030523114 Network Security

สาขาวิชาเทคโนโลยีอิเล็กทรอนิกส์ (ต่อเนื่อง)

ภาควิชาเทคโนโลยีวิศวกรรมอิเล็กทรอนิกส์

วิทยาลัยเทคโนโลยีอุตสาหกรรม

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ ดร.เลอสรรค์ กิรสมุทรานนท์

ครั้งที่ 11 “Malware”

Malware and Protection

- **Outline**
  - Intro Malware and Protection
  - มัลแวร์ (Malware)
  - โปรแกรมที่ไม่จัดเป็นมัลแวร์
  - คุณสมบัติของมัลแวร์
  - เทคนิคการตรวจจับไวรัส
  - อาการของเครื่องที่ติดไวรัสหรือมัลแวร์
  - สาเหตุที่เครื่องติดไวรัสหรือมัลแวร์
  - การป้องกันไวรัส
  - สรุป

Intro Malware & Protection

- โปรแกรมที่สามารถสาเนาตัวเองตั้งชื่อว่า "ไวรัส"
- ครั้งแรกในปี พ.ศ.2526 โดย ดร.เฟรดเดอริก โคเฮน
- ไวรัสที่แพร่ระบาดและสร้างความเสียหายครั้งแรกเมื่อปี พ.ศ. 2529
- "เบรน (Brain)" เขียนขึ้น โดยโปรแกรมเมอร์ชาวปากีสถานชื่ออัมจาด (Amjad) และเบซิท (Basit)
- ทำการ Copy Software ขาย พร้อมทั้งแอบปล่อยไวรัส “เบรน”
- ปัจจุบันนี้พบว่ามีมากกว่า 40,000 ชนิด
- เพิ่มขึ้นอีกอยู่ทุก ๆ วัน อย่างน้อยวันละ 4-6 ตัว

มัลแวร์ (Malware)

- “Malicious Logic เป็นชุดของคำสั่งที่สร้างปัญหาในการละเมิดนโยบายด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ”
- หรือส่วนใหญ่แล้วเรามักเรียกกันว่า“โปรแกรมประสงค์ร้าย (Malware: Malicious Software)”
- สามารถแบ่งชนิดของโปรแกรมประสงค์ร้ายได้โดยดูจากพฤติกรรม 3 ข้อดังนี้
- ชุดคาสั่ง(Code) นี้อยู่ได้อิสระหรือไม่ (Need host ?)
- สามารถเดินทางได้ด้วยตัวเองหรือไม่ (Propagation ?)
- สามารถสาเนาตัวเองได้หรือไม่ (Self-replicating ?)

มัลแวร์ (Malware)
ไวรัส (Virus)

- ไวรัส คือ โปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นให้สามารถจัดการกับตัวมันเอง
  - Need Host –จาเป็นต้องอยู่กับโปรแกรมอื่นหรือชุดคำสั่งอื่น
  - Not Propagation –ต้องใช้ตัวกลางอื่นในการแพร่กระจาย
  - Self-Replicating –จะพยายามทำสำเนาตัวเองกระจายไปยังชุดคาสั่งอื่น

มัลแวร์ (Malware)

หนอน (Worm)

