บทที่ 6 : การป้องกันไวรัส Part1

สธ412 ความมั่นคงของระบบสารสนเทศ

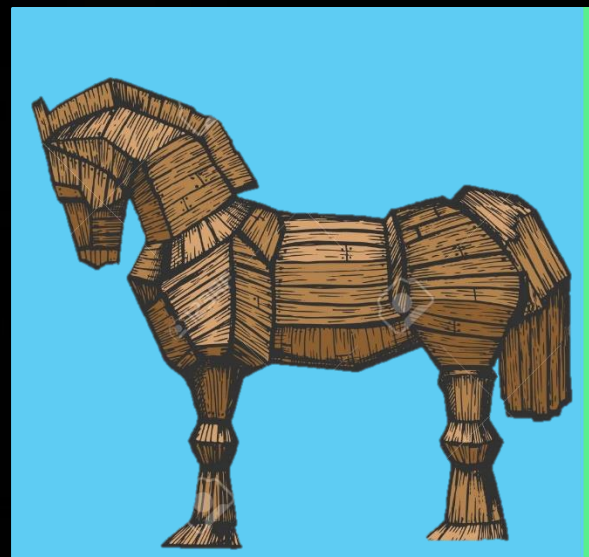
อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

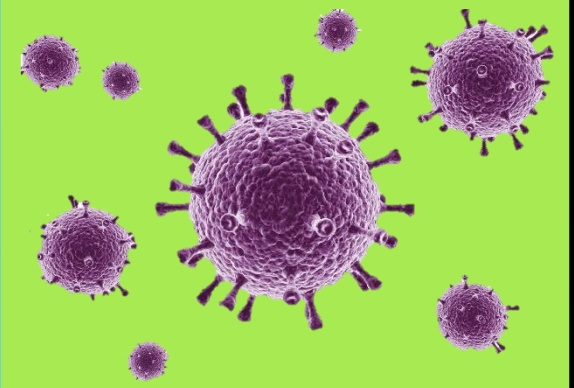
- ประเภทของมัลแวร์
- คุณสมบัติของมัลแวร์
- วงจรชีวิตของมัลแวร์

