Malware and Protection

กล่าวนำ

ไวรัส (Virus) หมายถึง โปรแกรมที่ทำลายระบบคอมพิวเตอร์ โดยจะแพร่กระจายไปยังไฟล์อื่นๆที่อยู่ในเครื่องเดียวกัน ไวรัสสามารถทำลายเครื่องได้ตั้งแต่ลบไฟล์ทั้งหมดที่อยู่ในฮาร์ดดิสก์ไปจนถึงเป็นแค่โปรแกรมที่สร้างความรำคาญให้กับผู้ใช้เครือข่าย เช่น แค่เปิดวินโดวส์แล้วเปิดป็อปอัพเพื่อแสดงข้อความบางอย่าง โดยธรรมชาติแล้วไวรัสไม่สามารถที่จะแพร่กระจายไปยังเครื่องอื่นๆ ได้ตัวตัวเอง แต่การแพร่กระจายไปยังเครื่องอื่นต้องอาศัยโปรแกรมอื่นหรือมนุษย์ เช่น การแชร์ไฟล์โดยใช้ Flash Dive เป็นต้น และไวรัสนั้นไม่สามารถรันได้ด้วยตัวเอง ต้องอาศัยคนเปิดไฟล์ที่ติดไวรัสนั้นจึงจะทำงานได้

วิวัฒนาการของไวรัสคอมพิวเตอร์

โปรแกรมที่สามารถสำเนาตัวเองได้เกิดขึ้น เป็นครั้งแรกในปี พ.ศ.2526 โดย ดร.เฟรดเดอริก โคเฮน นักวิจัยของมหาวิทยาลัยเพนซิลวาเนีย สหรัฐอเมริกา ได้ทำการศึกษาโปรแกรมลักษณะนี้และได้ตั้ง ชื่อว่า "ไวรัส" แต่ไวรัสที่แพร่ระบาดและสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ตามที่มี การบันทึกไว้ครั้งแรกเมื่อปี พ.ศ. 2529 ด้วยผลงานของไวรัสที่ชื่อ "เบรน (Brain)" ซึ่งเขียนขึ้น โดยโปรแกรมเมอร์สองพี่น้องชาวปากีสถานชื่อ อัมจาด (Amjad) และ เบซิท (Basit) เพื่อป้องกันการคัดลอกทำสำเนาโปรแกรมของพวกเขาโดยไม่จ่ายเงิน โดยทั้ง 2 คนนี้ยังได้เปิดร้านขายผลิตภัณฑ์คอมพิวเตอร์อยู่ทีเมือง Lahore ประเทศปากีสถาน สินค้าสวนใหญ่ที่สองพี่น้องนี้ขาย ก็คือ Software (โปรแกรม) ต่างๆ ที่เขาทำการ Copy ขาย ในราคาที่ถูกมากๆ พร้อมทั้งแอบปล่อยไวรัสเบรนไปกับแผ่นโปรแกรมเหล่านั้นด้วย และเนื่องจากการที่ประเทศปากีสถานไม่มีกฎหมายคุ้มครองลิขสิทธิ์ Software จึงทำให้กิจการของสองพี่น้องทำดำเนินไปได้อย่างดี โดยมีผู้นิยมซื้อโปรแกรมเหล่านี้ไ ปใช้จำนวนมาก ทั้งที่ชาวปากีสถานเองและชาวต่างประเทศที่เดินทางไปท่องเที่ยว ทำให้ไวรัสเบรนระบาดออกไปอย่างรวดเร็ว ทั่วโลกไวรัสคอมพิวเตอร์ในยุคแรกๆ จะระบาดโดยการสำเนาซอฟท์แวร์เถื่อนหรือซอฟท์แวร์ละเมิดลิขสิทธิ์ที่มี โปรแกรมไวรัสคอมพิวเตอร์ติดอยู่ด้วยการใช้แผ่น FLOPPY DISK หรือซีดีรอม แต่ในปัจจุบันเนื่องจากการเติบโตของเครือข่ายคอมพิวเตอร์ทำให้ไวรัสยุคหลังๆ มีความสามารถในการทำสำเนาคัดลอกและแพร่กระจายตัวเองได้มากขึ้นรวมทั้ง มีความรุนแรงมากกว่าเดิมในปัจจุบันนี้พบว่ามีมากกว่า 40,000 ชนิด และยังเกิดเพิ่มขึ้นอีกอยู่ทุกๆ วัน อย่างน้อยวันละ 4-6 ตัว

มัลแวร์ (Malware)

“Malicious Logic เป็นชุดของคำสั่งที่สร้างปัญหาในการละเมิดนโยบายด้านความปลอดภัยทางเทคโนโลยีสารสนเทศ” หรือส่วนใหญ่แล้วเรามักเรียกกันว่า“โปรแกรมประสงค์ร้าย (Malware: Malicious Software)” เนื่องจากที่พบเห็นจริงๆมักอยู่ในรูปของโปรแกรม (Software) แล้ว ทั้งนี้ที่ผ่านมาภัยคุกคามของชุดคำสั่งประสงค์ร้ายนั้น ดูจะเป็นสิ่งที่สร้างปัญหาและมีการกล่าวถึงมากที่สุดในบรรดารูปแบบของภัยคุกคามที่มีทั้งหมดอย่างไรก็ตามนอกจากโปรแกรมประสงค์ร้ายที่เรารู้จักในปัจจุบันแล้ว กลุ่มนักวิชาการทางคอมพิวเตอร์หลายท่านคาดการณ์ว่า “ในปัจจุบันอาจมีชุดคำสั่งประสงค์ร้ายบางอย่างที่เราไม่รู้จักและไม่สามารถอธิบายได้ในปัจจุบัน ได้แฝงตัวอยู่ใน

ระบบเครือข่ายที่พวกเรากำลังใช้งานอยู่ และรอเพียงเวลาที่มันจะทำงานอย่างเต็มรูปแบบโดยที่พวกเราไม่สามารถจะคาดเดาได้เลยว่าผลกระทบของมันจะออกมาเป็นอย่างไร”

โดยทั่วไปแล้วสามารถแบ่งชนิดของโปรแกรมประสงค์ร้ายได้โดยดูจากพฤติกรรม 3 ข้อดังนี้

- ชุดคำสั่ง (Code) นี้อยู่ได้อิสระหรือไม่ (Need host ?)
- สามารถเดินทางได้ด้วยตัวเองหรือไม่ (Propagation ?)
- สามารถสำเนาตัวเองได้หรือไม่ (Self-replicating ?)

ไวรัส (Virus)

ไวรัส คือ โปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นให้สามารถจัดการกับตัวมันเอง โดยมีลักษณะเลียนแบบสิ่งมีชีวิต คือเจริญเติบโตเองได้ ขยายและแพร่กระจายตัวเองได้สามารถอยู่รอดได้ด้วยการอำพรางตน เหมือนกับไวรัสที่เป็นเชื้อโรคร้ายทำลายสิ่งมีชีวิตทั้งหลายนั่นเอง

- Need Host – เป็นชุดคำสั่งที่จำเป็นต้องอยู่กับโปรแกรมอื่นหรือชุดคำสั่งอื่น
- Not Propagation – เป็นชุดคำสั่งที่ต้องใช้ตัวกลางอื่นในการแพร่กระจาย
- Self-Replicating – เป็นชุดคำสั่งที่จะพยายามทำสำเนาตัวเองกระจายไปยังชุดคำสั่งอื่น

หนอน (Worm)

หนอน (Worm) หมายถึง โปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ โดยจะแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆที่อยู่ในเครือข่าย หนอนจะใช้ประโยชน์จากแอพพลิเคชั่นที่รับส่งไฟล์โดยอัตโนมัติ และไม่ต้องอาศัยคนเพื่อเปิดไฟล์ใดๆ เพราะหนอนมีส่วนของโปรแกรมที่สามารถรันตัวเองเพื่อสร้างความเสียหายได้ เวิร์มนั้นบางที่อาจอาศัยอีเมล์ในการแพร่กระจายตัวเองเหมือนไวรัส โดยแนบไฟล์ไปกับอีเมล์ เมื่อผู้รับเปิดจดหมายอ่านหนอนก็จะเริ่มทำงานทันที อย่างไรก็ตามในครั้งแรกที่เกิดหนอนขึ้นในวงการคอมพิวเตอร์นั้น เพื่อใช้ช่วยเพิ่มความสะดวกในการลงโปรแกรมให้กับเครื่องคอมพิวเตอร์ที่มีอยู่ในระบบของตนเอง ซึ่งในบางครั้งอาจมีกว่าร้อยเครื่อง โดยหนอนจะทำการส่งตัวเองไปพร้อมกับโปรแกรมที่จะทำการลงไปยังทุกๆ เครื่องในระบบแล้วทำการลงโปรแกรมนั้นๆ ให้เองโดยอัตโนมัติไปเรื่อยๆ จนครบทุกเครื่อง