- หนอน (Worm) หมายถึง โปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ โดยจะแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่น ๆ ที่อยู่ในเครือข่าย หนอนจะใช้ประโยชน์จากแอพพลิเคชั่นที่รับส่งไฟล์โดยอัตโนมัติ และไม่ต้องอาศัยคนเพื่อเปิดไฟล์ใด ๆ เพราะหนอนมีส่วนของโปรแกรมที่สามารถรันตัวเองเพื่อสร้างความเสียหายได้ เวิร์มนั้นบางที่อาจอาศัยอีเมล์ในการแพร่กระจายตัวเองเหมือนไวรัส โดยแนบไฟล์ไปกับอีเมล์ เมื่อผู้รับเปิดจดหมายอ่านหนอนก็จะเริ่มทางานทันที อย่างไรก็ตามในครั้งแรกที่เกิดหนอนขึ้นในวงการคอมพิวเตอร์นั้น เพื่อใช้ช่วยเพิ่มความสะดวกในการลงโปรแกรมให้กับเครื่องคอมพิวเตอร์ที่มีอยู่ในระบบของตนเอง ซึ่งในบางครั้งอาจมีกว่าร้อยเครื่อง โดยหนอนจะทาการส่งตัวเองไปพร้อมกับโปรแกรมที่จะทาการลงไปยังทุก ๆ เครื่องในระบบแล้วทาการลงโปรแกรมนั้น ๆ ให้เองโดยอัตโนมัติไปเรื่อย ๆ จนครบทุกเครื่อง
  - Self-Sub Physical –สามารถอยู่เป็นโปรแกรมเดียว ๆ เองได้
  - Propagation –พยายามเคลื่อนที่ไปติดเครื่องอื่น ทั้งไปเองหรือสำเนาตัวเองไป
  - Not Replicating –จะไม่ทำสำเนาตัวเองภายในเครื่องเดิม

มัลแวร์ (Malware)
ม้าโทรจัน (Trojan Horse)

- ม้าโทรจัน (Trojan Horse) นี้เป็นคาที่มาจากสงครามโทรจันระหว่างทรอย (Troy) และกรีซ (Greek) ซึ่งเปรียบถึงม้าโครงไม้ขนาดใหญ่ที่ชาวกรีซสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างใน จากนั้นทาทีเป็นว่าถอนทัพกลับ เมื่อชาวทรอยออกมาดูเห็นม้าโครงไม้ทิ้งไว้และคิดว่าเป็นบรรณาการที่ทหารกรีซทิ้งไว้ให้เพื่อไม่ให้ตามไปโจมตีคืน จึงนากลับเข้าเมืองไปด้วย แต่พอตกดึกทหารกรีซที่ซ่อนอยู่ในม้าโครงไม้ก็ออกมาและเปิดประตูให้กับทหารกรีซเข้าไปทาลายเมืองทรอยได้ในที่สุด สำหรับในความหมายทางคอมพิวเตอร์แล้วม้าโทรจันหมายถึง โปรแกรมที่ทำลาย

มัลแวร์ (Malware)
ม้าโทรจัน (Trojan Horse)

- ระบบความปลอดภัยของคอมพิวเตอร์ไม่ทางใดก็ทางหนึ่ง โดยแฝงมากับโปรแกรมอื่น ๆ เช่น เกม, สกรีนเซิร์ฟเวอร์ เป็นต้น ซึ่งผู้ใช้อาจจะดาวน์โหลดโปรแกรมต่าง ๆ เหล่านี้มา และเมื่อติดตั้งแล้วรันโปรแกรม ม้าโทรจันที่แฝงมาด้วยก็จะทำลายระบบความปลอดภัยของคอมพิวเตอร์ เช่น เปิดช่องทางการสื่อสาร(Port) ที่ไม่ได้ใช้เอง เพื่อเป็นการสร้างประตูหลังให้กับโปรแกรมอื่นเข้ามาทาลายระบบได้ หรืออาจทาการบันทึกการใช้งานต่าง ๆ ของผู้ใช้งาน (Logs) เพื่อให้เจ้าของม้าโทรจันนั้นสามารถเข้ามาดูข้อมูลที่บันทึกไว้ได้ เป็นต้น
  - Self-Sub Physical –สามารถอยู่เป็นโปรแกรมเดียว ๆ เองได้
  - Not Propagation –ต้องถูกชักนำเข้ามาจากผู้ถูกโจมตีเองไม่สามารถเคลื่อนที่เองได้
  - Not Replicating –จะไม่ทำสำเนาตัวเอง

มัลแวร์ (Malware)
ม้าโทรจัน (Trojan Horse)

