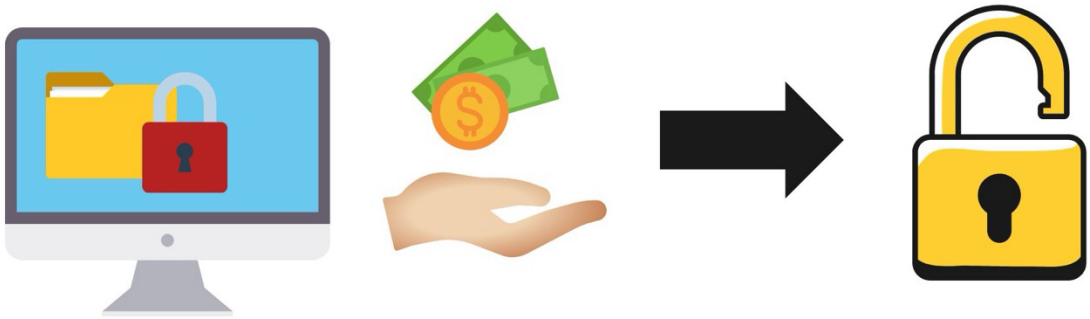
Ransomware

Ransomeware **ถูกออกแบบมาเพื่อทำการเข้ารหัสข้อมูลของผู้ใช้งานหรือระบบคอมพิวเตอร์** เช่น ทำให้ผู้ใช้ไม่สามารถเปิดไฟล์ที่สำคัญได้, ไม่สามารถใช้งาน Website ได้ เป็นต้น ซึ่งถ้าหากอยากถอดรหัสไฟล์นั้นๆ ก็จะต้องจ่ายเงินให้กับแฮคเกอร์เพื่อทำการถอดรหัส



ลักษณะของ Ransomware

1. **การเข้ารหัสข้อมูล** Ransomware ถูกออกแบบมาเพื่อทำการเข้ารหัสข้อมูลของผู้ใช้หรือระบบคอมพิวเตอร์ เช่น ไฟล์สำคัญ หรือเว็บไซต์ ทำให้ผู้ใช้ไม่สามารถเข้าถึงข้อมูลได้
2. **เรียกร้องค่าไถ่** เมื่อข้อมูลถูกเข้ารหัสแล้ว แฮกเกอร์จะเรียกร้องเงินค่าไถ่จากผู้ใช้เพื่อให้ถอดรหัสข้อมูลคืน โดยการจ่ายเงินจะเป็นวิธีเดียวในการกู้ข้อมูลกลับ
3. **ขโมยข้อมูลเพื่อประโยชน์ส่วนตัว** Ransomware อาจจะขโมยข้อมูลสำคัญ เช่น รหัสบัตรเครดิต หรือข้อมูลการเงิน และนำไปใช้ประโยชน์ในทางที่ผิด
4. **ใช้ข้อมูลไปในทางที่ไม่ถูกต้อง** แฮกเกอร์อาจใช้ข้อมูลที่ขโมยไปเพื่อสร้างบัตรเครดิตปลอม หรือยึดบัญชีผู้ใช้เช่น Facebook เพื่อนำไปใช้ในทางที่ไม่เหมาะสม
5. **ทำให้คอมพิวเตอร์ไม่สามารถใช้งานได้** บางประเภทของ Ransomware อาจทำให้คอมพิวเตอร์ไม่สามารถใช้งานได้ หรือทำให้ระบบหยุดทำงาน

ตัวอย่างของ Ransomware ที่มีชื่อเสียง

1. WannaCry (2017)

เป็น Ransomware ที่แพร่กระจายผ่านช่องโหว่ของโปรโตคอล SMB ในระบบ Windows (ช่องโหว่ EternalBlue) ทำให้ติดไวรัสคอมพิวเตอร์หลายแสนเครื่องทั่วโลก รวมถึงเครื่องในองค์กรใหญ่ๆ เช่น NHS ในสหราชอาณาจักร และบริษัทหลายแห่งในเกาหลีใต้

2. **NotPetya (2017)**

ออกแบบมาเพื่อทำลายข้อมูลจริงๆ มากกว่าการเรียกร้องค่าไถ่ มันแพร่กระจายผ่านช่องโหว่ของระบบ Windows และส่งผลกระทบต่อองค์กรในหลายประเทศ โดยเฉพาะในยูเครน

3. **Ryuk (2018)**

เป็น Ransomware ที่มักถูกใช้ในการโจมตีเป้าหมายองค์กรขนาดใหญ่ โดยจะล็อกข้อมูลสำคัญและขอเรียกร้องค่าไถ่ในจำนวนเงินสูง

วิธีรับมือกับ Ransomware

1. **ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส** การใช้โปรแกรมแอนตี้ไวรัสที่อัปเดตอย่างสม่ำเสมอจะช่วยป้องกัน Ransomware และมัลแวร์ชนิดอื่นๆ

2. **หลีกเลี่ยงการดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ** ควรดาวน์โหลดโปรแกรมหรือไฟล์จากแหล่งที่เชื่อถือได้เท่านั้น และหลีกเลี่ยงการเปิดไฟล์แนบจากอีเมลที่ไม่น่าเชื่อถือ

3. **สำรองข้อมูลสำคัญ** การสำรองข้อมูลอย่างสม่ำเสมอในที่เก็บข้อมูลภายนอกหรือในระบบคลาวด์จะช่วยป้องกันความสูญหายของข้อมูลในกรณีที่ติด Ransomware

4. **ไม่จ่ายเงินค่าไถ่** การจ่ายเงินให้กับแฮกเกอร์ไม่รับประกันว่าจะได้ข้อมูลคืน และอาจสนับสนุนการกระทำผิด ควรหลีกเลี่ยงการจ่ายเงิน

5. **อัปเดตระบบและซอฟต์แวร์** การอัปเดตระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอจะช่วยป้องกันช่องโหว่ที่อาจถูกแฮกเกอร์ใช้ประโยชน์จาก

6. **ใช้ไฟร์วอลล์** การใช้ไฟร์วอลล์จะช่วยป้องกันการเข้าถึงระบบจากภายนอกและตรวจจับพฤติกรรมที่อาจเป็นอันตราย