- *Self-Sub Physical* – เป็นชุดคำสั่งที่สามารถอยู่เป็นโปรแกรมเดียวๆ เองได้
- *Propagation* – เป็นชุดคำสั่งที่พยายามเคลื่อนที่ไปติดเครื่องอื่น ทั้งไปเองหรือสำเนาตัวเองไป
- *Not Replicating* – เป็นชุดคำสั่งที่จะไม่ทำสำเนาตัวเองภายในเครื่องเดิม

ม้าโทรจัน (Trojan Horse)

ม้าโทรจัน (Trojan Horse) นี้เป็นคำที่มาจากสงครามโทรจันระหว่างทรอย(Troy) และกรีซ (Greek) ซึ่งเปรียบถึงม้าโครงไม้ขนาดใหญ่ที่ชาวกรีซสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างใน จากนั้นทำทีเป็นว่าถอนทัพกลับ เมื่อชาวทรอยออกมาดูเห็นม้าโครงไม้ทิ้งไว้และคิดว่าเป็นบรรณาการที่ทหารกรีซทิ้งไว้ให้เพื่อไม่ให้ตามไปโจมตีคืน จึงนำกลับเข้าเมืองไปด้วย แต่พอตกดึกทหารกรีซที่ซ่อนอยู่ในม้าโครงไม้ก็ออกมาและเปิดประตูให้กับทหารกรีซเข้าไปทำลายเมืองทรอยได้ในที่สุด สำหรับในความหมายทางคอมพิวเตอร์แล้วม้าโทรจันหมายถึง โปรแกรมที่ทำลาย

ระบบความปลอดภัยของคอมพิวเตอร์ไม่ทางใดก็ทางหนึ่ง โดยแฝงมากับโปรแกรมอื่นๆ เช่น เกม, สกรีนเซิร์ฟเวอร์ เป็นต้น ซึ่งผู้ใช้อาจจะดาวน์โหลดโปรแกรมต่างๆเหล่านี้มาและเมื่อติดตั้งแล้วรันโปรแกรม ม้าโทรจันที่แฝงมาด้วยก็จะทำลายระบบความปลอดภัยของคอมพิวเตอร์ เช่น เปิดช่องทางการสื่อสาร(Port) ที่ไม่ได้ใช้เอง เพื่อเป็นการสร้างประตูหลังให้กับโปรแกรมอื่นเข้ามาทำลายระบบได้ หรืออาจทำการบันทึกการใช้งานต่างๆของผู้ใช้งาน (Logs) เพื่อให้เจ้าของม้าโทรจันนั้นสามารถเข้ามาดูข้อมูลที่บันทึกไว้ได้ เป็นต้น

- *Self-Sub Physical* – เป็นชุดคำสั่งที่สามารถอยู่เป็นโปรแกรมเดียวๆเองได้
- *Not Propagation* – เป็นชุดคำสั่งที่ต้องถูกชักนำเข้ามาจากผู้ถูกโจมตีเองไม่สามารถเคลื่อนที่เองได้
- *Not Replicating* – เป็นชุดคำสั่งที่จะไม่ทำสำเนาตัวเอง

ทั้งนี้ม้าโทรจันอาจมีชื่อเรียกอื่นซึ่งอธิบายถึงลักษณะการทำงานของมัน เช่น

รูทคิท(Root Kits) เป็นชุดโปรแกรมขนาดเล็กที่หลอกให้ผู้ใช้เชื่อว่าจำเป็นต่อการทำงานของระบบคอมพิวเตอร์ โดยพวกผู้โจมตีนิยมใช้สำหรับเจาะเข้าระบบเพื่อควบคุมระบบหรือขโมยข้อมูล โปรแกรมประเภทนี้อาจใช้เทคนิคต่างๆ เช่น การเฝ้าดูสิ่งที่ผู้ใช้พิมพ์บนคีย์บอร์ด (Key Stroke), แก้ไขไฟล์บันทึก (Log file) ของระบบ, สร้างประตูหลัง (Back Door) เพื่อสำหรับการเจาะเข้าระบบในภายหลังหรืออาจใช้ระบบนี้เพื่อเป็นฐานในการโจมตีระบบอื่นๆ ผ่านทางเครือข่าย โดยทั่วไปรูทคิทจะถูกจัดไว้เป็นชุดเพื่อใช้สำหรับโจมตีระบบปฏิบัติการประเภทใดประเภทหนึ่งโดยเฉพาะ รูทคิทเกิดขึ้นครั้งแรกในปี 1990 โดยในช่วงนั้น ระบบปฏิบัติการซันยูนิกซ์ (SUN Unix) และลีนุกซ์ (Linux) เป็นเป้าหมายของการโจมตี แต่ในปัจจุบันมีรูทคิทหลายประเภทเพื่อใช้กับระบบปฏิบัติการต่างๆ ซึ่งรวมถึงไมโครซอฟท์วินโดวส์ (Microsoft Window) และแม็คอินทอช (Mac OS) ด้วย

Remote Access Trojan (RAT) เป็นม้าโทรจันที่จะสร้างประตูหลัง (Back Door) ให้ผู้โจมตีสามารถเข้ามาในระบบเพื่อขโมยข้อมูลหรือควบคุมระบบจากระยะไกลตัวอย่างเช่น แบ็คออริไฟซี (Back Orifice), คาฟีน (Cafeene) และซับเซเว่น(Sub Seven) เป็นต้นข้อสังเกตอย่างหนึ่งคือ ถึงแม้ว่าชุดโปรแกรม RAT หรือรูทคิดบางโปรแกรมเป็นเครื่องมือที่สามารถใช้งานอย่างถูกต้องตามกฎหมายเพื่อจุดประสงค์สำหรับการดูแลระบบ (Monitoring System) อย่างไรก็ตามเครื่องมือเหล่านี้อาจเป็นอันตรายต่อระบบหรือองค์กรได้ถ้ามีการใช้งานในทางที่ผิด

Data Sending and Password Sending Trojan เป็นโทรจันที่โขมยรหัสผ่านต่างๆ แล้วส่งไปให้ผู้ไม่ประสงค์ดี

Keylogger Trojan เป็นโทรจันที่ดักจับทุกข้อความที่พิมพ์ผ่านแป้นพิมพ์ของคีย์บอร์ด

Destructive Trojan เป็นโทรจันที่สามารถลบไฟล์บนเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อได้

Denial of Service(DoS) Attack Trojan เป็นโทรจันที่ใช้ทำ DDoS (Distributed Denial-of-Service) ให้โจมตีระบบคอมพิวเตอร์ที่เป็นเป้าหมายบนอินเทอร์เน็ต เพื่อทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการให้บริการ (Denial-of-Service) การโจมตีจะเกิดขึ้นพร้อมๆ กันและมีเป้าหมายเดียวกัน โดยเครื่องที่ตกเป็นเหยื่อทั้งหมดจะสร้างข้อมูลขยะขึ้นมาแล้วส่งไปที่ระบบเป้าหมาย เพื่อสร้างกระแสข้อมูลให้ไหลเข้าไปในปริมาณมหาศาลทำให้ระบบเป้าหมายต้องทำงานหนักขึ้นและช้าลงเรื่อยๆ เมื่อเกินกว่าระดับที่จะรับได้ก็จะหยุดการทำงานลงในที่สุด อันเป็นเหตุให้ผู้ใช้ไม่สามารถใช้บริการระบบเป้าหมายได้ตามปกติ ส่วนรูปแบบของการโจมตีที่นิยมใช้กันก็มี เช่น SYN Flood, UDP Flood, ICMP Flood, Surf, Fraggle เป็นต้น

Proxy Trojan เป็นโทรจันที่ทำให้เครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกลายเป็นเครื่อง Proxy Server, Web Server หรือ Mail Server เพื่อสร้าง Zombie Network ซึ่งจะถูกใช้ให้เป็นฐานปฏิบัติการเพื่อจุดประสงค์อย่างอื่น

