บทที่ 7 : การป้องกันไวรัส Part2

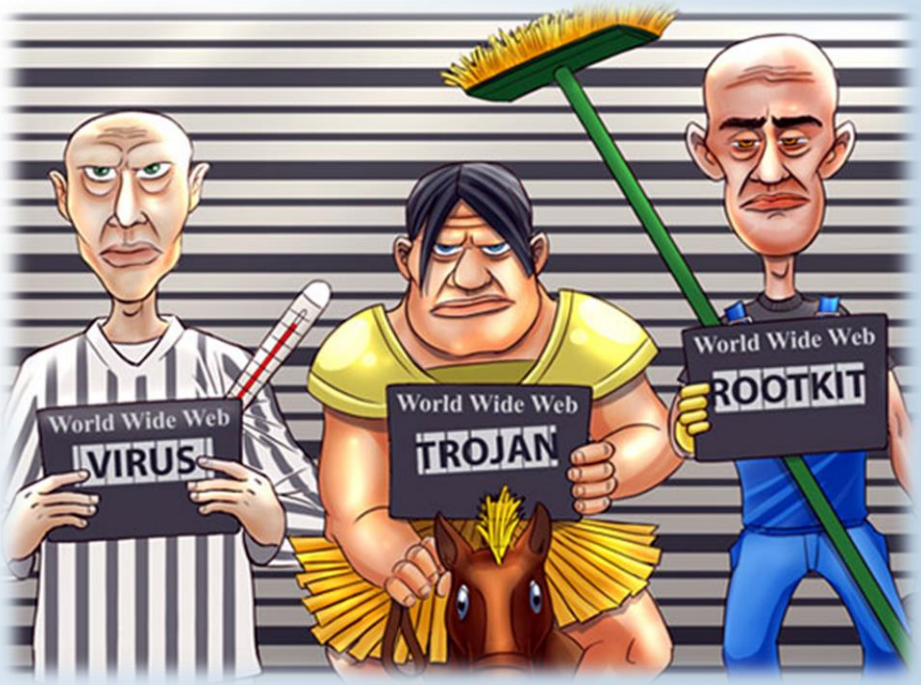
สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- คุณสมบัติของมัลแวร์
- เทคนิคการตรวจจับไวรัส
- วงจรชีวิตของมัลแวร์



คุณสมบัติของมัลแวร์

คุณสมบัติพื้นฐานของมัลแวร์มีดังต่อไปนี้

- คุณสมบัติของเป้าหมาย
- พาหะนำมัลแวร์
- กลไกในการแพร่กระจาย
- เพย์โหลด
- การจุดชนวน
- กลไกการป้องกันตัวเอง

คุณสมบัติของมัลแวร์

: คุณสมบัติของมัลแวร์

- **ประเภทของอุปกรณ์** เช่น คอมพิวเตอร์ PC, คอมพิวเตอร์ Mac, Mobile Phone เป็นต้น
- **ระบบปฏิบัติการ** มัลแวร์ส่วนมากจะสามารถรันได้เฉพาะกับระบบปฏิบัติการหนึ่งเท่านั้น เช่น Windows, Unix
- **แอพพลิเคชั่น** มัลแวร์บางตัวต้องอาศัยแอพพลิเคชั่นบางตัวเพื่อทำให้สามารติดมัลแวร์ได้ เช่น Adobe Flash Player เป็นต้น

คุณสมบัติของมัลแวร์

: พาหะนำมัลแวร์

- **Executable File** เป็นเป้าหมายที่คลาสสิค นามสกุลของไฟล์จะเป็น .exe, .com, .sys, .dll, .ovl, .ocx และ .prg
- **Script** ใช้ภาษาสคริปต์เพื่อรัน จะมีนามสกุล .vbs, .js, .wsh, .pl
- **Macro** เป็นภาษาสคริปต์ของแอพพลิเคชั่นบางตัว เช่น MS Office
- **Boot Sector** เป็นพื้นที่บางส่วนของฮาร์ดดิสก์, USB Flash Drive หรือ CD-ROM ซึ่งเป็นส่วนที่สามารถรันโค้ดสำหรับบู๊ตระบบได้

คุณสมบัติของมัลแวร์
: กลไกการแพร่กระจาย

- Removable Media
- Network Shares
- Network Scanning
- Peer-to-Peer Networks
- E-mail
- Remote Exploit

คุณสมบัติของมัลแวร์

: เพย์โหลด

เพย์โหลด คือ ส่วนที่ไวรัสใช้รันบนโฮสต์ เพื่อทำการโจมตี

- **Backdoor** เรียกอีกชื่อหนึ่งว่า Remote Access Trojan
- **Data Corruption and Deletion** เป็นการทำลายไฟล์ข้อมูล
- **Information Theft** ใช้ขโมยข้อมูลสำคัญจากระบบ
- **Denial of Service** (DoS) และ **Distributed Denial of Service** (DDoS)

คุณสมบัติของมัลแวร์

: เพย์โหลด [2]