ประเภทของมัลแวร์



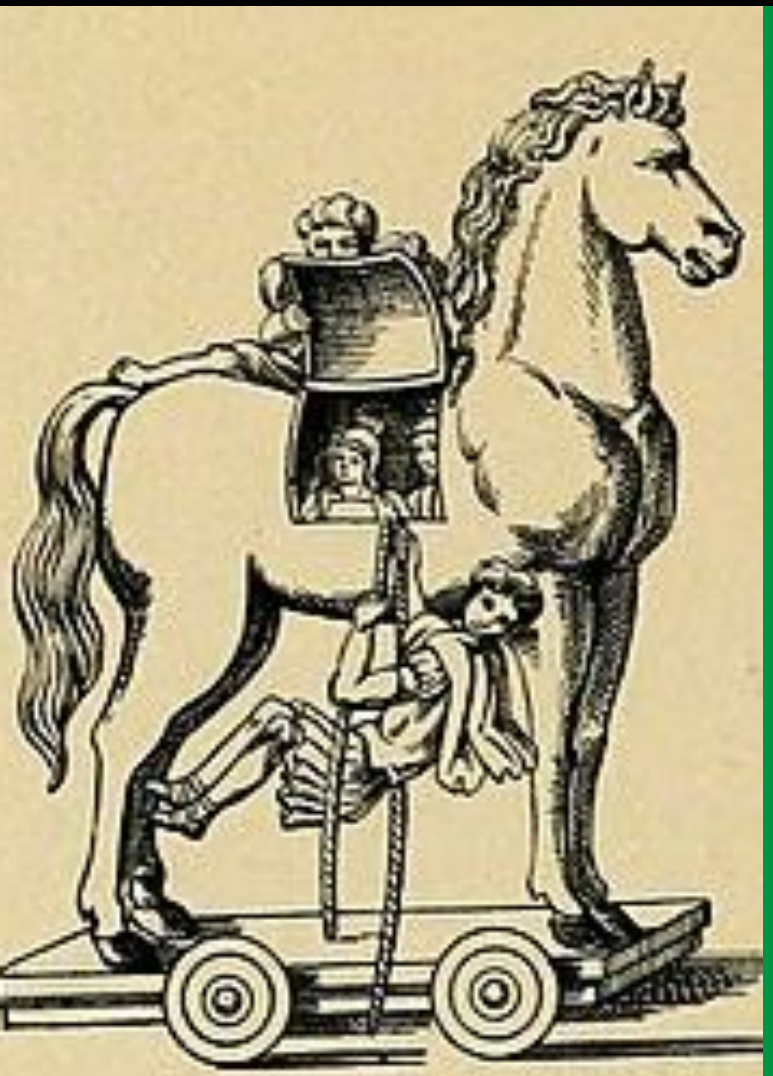
Trojan Horse

Worm



Virus

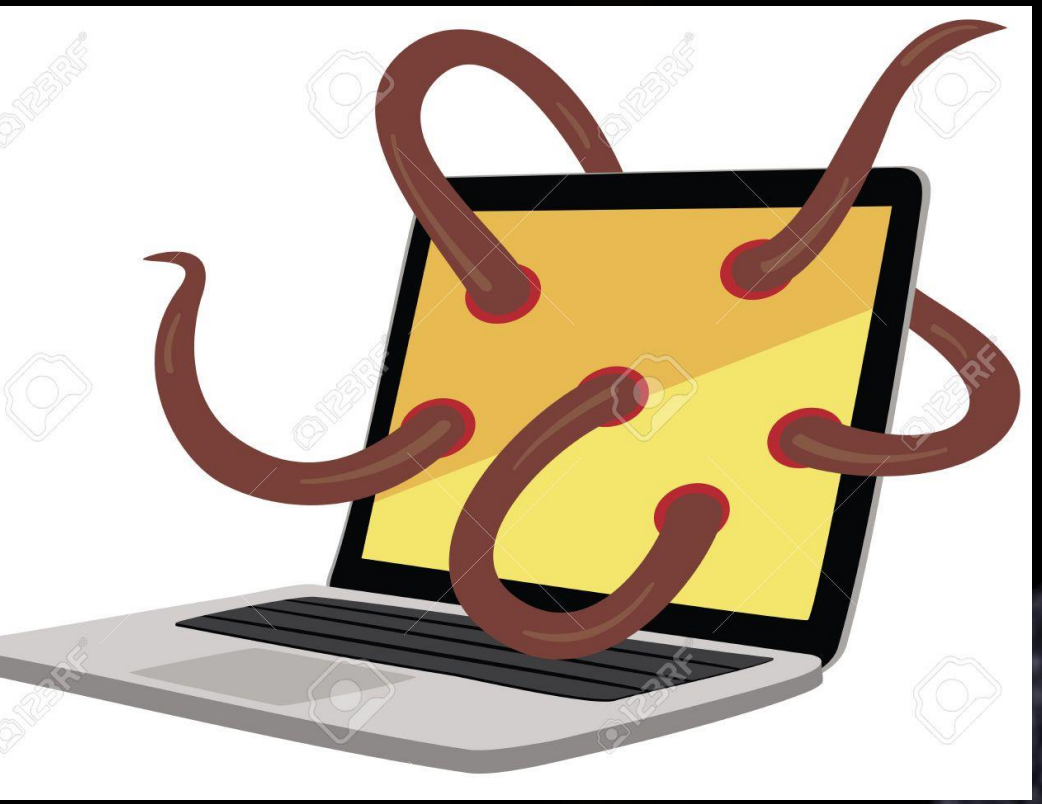
Trojan Horse



มักแฝงมากับโปรแกรมพาหะ หรือช่องทางต่าง ๆ บนอินเทอร์เน็ต ไม่สามารถแพร่กระจายตัวเองได้ มี 3 รูปแบบ คือ

