ไวรัสคอมพิวเตอร์

นาย สัญญา คล่องในวัย
หน่วยปฏิบัติการวิจัยและพัฒนาเทคโนโลยีคอมพิวเตอร์และระบบอัตโนมัติ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม

ABSTRACT – In the past, computer viruses have created a huge damage to the computer systems over the world. The objective of the new viruses is to destroy the system and cause the effects to the societies and economics. Virus's development and concepts of writing it has trended to be more powerful and cause more damage everyday. This paper presents information about computer viruses in the detail of techniques and concepts of the way they work, objective of the attack, trend, producing techniques, protection methods, and the future technology.

KEY WORDS – Computer Virus, Virus Technique

บทคัดย่อ – ระยะเวลาที่ผ่านมาไวรัสคอมพิวเตอร์ ได้สร้างความเสียหายแก่ระบบคอมพิวเตอร์ทั่วโลกเป็นอย่างมาก เป้าหมายการสร้างความเสียหายที่เกิดจากไวรัสคอมพิวเตอร์ชนิดใหม่ๆ ในปัจจุบัน ได้สร้างผลกระทบต่อสังคมและเศรษฐกิจในทุกๆด้าน การพัฒนาการของไวรัสโดยเทคนิคแบบใหม่ แนวคิดในการเขียนโปรแกรมมีแนวโน้มสู่ความรุนแรง และสร้างความเสียหายในวงกว้างมากขึ้น บทความนี้เป็นการนำเสนอข้อมูลเกี่ยวกับไวรัสคอมพิวเตอร์ แนวคิดเทคนิคการทำงาน เป้าหมายการโจมตี แนวโน้มของการเกิดไวรัสเทคนิค, แนวคิดใหม่ในการสร้างไวรัสคอมพิวเตอร์, การป้องกันไวรัส และเทคโนโลยีในอนาคต

คำสำคัญ – ไวรัสคอมพิวเตอร์, เทคนิคไวรัส

1. บทนำ

ไวรัสคอมพิวเตอร์เป็นโปรแกรมสำหรับทำงานบนระบบคอมพิวเตอร์ประเภทหนึ่งมีการทำงานเหมือนกับโปรแกรมประยุกต์โดยทั่วไป แต่วัตถุประสงค์ในการทำงานของไวรัสคอมพิวเตอร์เป็นไปในทางลบมากกว่าการสร้างสรรค์ มีรูปแบบการทำงานเฉพาะตัวการแพร่กระจาย, การฟักตัว, การทำลายที่คล้ายคลึงกับการทำงานของเชื้อไวรัส แนวคิดของโปรแกรมเชิงทำลายในยุคแรกเกิดขึ้นบนระบบยูนิกซ์ ซึ่งมีการพัฒนามาจากการเขียนโปรแกรมสคริปต์บนยูนิกซ์เพื่อความสะดวกในการทำงาน เช่น การเขียนเชลล์สคริปต์ให้มีการลบไฟล์ที่ไม่ต้องการเมื่อถึงกำหนดเวลา, วันที่ ที่ตั้งไว้ โดยโปรแกรมพวกนี้ยังไม่นับว่าเป็น “ไวรัส” เพราะยังไม่มีการแพร่กระจาย แต่ต่อมาได้พัฒนากลายมาเป็นไวรัสที่ใช้วันที่ในการทำงาน (Date Trigger) หรือการลักลอบทำสำเนาเชลล์ควบคุมการเซ็ต uid, การทำสำเนาไฟล์บัญชีรายชื่อผู้ใช้ระบบ และรหัสผ่าน วิธีที่ใช้คือการวางหลุมพราง การใช้โปรแกรมพวก Trojan ทำสำเนาไฟล์ไปยังไดเรกทอรี่ที่สามารถเข้าถึงโดยทั่วไป เช่น การเพิ่มคำสั่ง suid ลงในไฟล์ “.login” ดังตัวอย่าง “cp/bin/sh/tmp/gotu ; chmod 4777 /tmp/gotu สำเนาของข้อมูลที่สร้างขึ้นจะถูกเก็บที่ไดเรกทอรี่ /tmp *(ไฟล์หรือข้อมูลต่างๆ จะเข้าถึงได้โดยผู้เป็นเจ้าของไฟล์และการตรวจสอบ uid ที่ถูกต้องเท่านั้น)* นอกจากนี้ยังมีโปรแกรมประเภทหนอน (Worm) ซึ่งฝังตัวเองภายในระบบพยายามทำลายระบบรักษาความปลอดภัยของระบบปฏิบัติการ โปรแกรมหนอน เริ่มมีการแพร่กระจายตัวเองซึ่งเป็นจุดเริ่มต้นของไวรัสหนอน และ