- **System Shutdown** ทำให้เครื่องหรือระบบที่ถูกโจมตีชัตดาวน์ลง
- **Bandwidth Flooding** มัลแวร์จะส่งแพ็คเก็ตจนแบนด์วิดธ์เต็ม ทำให้ผู้ใช้ทั่วไปไม่สามารถใช้งานระบบได้
- **Service Disruption** ทำให้เครื่องที่ถูกโจมตีไม่สามารถใช้งาน DNS ได้ ส่งผลให้บริการ เช่น เว็บ เมล ไม่สามารถใช้งานได้

คุณสมบัติของมัลแวร์

: การจุดชนวน

- **Manual Execution** คือการที่ผู้ใช้รันโปรแกรมโดยตรงซึ่งอาจกระทำโดยไม่รู้ตัวหรือถูกหลอกให้รันโปรแกรม
- **Semi-Automation Execution** เริ่มจากผู้ใช้รันโปรแกรมเอง หลังจากนั้นโปรแกรมจะทำงานอัตโนมัติ
- **Automatic Execution** มัลแวร์ประเภทนี้จะรันตัวเองได้โดยไม่ต้องอาศัยผู้ใช้เลย

คุณสมบัติของมัลแวร์

: การจุดชนวน [2]

- Time Bomb มัลแวร์จะรันหลังจากติดไวรัสในช่วงเวลาใดช่วงเวลาหนึ่ง หรือวันใดวันหนึ่ง
- Conditional หรือ Logic Bomb เป็นการจุดชนวนโดยเริ่มเมื่อสภาพแวดล้อมตรงตามเงื่อนไข เช่น เมื่อเปิดบางโปรแกรม กดคีย์บอร์ดบางคีย์

คุณสมบัติของมัลแวร์

: กลไกการป้องกันตัวเอง

- Armor มัลแวร์จะพยายามและป้องกันการวิเคราะห์โค้ดจากโปรแกรมดีบักเกอร์ เช่น การเพิ่มโค้ดให้วิเคราะห์ยาก
- Stealth การพรางตัว เช่น มัลแวร์จะบันทึกไฟล์ที่ยังไม่ติดไวรัสในบู๊ตเซกเตอร์ เพื่อป้องกันการตรวจพบ
- Encryption มัลแวร์จะเข้ารหัสตัวเองและเพย์โหลด และเปลี่ยนคีย์ในการเข้ารหัสและถอดรหัสทุกๆการก็อปปี้ มีสองแบบคือ การเข้ารหัสแบบจำกัดจำนวนครั้ง และการเข้ารหัสแบบไม่จำกัดจำนวนครั้ง

เทคนิคการตรวจจับไวรัส

เทคนิคการตรวจจับไวรัสที่ได้ผลประกอบไปด้วย

- **การสแกนหาซิกเนเจอร์**
- **การสแกนหาคุณลักษณะเฉพาะ**
- **การมอนิเตอร์พฤติกรรม**

เทคนิคการตรวจจับไวรัส

: การสแกนหาซิกเนเจอร์

- เป็นวิธีที่โปรแกรมป้องกันไวรัสส่วนใหญ่ใช้
- วิธีการคือการสแกนไฟล์ทั้งในฮาร์ดดิสก์และเมมโมรี เพื่อค้นหาโค้ดที่อาจเป็นส่วนหนึ่งของมัลแวร์ โดยนำไฟล์ที่สแกนไปเทียบกับซิกเนเจอร์
- ปัญหาของวิธีนี้คือไวรัสจะแพร่กระจายไปก่อนที่โปรแกรมป้องกันไวรัสจะอัพเดตซิกเนเจอร์

เทคนิคการตรวจจับไวรัส

: การสแกนหาคุณลักษณะเฉพาะ

- วิธีนี้สามารถตรวจพบได้ทั้งมัลแวร์เก่าและใหม่ โดยการค้นหาคุณลักษณะทั่วไปของมัลแวร์
- ปัญหาของวิธีนี้ คือ
  - **การแจ้งเตือนผิด** (False Positive) โปรแกรมป้องกันไวรัสอาจรายงานว่าโปรแกรมทั่วไปที่คุณลักษณะคล้ายไวรัสเป็นไวรัสได้
  - **การสแกนที่ช้า** เพราะวิธีการสแกนมีความซับซ้อน
  - **ไวรัสอาจมีคุณลักษณะใหม่** ไวรัสบางตัวอาจมีคุณลักษณะพิเศษที่ไม่เคยรู้จักมาก่อน

เทคนิคการตรวจจับไวรัส

: การมอนิเตอร์พฤติกรรม

- จะเน้นความสนใจเฉพาะพฤติกรรมการโจมตีของไวรัสมากกว่าลักษณะโค้ดของไวรัส
- เช่น บางแอพพลิเคชั่นจะพยายามเปิดพอร์ตบางพอร์ตที่ไม่ได้รับอนุญาต โปรแกรมป้องกันไวรัสจะคาดเดาว่าการเปิดพอร์ตนั้นเป็นพฤติกรรมของไวรัส และพยายามแจ้งเตือนหรือสกัดการโจมตี

วงจรชีวิตของมัลแวร์

1. การค้นพบช่องโหว่
2. การพัฒนา
3. การแพร่ระบาด
4. การทำลาย
5. การตรวจพบและแจ้งเตือน
6. การตรวจจับ
7. การป้องกันและกำจัด