ความรู้เบื้องต้นเกี่ยวกับไวรัสคอมพิวเตอร์

ประวัติไวรัสคอมพิวเตอร์

Virus (ไวรัสคอมพิวเตอร์) คืออะไร

ประเภทและวิธีการทำงานของไวรัสคอมพิวเตอร์

ประวัติไวรัสคอมพิวเตอร์

โปรแกรมที่สามารถสำเนาตัวเองได้เกิดขึ้นเป็นครั้งแรกในปี พ.ศ. 2526 โดย ดร.เฟรดเดอริก โคเฮน นักวิจัยของมหาวิทยาลัยเพนซิลวาเนีย สหรัฐอเมริกา ได้ทำการศึกษาโปรแกรมลักษณะนี้และได้ตั้งชื่อว่า "ไวรัส" แต่ไวรัสที่แพร่ระบาดและสร้างความเสียหายให้กับคอมพิวเตอร์ตามที่มีการบันทึกไว้ครั้งแรกเมื่อปี พ.ศ. 2529 ด้วยผลงานของไวรัสที่มีชื่อ "เบรน(Brain)" ซึ่งเขียนขึ้นโดยโปรแกรมเมอร์สองพี่น้องชาวปากีสถาน ชื่อ อัมจาด (Amjad) และ เบซิท(Basit) เพื่อป้องกันการคัดลอกทำสำเนาโปรแกรมของพวกเขาโดยไม่จ่ายเงิน

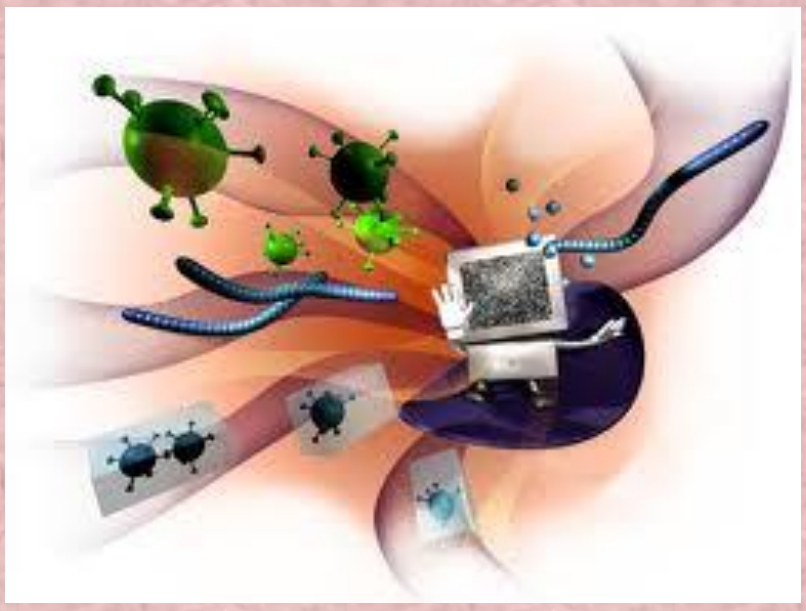
Virus (ไวรัสคอมพิวเตอร์) คืออะไร

คือ โปรแกรมคอมพิวเตอร์โปรแกรมหนึ่งที่มีผู้เขียนขึ้นมา โดยมีเป้าหมายที่ชัดเจน คือ สร้างความเสียหายให้กับคอมพิวเตอร์ มีลักษณะคล้ายเชื้อโรคขนาดเล็ก ซึ่งถ้าไวรัสมันได้เข้าไปอยู่ในเครื่องคอมพิวเตอร์แล้ว มันจะทำงานด้วยตัวของมันเอง และจะก่อให้เกิดปัญหาตามมามากมาย เช่น ขัดขวางการอ่านข้อมูล ขัดขวางการเข้าถึงข้อมูลในหน่วยความจำ ขัดขวางการทำงานของอุปกรณ์ต่อพ่วงต่างๆ และที่สร้างความเสียหายอย่างมากที่สุด คือ การเข้าไปทำลายแฟ้มข้อมูลหรือเข้าไปทำลายระบบต่างๆ ของเครื่องคอมพิวเตอร์ จนบางครั้งไม่สามารถใช้งานได้อีกต่อไป การทำงานของไวรัสแต่ละตัวจะขึ้นอยู่กับวัตถุประสงค์ของผู้เขียนโปรแกรมนั้นขึ้นมา เช่น ทำลายระบบปฏิบัติการ โปรแกรมใช้งานหรือข้อมูลอื่น ๆ ที่อยู่ในคอมพิวเตอร์ หรือรบกวนการทำงาน เช่น การบู๊ตระบบช้าลง เรียกใช้โปรแกรมได้ไม่สมบูรณ์ หรือเกิดอาการค้าง (แฮงก์ไม่ทราบสาเหตุ) เกิดข้อความวิ่งไปมาที่หน้าจอ หรือกรอบข้อความเตือนไม่ทราบสาเหตุ เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้น โดยมีการรายงานว่ามีจำนวนเซกเตอร์ที่เสียเพิ่มขึ้นทั้ง ๆ ที่ยังไม่ได้ใช้โปรแกรมใด ๆ เข้าไปตรวจหาเลย ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ ๆ ก็หายไป

