บทที่ 6 : การป้องกันไวรัส Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

- แนวทางการป้องกันมัลแวร์
- เทคนิคการตรวจจับมัลแวร์
- การป้องกันมัลแวร์ที่ไคลเอนต์

แนวทางการป้องกันมัลแวร์

Physical

Client	Server	Network
• Data • App • Host	• Data • App • Host	• Internal • Perimeter

Policies, Procedures, Awareness

Data Security

- การเข้าถึงข้อมูลต่าง ๆ เช่น ข้อมูลคอนฟิก ข้อมูลองค์กร ข้อมูลที่อ่อนไหว ข้อมูลส่วนตัว
- เป็นความเสี่ยงที่แฮกเกอร์ต้องการนำไปใช้ประโยชน์

Application Security

อาจเจาะผ่านช่องโหว่ของแอพฯ หรือพอร์ตที่แอพฯเปิดให้บริการ

Host Security

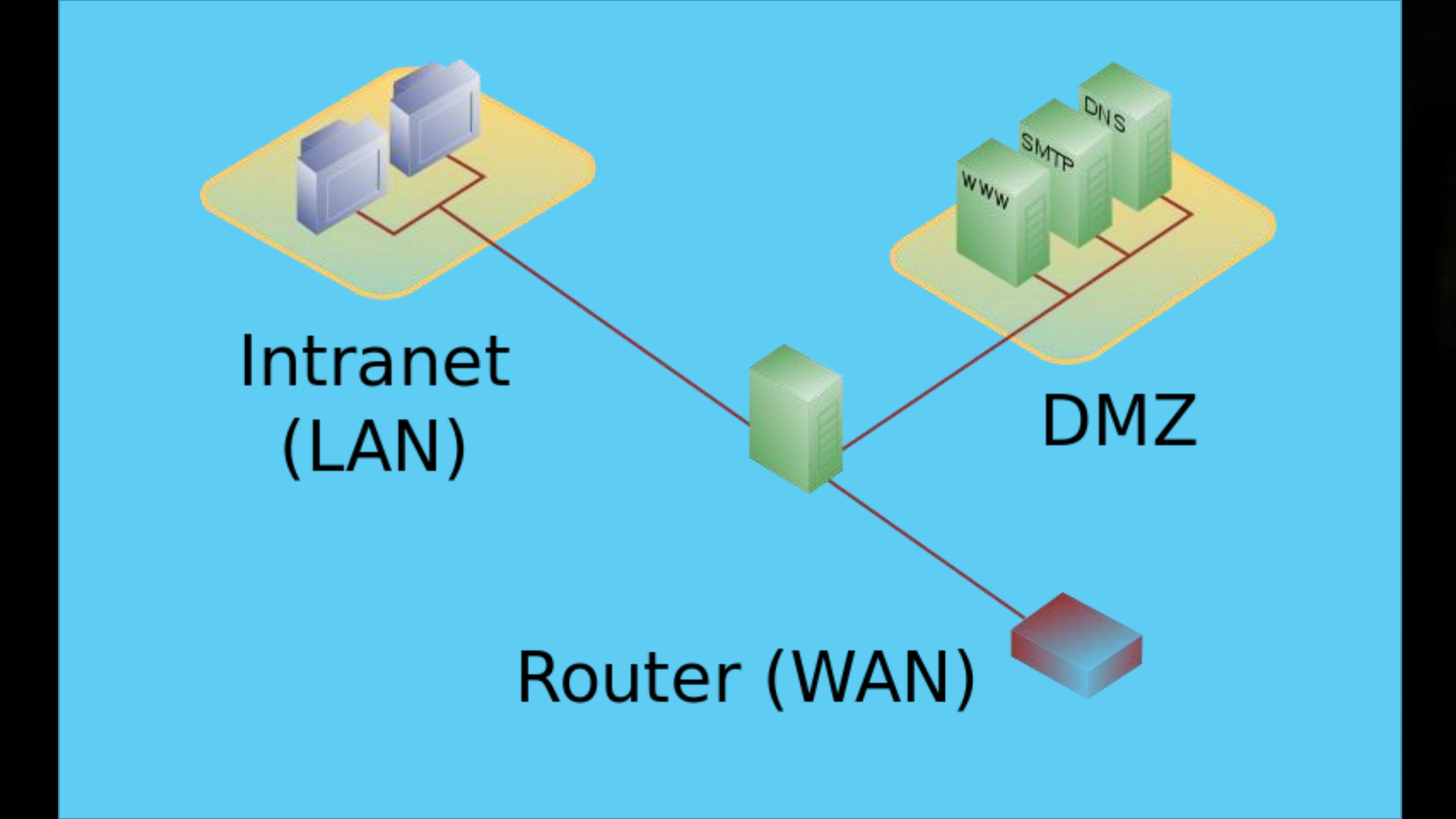
- การโจมตีอาจอาศัยช่องโหว่ของโฮสต์ (OS หรือ Hardware)
- การป้องกันที่ดีที่สุดคือการอัพเดตแพทช์