- ทั้งนี้ม้าโทรจันอาจมีชื่อเรียกอื่นซึ่งอธิบายถึงลักษณะการทางานของมัน เช่น
- รูทคิท(Root Kits) เป็นชุดโปรแกรมขนาดเล็กที่หลอกให้ผู้ใช้เชื่อว่าจาเป็นต่อการทำงานของระบบคอมพิวเตอร์ โดยพวกผู้โจมตีนิยมใช้สาหรับเจาะเข้าระบบเพื่อควบคุมระบบหรือขโมยข้อมูล โปรแกรมประเภทนี้อาจใช้เทคนิคต่าง ๆ เช่น การเฝ้าดูสิ่งที่ผู้ใช้พิมพ์บนคีย์บอร์ด (Key Stroke), แก้ไขไฟล์บันทึก (Log file) ของระบบ, สร้างประตูหลัง (Back Door) เพื่อสาหรับการเจาะเข้าระบบในภายหลังหรืออาจใช้ระบบนี้เพื่อเป็นฐานในการโจมตีระบบอื่น ๆ ผ่านทางเครือข่าย โดยทั่วไปรูทคิทจะถูกจัดไว้เป็นชุดเพื่อใช้สาหรับโจมตีระบบปฏิบัติการประเภทใดประเภทหนึ่งโดยเฉพาะ รูทคิทเกิดขึ้นครั้งแรกในปี 1990 โดยในช่วงนั้น ระบบปฏิบัติการซันยูนิกซ์ (SUN Unix) และลีนุกซ์ (Linux) เป็นเป้าหมายของการโจมตี แต่ในปัจจุบันมีรูทคิทหลายประเภทเพื่อใช้กับระบบปฏิบัติการต่างๆ ซึ่งรวมถึงไมโครซอฟท์วินโดวส์ (Microsoft Window) และแม็คอินทอช (Mac OS) ด้วย

มัลแวร์ (Malware)
ม้าโทรจัน (Trojan Horse)

- Remote Access Trojan (RAT) เป็นม้าโทรจันที่จะสร้างประตูหลัง (Back Door) ให้ผู้โจมตีสามารเข้ามาในระบบเพื่อขโมยข้อมูลหรือควบคุมระบบจากระยะไกลตัวอย่างเช่น แบ็คออริไฟซี (Back Orifice), คาฟีน (Cafeene) และซับเซเว่น (Sub Seven) เป็นต้นข้อสังเกตอย่างหนึ่งคือ ถึงแม้ว่าชุดโปรแกรม RAT หรือรูทคิดบางโปรแกรมเป็นเครื่องมือที่สามารถใช้งานอย่างถูกต้องตามกฎหมายเพื่อจุดประสงค์สาหรับการดูแลระบบ (Monitoring System) อย่างไรก็ตามเครื่องมือเหล่านี้อาจเป็นอันตรายต่อระบบหรือองค์กรได้ถ้ามีการใช้งานในทางที่ผิด

มัลแวร์ (Malware)
ม้าโทรจัน (Trojan Horse)

- **Data Sending and Password Sending Trojan** เป็นโทรจันที่ขโมยรหัสผ่านต่าง ๆ แล้วส่งไปให้ผู้ไม่ประสงค์ดี
- **Keylogger Trojan** เป็นโทรจันที่ดักจับทุกข้อความที่พิมพ์ผ่านแป้นพิมพ์ของคีย์บอร์ด
- **Destructive Trojan** เป็นโทรจันที่สามารถลบไฟล์บนเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อได้
- **Denial of Service(DoS) Attack Trojan** เป็นโทรจันที่ใช้ทา DDoS (Distributed Denial-of-Service) ให้โจมตีระบบคอมพิวเตอร์ที่เป็นเป้าหมายบนอินเทอร์เน็ต เพื่อทาให้ระบบเป้าหมายปฏิเสธหรือหยุดการให้บริการ (Denial-of-Service) การโจมตีจะเกิดขึ้นพร้อมๆ กันและมีเป้าหมายเดียวกัน โดยเครื่องที่ตกเป็นเหยื่อทั้งหมดจะสร้างข้อมูลขยะขึ้นมาแล้วส่งไปที่ระบบเป้าหมาย เพื่อสร้างกระแสข้อมูลให้ไหลเข้าไปในปริมาณมหาศาลทาให้ระบบเป้าหมายต้องทางานหนักขึ้นและช้าลงเรื่อยๆ เมื่อเกินกว่าระดับที่จะรับได้ก็จะหยุดการทางานลงในที่สุด อันเป็นเหตุให้ผู้ใช้ไม่สามารถใช้บริการระบบเป้าหมายได้ตามปกติ ส่วนรูปแบบของการโจมตีที่นิยมใช้กันก็มีเช่น SYN Flood, UDP Flood, ICMP Flood, Surf, Fraggle เป็นต้น