FTP Trojan เป็นโทรจันที่ทำให้เครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกลายเป็นเครื่อง FTP Server

Security Software Killer Trojan เป็นโทรจันที่ Kill Process หรือลบโปรแกรมป้องกันไวรัสหรือลบไฟร์วอลล์บนเครื่องที่ตกเป็นเหยื่อ เพื่อง่ายต่อการปฏิบัติการอย่างอื่นต่อไป

Trojan Downloader เป็นโทรจันที่ดาวน์โหลด Adware, Spyware และ Worm ให้มาติดตั้งบนเครื่องเหยื่อ

ไฟล์ประเภทที่ปลอดภัย 100% ก็คือไฟล์ประเภท Text File ทั้งหมด เช่น .txt, .rtf(Rich Text Format) เป็นต้น เนื่องจากไฟล์เหล่านี้ไม่ใช่ชุดคำสั่ง

Malware ต่างๆไม่สามารถทำงานข้าม OS (ระบบปฏิบัติการ : Operating System) กันได้ เนื่องจากในแต่ละ OS จะมีการใช้นามสกุลของไฟล์ที่เรียกใช้งานได้ไม่เหมือนกัน เช่น ใน Windows OS จะใช้ไฟล์ .exe แต่ใน MAC OS นั้นจะไม่สามารถรันไฟล์ .exe ได้ ดังนั้น Malware บน Windows จึงไม่มีผลกระทบต่อ MAC OS อย่างไรก็ตามทำนองเดียวกัน Malware บน MAC OS ก็ไม่มีผลกับ Windows OS เช่นกัน

โปรแกรมที่ไม่จัดเป็นมัลแวร์

- **โจ๊กแอพพลิเคชัน** เป็นซอฟต์แวร์ที่ออกแบบเพื่อสร้างความสนุกสนาน แต่ก็ทำให้เสียเวลาการทำงานของระบบคอมพิวเตอร์ แอพพลิเคชันประเภทนี้มีมานานพร้อมๆ กับการเริ่มใช้คอมพิวเตอร์ เนื่องจากแอพพลิเคชันประเภทนี้มิได้ออกแบบเพื่อการทำลาย
- **โฮแอคซ์(Hoaxes)** โดยทั่วไปโฮแอคซ์(Hoaxes) หมายถึง โปรแกรมที่เขียนขึ้นเพื่อหลอกให้ผู้ใช้ทำบางอย่างให้ โดยโฮแอคซ์จะใช้เทคนิคทางด้านวิศวกรรมสังคม(Social Engineering) เพื่อหลอกให้ผู้ใช้งานคอมพิวเตอร์ทำบางอย่างให้
- **สแปม(Spam)** คือ การส่งอีเมล์ยังผู้ใช้จำนวนมาก โดยมีจุดประสงค์เพื่อการโฆษณาสินค้าหรือบริการ สแปมจัดอยู่ในประเภทสิ่งที่ก่อให้เกิดความรำคาญ
- **สปายแวร์(Spyware)** บางทีก็รู้จักกันในชื่อ สปายบ็อท (Spybot) หรือแทร็คกิ้งซอฟต์แวร์ (Tracking Software) สปายแวร์เป็นโปรแกรมที่ใช้บางอย่างเพื่อลวงตาแต่ทำกิจกรรมบางอย่างในเครื่องคอมพิวเตอร์ โดยที่ไม่ได้รับความยินยอมจากผู้ใช้เช่น การเก็บข้อมูลส่วนตัวของผู้ใช้ การปรับเปลี่ยนเซตติ้งของบราวเซอร์ ลดประสิทธิภาพโดยรวมของคอมพิวเตอร์ไปจนถึงการละเมิดสิทธิส่วนบุคคลของผู้ใช้
- **แอดแวร์ (Adware)** เป็นโปรแกรมโฆษณาสินค้าซึ่งจะเปิดป๊อบอัพวินโดวส์ แอดแวร์ส่วนใหญ่จะรวมอยู่ในแอพพลิเคชันที่ให้ใช้ได้ฟรีและจะฝังตัวอยู่ เนื่องจากได้รับความยินยอมจากผู้ใช้ แอดแวร์จะติดตั้งก็ต่อเมื่อผู้ใช้ได้ยินยอมตามข้อตกลงเกี่ยวกับลิขสิทธิ์
- **อินเทอร์เน็ตคุกกี้ (Internet Cookies)** คือ เท็กซ์ไฟล์ที่เก็บไว้ที่เครื่องคอมพิวเตอร์ของผู้ใช้โดยเว็บไซต์ที่เข้าไปเยี่ยมชมคุกกี้จะเก็บข้อมูลบางอย่างที่เว็บไซต์นั้นใช้เมื่อครั้งหน้าที่ผู้ใช้เข้าไปเยี่ยมชมอีกครั้ง ซึ่งส่วนใหญ่จะเป็นข้อมูลที่ใช้บอกว่าเป็นผู้ใช้คนนี้ นอกจากนี้ในไฟล์อาจมีข้อมูลอื่นๆ ก็ได้

คุณสมบัติของมัลแวร์

คุณสมบัติของมัลแวร์แต่ละประเภทนั้นบางทีก็มีความคล้ายกันอยู่บ้างเช่น ไวรัสและเวิร์ม อาจใช้เครือข่ายเพื่อเป็นช่องทางในการแพร่กระจาย อย่างไรก็ตามไวรัสนั้นพยายามที่จะฝังตัวในไฟล์ ในขณะที่เวิร์มนั้นแค่พยายามจะก๊อปปี้ตัวเองไปไว้หลายๆที่ ต่อไปนี้เป็นคุณสมบัติทั่วไปของมัลแวร์

คุณสมบัติของเป้าหมาย ในขณะที่มัลแวร์พยายามจะโจมตีโฮสต์ใดๆ ระบบนั้นอาจต้องมีองค์ประกอบบางอย่างก่อนที่จะทำให้การโจมตีเป็นผลสำเร็จได้ ต่อไปนี้เป็นตัวอย่างขององค์ประกอบของระบบที่ต้องมี

- *ประเภทของอุปกรณ์* มัลแวร์บางตัวอาจจะตั้งเป้าหมายไปที่อุปกรณ์เฉพาะอย่าง เช่น คอมพิวเตอร์ที่เป็นระบบวินโดวส์ แมคอินทอช หรือแม้กระทั่ง PDA เป็นต้น
- *ระบบปฏิบัติการ* มัลแวร์อาจสามารถรันได้กับเฉพาะระบบปฏิบัติการหนึ่งเท่านั้น ยกตัวอย่าง เช่น ไวรัส CIH หรือ Chernobyl จะโจมตีเฉพาะ Windws 95,98 เท่านั้น
- *แอพพลิเคชัน* มัลแวร์อาจต้องอาศัยแอพพลิเคชันบางตัวเพื่อช่วยทำให้สามารถติดได้ เช่น ไวรัส LFM.926 ในปี 2002 สามารถโจมตีได้กับเฉพาะโปรแกรม Shockwave(.swf)

พาหะนำมัลแวร์ ถ้ามัลแวร์เป็นไวรัส มันจะพยายามจะทำให้เป้าหมายติดไวรัส จำนวนและประเภทของออบเจ็กต์ที่เป็นเป้าหมายนั้นมีหลากหลาย ต่อไปนี้เป็นตัวอย่างบางออฟเจ็กต์ที่เป็นเป้าหมายของไวรัส