Internal Network Security

- ความเสี่ยงจากเครือข่ายภายในองค์กร
- การเชื่อมต่อภายในเครือข่ายเป็นสิ่งที่ต้องคำนึงถึงความปลอดภัย

Perimeter Network Security

- Perimeter Network หรือที่เรียกว่า DMZ (Demilitarized Zone) คือเน็ตเวิร์คขององค์กรที่ต้องติดต่อกับเน็ตเวิร์คภายนอก
- ควรคำนึงในการเปิดพอร์ตให้บริการบางพอร์ตที่อาจเป็นช่องทางการโจมตีได้


Intranet
(LAN)
WWW
SMTP
DNS
DMZ
Router (WAN)

Physical Security

- คือการที่ผู้โจมตีอาจเข้าถึงอุปกรณ์ได้โดยตรง หรือเป็นการโจมตีโดยใช้ Removable Media

Policies, Procedure, Awareness

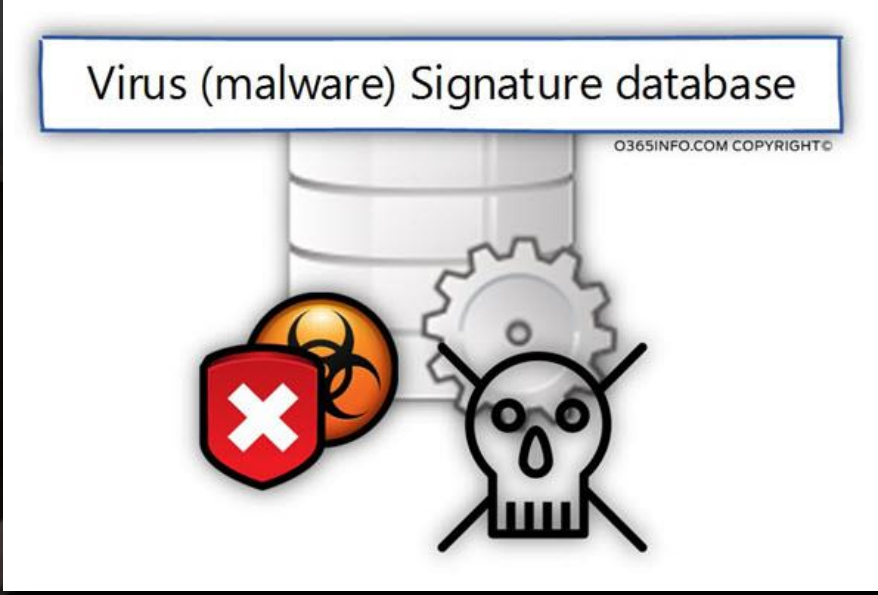
- นโยบาย ระเบียบปฏิบัติ และข้อควรระวัง เป็นเลเยอร์ที่องค์กรควรตระหนักถึงมากที่สุด
- ควรสร้างความตระหนักและให้ผู้ใช้เกิดความสนใจในความปลอดภัยไซเบอร์

