส (Virus) กับเวอร์ม (Worms)
5. จงระบุประเภทมัลแวร์ (Malware) ที่น่าจะสร้างความเสียหายให้กับระบบคอมพิวเตอร์น้อยที่สุด พร้อมให้เหตุผลพอสังเขป
6. จงสรุปการโจมตีเครือข่ายในแต่ละประเภท พอสังเขป

7. จงอธิบายแนวทางการตั้งรหัสผ่านที่ดี
8. จงอธิบายแนวทางในการซื้อสินค้าหรือทำธุรกรรมออนไลน์ให้ปลอดภัย
9. อะไรคือข้อควรระวังในการใช้สื่อสังคมออนไลน์ (Social Media) เพื่อให้มีความมั่นคงปลอดภัย
10. การทำธุรกรรมการเงินผ่านทาง Wi-fi สาธารณะ เป็นสิ่งที่เหมาะสมหรือไม่เพราะอะไร

เอกสารประกอบการเรียนการสอน

- คู่มือแนวทางปฏิบัติการรักษาความปลอดภัยบนโลกไซเบอร์ภาคประชาชน, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

- ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security), สานักงานรัฐบาลอิเล็กทรอนิกส์(องค์การมหาชน)(สรอ.)