มัลแวร์ (Malware)
ม้าโทรจัน (Trojan Horse)

- Proxy Trojan เป็นโทรจันที่ทำให้เครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกลายเป็นเครื่อง Proxy Server, Web Server หรือ Mail Server เพื่อสร้าง Zombie Network ซึ่งจะถูกใช้ให้เป็นฐานปฏิบัติการเพื่อจุดประสงค์อย่างอื่น FTP Trojan เป็นโทรจันที่ทำให้ครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกลายเป็นเครื่อง FTP Server Security Software Killer Trojan เป็นโทรจันที่ Kill Process หรือลบโปรแกรมป้องกันไวรัสหรือลบไฟร์วอลล์บนเครื่องที่ตกเป็นเหยื่อ เพื่อง่ายต่อการปฏิบัติการอย่างอื่นต่อไป Trojan Downloader เป็นโทรจันที่ดาวน์โหลด Adware, Spyware และ Worm ให้มาติดตั้งบนเครื่องเหยื่อ
- ไฟล์ประเภทที่ปลอดภัย 100% ก็คือไฟล์ประเภท Text File ทั้งหมด เช่น .txt, .rtf(Rich Text Format)เป็นต้น เนื่องจากไฟล์เหล่านี้ไม่ใช่ชุดคำสั่ง
- Malware ต่าง ๆ ไม่สามารถทางานข้าม OS (ระบบปฏิบัติการ : Operating System) กันได้ เนื่องจากในแต่ละ OS จะมีการใช้นามสกุลของไฟล์ที่เรียกใช้งานได้ไม่เหมือนกัน เช่น ใน Windows OS จะใช้ไฟล์ .exe แต่ใน MAC OS นั้นจะไม่สามารถรันไฟล์ .exe ได้ ดังนั้น Malware บน Windows จึงไม่มีผลกระทบต่อ MAC OS อย่างไรก็ตามทานองเดียวกัน Malware บน MAC OS ก็ไม่มีผลกับ Windows OS เช่นกัน

มัลแวร์ (Malware)
โปรแกรมที่ไม่จัดเป็นมัลแวร์

- โจ๊กแอพพลิเคชัน
- โฮแอคซ์(Hoaxes)
- สแปม(Spam)
- สปายแวร์(Spyware)
- แอดแวร์ (Adware)
- อินเทอร์เน็ตคุกกี้ (Internet Cookies)

โปรแกรมที่ไม่จัดเป็นมัลแวร์

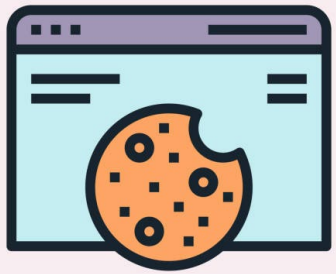
- - โจ๊กแอพพลิเคชัน เป็นซอฟต์แวร์ที่ออกแบบเพื่อสร้างความสนุกสนาน แต่ก็ทาให้เสียเวลาการทางานของระบบคอมพิวเตอร์ แอพพลิเคชันประเภทนี้มีมานานพร้อม ๆ กับการเริ่มใช้คอมพิวเตอร์ เนื่องจากแอพพลิเคชันประเภทนี้มิได้ออกแบบเพื่อการทำลาย
- - โฮแอคซ์(Hoaxes) โดยทั่วไปโฮแอคซ์(Hoaxes) หมายถึง โปรแกรมที่เขียนขึ้นเพื่อหลอกให้ผู้ใช้ทาบางอย่างให้ โดยโฮแอคซ์จะใช้เทคนิคทางด้านวิศวกรรมสังคม(Social Engineering) เพื่อหลอกให้ผู้ใช้งานคอมพิวเตอร์ทาบางอย่างให้
- - สแปม(Spam) คือ การส่งอีเมล์ยังผู้ใช้จานวนมาก โดยมีจุดประสงค์เพื่อการโฆษณาสินค้าหรือบริการ สแปมจัดอยู่ในประเภทสิ่งที่ก่อให้เกิดความรำคาญ