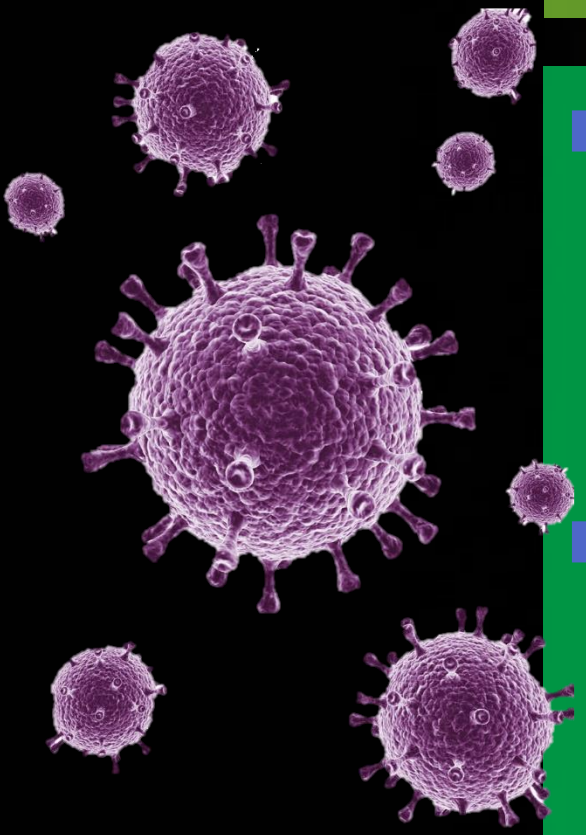
- RAT (Remote Access Trojan)
- Backdoor
- Rootkits

Worm



- เป็นมัลแวร์ที่ก็อปปี้ตัวเองเพื่อแพร่กระจายไปในเครือข่ายได้ โดยไม่ต้องอาศัยพาหะ โดยส่วนมากจะอาศัยช่องโหว่ของระบบ

Virus



- เป็นมัลแวร์ที่ต้องอาศัยพาหะในการแพร่กระจาย เช่น ไฟล์เอกสาร หรือในบูตเซ็กเตอร์ของฮาร์ดดิสก์หรือ USB Drive
- เน้นทำให้ไฟล์ใช้งานไม่ได้ หรือพยายามใช้ทรัพยากรของระบบ

Ransomware

- มัลแวร์เรียกค่าไถ่ ใช้วิธีการเข้ารหัสไฟล์ทั้งหมดในเครื่องเหยื่อ (ปกติจะใช้ Public Key Cryptography) แล้วแสดงข้อความเพื่อเรียกค่าไถ่เป็นสกุลเงินคริปโตเพื่อแลกกับการถอดรหัส
- สร้างความเสียหายบนโลกไซเบอร์อย่างมหาศาล

ซอฟต์แวร์อันตราย แต่ไม่จัดเป็นมัลแวร์

- Joke Application – App ที่ทำเอาฮา
- Hoaxes – การปล่อยข่าวลวง
- Scams – การหลอกลวงผู้ใช้
- Spam – การส่งเมลหรือข้อความจำนวนมาก
- Spyware – เฝ้าติดตามพฤติกรรมผู้ใช้
- Adware – แสดงโฆษณาที่น่ารำคาญ