เทคนิคการตรวจจับมัลแวร์

- การสแกนหาซิกเนเจอร์
- การสแกนหาคุณลักษณะเฉพาะ
- การมอนิเตอร์พฤติกรรม

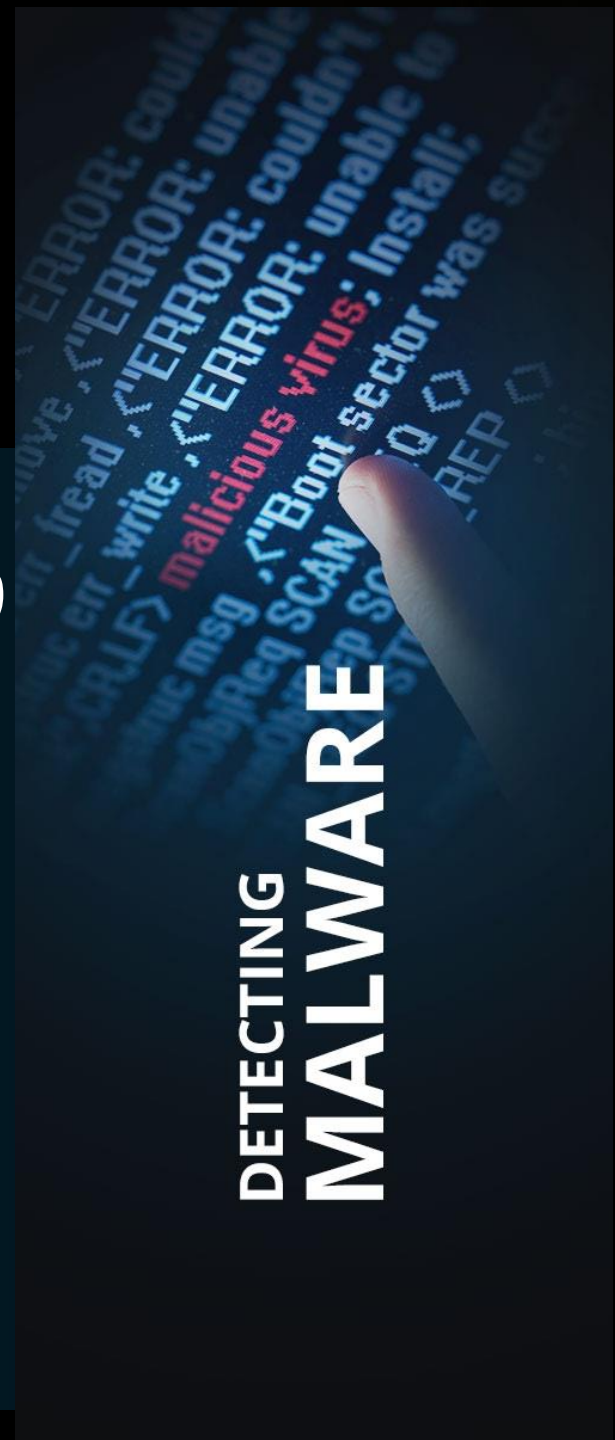
การสแกนหาซิกเนเจอร์

- เป็นวิธีที่โปรแกรมป้องกันมัลแวร์ส่วนใหญ่ใช้
- วิธีการคือการสแกนไฟล์ทั้งในสตอเรจและเมมโมรี เพื่อค้นหาโค้ดที่อาจเป็นส่วนหนึ่งของมัลแวร์ โดยนำไฟล์ที่สแกนไปเทียบกับฐานข้อมูลซิกเนเจอร์
- **ปัญหาของวิธีนี้คือมัลแวร์จะแพร่กระจายไปก่อนที่โปรแกรมป้องกันไวรัสจะอัพเดตซิกเนเจอร์เสมอ**