- *Executable File* เป้าหมายนี้เป็นเป้าหมายคลาสสิกหรือดั้งเดิม ไวรัสสามารถแพร่กระจายโดยการฝังตัวเองไปกับโปรแกรมอื่นๆ นอกเหนือจากไฟล์ที่สามารถเอ็กซ์คิวต์ได้ ซึ่งจะมีนามสกุลเป็น .exe ไฟล์อื่นที่สามารถรันได้ เช่น .com, .sys, .dll, .ocx และ .prg ก็สามารถรันได้เช่นกัน
- *Script* การโจมตีนี้อาจอาศัยภาษาสคริปต์เพื่อรันและทำให้ติดไวรัส ซึ่งภาษาสคริปต์ที่ว่านี้ เช่น Visual Basic, javaScript, AppleScript หรือ Perl เป็นต้น
- *Macros* มาโครเป็นภาษาสคริปต์ของแอพพลิเคชันบางตัว เช่น ไมโครซอฟท์ออฟฟิศ มัลแวร์จะอาศัยอการรันมาโครสคริปต์นี้ ในการแพร่กระจายหรือติดต่อไปยังไฟล์อื่นหรือระบบอื่น หรือทำอันตรายให้กับระบบที่ติด เช่น ไวรัสามารถใช้ภาษามาโครของไมโครซอฟท์เวิร์ค เพื่อสร้างผลกระทบให้กับระบบหรือ ลบฮาร์ดดิสก็ได้
- *Boot Sector* พื้นที่บางส่วนของฮาร์ดดิสหรือ CD-ROM เช่น MBR (Master Boot Record) หรือ DOS Boot Record อาจเป็นเป้าหมายก็ได้ เนื่องจากส่วนนี้สามารถรันโค้ดได้ เมื่อดิสก์ติดไวรัสในส่วนนี้แล้ว การแพร่กระจายก็สามารถเกิดขึ้นได้เมื่อดิสก์นี้ใช้สำหรับบู๊ตระบบอื่น ถ้าไวรัสนั้นสามารถติดได้ทั้งไฟล์ทั่วไปและบู๊ตเซ็กเตอร์ ไวรัสประเภทนี้เรียกว่า มัลติพาร์ไทต์ไวรัส(Multipartite Virus)

กลไกการแพร่กระจาย มัลแวร์อาจใช้หลากหลายวิธีในการแพร่กระจายตัวเองไปยังเครื่องอื่นๆ และต่อไปนี้เป็นตัวอย่างทั่วๆไปที่มัลแวร์มักจะใช้ในการแพร่กระจายตัวเอง

- *Removable Media* การแพร่กระจายแบบดั้งเดิมของไวรัสและแบบที่เกิดขึ้นมากที่สุดคือ การก๊อปปี้ไฟล์ อย่างไรก็ตามอัตราการแพร่กระจายโดยอาศัยมีเดียต่างๆ นี้ยังไม่เร็วเท่ากับการแพร่กระจายโดยอาศัยเครือข่ายคอมพิวเตอร์
- *Network Shares* การแชร์ไฟล์ผ่านเครือข่ายนี้ก็กลายเป็นอีกช่องทางหนึ่งที่มัลแวร์ใช้ในการแพร่กระจายตัวเองไปอย่างรวดเร็ว ถ้าเครือข่ายไม่มีระบบป้องกันและรักษาความปลอดภัยที่ดี

- *Network Scanning* มัลแวร์อาจใช้เทคนิคนี้ในการสแกนเครือข่ายเพื่อค้นหาระบบที่มีจุดอ่อนหรือช่องโหว่และโจมตี ยกตัวอย่างเช่น กลไกนี้อาจส่งแพ็กเก็ตที่สามารถเจาะเข้าระบบที่มีช่องโหว่ผ่านทางพอร์ตเฉพาะเพื่อค้นหาหรือทดสอบว่ามีระบบใดบ้างที่มีจุดอ่อนหรือช่องโหว่อยู่
- *E-Mail* เป็นวิธีการที่ง่ายและคนส่วนใหญ่ก็ใช้อีเมล์ในการสื่อสารกับผู้ใช้คนอื่นผ่านทางเครือข่ายและอินเทอร์เน็ตอยู่แล้ว
- *Remote Exploit* มัลแวร์อาจพยายามใช้ช่องโหว่หรือจุดอ่อนจากเซอร์วิส หรือแอพพลิเคชันเพื่อแพร่กระจายตัวเอง พฤติกรรมอย่างนี้มักพบกันมากสำหรับมัลแวร์ประเภทเวิร์ม ยกตัวอย่างเช่น สแลมเมอร์เวิร์ม (Slammer Worm) ใช้ประโยชน์จากช่องโหว่ในไมโครซอฟท์ SQL Server 2000 เวิร์มนี้จะทำให้เกิดบัฟเฟอร์โอเวอร์รัน (Buffer Overrun) จนทำให้มันสามารถเขียนโค้ดลงบนบางส่วนของเมนโมรีของระบบ ซึ่งโค้ดส่วนนี้สามารถรันตัวเองได้เหมือนกับเป็นเซอร์วิสของ SQL Server บัฟเฟอร์โอเวอร์รัน หมายถึง สภาพที่เกิดจากการป้อนข้อมูลเข้าไปในบัฟเฟอร์มากกว่าที่บัฟเฟอร์นั้นจะสามารถรองรับได้ แฮคเกอร์มักนิยมใช้เทคนิคนี้ในการเจาะเข้าควบคุมระบบ ไมโครซอฟท์ได้ใช้เวลาหลายเดือนในการแก้ไขหรือปิดช่องโหว่นี้หลังจากที่สแลมเมอร์ออกมาโจมตี อย่างไรก็ตามถึงแม้ว่าจะมีแพตซ์ที่ใช้สำหรับปิดช่องโหว่เหล่านี้แล้วก็ตาม แต่ก็มีแค่บางระบบเท่านั้นที่มีการดาวน์โหลดและอัพเดตแพตซ์ ทำให้เวิร์มนี้ยังสามารถแพร่กระจายและทำลายระบบได้

การจุดชนวน ไวรัสหรือมัลแวร์จะต้องมีการจุดชนวนเพื่อให้ไวรัสเริ่มทำงานเพื่อทำลายระบบหรือเริ่มขบวนการแพร่กระจายไปยังเครื่องอื่นๆ การจุดชวนโดยส่วนใหญ่อาจเกิดได้เนื่องจากดังนี้

- *Manual Execution* การที่ผู้ใช้รันโปรแกรมที่เครื่องโดยตรง ซึ่งอาจจะทำโดยไม่รู้ตัวหรือเป็นการหลอกให้รันโปรแกรม
- *Semi-Automatic Execution* เกิดจากที่ผู้ใช้รันโปรแกรมมัลแวร์เอง แล้วหลังจากนั้นโปรแกรมก็จะทำงานต่อโดยอัตโนมัติ
- *Automatic Execution* มัลแวร์ประเภทนี้จะรันตัวเองโดยอัตโนมัติโดยไม่ต้องอาศัยผู้ใช้
- *Time Bomb* จะรันในช่วงเวลาหนึ่งหลังจากที่เครื่องติดไวรัสแล้ว
- *Conditional* จะเริ่มต้นเมื่อสภาพแวดล้อมตรงตามเงื่อนไขที่กำหนด ยกตัวอย่างเช่น จะมีการเปลี่ยนชื่อไฟล์ เมื่อมีการกดคีย์บอร์ดบางคีย์ เป็นต้น

กลไกการป้องกันตัวเอง มัลแวร์หลายตัวใช้กลไกบางอย่างเพื่อป้องกันหรือช่วยลดโอกาสที่จะถูกตรวจสอบเจอหรือถูกกำจัดทิ้ง ต่อไปนี้เป็นบางเทคนิคที่มัลแวร์ส่วนใหญ่นิยมใช้

- *Armor* เทคนิคการป้องกันประเภทนี้จะพยายามและป้องกันการวิเคราะห์โค้ดของมัลแวร์ เช่น มัลแวร์จะตรวจดูว่าโปรแกรมดีบั๊กเกอร์ (Debugger) กำลังรันอยู่หรือไม่และป้องกันหรือทำให้ดีบั๊กเกอร์ทำงานไม่ถูกต้องหรือเพิ่มโค้ดจำนวนมากที่ไม่มีความหมายใดๆ เพื่อทำให้ยากต่อการวิเคราะห์จุดมุ่งหมายของโค้ดมัลแวร์นี้
- *Stealth* มัลแวร์ใช้เทคนิคการซ่อนพรางตัวโดยการให้ข้อมูลที่ผิดๆ เมื่อโปรแกรมสแกนไวรัสพยายามจะสแกนมัลแวร์ ยกตัวอย่างเช่น ไวรัสบางตัวอาจจะบันทึกไฟล์หรืออิมเมจที่ยังไม่ติดไวรัสในบู๊ตเซ็กเตอร์เมื่อขณะมีการพยายามที่จะตรวจเช็คว่าบู๊ตเซ็กเตอร์ติดไวรัสหรือไม่ ไวรัสเก่าแก่อย่างเช่น เบรน (Brain Virus) ใช้เทคนิคนี้ในปี 1986
- *Encryption* มัลแวร์บางประเภทจะใช้วิธีการเข้ารหัสโค้ดตัวเองหรือบางทีอาจรวมทั้งข้อมูลระบบด้วย เพื่อป้องกันการตรวจพบ มัลแวร์ที่เข้ารหัสประกอบด้วยฟังก์ชันการเข้ารหัส คีย์ และโค้ดมัลแวร์ที่ถูกเข้ารหัส