เริ่มมีการใช้คำว่าไวรัสคอมพิวเตอร์ ในปี 1988 ไวรัสได้แพร่กระจายบนระบบเน็ตเวิร์คแต่การทำลายไม่รุนแรงมากนักเนื่องจากขณะนั้นระบบเน็ตเวิร์คถูกใช้ในวงจำกัด จากนั้นการพัฒนาของไวรัสก็เปลี่ยนจากการทำงานบนระบบยูนิกซ์ ซึ่งมีหลายตระกูล มาเป็นไวรัสที่ทำงานบนระบบดอส และโค้ดแบบ X86 ซึ่งมีการใช้งานอย่างกว้างขวาง การเพิ่มจำนวนของไวรัสคอมพิวเตอร์ในปัจจุบันมีอัตราคงที่ ในแต่ละปีจะมีไวรัสที่ถูกค้นพบประมาณ 1,000 ตัวต่อปี หรือกล่าวได้ว่ามีไวรัสคอมพิวเตอร์เกิดขึ้นวันละ 2 – 3 ตัว [1] การศึกษาทำความเข้าใจเกี่ยวกับไวรัส เป็นสิ่งจำเป็นเพื่อนำมาใช้ในการควบคุมการแพร่กระจาย การปกป้องข้อมูลและระบบไม่ให้ถูกทำลายจากไวรัสคอมพิวเตอร์

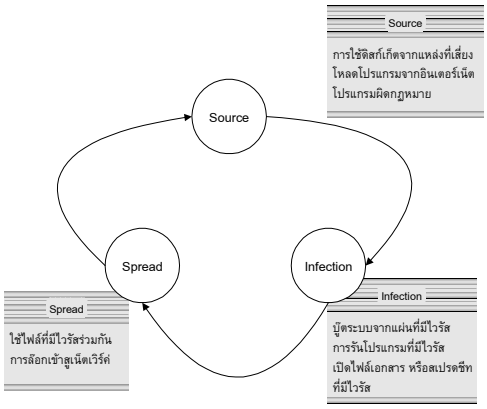
2. ไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ สามารถแพร่กระจายไปกับโปรแกรมไฟล์, แฟ้มข้อมูลเอกสาร, สเปรดชีต, ไฟล์ระบบปฏิบัติการ, แผ่นดิสก์ข้อมูล, การแลกเปลี่ยนข้อมูลโดยแผ่นดิสก์เก็ต, การบู๊ตระบบจากแผ่นดิสก์เก็ตที่ไม่ปลอดภัย, การแนบไฟล์ต่างๆ ไปกับจดหมายอิเล็กทรอนิกส์ ไวรัสจะทำงานตามรหัสของโปรแกรมที่บรรจุเอาไว้เพื่อสร้างความเสียหายแก่ข้อมูล หรือโปรแกรมระบบ ไวรัสคอมพิวเตอร์จะไม่สามารถทำลายระบบฮาร์ดแวร์ เช่น โพรเซสเซอร์ จอภาพ หรือคีย์บอร์ดได้ แต่ไวรัสสามารถควบคุม หรือก่อกวนการทำงานของระบบฮาร์ดแวร์ ทำให้ระบบไม่สามารถทำงานได้ตามปกติเช่น การเข้าทำลายข้อมูลของ BIOS ที่ใช้ FLASH BIOS [ไวรัสเชอร์โนบิล, Win CIH] ทำให้ไม่สามารถบูตระบบได้ หรือไวรัสบางตัวจะเข้าควบคุมการทำงานของการ์ดแสดงผล ทำให้ภาพที่ปรากฏหน้าจอหายไป ไม่แสดงตัวอักษร มีตัวอักษรที่อยู่บรรทัดบนของจอตกลงมาขณะใช้งาน หรือกำหนดค่าที่ผิดพลาดให้แก่ตัวควบคุมบังคับให้ลำอิเล็กตรอนในหลอดภาพยิงที่ตำแหน่งเดิมเป็นเวลานานๆ จะทำให้สารฟอสเฟอร์ที่เคลือบจอภาพให้เรืองแสงเกิดการไหม้เป็นจุดได้ นอกจากนี้ยังมีไวรัสที่สร้างขึ้นเพื่อความสนุกสนานมีเสียงดนตรีขณะที่ไวรัสทำงาน เช่น ไวรัส ลาวดวงเดือนที่เคยระบาดในเมืองไทยช่วงหนึ่ง หรือไวรัสหลอกลวงที่เป็นจดหมายเวียนต่างๆ (Hoax Virus) ซึ่งได้สร้างความตื่นตระหนก และการก่อกวนมากกว่าการมุ่งเน้นทำลายระบบเป็นต้น