ประเภทและวิธีการทำงานของไวรัสคอมพิวเตอร์

1. บู๊ตเซกเตอร์ไวรัส (Boot Sector Viruses หรือ Boot Infector Viruses) คือ ไวรัสที่เก็บตัวเองอยู่ในบู๊ตเซกเตอร์ของฮาร์ดดิสก์ การทำงานของบู๊ตเซกเตอร์ไวรัส บู๊ตเซ็กเตอร์ไวรัสจะทำงานได้ก็ต่อเมื่อเราเสียบแผ่นดิสก์เก็ตคาไว้ที่ไดรว์ พอเราเปิดเครื่องคอมพิวเตอร์ขึ้นมาเครื่องจะบู๊ตข้อมูลจากแผ่นดิสก์ก่อน ถึงแม้ว่าแผนนี้จะเป็น Boot disk หรือไม่ก็ตาม แต่ถ้ามีไวรัสประเภทบู๊ตเซ็กเตอร์อยู่ก็จะสามารถส่งไวรัสเข้ามาเล่นงานเครื่องคอมพิวเตอร์ของเราได้ทัน ไวรัสประเภทนี้บางตัวก็ไม่มีอันตราย แต่บางตัวก็มีอันตรายมากถึงขั้นทำให้เครื่องคอมพิวเตอร์บู๊ตไม่ขึ้นเลยทีเดียวคือ เมื่อคอมพิวเตอร์เริ่มทำงานขึ้นมาตอนแรก เครื่องจะเข้าไปอ่านบู๊ตเซกเตอร์ โดยในบู๊ตเซกเตอร์จะมีโปรแกรมเล็ก ๆ ไว้ใช้ในการเรียกระบบปฏิบัติการขึ้นมาทำงานอีกทีหนึ่ง ไวรัสจะเข้าไปแทนที่โปรแกรมดังกล่าว และไวรัสประเภทนี้ถ้าไปติดอยู่ในฮาร์ดดิสก์โดยทั่วไป จะเข้าไปอยู่บริเวณที่เรียกว่า Master Boot Sector หรือ Parition Table ของฮาร์ดดิสก์นั้น ถ้าบู๊ตเซกเตอร์ของดิสก์ใดมีไวรัสประเภทนี้ติดอยู่ทุก ๆ ครั้งที่บู๊ตเครื่องขึ้นมา ตัวโปรแกรมไวรัสจะทำงานก่อนและจะเข้าไปฝังตัว อยู่ในหน่วยความจำเพื่อเตรียมพร้อมที่ จะทำงานตามที่ได้ถูกโปรแกรมมา แล้วตัวไวรัสจึงค่อยไปเรียกระบบปฏิบัติการให้ขึ้นมาทำงานต่อไป ทำให้เหมือนไม่มีอะไรเกิดขึ้น

2. โปรแกรมไวรัส (Program Viruses หรือ File Intector Viruses) เป็นไวรัสอีกประเภทหนึ่งที่จะติดอยู่กับโปรแกรมซึ่งปกติก็คือ ไฟล์ที่มีนามสกุลเป็น COM หรือ EXE และไวรัสบางชนิดสามารถเข้าไปติดอยู่ในโปรแกรมที่มีนามสกุลเป็น sysและโปรแกรมประเภท Overlay Programsได้ด้วย โปรแกรมโอเวอร์เลย์ปกติจะเป็นไฟล์ที่มีนามสกุลที่ขึ้นต้นด้วย OV วิธีการที่ไวรัสใช้เมื่อที่จะ เข้าไปติดโปรแกรมมีอยู่สองวิธี คือ การแทรกตัวเองเข้าไปอยู่ในโปรแกรมผลก็คือหลังจากที่โปรแกรมนั้นติดไวรัสไปแล้ว ขนาดของโปรแกรมจะใหญ่ขึ้น หรืออาจมีการสำเนาตัวเองเข้าไปทับส่วนของโปรแกรมที่มีอยู่เดิม ดังนั้นขนาดของโปรแกรมจะไม่เปลี่ยนและยากที่จะซ่อมให้กลับเป็นดังเดิม การทำงานของโปรแกรมไวรัสโดยทั่วไป คือ เมื่อมีการเรียกโปรแกรมที่ติดไวรัส ส่วนของไวรัสจะทำงานก่อนและจะถือโอกาสนี้ฝังตัวเข้าไปอยู่ในหน่วยความจำทันทีแล้วจึงค่อยให้ โปรแกรมนั้นทำงานตามปกติต่อไป เมื่อไวรัสเข้าไปฝังตัวอยู่ในหน่วยความจำแล้ว หลังจากนี้ไปถ้ามีการเรียกโปรแกรมอื่น ๆ ขึ้นมาทำงานต่อ ตัวไวรัสก็จะสำเนาตัวเองเข้าไป ในโปรแกรมเหล่านี้ทันที เป็นการแพร่ระบาดต่อไป วิธีการแพร่ระบาดของโปรแกรมไวรัสอีกแบบหนึ่งคือ เมื่อมีการเรียกโปรแกรมที่มีไวรัสติดอยู่ ตัวไวรัสจะเข้าไปหาโปรแกรมอื่น ๆ ที่อยู่ในดิสก์เพื่อทำสำเนาตัวเองลงไปทันทีแล้วจึงค่อยให้โปรแกรมที่ถูกเรียก นั้นทำงานตามปกติต่อไป