แล้ว เมื่อมัลแวร์ถูกรันแล้วก็จะใช้ฟังก์ชันการเข้ารหัสและคีย์เพื่อถอดรหัสโค้ดมัลแวร์ หลังจากนั้นก็จะก๊อปปี้ตัวเองไปยังไฟล์ใหม่พร้อมทั้งสร้างคีย์ใหม่ขึ้นมาเพื่อเข้ารหัสตัวเองอีกครั้ง แล้วแนบคีย์และฟังก์ชันการเข้ารหัสไปกับมัลแวร์ที่เข้ารหัสแล้ว ซึ่งทำให้กลายเป็นก๊อปปี้ใหม่ของมัลแวร์ มัลแวร์ประเภทนี้จะต่างจากไวรัสประเภทโพลิมอร์ฟิก เพราะมัลแวร์จะใช้ฟังก์ชันในการเข้ารหัสเดียวกันเสมอแต่คีย์จะถูกเปลี่ยนไปทุกครั้ง ซอฟต์แวร์ป้องกันไวรัสอาจตรวจสอบเจอฟังก์ชันที่ใช้สำหรับเข้ารหัสและทำให้ตรวจเจอมัลแวร์ประเภทนี้ได้ง่ายกว่า

- *Oligomorphic* มัลแวร์ประเภทนี้จะใช้เทคนิคการเข้ารหัสเหมือนกันมัลแวร์ที่ใช้วิธีการเข้ารหัสแต่สามารถเปลี่ยนฟังก์ชันในการเข้ารหัสได้ในจำนวนที่จำกัด เช่น อาจมีฟังก์ชัน 2 ฟังก์ชันในการเข้ารหัสสลับกันไปมาในระหว่างการแพร่กระจายตัวเอง
- *Polymorphic* มัลแวร์ประเภทนี้ใช้เทคนิคการเข้ารหัสเป็นกลไกในการป้องกันการตรวจเจอ โดยส่วนใหญ่จะเข้ารหัสโค้ดมัลแวร์เองด้วยฟังก์ชันการเข้ารหัส และสร้างคีย์สำหรับการถอดรหัสเฉพาะในแต่ละครั้ง ดังนั้น โพลีมอร์ฟิกมัลแวร์จะใช้ฟังก์ชันเข้ารหัสในจำนวนที่ไม่จำกัด เมื่อมีการแพร่กระจายบางส่วนของโค้ดที่เข้ารหัสจะเปลี่ยนไปทุกครั้ง ขึ้นอยู่กับมัลแวร์แต่ละตัว

เทคนิคการตรวจจับไวรัส

ซอฟต์แวร์ป้องกันไวรัสเป็นสิ่งที่จำเป็นสำหรับการป้องกัน และรักษาความปลอดภัยให้กับคอมพิวเตอร์ ถ้ามีการติดตั้งและใช้งานอย่างถูกต้อง มันสามารถที่จะลดความเสี่ยงต่อโปรแกรมประสงค์ร้ายต่างๆได้ อย่างไรก็ตามมันไม่สามารถที่จะป้องกันไวรัสได้ทุกชนิด เนื่องจากปัจจุบันจะมีไวรัสใหม่ๆออกมาอยู่เรื่อยๆ การใช้งานซอฟต์แวร์ป้องกันไวรัสนั้น จำเป็นที่ต้องอัพเดตฐานข้อมูลไวรัส (Virus Signature) เป็นประจำพร้อมทั้งสแกนระบบเป็นประจำเช่นกัน แต่ทั้งนี้โปรแกรมป้องกันไวรัสก็ไม่สามารถที่จะป้องกันผู้บุกรุกจากที่อื่นที่เจาะระบบเข้ามาแล้วรันโปรแกรมประสงค์ร้ายได้ นอกจากนี้โปรแกรมป้องกันไวรัสยังไม่สามารถป้องกันผู้ใช้ที่ได้รับอนุญาตแต่พยายามที่จะเข้าถึงไฟล์หรือโปรแกรมที่ไม่ได้รับอนุญาตได้

ทั้งนี้ท่านทราบหรือไม่ว่าเราสามารถลงโปรแกรมป้องกันไวรัสได้มากกว่า 1 โปรแกรมใน 1 เครื่อง แต่ทั้งนี้จะสามารถทำได้กับโปรแกรมป้องกันไวรัสบางตัวเท่านั้นเช่น คุณสามารถลง AntiVir ร่วมกับ NOD32 และ Bitdefender เนื่องจากโปรแกรมเหล่านี้จะไม่ทำการเข้าไปยุ่งกับการทำงานของระบบในจุดที่มีผลกระทบซึ่งกันและกัน แต่สำหรับ Norton Antivirus แล้วจะไม่สามารถลงร่วมกับโปรแกรมป้องกันไวรัสตัวอื่นได้เลยเพราะมันจะมองว่าโปรแกรมป้องกันไวรัสตัวอื่นๆเป็นโปรแกรมประสงค์ร้ายด้วยเป็นต้น แต่ถึงกระนั้นก็ไม่ได้หมายความว่าโปรแกรมป้องกันไวรัสที่ไม่สามารถลงร่วมกับโปรแกรมไวรัสตัวอื่นไม่ได้นั้นไม่ดีเสมอไป ทั้งนี้อาจเป็นเพราะโปรแกรมป้องกันไวรัสเหล่านั้น อาจมีการป้องกันที่ครอบคลุมการทำงานของระบบในแทบจะทุกส่วนหรือมีความอ่อนไหวและทำการป้องกันต่อการโจมตีแม้เพียงเล็กน้อย ซึ่งสิ่งเหล่านี้ก็จะทำให้โปรแกรมป้องกันไวรัสเหล่านั้น ยิ่งมีประสิทธิภาพมากยิ่งขึ้น (แต่การอ่อนไหวมากก็อาจสร้างความรำคาญให้แก่ผู้ใช้ได้พอสมควรเช่นกัน)

อย่างไรก็ตามผู้เชี่ยวชาญส่วนใหญ่ไม่แนะนำให้ทำการลงโปรแกรมป้องกันไวรัสมากกว่า 1 โปรแกรมต่อเครื่อง เพราะถึงแม้ว่าจะช่วยให้การป้องกันดีขึ้น แต่ก็ไม่ทำให้สามารถป้องกันได้ 100% อยู่ดี อีกทั้งยังทำให้ระบบการทำงานของคอมพิวเตอร์ช้าลงเป็นอย่างมากหรืออาจมีปัญหาการทำงานในบางส่วนได้อีกด้วยและหากเราต้องการทดสอบว่าโปรแกรมป้องกันไวรัสที่เราใช้อยู่นั้นตอบสนองกับพวก Script หรือมัลแวร์ได้ดีแค่ไหน เรา

สามารถทดสอบด้วยการนำ Script ต่อไปนี้สร้างไว้เป็น Text file ธรรมดา โดยอาจเปิด Notepad ขึ้น มาจากนั้นให้ก็อปปี้ Script นี้ลงไป

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

จากนั้น ให้ตั้งชื่อไฟล์และบันทึกลงในเครื่อง ในจังหวะนี้เองให้ดูว่าเครื่องเรามีการตอบสนองอย่างไรบ้าง เช่น

1. แจ้งเตือน (Alert!) ขึ้นมาทันที และไม่ยอมให้บันทึกไฟล์นั้น
2. ยอมให้บันทึกไฟล์นั้นลงไป แต่เมื่อพยายามเปิดไฟล์นั้นขึ้นมาถึงจะมีการแจ้งเตือนพร้อมทั้งลบไฟล์นั้นออกจากเครื่องของคุณทันที
3. ยอมให้บันทึกไฟล์นั้นลงไป แต่เมื่อพยายามเปิดไฟล์นั้นขึ้นมาถึงจะมีการแจ้งเตือน
4. ยอมให้บันทึกไฟล์ และแม้ว่าจะเปิดไฟล์ขึ้นมาดูอีกครั้งก็ไม่มีการแจ้งเตือนใดๆทั้งสิน

หากเครื่องของใครเข้าข่ายการตอบสนองแบบที่ 4 ก็ให้คุณหาโปรแกรมแอนตี้ไวรัสตัวอื่นมาใช้แทนสำหรับเครื่องที่ตอบสนองตามแบบที่ 1 จะให้ผลลัพธ์ดีที่สุด ซึ่งตัวอย่างของโปรแกรมก็เช่น McAfee, NOD32, Kaspersky เป็นต้น ส่วนการตอบสนองในแบบที่ 2 หรือ 3 นั้น ก็เป็นปกติทั่วไป โดยแบบที่ 2 จะดูดีกว่าแบบที่ 3

