ไวรัสคอมพิวเตอร์ Computer Virus

ไวรัสคอมพิวเตอร์ คือ โปรแกรมคอมพิวเตอร์ที่พัฒนาขึ้นมาเพื่อประสงค์ร้ายต่อระบบของผู้อื่น โดยการแฝงตัวมากับโปรแกรมหรือไฟล์ ซึ่งไวรัสคอมพิวเตอร์สามารถที่จะสำเนาตัวเองได้โดยอัตโนมัติ และสามารถกระจายตัวเองโดยการแทรกตัวติดไฟล์ต่างๆ นอกจากนี้โปรแกรมในกลุ่มของไวรัสยังมีความสามารถที่จะสำเนาตัวเองไปยังคอมพิวเตอร์เครื่องอื่นได้โดยผ่านทางระบบเครือข่ายคอมพิวเตอร์ หรืออาศัยสื่อ หรือพาหะทางคอมพิวเตอร์อื่น เช่น แผ่นดิสก์ ซีดี เป็นต้น

ประเภทของไวรัส

1. ไวรัสในบูตเซกเตอร์

สาเหตุ ไวรัสประเภทนี้จะอาศัยพื้นที่บนแผ่นดิสก์และฮาร์ดดิสก์ ในส่วนที่เรียกว่า "บูตเซกเตอร์" ซึ่งไวรัสจะฝังตัวอยู่ในส่วนดังกล่าว จะเริ่มทำงานทันทีที่มีการเปิดเครื่องใช้งาน (บูตเครื่อง) และจะกระจายตัวเองไปยังเครื่องอื่นโดยการสำเนาตัวเองลงบนแผ่นดิสก์ หรือฮาร์ดดิสก์ทุกครั้งที่มีการเรียกใช้งาน หรือสำเนาไฟล์ไปยังเครื่องอื่น ไวรัสประเภทนี้พบน้อยมากในปัจจุบัน

อาการ เครื่องคอมพิวเตอร์ไม่สามารถเปิดการใช้งานได้

ตัวอย่างไวรัส Stoned, Laoduong, Joshi, Print Screen, Ping pong B, Invader และ Michelangelo ฯลฯ

2. ไวรัสติดอยู่ในไฟล์

สาเหตุ ไวรัสประเภทนี้จะแทรกตัวเองมากับไฟล์ข้อมูล ไฟล์โปรแกรม หรือแนบมากับจดหมายอิเล็กทรอนิกส์ (e-mail) ในรูปของไฟล์ที่มีส่วนขยายในไฟล์ .exe, .dll, .com, .bat, .pif, .scr หรือมาในรูปแบบของเกมต่างๆ และยังมีอีกประเภทคือ มาโครไวรัส (Macro Virus) จะมากับไฟล์ของโปรแกรมไมโครซอฟต์ออฟฟิศ ซึ่งอยู่ในไฟล์ .doc, .xls, .ppt และเข้าไปเปลี่ยนไฟล์ normal.dot ซึ่งเป็นเท็มเพลตที่สำคัญของโปรแกรมไมโครซอฟต์ออฟฟิศ เมื่อทำการเก็บไฟล์ลงเครื่องหรือแผ่นดิสก์ ไวรัสจะถูกเก็บไว้ในไฟล์ทันที เมื่อมีการเรียกใช้โปรแกรมในครั้งต่อไป ไวรัสก็จะทำงาน

อาการ
1. ไฟล์จะมีขนาดใหญ่ขึ้น
2. ทำลายไฟล์งานจนเสียหายไม่สามารถเปิดใช้งานได้
3. รบกวนการทำงานของเครื่อง หรือโปรแกรมต่างๆ ที่เปิดใช้งานอยู่

ตัวอย่างไวรัส Taiwan3, Keypress, Darth Vader, Friday13th, Saddam, JoJor, WM.Comcept, WM.Cap, Melissa ฯลฯ

3. ไวรัสที่มาทางอินเทอร์เน็ต (Mobile treat and Malicious code)

สาเหตุ ไวรัสประเภทนี้จะอาศัยช่องโหว่ของโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมเว็บบราวเซอร์ (Web Browser) โปรแกรมอ่านจดหมายอิเล็กทรอนิกส์ (e-mail) โดยการกระจายตัวเองผ่านทางอีเมล์ การดาวน์โหลด โปรแกรมเกม และจากเว็บไซต์ที่มีการใช้ Active X Control เว็บไซต์ที่เขียนด้วยภาษาจาวา (Java) หรือเว็บไซต์ที่ใช้สคริปต์ในการทำงาน (script based)

อาการ
1. เครื่องสั่งเปิด/ปิด โปรแกรมด้วยตนเอง หรือปิดเครื่องอัตโนมัติ
2. จะมีการส่งอีเมล์พร้อมกับแนบไฟล์ไวรัสไปด้วยจากบัญชีรายชื่อ (address book) ที่เรามีอยู่ในเครื่องโดยที่เราไม่รู้ตัว
3. ส่งข้อมูล (packet) เป็นจำนวนมากไปยังเครื่องเซิร์ฟเวอร์ ทำให้เกิดการล่มของระบบเน็ตเวิร์ก
4. เครื่องหยุดทำงาน (hang) โดยไม่ทราบสาเหตุ
5. ทำลายข้อมูลบนฮาร์ดดิสก์