2.1 วงจรชีวิตของไวรัสคอมพิวเตอร์

การทำงานของไวรัสคอมพิวเตอร์ มีรูปแบบเฉพาะที่แตกต่างจากโปรแกรมโดยทั่วไป ซึ่งลักษณะหรือพฤติกรรมที่แสดงออกนั้นทำให้สามารถศึกษาถึงวงจรชีวิตและการทำงานในแต่ละช่วงของการทำงานของไวรัส

วงจรชีวิตของไวรัสคอมพิวเตอร์แบ่งออกได้เป็น 3 ช่วง คือ แหล่งที่มาของไวรัส (Source) ช่วงการติดเชื้อ (Infection) และช่วงการแพร่กระจาย (Spread) แหล่งที่มาของไวรัสจะมาได้จากสื่อต่างๆ โดยในช่วงการติดเชื้อนี้เป็นช่วงที่เครื่องคอมพิวเตอร์มีไวรัส จากนั้นไวรัสก็พร้อมที่จะแพร่กระจายต่อไป



รูปที่ 1. แสดงวงจรชีวิตของไวรัสคอมพิวเตอร์

2.2 เทคโนโลยีของไวรัสคอมพิวเตอร์

เทคนิคต่างๆ ถูกนำมาใช้ในการพัฒนาขีดความสามารถของไวรัสเพื่อให้สามารถหลบหลีกการตรวจสอบและค้นหา โดยเทคนิคเหล่านี้มีการเปลี่ยนแปลงไปในทางที่ซับซ้อนมากขึ้นตามประเภทการทำลาย

2.2.1 Stealth เป็นเทคนิคที่ออกแบบให้โปรแกรมสามารถป้องกันตัวเองจากการค้นหา หรือกำจัดได้ โดยทั่วไปจะใช้วิธีขัดขวาง (Interrupt) การทำงานของกระบวนการอ่านของระบบดิสก์โดยเมื่อไฟล์ที่ไม่มีไวรัสถูกอ่านขึ้นมามันจะถูกแทรกรหัสของไวรัสเข้าไป

(Read Stealth Virus) นอกจากนี้ไวรัสที่ทำการเปลี่ยนแปลงขนาดของไฟล์ข้อมูล, ไดเรกทรอรี่ของข้อมูล (Size Stealth Virus) เมื่อไวรัสทำงานจะทำการแทรกรหัสระหว่างการอ่านข้อมูล เช่น ไวรัสมีขนาดข้อมูล 1,024 ไบต์ และไฟล์ข้อมูลเดิมมีขนาด 4,096 ไบต์ ขนาดของไฟล์จะเป็น (1,024 + 4,096) 5,120 ไบต์ ซึ่งขนาดของไฟล์ถูกเปลี่ยนแปลง และจะถูกตรวจพบได้ ไวรัสจะขัดขวางการทำงานระบบของไดเรกทอรี่ โดยการอ่านค่าขนาดไฟล์ที่เป็น 5,120 ไบต์ขึ้นมา และลบออกด้วยขนาดของตัวเอง และจะส่งผลที่ได้ไปยังระบบเพื่อแสดงผลอีกครั้ง

2.2.2 Polymorphic อาศัยการเปลี่ยนแปลงรูปแบบของไวรัส มีการแบ่งรหัสของตัวไวรัสเป็นส่วนย่อยแทรกอยู่ระหว่างแฟ้มข้อมูล เมื่อแฟ้มข้อมูลทำงานรหัสไวรัสจะถูกนำไปรวมกันในหน่วยความจำ การใช้การเข้ารหัสและการถอดรหัสก่อนการทำงานด้วยคีย์เฉพาะ ทำให้ยากต่อการตรวจสอบจากรหัสลายเซ็นไวรัส *(รหัสลายเซ็นไวรัส Virus Signature เป็นรหัสเฉพาะของไวรัสที่ผู้เขียนโปรแกรมป้องกันไวรัสได้ทำการถอดรหัสออกมา ซึ่งไวรัสแต่ละตัวก็จะมีรูปแบบของข้อมูลที่แตกต่างกัน)* โดยพื้นฐานของไวรัสประเภทนี้มาจากโครงสร้างของ TPE (Trident Polymophic Engine) และ MtE (Mutation Engine) ซึ่งมีรายงานการค้นพบในยุโรปช่วงปี1992 [2]