โปรแกรมที่ไม่จัดเป็นมัลแวร์

- - สปายแวร์(Spyware) บางทีก็รู้จักกันในชื่อ สปายบ็อท (Spybot) หรือ แทร็คกิ้งซอฟต์แวร์ (Tracking Software) สปายแวร์เป็นโปรแกรมที่ใช้บางอย่างเพื่อลวงตาแต่ทำกิจกรรมบางอย่างในเครื่องคอมพิวเตอร์ โดยที่ไม่ได้รับความยินยอมจากผู้ใช้เช่น การเก็บข้อมูลส่วนตัวของผู้ใช้ การปรับเปลี่ยนเซตติ้งของบราวเซอร์ ลดประสิทธิภาพโดยรวมของคอมพิวเตอร์ไปจนถึงการละเมิดสิทธิส่วนบุคคลของผู้ใช้
- - แอดแวร์ (Adware) เป็นโปรแกรมโฆษณาสินค้าซึ่งจะเปิดป๊อบอัพวินโดวส์ แอดแวร์ส่วนใหญ่จะรวมอยู่ในแอพพลิเคชันที่ให้ใช้ได้ฟรีและจะฝังตัวอยู่ เนื่องจากได้รับความยินยอมจากผู้ใช้ แอดแวร์จะติดตั้งก็ต่อเมื่อผู้ใช้ได้ยินยอมตามข้อตกลงเกี่ยวกับลิขสิทธิ์

โปรแกรมที่ไม่จัดเป็นมัลแวร์

- อินเทอร์เน็ตคุกกี้ (Internet Cookies) คือ เท็กซ์ไฟล์ที่เก็บไว้ที่เครื่องคอมพิวเตอร์ของผู้ใช้โดยเว็บไซต์ที่เข้าไปเยี่ยมชมคุกกี้จะเก็บข้อมูลบางอย่างที่เว็บไซต์นั้นใช้เมื่อครั้งหน้าที่ผู้ใช้เข้าไปเยี่ยมชมอีกครั้ง ซึ่งส่วนใหญ่จะเป็นข้อมูลที่ใช้บอกว่าเป็นผู้ใช้คนนี้ นอกจากนี้ในไฟล์อาจมีข้อมูลอื่นๆ ก็ได้



มัลแวร์ (Malware) คุณสมบัติของมัลแวร์

- คุณสมบัติของเป้าหมาย ประเภทของอุปกรณ์, ระบบปฏิบัติการ, แอพพลิเคชัน
- พาหะนำมัลแวร์ Executable File, Script, Boot Sector
- กลไกการแพร่กระจาย Removable Media, Network Shares
- การจุดชนวน Manual Execution, Automatic Execution
- กลไกการป้องกันตัวเอง Stealth, Encryption

มัลแวร์ (Malware)
เทคนิคการตรวจจับไวรัส

- *การสแกนหาซิกเนเจอร์ (Signature Scanning)* เปรียบเทียบฐานข้อมูลกับไฟล์ที่กำลังสแกนเพื่อจะตัดสินว่าไฟล์นั้นติดไวรัสหรือไม่
- *การสแกนหาคุณลักษณะเฉพาะ* เทคนิคประเภทนี้จะตรวจพบทั้งมัลแวร์เก่าและใหม่ โดยการค้นหาคุณลักษณะทั่วไปของมัลแวร์
  - *การแจ้งเตือนผิดๆ (False Positive)*
  - *การสแกนที่ช้า*
- *การมอนิเตอร์พฤติกรรม* เทคนิคประเภทนี้จะเน้นที่พฤติกรรมของการโจมตี