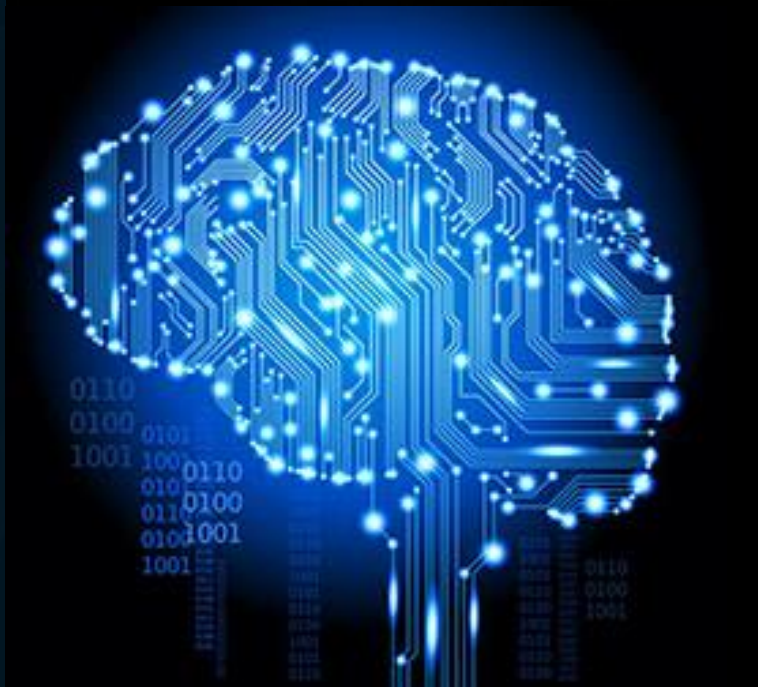
การสแกนหาคุณลักษณะเฉพาะ

- วิธีนี้สามารถตรวจพบได้ทั้งมัลแวร์เก่าและใหม่ โดยการค้นหาคุณลักษณะทั่วไปของมัลแวร์ โดยที่ไม่ต้องใช้ซิกเนเจอร์
- ปัญหาของวิธีนี้ คือ
  - **การแจ้งเตือนผิด** (False Positive) โปรแกรมป้องกันอาจรายงานว่าโปรแกรมทั่วไปที่คุณลักษณะคล้ายมัลแวร์เป็นมัลแวร์ได้
  - **การสแกนที่ช้า** เพราะวิธีการสแกนมีความซับซ้อน
  - **มัลแวร์อาจมีคุณลักษณะใหม่ที่ไม่เคยรู้จักมาก่อน**



การมอนิเตอร์พฤติกรรม

- จะเน้นความสนใจเฉพาะพฤติกรรมการโจมตีของไวรัสมากกว่าลักษณะ Source Code ของไวรัส
- เช่น บางแอพพลิเคชั่นจะพยายามเปิดพอร์ตบางพอร์ตที่ไม่ได้รับอนุญาต แอนตี้ไวรัสจะพยายามแจ้งเตือนหรือสกัดการโจมตี
- ปัจจุบันเริ่มมีการใช้เทคโนโลยี Artificial Intelligence (AI) และ Machine Learning เข้ามาช่วยในการมอนิเตอร์พฤติกรรม และสามารถเรียนรู้พฤติกรรมของมัลแวร์รูปแบบใหม่ๆได้

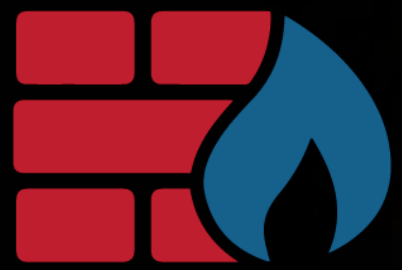


ระบบป้องกันมัลแวร์ในปัจจุบัน (Security Solution)
ส่วนใหญ่จะใช้ทั้ง 3 เทคนิคร่วมกันในการตรวจจับมัลแวร์

