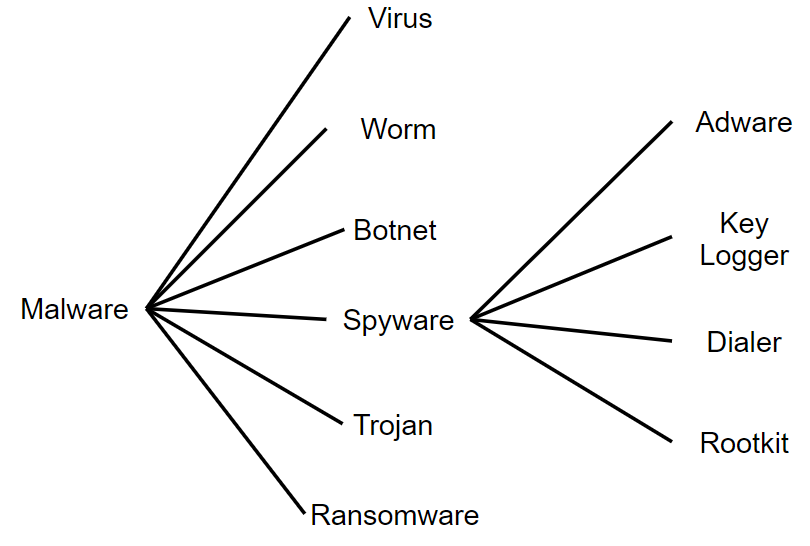
มัลแวร์

มัลแวร์ คือภัยคุกคามคอมพิวเตอร์ที่ถูกสร้างขึ้นจากโค้ดโปรแกรมตามจุดประสงค์ของผู้เขียน เช่น ทำให้ผู้ใช้รำคาญ ดักจับรหัสผ่าน และข้อมูลอื่น ๆ เรียกค่าไถ่ข้อมูล ฯลฯ โดยหลักการแล้วมีความสามารถในการทำสำเนาตัวเอง โดยแยกประเภทออกดังนี้



**Virus (ไวรัส)**

ไวรัสมีความสามารถในการก่อกวน รบกวน ทำให้เครื่องคอมพิวเตอร์ใช้การไม่ได้

**Worm (เวิร์ม)**

เวิร์มมีความสามารถในการรบกวนงานประมวลผล ทำให้เครื่องคอมพิวเตอร์ทำงานช้าลง

**Botnet (บอทเน็ต)**

บอทเน็ตเป็นการปล่อยโค้ดเข้ายึดเครื่องคอมพิวเตอร์ โดยมากมักจะเป็นเครื่องเซิฟเวอร์ เพื่อในเป็นฐานในการโจมตีเซิฟเวอร์อื่น ๆ ต่อไป

**Ransomware (แรมซัมแวร์)**

แรมซัมแวร์มีคุณสมบัติในการบุกยึดไฟล์ของเครื่องเป้าหมายโดยเข้ารหัสไฟล์ด้วยอัลกอริทึม AES ทำให้ยากต่อการถอดรหัสด้วยตัวเอง จึงจำเป็นต้องจ่ายค่าไถ่ด้วยเงินคริปโตหรือทิ้งไฟล์นั้น

แต่ในแรมซัมแวร์บางตัวก็มีกุญแจถอดรหัสหลุดมาบ้างบางรายอันเกิดจากการจับกุมของเจ้าหน้าที่รัฐ การใช้รหัสถอดไฟล์เดิมในหลาย ๆ เครื่อง และการยุบกลุ่ม

**Spyware (สปายแวร์)** เป็นกลุ่มของซอฟท์แวร์ที่เน้นการดักจับและขโมยข้อมูลจากเครื่องเป้าหมาย ได้แก่

**Adware (แอดแวร์)** คือโปรแกรมที่แสดงโฆษณารบกวนผู้ใช้งาน มักจะเป็นโปรแกรมป้องกันไวรัสปลอม โปรแกรมช่วยดาวน์โหลดฟรี

**Key Logger (คีย์ล็อกเกอร์)** มีความสามารถในการดักจับการกดคีย์บอร์ดของผู้ใช้งาน โดยเป้าหมายมักจะเป็นชื่อผู้ใช้งานและรหัสผ่าน

**Dialer (ไดอัลเลอร์)** มีคุณสมบัติในการเรียกการเชื่อมต่อโมเด็มเพื่อส่งข้อมูลกลับไปยังเครื่องของคนร้าย

**Rootkit (รูทคิท)** เป็นโปรแกรมที่มีขนาดเล็กมากปะปนไปกับซอฟท์แวร์ โดยมีวัตถุประสงค์ต่าง ๆ ได้แก่

* เน้นการโจมตีเครื่องเพื่อขโมยข้อมูล
* เพื่อตรวจจับลิขสิทธิ์ซอฟท์แวร์ สื่อบันเทิง

**ที่มาของมัลแวร์**

* จากเว็บไซต์, อีเมล
* จากสื่อที่เชื่อมต่อกับคอมพิวเตอร์ เช่น แฟลชไดร์ฟ
* ไฟล์ Excel ที่ฝังสคริปต์มาโครอันตรายไว้
* จากเครื่องอื่น ๆ ที่ติดมัลแวร์ในเครือข่าย
* จากโปรแกรมที่ถูกปรับแก้ลิขสิทธิ์ (แคร๊ก)
* จากการโจมตีของแฮกเกอร์
* 0day หมายถึง ช่องโหว่ของโปรแกรมที่ไม่ได้รับรายงาน แต่มีการโจมตีมาก่อนแล้ว

**การป้องกันมัลแวร์**

* ใช้โปรแกรมป้องกันมัลแวร์ที่มีประสิทธิภาพ
* ใช้ซอฟท์แวร์ลิขสิทธิ์แท้ หรือใช้ซอฟท์แวร์ประเภทโอเพ่นซอร์สทดแทน
* หมั่นอัพเดทซอฟท์แวร์ให้ทันสมัยอยู่เสมอ
* ตรวจสอบที่มาของเว็บไซต์ก่อนคลิกเสมอ
* สำรองข้อมูลลงในสื่ออื่นที่ไม่เชื่อมต่อตลอดเวลา
* เปลี่ยนสมาร์ทโฟนหากไม่ได้รับอัพเดทเป็นเวลานาน
* ผู้ดูแลระบบควรตรวจหาช่องโหว่อยู่เสมอ