มัลแวร์ (Malware)
อาการของเครื่องที่ติดไวรัสหรือมัลแวร์

- เครื่องทำงานช้าลง
- เครื่องแฮ้งค้าง หรือหยุดทำงานโดยไม่ทราบสาเหตุ
- ขนาดของหน่วยความจำที่เหลืออยู่ลดน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
- ซีพียูถูกเรียกใช้งานมากเกินกว่า 90 เปอร์เซ็นต์ขึ้นไปตลอดเวลา
- อุณหภูมิสูงเนื่องจากการประมวลผลตลอดเวลา
- แป้นพิมพ์ทางานผิดปกติหรือไม่ทำงานเลย
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่หายไปเฉยๆ
- พบไฟล์มีชื่อแปลกๆที่ไม่เคยพบมาก่อนอยู่ในโฟลเดอร์ต่าง ๆ
- ขนาดของไฟล์โปรแกรมหรือไฟล์งานใหญ่ขึ้น
- หน่วยความจำชัวร์คราวเต็ม

มัลแวร์ (Malware)
สาเหตุที่เครื่องติดไวรัสหรือมัลแวร์

- จากทางแผ่นดิสก์หรือแฟลชไดร์ฟ
- จากทางอีเมล์
- จากการเข้าไปเปิดเว็บที่มีสคริปต์มุ่งร้าย (Malicious Script)
- จากการดาวโหลดไฟล์
- จากช่องโหว่ (Vulnerability)
- จากการเล่นหรือรับไฟล์
- ลิ้งค์จาก SMS
- แอปพลิเคชั่นที่ไม่มีที่มา

มัลแวร์ (Malware)
การป้องกันไวรัส

-การป้องกันไวรัสที่เครื่องไคลเอนท์

การลบโปรแกรมที่ไม่ได้ใช้งาน, การอัพเดตแพตซ์

การติดตั้งโฮสต์เบสไฟร์วอลล์, การติดตั้งซอฟต์แวร์ป้องกันไวรัส

-การป้องกันไวรัสที่เซิร์ฟเวอร์

อัพเดตซีเคียวริตี้แพตซ์, ไม่ติดตั้งโปรแกรมหรือเซอร์วิสที่ไม่จำเป็น

การป้องกันไวรัสเมล์เซิร์ฟเวอร์, การป้องกันไวรัสที่ดาต้าเบสเซิร์ฟเวอร์

-การป้องกันไวรัสระดับเครือข่าย

การติดตั้ง IDS, การกรองข้อมูลในระดับแอพพลิเคชัน

การบล๊อคเว็บไซต์, การสร้างเครือข่ายกักกันเฉพาะ

มัลแวร์ (Malware)
สรุป

การป้องกันไวรัสที่จะให้ได้ผลนั้นไม่ใช่แค่การติดตั้งโปรแกรมป้องกันไวรัสเท่านั้น จากตัวอย่างของเหตุการณ์ในการโจมตีหลายเหตุการณ์ล่าสุดนั้นได้พิสูจน์ให้เห็นแล้วการป้องกันไวรัสนั้นต้องทำแบบเป็นระบบและต่อเนื่อง คอมพิวเตอร์ไวรัสนั้นมีการพัฒนาตัวเองและปรับเปลี่ยนเทคนิคในการโจมตีเรื่อย ๆ

องค์กรควรทบทวนมาตรการป้องกันไวรัสเป็นประจำและปรับปรุงและปรับเปลี่ยนเมื่อจำเป็น การป้องกันไวรัสทุก ๆ ด้านมีความสำคัญทั้งหมด

Reference

- http://www.cisco.com . วิธีสืบค้นวัสดุสารสนเทศ. [ออนไลน์]. เข้าถึงได้จาก : http อาจารย์ ธนัญชัย ตรีภาค สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons Inc, December 1995
- Security Focus
  - www.securityfocus.com