การสแกนหาซิกเนเจอร์ (Signature Scanning) ซอฟต์แวร์ป้องกันไวรัสส่วนใหญ่จะใช้วิธีนี้ ซึ่งจะเกี่ยวกับการสแกนไฟล์ทั้งในฮาร์ดดิสก์และเมมโมรีเพื่อค้นหาโค้ดที่อาจเป็นส่วนหนึ่งของไวรัสและมัลแวร์ ข้อมูลที่ซอฟต์แวร์ประเภทนี้ใช้สำหรับการเปรียบเทียบกับไฟล์ที่กำลังสแกนเพื่อจะตัดสินว่าไฟล์นั้นติดไวรัสหรือไม่จะเรียกว่า *ซิกเนเจอร์(Signature)* ซึ่งซิกเนเจอร์นี้จะถูกอัพเดตเป็นประจำเพื่อให้โปรแกรมป้องกันไวรัสสามารถค้นหาและตรวจจับไวรัสตัวใหม่ๆ ให้ได้มากที่สุด ปัญหาของการใช้เทคนิคนี้คือไวรัสนั้นอาจจะแพร่กระจาย และทำลายระบบก่อนที่โปรแกรมป้องกันไวรัสจะถูกอัพเดตซิกเนเจอร์ใหม่ๆ ซึ่งถ้าไม่มีซิกเนเจอร์ของไวรัสประเภทนั้นอยู่ซอฟท์แวร์นั้นก็จะตรวจจับไวรัสประเภทนั้นไม่เจอ

การสแกนหาคุณลักษณะเฉพาะ เทคนิคประเภทนี้จะตรวจพบทั้งมัลแวร์เก่าและใหม่โดยการค้นหาคุณลักษณะทั่วไปของมัลแวร์ ข้อได้เปรียบของการใช้เทคนิคนี้คือ การที่โปรแกรมไม่ต้องใช้ซิกเนเจอร์เพื่อค้นหาและตรวจจับไวรัส อย่างไรก็ตามการใช้เทคนิคประเภทนี้ก็ยังมีปัญหาบางอย่างคือ

- *การแจ้งเตือนผิดๆ (False Positive)* เทคนิคนี้จะใช้คุณลักษณะทั่วไปในการตรวจจับไวรัส ดังนั้นก็มีโอกาศที่โปรแกรมทั่วไปอาจมีคุณลักษณะคล้ายกับไวรัสหรือมัลแวร์ ดังนั้นโปรแกรมอาจรายงานว่าตรวจเจอไวรัสทั้งๆที่ไม่ใช่ไวรัสจริงๆ
- *การสแกนที่ช้า* โพรเซสการค้นหาลักษณะของไวรัสนั้นเป็นสิ่งที่ยาก และซับซ้อนกว่าการใช้ซิกเนเจอร์ ด้วยเหตุนี้โปรแกรมประเภทนี้อาจใช้เวลานานในการสแกน
- *ไวรัสอาจมีคุณลักษณะใหม่* ก็อาจเป็นไปได้ที่มัลแวร์ตัวใหม่จะมีคุณลักษณะพิเศษที่อาจไม่ได้รู้จักก่อนล่วงหน้า ดังนั้นเทคนิคนี้ก็จะไม่สามารถตรวจเจอไวรัสประเภทนี้ได้

การมอนิเตอร์พฤติกรรม เทคนิคประเภทนี้จะเน้นที่พฤติกรรมของการโจมตีโดยไวรัสมากกว่าลักษณะของโค้ดไวรัสเอง ยกตัวอย่างเช่น บางแอพพลิเคชันอาจพยายามเปิดพอร์ตบางพอร์ตที่ไม่ควรเปิด โปรแกรมป้องกันไวรัสก็จะคาดเดาเอาว่าการเปิดพอร์ตนั้นเป็นพฤติกรรมของไวรัส และแจ้งเตือนว่าระบบถูกโจมตีแล้ว

มัลแวร์ในปัจจุบัน

ความท้าทายในการปกป้องรักษาความปลอดภัยข้อมูล และระบบสารสนเทศมีเพิ่มขึ้นเรื่อยๆ แนวโน้มได้แสดงให้เห็นว่าการรักษาความปลอดภัยนั้นเป็นเรื่องที่ยากและซับซ้อนขึ้นเรื่อยๆ ยกตัวอย่างเช่น

- *ความเร็วในการโจมตี* ด้วยความสามารถของเครื่องมือสมัยใหม่และความง่ายในการได้มาซึ่งเครื่องมือเหล่านี้ ทำให้ผู้โจมตีสามารถสแกนเพื่อค้นหาเป้าหมายที่มีจุดอ่อนหรือช่องโหว่และโจมตีด้วยความรวดเร็ว
- *ความซับซ้อนในการโจมตี* การโจมตีในปัจจุบันมีความซับซ้อนมากขึ้นเรื่อยๆ บางเครื่องมือที่ใช้สำหรับการโจมตีมีความหลากหลายในตัวเอง ทำให้วิธีการโจมตีเดียวกันแต่มีความแตกต่างในแต่ละครั้งที่โจมตี ทำให้การตรวจจับนั้นทำได้ยาก
- *ความรวดเร็วในการค้นหาจุดอ่อน* การโจมตีที่เกิดขึ้นโดยผู้โจมตีนั้นสามารถค้นหาช่องโหว่เอง โดยอาศัยช่องโหว่นี้ยังไม่มีใครค้นพบมาก่อนและสร้างเครื่องมือการโจมตีผ่านช่องโหว่นี้ทำให้เป้าหมายไม่นั้นไม่รู้เลยว่าถูกโจมตีผ่านช่องโหว่ใด และยิ่งเป็นการยากและใช้เวลานานมากขึ้นในการแก้ปัญหาการโจมตีประเภทนี้
- *การโจมตีแบบแยกกระจาย* ปัจจุบันนักโจมตีสามารถใช้คอมพิวเตอร์หลายพันหลายแสนเครื่องเพื่อโจมตีเป้าหมายเดียวกัน โดยขั้นตอนแรกนั้นนักโจมตีก็จะค้นหาเครื่องร่วมโจมตี ฝังโค้ดและตั้งเวลาในการโจมตีพร้อมกัน การโจมตีแบบแยกกระจายนี้ทำให้ยากต่อการป้องกันและหยุดหยั้งการโจมตีได้เพราะแหล่งที่มานั้นมากเกินไปที่จะสามารถบล๊อกได้
- *ความซับซ้อนในการติดตั้งแพตซ์* การป้องกันการโจมตีในรูปแบบต่างๆ ที่ได้ผลที่สุดก็โดยการติดตั้งแพตซ์ ซึ่งก็คือซอฟต์แวร์ที่ปิดช่องโหว่หรือจุดอ่อนที่มีอยู่ในแอพพลิเคชันหรือระบบปฏิบัติการอย่างไรก็ตามการจัดการเกี่ยวแพตซ์และความต้องรู้ว่าจะต้องติดตั้งแพตซ์ไหนบ้างกลายเป็นสิ่งที่ยากและซับซ้อน การโจมตีที่สำเร็จโดยส่วนใหญ่นั้นเกิดจากการที่ผู้ใช้ไม่ได้ติดตั้งแพตซ์ที่ได้ออกมานานและก่อนการโจมตีด้วยซ้ำ

อาการของเครื่องที่ติดไวรัสหรือมัลแวร์

สามารถสังเกตุการทำงานของเครื่องคอมพิวเตอร์ได้ด้วยตนเอง ถ้ามีอาการดังต่อไปนี้อาจเป็นไปได้ว่ามีไวรัสเข้าไปติดอยู่ในเครื่องคอมพิวเตอร์แล้ว หรืออาจเกิดจากสาเหตุอื่นเช่นเป็นจุดบกพร่องของระบบปฏิบัติการหรือตัวอุปกรณ์ฮาร์ดแวร์มีปัญหาก็เป็นได้ อาการของเครื่องที่ติดไวรัสนั้นได้แก่