3. ม้าโทรจัน (Trojan Horse) เป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็นโปรแกรมธรรมดาทั่ว ๆ ไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียกขึ้นมาทำงาน แต่เมื่อถูกเรียกขึ้นมาแล้ว ก็จะเริ่มทำลายตามที่โปรแกรมถูกเรียกใช้ทันที ม้าโทรจันบางตัวถูกเขียนขึ้นมาใหม่ทั้งชุดโดยคนเขียนจะทำการตั้งชื่อโปรแกรมพร้อมชื่อรุ่นและคำอธิบายการใช้งานที่ดูสมจริงเพื่อหลอกให้คนที่จะเรียกใช้ตายใจ จุดประสงค์ของคนเขียนม้าโทรจันอาจจะเช่นเดียวกับคนเขียนไวรัส คือ เข้าไปทำ อันตรายต่อข้อมูลที่มีอยู่ในเครื่อง หรืออาจมีจุดประสงค์เพื่อที่จะล้วงเอาความลับของระบบ คอมพิวเตอร์ ม้าโทรจันนี้อาจจะถือว่าไม่ใช่ไวรัส เพราะเป็นโปรแกรมที่ถูกเขียนขึ้นมาโดด ๆ และจะไม่มีการเข้าไปติดในโปรแกรมอื่นเพื่อสำเนาตัวเอง แต่จะใช้ความรู้เท่าไม่ถึงการณ์ของผู้ใช้เป็นตัวแพร่ระบาดซอฟต์แวร์ที่มีม้าโทรจันอยู่ในนั้น และนับว่าเป็นหนึ่งในประเภทของโปรแกรมที่มีความอันตรายสูง เพราะยากที่จะตรวจสอบและสร้างขึ้นมาได้ง่าย ซึ่งอาจใช้แค่แบตซ์ไฟล์ก็สามารถโปรแกรมประเภทม้าโทรจันได้

4. โพลีมอร์ฟิกไวรัส (Polymorphic Viruses) เป็นชื่อที่ใช้ในการเรียกไวรัสที่มีความสามารถในการแปรเปลี่ยนตัวเองได้เมื่อสร้างสำเนาตัวเองเกิดขึ้น ซึ่งอาจเกิดได้ถึงหลายร้อยรูปแบบ ผลก็คือทำให้ไวรัสเหล่านี้ยากต่อการถูกตรวจจับโดยโปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกนอย่างเดียว ไวรัสใหม่ ๆ ในปัจจุบันที่มีความสามารถนี้เริ่มมีจำนวนเพิ่มมากขึ้นเรื่อย

5. สทีลต์ไวรัส (Stealth Viruses) เป็นชื่อเรียกไวรัสที่มีความสามารถในการพรางตัวต่อการตรวจจับได้ เช่น ไฟล์อินเฟกเตอร์ ไวรัสประเภทที่ไปติดโปรแกรมใดแล้วจะทำให้ขนาดของ โปรแกรมนั้นใหญ่ขึ้น ถ้าโปรแกรมไวรัสนั้นเป็นแบบสทีลต์ไวรัส จะไม่สามารถตรวจดูขนาดที่แท้จริงของโปรแกรมที่เพิ่มขึ้นได้ เนื่องจากตัวไวรัสจะเข้าไปควบคุมดอส เมื่อมีการใช้คำสั่ง DIRหรือโปรแกรมใดก็ตามเพื่อตรวจดูขนาดของโปรแกรม ดอสก็จะแสดงขนาดเหมือนเดิมทุกอย่างราวกับว่าไม่มีอะไรเกิดขึ้น

ผู้หาข้อมูล : ตรีรัตน์ ศรีธัชชนก
ที่มา: http://www.com4child.org