อย่างไรก็ตามเทคโนโลยีการตรวจจับมัลแวร์มักจะช้ากว่า
ผู้พัฒนามัลแวร์อยู่ก้าวหนึ่งเสมอ

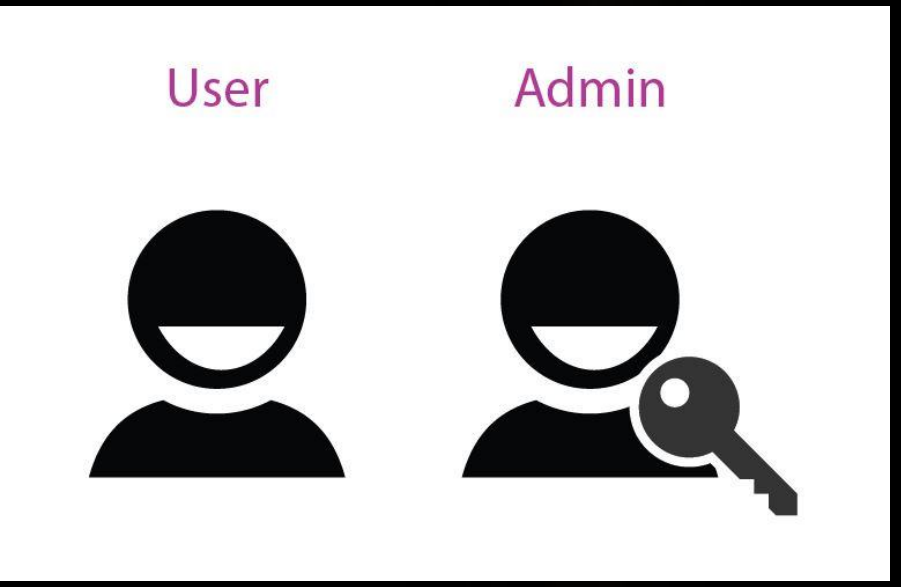
การป้องกันมัลแวร์ที่ไคลเอนต์

- การป้องกันไคลเอนต์จำเป็นต้องติดตั้งซอฟต์แวร์ป้องกันมัลแวร์เพื่อป้องกันและหยุดยั้งการแพร่กระจายไปยังเครื่องอื่นๆ ทั่วทั้งองค์กร
- หากมัลแวร์สามารถติดที่เครื่องไคลเอนต์ได้แล้ว ก็จะมีโอกาสผ่านการป้องกันอื่น ๆ และลุกลามไปยังระดับต่าง ๆ ได้



การป้องกันมัลแวร์ที่ไคลเอนต์

- **การลบโปรแกรมที่ไม่ได้ใช้งาน**
- **การอัพเดตแพตช์** ทั้งระบบปฏิบัติการและแอพพลิเคชั่น
- **การเปิดใช้งานโฮสต์เบสไฟร์วอลล์**
- **การติดตั้งซอฟต์แวร์ป้องกันมัลแวร์** โดยมีการอัพเดตฐานข้อมูลไวรัสเป็นประจำ



การป้องกันไวรัสที่ไคลเอนต์

- การสแกนหาจุดอ่อนของระบบ
- กำหนดสิทธิ์ของผู้ใช้งานระบบให้**น้อยที่สุด** โดยกำหนดสิทธิ์ให้เพียงพอต่อการทำงานประจำของแต่ละคน *ไม่ควรล็อกอินในฐานะผู้ดูแลระบบเพื่อทำงานทั่วไป*

How to do when infected with malware?

1. Disconnect from internet
2. Enter Safe Mode
3. Run Disk Cleanup
4. Run Antivirus
5. Download & Scan with Malwarebytes

If you cannot destroy it... you need to do this...

Reinstall Windows with clean drives

After that... you should have to change all of passwords and always keep your PC clean and up-to-date

Ref: https://www.pcworld.com/article/243818/how-to-remove-malware-from-your-windows-pc.html