- เครื่องทำงานช้าลง โดยใช้เวลานานผิดปกติในการสตาร์ทเครื่องและเรียกโปรแกรมขึ้นมาทำงาน
- เครื่องบูตตัวเองโดยไม่ได้สั่งให้รีสตาร์ท
- เครื่องแฮ้งค้าง หรือหยุดทำงานโดยไม่ทราบสาเหตุ
- ขนาดของหน่วยความจำที่เหลืออยู่ลดน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
- ซีพียูถูกเรียกใช้งานมากเกินกว่า 90 เปอร์เซ็นต์ขึ้นไปตลอดเวลา
- แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่หายไปเฉยๆ
- พบไฟล์มีชื่อแปลกๆที่ไม่เคยพบมาก่อนอยู่ในโฟลเดอร์ต่างๆ
- ข้อความที่ไม่เคยได้เห็นกลับถูกแสดงขึ้นมาบ่อยๆ
- เกิดข้อความหรือภาพประหลาดบนหน้าจอ
- ขนาดของไฟล์โปรแกรมหรือไฟล์งานใหญ่ขึ้น

- วันเวลาของโปรแกรมหรือของไฟล์งานเปลี่ยนแปลงไป
- ไฟแสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
- มีเสียงดังออกมาทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้งานอยู่

สาเหตุที่เครื่องติดไวรัสหรือมัลแวร์

สาเหตุสำคัญที่ทำให้เครื่องคอมพิวเตอร์ติดไวรัสหรือมัลแวร์ต่างๆ เกิดจากพฤติกรรมการใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้เป็นหลัก ถ้าผู้ใช้มีความระมัดระวังการใช้สื่อบันทึกข้อมูล ไม่ติดตั้งโปรแกรมที่เป็นการละเมิดลิขสิทธิ์ของผู้อื่น เครื่องคอมพิวเตอร์มีโปรแกรมตรวจหาไวรัสและอัพเดทอยู่เสมอ เมื่อเข้าไปใช้บริการอินเตอร์เน็ตเปิดเว็บไซต์ที่น่าเชื่อถือเท่านั้นและจะคลิกอะไรควรอ่านคิดดูให้รอบคอบเปอร์เซ็นต์การติดไวรัสของเครื่องคอมพิวเตอร์ก็จะลดน้อยลง แต่ไม่ได้หมายความว่าไวรัสคอมพิวเตอร์จะหมดไปจากโลก เพราะยังมีช่องทางอื่นๆที่ทำให้เครื่องคอมพิวเตอร์ติดไวรัสได้อีก เช่น

- *จากทางแผ่นดิสก์หรือแฟลชไดร์ฟ* ที่ได้ทำการคัดลอกไฟล์จากเครื่องหนึ่ง ไปใช้กับอีกเครื่องหนึ่ง โดยหารู้ไม่ว่า ไวรัสได้สำเนาตัวเองติดไปกับดิสก์หรือแฟลชไดร์ฟ เพื่อไปติดคอมพิวเตอร์เครื่องอื่นต่อไป
- *จากทางอีเมล์* โดยเฉพาะจากการดาวน์โหลดอีเมล์ผ่านทางโปรโตคอล POP3 ซึ่งอาจมีไวรัสหรือมัลแวร์แอบแฝงเข้ามาได้ ส่วนใหญ่จะเป็นพวกหนอนอินเตอร์เน็ตประเภท Mass-Mailing Worm หรือพวก Netsky, Beagle และ Mydoom เป็นต้น
- *จากการเข้าไปเปิดเว็บที่มีสคริปต์มุ่งร้าย* (Malicious Script) ซ่อนอยู่ เช่น พวกเว็บโป๊ และเว็บแคร็กต่างๆ อาจมีมัลแวร์ซ่อนตัวอยู่และพร้อมที่จะทำงานตามที่ได้ถูกโปรแกรมไว้
- *จากการดาวโหลดไฟล์* ต่างๆบนเครือข่าย P2P หรือจากแหล่งที่ไม่น่าเชื่อถือซึ่งนิยมเรียกกันว่า โหลดบิท
- *จากการเล่นหรือรับไฟล์* จากโปรแกรมประเภท Instant Messaging เช่นโปรแกรมประเภท MSN และ ICQ เป็นต้น
- *จากช่องโหว่* (Vulnerability) ของระบบปฏิบัติการหรือของโปรแกรมต่างๆ ซึ่งพวก Network Worm และที่เคยเป็นข่าวได้แก่ Blaster, Sasser และ Bobax จะอาศัยช่องโหว่ที่พบนี้เข้าโจมตีเครื่องเป้าหมาย และต่อไปอาจจะเป็นพวก Zero-Day Attack ก็เป็นได้

การป้องกันไวรัส

การป้องกันไวรัสที่เครื่องไคลเอนท์ การป้องกันไวรัสที่เครื่องไคลเอนท์นั้นมีหลากหลายรูปแบบ ขั้นตอนต่อไปนี้เป็นตัวอย่างที่แนะนำให้ปฏิบัติตามอย่างเคร่งครัด

- *การลบโปรแกรมที่ไม่ได้ใช้งาน* ขั้นตอนแรกในการป้องกันคือ การลดช่องทางไวรัสอาจจะใช้เป็นสื่อที่จะเข้ามาในเครื่อง ตัวอย่าง เช่น การลบแอพพลิเคชันหรือเซอร์วิสที่ไม่จำเป็นออกจากเครื่อง ซึ่งเป็นการลดจำนวนช่องทางที่แฮคเกอร์ หรือไวรัสอาจใช้ประโยชน์ได้บางระบบปฏิบัติการนั้นเมื่อติดตั้งโดยดีฟอลต์อาจมีบางเซอร์วิสที่ไม่จำเป็นต้องใช้ เช่น เว็บเซิร์ฟเวอร์, FTP และเมล์เซิร์ฟเวอร์ เป็นต้น ซึ่งถ้าไม่จำเป็นต้องใช้ก็ไม่ควรติดตั้ง
- *การอัพเดตแพตซ์* เครื่องไคลเอนท์ที่ใช้งานและเชื่อมต่อเข้ากับเครือข่ายอาจมีมากมายและใช้ระบบปฏิบัติการและซอฟต์แวร์ที่ต่างกัน ทำให้การอัพเดตแพตซ์ทั้งของระบบปฏิบัติการเองและซอฟต์แวร์อื่นๆ เป็นเรื่องที่ยุ่งยากอยู่บ้าง อย่างไรก็ตามขั้นตอนนี้ก็เป็นขั้นตอนที่สำคัญที่จะทำให้มาตรการป้องกันไวรัสได้ผล

- *การติดตั้งโฮสต์เบสไฟร์วอลล์* ไฟร์วอลล์จะทำหน้าที่กรองข้อมูลที่ไหลเข้าออกคอมพิวเตอร์เครื่องนั้น โดย Windows XP มีไฟร์วอลล์ในตัวซึ่งเรียกว่า ICF (Internet Connection Firewall) คอยตรวจเช็คต้นทางและปลายทางของทุกๆ แพ็กเก็ตเพื่อตรวจดูว่าจะอนุญาติให้แพ็กเก็ตผ่านเข้าออกหรือไม่

- *การติดตั้งซอฟต์แวร์ป้องกันไวรัส* ซอฟต์แวร์เหล่านี้ถูกออกแบบมาเพื่อป้องกันคอมพิวเตอร์จากการโจมตีของไวรัส และพยายามให้มีผลกระทบต่อการใช้งานของผู้ใช้ให้น้อยที่สุด ส่วนใหญ่แล้วซอฟต์แวร์เหล่านี้จะมีประสิทธิภาพสูงในการป้องกันและกำจัดไวรัส แต่ต้องมีการอัพเดตซิกเนเจอร์เป็นประจำเพื่อป้องกันไวรัสใหม่ๆ ซอฟต์แวร์ป้องกันไวรัสควรมีบริการในการอัพเดตซิกเนเจอร์ไฟล์อย่างรวดเร็วและง่ายที่สุด

การป้องกันไวรัสที่เซิร์ฟเวอร์ การป้องกันไวรัสในเซิร์ฟเวอร์แต่ละประเภทนั้นอาจมีความแตกต่างกันได้ขึ้นอยู่กับฟังก์ชันหลักและการให้บริการของเซิร์ฟเวอร์ ขบวนการในการทำให้เซิร์ฟเวอร์มีความปลอดภัยสูงจะเรียกว่า การฮาร์ดเด็นนิ่ง(Hardening) เช่น