คุณสมบัติของมัลแวร์

คุณสมบัติพื้นฐานของมัลแวร์มีดังต่อไปนี้

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

คุณสมบัติของเป้าหมาย

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

พาหะนำมัลแวร์

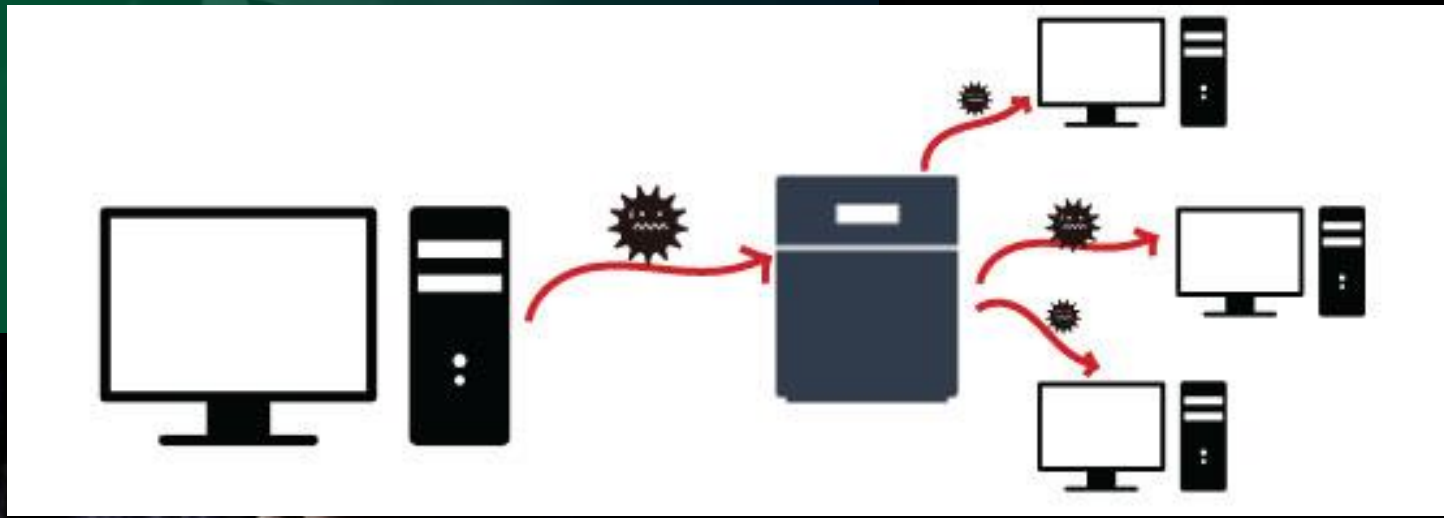
- **Executable File** เป็นเป้าหมายที่คลาสสิค นามสกุลของไฟล์จะเป็น .exe, .com, .sys, .dll, .ovl, .ocx และ .prg
- **Script** ใช้ภาษาสคริปต์เพื่อรัน จะมีนามสกุล .vbs, .js, .wsh, .pl
- **Macro** เป็นภาษาสคริปต์ของแอพพลิเคชั่นบางตัว เช่น MS Office
- **Boot Sector** เป็นพื้นที่บางส่วนของฮาร์ดดิสก์, USB Flash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

กลไกการแพร่กระจาย

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

สื่อที่ใช้แพร่ระบาด

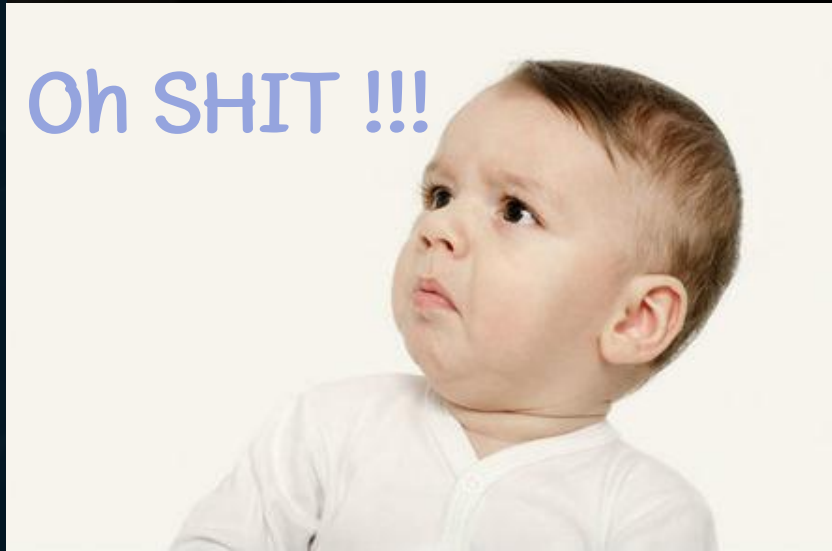
- เครือข่ายภายนอก
- คอมพิวเตอร์ของแขกที่มาเยือน
- Execute File
- Document File
- E-mail
- Removable Media