ตัวอย่างไวรัส CIH, LoveBug, Trojan, SirCam, W32.Navidad, CodeRed, Nimda ฯลฯ

ไวรัสควรรู้

หนอน (Worms) โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยอาศัยระบบเน็ตเวิร์ก (e-mail) ซึ่งการแพร่กระจายสามารถทำได้ด้วยตัวของมันเอง ซึ่งจะแพร่กระจายได้อย่างรวดเร็วและทำความเสียหายรุนแรงกว่าไวรัสมาก

โทรจัน (Trojan) โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้แฝงตัวเองเข้าไปในระบบและจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่างๆ และส่งกลับไปยังผู้ประสงค์ร้าย เพื่อเข้าใช้หรือโจมตีระบบในภายหลัง โปรแกรมโทรจันไม่ได้ถูกออกแบบมาเพื่อทำลายระบบ หรือสร้างความเสียหายต่อระบบคอมพิวเตอร์ ไม่สามารถทำสำเนาตัวเองและแพร่กระจายตัวเองได้

การป้องกัน

1. ติดตั้งโปรแกรมป้องกันไวรัส และปรับปรุง (update) ข้อมูลป้องกันไวรัสอยู่เสมอๆ
2. สแกนไวรัสบนเครื่อง และแผ่นดิสก์ ทุกครั้งที่ใช้เครื่อง (ใช้โปรแกรมป้องกันไวรัส)
3. ทำการสำรองข้อมูลสม่ำเสมอ
4. ตรวจสอบไวรัสก่อนเปิดไฟล์ที่แนบมาพร้อมกับอีเมล์ และไฟล์ที่ต้องการแนบพร้อมกับอีเมล์ควรตรวจสอบก่อนส่งถึงผู้อื่น
5. ควรทำการ Disable Javascript หรือ Cookies ในเว็บบราวเซอร์ และ Disable Macros ในไมโครซอฟต์ออฟฟิศ โดยอาจจะเรียกใช้เป็นครั้งคราวเมื่อจำเป็นและมั่นใจ
6. ป้องกันการเขียนให้กับแผ่นดิสก์ หรือสื่อคอมพิวเตอร์อื่นๆ ที่สามารถเคลื่อนย้ายได้
7. สร้างแผ่น Start-up ของเครื่อง เพื่อไว้ในกรณีที่เครื่องคอมพิวเตอร์ติดไวรัส และไม่สามารถเปิดใช้งานได้ ให้ใช้แผ่น Start-up ทำการบูตเครื่อง เพื่อกำจัดไวรัส

ECTI-21 NECTEC

Kevin Poulsen มีนามแฝงว่า Dark Dante
Poulsen ดังขึ้นมาเพราะเรื่องที่เขาลักลอบไปแอบดูการควบคุมระบบโทรศัพท์ของ Pacific Bell นอกจากนี้เขายังเคยใช้วิธีดโกงโดยการควบคุมระบบโทรศัพท์ทั้งหมดเพื่อให้เขาสามารถโทรฯ เข้าไปได้คนเดียว เพื่อเอาชนะการแข่งขันโทรศัพท์เข้าไปชิงรางวัลรถพอร์ชได้เป็นผลสำเร็จมาแล้ว Poulsen มีความสามารถในการเจาะเข้าไปตามเว็บไซต์แทบทุกชนิด ปัจจุบันเขาได้ชื่อว่าเป็นแคร็กเกอร์ที่ถูกจำคุกเป็นเวลานานที่สุดในสหรัฐอเมริกา (5 ปี)

Kevin Mitnick หรือที่เรียกกันอีกชื่อว่า Condor
เขาเป็นแคร็กเกอร์ที่มีคนรู้จักมากที่สุดในโลก Mitnick เริ่มอาชีพของเขาด้วยการแคร็กระบบโทรศัพท์ หลังจากนั้นเพียงไม่กี่ปีเขาประสบความสำเร็จอย่างสูงในการแคร็กระบบรักษาความปลอดภัยแทบทุกที่ ไม่ว่าจะเป็นหน่วยงานทางทหาร การพาณิชย์ บริษัทซอฟต์แวร์ และบริษัทอื่นๆ อีกมากมาย เขาสามารถแคร็ก North American Aerospace Defense Command ได้ตั้งแต่ยังเป็นวัยรุ่น ปัจจุบันเขาได้รับการลงโทษให้จำคุกเนื่องมาจากผลงานที่ได้ทำไว้ในปี 2537-2538

พฤศจิกายน ๒๕๔๕ November 2002

อาทิตย์ SUN	จันทร์ MO	อังคาร TUE	พุธ WED	พฤหัสบดี THU	ศุกร์ FRI	เสาร์ SAT
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

ฟอนต์: อีเอซี อู่ทอง/EACUThong ขนาด 14 พอยต์

ฟอนต์: พีเอสแอล พจมาน/PSL-Pojamarn ขนาด 15 พอยต์