- *ลดช่องทางการถูกโจมตี* เช่นไม่ติดตั้งโปรแกรมหรือเซอร์วิสที่ไม่จำเป็น

- *อัพเดตซีเคียวริตี้แพตซ์* อัพเดตแพตซ์เพื่อปิดช่องโหว่หรือจะอ่อนหรือแก้ไขบั๊กของซอฟต์แวร์และระบบปฏิบัติการ ควรตรวจสอบให้ดีว่ามีผลกระทบต่อการให้บริการหรือไม่

- *การป้องกันไวรัสที่เว็บเซิร์ฟเวอร์* การคอนฟิกเว็บเซิร์ฟเวอร์เพื่อป้องกันการโจมตีนั้นเป็นสิ่งที่สำคัญยิ่งหรืออาจใช้เครื่องมือ เช่น IIS LockDown Tool ซึ่งเป็นเครื่องมือช่วยในการคอนฟิกเว็บเซิร์ฟเวอร์ โดยเครื่องมือนี้จะช่วยให้ติดตั้งเฉพาะเซอร์วิสที่จำเป็นเพื่อลดช่องทางในการถูกโจมตี

- *การป้องกันไวรัสเมล์เซิร์ฟเวอร์* โดยส่วนใหญ่ซอฟท์แวร์ป้องกันไวรัสที่ออกแบบเพื่อทำงานสำหรับเมลเซิร์ฟเวอร์อยู่ 2 ประเภทคือ SMTP Gateway Scanner ออกแบบมาเพื่อทำงานร่วมกับ SMTP Service มากกว่าที่จะทำงานร่วมกับซอฟต์แวร์อีเมล์ที่ใช้ อาจมีข้อจำกัดเกี่ยวกับสิ่งที่สามารถทำได้ เนื่องจากการทำงานของมันจะขึ้นอยู่กับโปรโตคอล SMTP เท่านั้น ส่วนประเภทที่ 2 คือ Integrated Server Scanner ซอฟต์แวร์ป้องกันไวรัสประเภทนี้จะทำงานร่วมกับซอฟต์แวร์อีเมล์ที่ใช้ ข้อดีคือมันสามารถทำงานร่วมกับซอฟต์แวร์อีเมล์ได้เป็นอย่างดีในการสแกนอีเมล์และไฟล์ที่แนบมาด้วย

- *การป้องกันไวรัสที่ดาต้าเบสเซิร์ฟเวอร์* การป้องกันดาต้าเบสเซิร์ฟเวอร์นั้นสามารถแบ่งออกเป็น 4 ส่วนหลักคือ 1). การปกป้องโฮสต์ คือการป้องกันตัวเซิร์ฟเวอร์ 2). การปกป้องด้ตาเบสเซอร์วิส คือแอพพลิเคชันหรือเซอร์วิสที่รันบนเซิร์ฟเวอร์เพื่อสามารถให้บริการดาต้าเบสผ่านเครือข่ายได้ 3). ดาต้าสโตร์ คือข้อมูลที่จัดเก็บในดาต้าเบส และ 4). ดาต้าเบสคอมมิวนิเคชัน การสื่อสารและโปรโตคอลต่างๆที่ใช้ระหว่างไคลเอนท์และเซิร์ฟเวอร์

การป้องกันไวรัสระดับเครือข่าย คือการป้องกันไวรัสจากข้างนอกไม่ให้สามารถเข้ามาในเครือข่ายภายในได้ ข้างนอกในที่นี้อาจเป็นเครือข่ายอินเทอร์เน็ต ดังนั้นการวางระบบป้องกันไวรัสควรทำให้ควบคู่และสอดคล้องกับมาตรการรักษาความปลอดภัยโดยทั่วไปขององค์กร

- *การติดตั้ง IDS* เนื่องจาก DMZ โซนเป็นส่วนที่มีความเสี่ยงต่อการถูกโจมตีมากที่สุด ดังนั้น ระบบบริหารเครือข่ายต้องสามารถตรวจจับและแจ้งเตือนการถูกโจมตีได้ทันที NIDS(Network Intrusion Detection System) เป็นระบบที่จะทำหน้าที่นี้ ถึงแม้ว่า NIDS จะเป็นส่วนหนึ่งของระบบการรักษาความปลอดภัยโดยรวมไม่ใช่ใช้เฉพาะการป้องกันไวรัส อย่างไรก็ตาม การตรวจจับและแจ้งเตือนโดย IDS นั้นก็เป็นอาการแรกที่จะนำไปสู่การถูกโจมตีในรูปแบบต่างๆ

- *การกรองข้อมูลในระดับแอพพลิเคชัน* การใช้แพ็กเก็ตฟิลเตอร์ริง เช่น เพื่อให้เฉพาะทราฟฟิกที่วิ่งผ่านพอร์ต 80 เท่านั้น ทำให้ผู้ใช้สามารถรับ/ส่งข้อมูลผ่านทางเว็บเพจเท่านั้น อย่างไรก็ตามการป้องกันเท่านี้อาจไม่เพียงพอ เพราะไวรัสอาจสามารถถ่ายโอนผ่านพอร์ต 80 ได้เช่นกัน ดังนั้น ควรติดตั้งระบบที่ใช้สแกนข้อมูลผ่านทางพอร์ต 80 เพื่อป้องกันไวรัสอีกชั้นหนึ่งด้วย เช่น ISA สามารถสแกนแพ็กเก็ตที่ผ่านเข้าออกไฟร์วอลล์ได้ เว็บและอีเมล์อาจถูกสแกนเพื่อตรวตเช็คว่าข้อมูลนั้นไม่มีไวรัสหรือเวิร์มแฝงมาด้วย
- *การบล๊อคเว็บไซต์* การฟิลเตอร์ URL เพื่อใช้สำหรับการบล๊อกเว็บไซต์ที่อาจเป็นอันตรายต่อองศ์กร เช่น เว็บแฮคเกอร์ เว็บโป๊อนาจาร เป็นต้น ซึ่งอาจจะมีไวรัสแฝงมาด้วย
- *การสร้างเครือข่ายกักกันเฉพาะ* การสร้างเครือข่ายกักกันเฉพาะสำหรับไคลเอนท์ที่ไม่ผ่านมาตรการรักษาความปลอดภัยขั้นพื้นฐาน เครือข่ายกักกันนี้อาจถูกจำกัดสิทธิ์หรือแม้กระทั่งบล๊อคการเข้าถึงทรัพยากรที่สำคัญของเครือข่ายภายใน เป็นต้น

สรุป

การป้องกันไวรัสที่จะให้ได้ผลนั้นไม่ใช่แค่การติดตั้งโปรแกรมป้องกันไวรัสเท่านั้น จากตัวอย่างของเหตุการณ์ในการโจมตีหลายเหตุการณ์ล่าสุดนั้นได้พิสูจน์ให้เห็นแล้วการป้องกันไวรัสนั้นต้องทำแบบเป็นระบบและต่อเนื่อง คอมพิวเตอร์ไวรัสนั้นมีการพัฒนาตัวเองและปรับเปลี่ยนเทคนิคในการโจมตีเรื่อยๆ ในเอกสารนี้ได้แนะนำแนวทางในการป้องกันไวรัสอย่างได้ผล และช่วยลดความรุนแรงในการถูกโจมตี เมื่อใช้ระบบนี้อาจช่วยในการวิเคราะห์หาจุดอ่อนของทั้งระบบ ตั้งแต่รั้วที่กั้นขวางไปจนถึงไคลเอนท์ที่ใช้งานในสำนักงานทั่วไป การที่ไม่ป้องกันในระดับใดระดับหนึ่งที่กล่าวมาอาจเป็นจุดอ่อนหรือช่องโหว่ของการถูกโจมตีก็ได้

องศ์กรควรทบทวนมาตรการป้องกันไวรัสเป็นประจำและปรับปรุงและปรับเปลี่ยนเมื่อจำเป็น การป้องกันไวรัสทุกๆ ด้านมีความสำคัญทั้งหมด ตั้งแต่การดาวน์โหลดซิกเนเจอร์ไฟล์เพื่ออัพเดต ไปจนถึงการปรับเปลี่ยนนโยบายในการรักษาความปลอดภัยขององศ์กร และการจัดฝึกอบรมเจ้าหน้าที่ พนักงานให้มีความรู้เกี่ยวกับการป้องกันไวรัสเบื้องต้น และแจ้งให้ผู้ดูแลระบบทราบถ้าเครื่องตนเองทำงานผิดปกติหรือคาดว่าจะติดไวรัส