เพย์โหลด

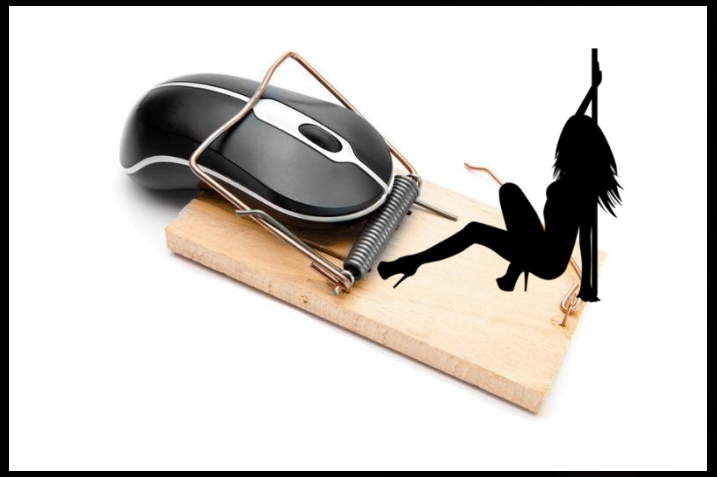
เพย์โหลด คือ ส่วนที่ไวรัสใช้รันบนโฮสต์ เพื่อทำการโจมตี มีรูปแบบดังนี้

- Backdoor
- Data Corruption and Deletion
- Information Theft ใช้ขโมยข้อมูลสำคัญจากระบบ
- Denial of Service (DoS) และ Distributed Denial of Service (DDoS)



เพย์โหลด

- System Shutdown
- Bandwidth Flooding
- Service Disruption เช่นการโจมตี DNS Server ทำให้ไม่สามารถใช้งาน DNS ได้ ส่งผลให้บริการ เช่น เว็บ เมล ไม่สามารถใช้งานได้



การจุดชนวน

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

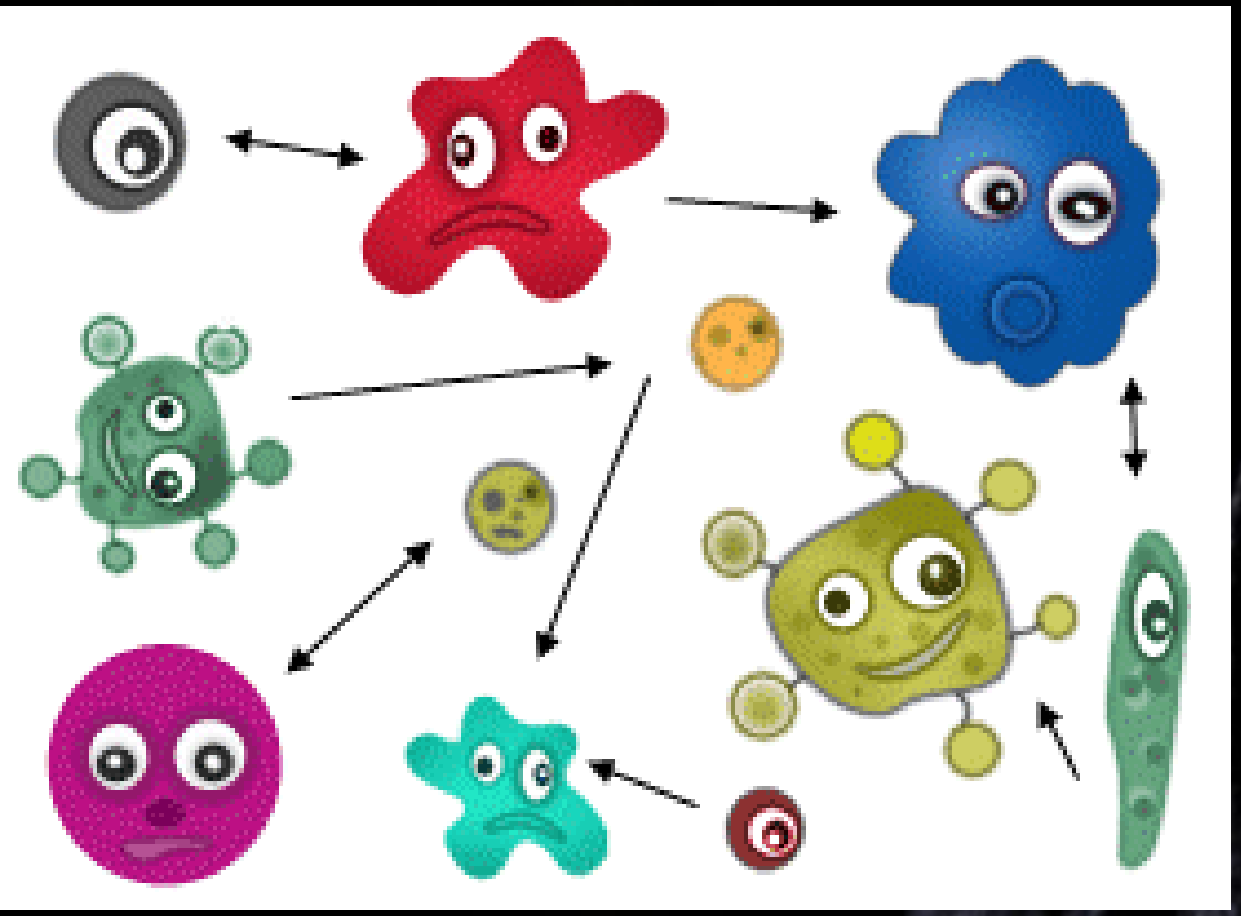
การจุดชนวน

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

กลไกการป้องกันตัวเองของมัลแวร์

- **Armor** เป็นการป้องกันการวิเคราะห์โค้ดของมัลแวร์ เช่น การเพิ่มโค้ดให้วิเคราะห์ยาก
- **Stealth** การอำพรางตัว เช่น มัลแวร์จะบันทึกไฟล์ที่ยังไม่ติดไวรัสในบู๊ตเซกเตอร์เพื่อป้องกันการตรวจพบ
- **Encryption** มัลแวร์จะเข้ารหัสตัวเองและเพย์โหลด

กลไกการป้องกันตัวเองของมัลแวร์



- **Oligomorphic** ใช้เทคนิคการเข้ารหัส แต่เปลี่ยนฟังก์ชั่นในการเข้ารหัสสลับไป-มาระหว่างการแพร่กระจาย
- Polymorphic ใช้เทคนิคการเข้ารหัสที่เปลี่ยนแปลงไปทุกครั้ง ไม่จำกัดจำนวนครั้ง

วงจรชีวิตของมัลแวร์

START HERE

- ค้นพบช่องโหว่
- พัฒนามัลแวร์
- แพร่ระบาด
- ทำลายเป้าหมาย
- ตรวจพบและแจ้งเตือน
- ตรวจจับ
- ป้องกันและกำจัด