2.2.3 Multipartite การทำงานหลากรูปแบบในตัวเอง สามารถแพร่กระจายทางไฟล์ปกติ และสามารถแพร่กระจายในส่วนของ Boot Record ของระบบดิสก์ได้ เมื่อไฟล์ข้อมูลเอกสารที่ติดไวรัสประเภทนี้ ถูกอ่านขึ้นมาทำงาน ไวรัสก็จะทำงานโดยการคัดลอกตัวเองเข้าไปบันทึกหรือเขียนทับข้อมูลในส่วนของระบบ Boot Record เมื่อมีการบูตระบบครั้งต่อไป ไฟล์ทุกไฟล์ที่ถูกเรียกใช้งานก็จะติดไวรัส

2.2.4 Companion Virus เทคนิคนี้ถูกคิดค้นขึ้นมาโดยอาศัยช่องว่างในการทำงานของระบบปฏิบัติการ และการทำงานตามเงื่อนไขที่ถูกต้องของระบบปฏิบัติการในการทำลายระบบและแพร่กระจาย การทำตัวเสมือนหนึ่งเป็นโปรแกรมปกติของระบบถูกนำมาใช้ โดยอาศัยหลักการในการรันโปรแกรมแบบลำดับ ถ้าชื่อไฟล์เหมือนกัน ไฟล์ที่มีนามสกุลเป็น .COM จะทำงานก่อนไฟล์ที่มีนามสกุลเป็น .EXE เสมอ เมื่อไฟล์ CHKDSK.EXE ติดไวรัส ไวรัสจะทำการสร้างไฟล์ใหม่ในชื่อ CHKDSK.COM ซึ่งเป็นโปรแกรมไวรัส เมื่อเราเรียกไฟล์ CHKDSK มาทำงานในครั้งต่อไปไฟล์ CHKDSK.COM ซึ่งเป็นไวรัสจะทำงานก่อน

2.2.5 Malicious Programs เทคนิคเป็นเทคนิคที่เกิดขึ้นในช่วงหลังๆ จากที่มีการใช้โปรแกรมภาษาจาวาและ Active X ซึ่งเป็นภาษาที่นิยมใช้กับอินเทอร์เน็ต โดยอาศัยช่องว่างของตัวรักษาความปลอดภัยภายในโปรแกรม Browser, E-mail, โปรแกรมที่ใช้การสื่อสารพูดคุยผ่านเน็ตเวิร์ค โดยไวรัสจะเข้าควบคุมระบบจากระยะไกล หรือการขโมยข้อมูลรหัสผ่านเข้าสู่ระบบจากเครื่องเป้าหมายส่งคืนไปยังผู้ที่เข้าโจมตีระบบ ลักษณะเหล่านี้มักจะเป็นโปแกรมประเภทหลุมพลาง (Trojan Horse) เป้าหมายจะไม่ได้เน้นการทำลายไฟล์หรือข้อมูล แต่มีจุดประสงค์ในการเข้ายึดครองระบบ

2.3 ประเภทของไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ที่มีอยู่ในปัจจุบันสามารถจัดประเภทต่างๆ ได้ 3 ประเภทใหญ่คือ

2.3.1 โปรแกรมไฟล์ไวรัส (Program Viruses) เป็นไวรัสที่ทำงานและแพร่กระจายกับไฟล์ทั่วๆ ไป ปกติจะเป็นไฟล์ที่มีนามสกุลเป็น .COM, .EXE นอกจากนี้ในปัจจุบันยังสามารถทำงานได้กับไฟล์ของระบบในลักษณะต่างๆ เช่น .SYS, .DLL, .OVL และ .SCR ไวรัสแฟ้มข้อมูลยังเป็นไวรัสที่เฉพาะเจาะจงสำหรับแต่ละระบบปฏิบัติการอีกด้วย เช่น DOS, WINDOWS, UNIX ฯลฯ

2.3.2 บูตไวรัส (Boot Viruses) เป็นไวรัสที่ไม่ทำงานกับไฟล์ข้อมูล แต่จะทำงานในพื้นที่เฉพาะของแผ่นดิสก์เก็ต และฮาร์ดดิสก์ สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งผ่านทางดิสก์เก็ต ไวรัสประเภทนี้มีการแพร่กระจาย และทำงานได้ดีกว่าไวรัสประเภทแรก

บูตไวรัสจะแฝงตัวเองในพื้นที่ที่ เรียกว่า Boot Sector ของระบบดิสก์ ซึ่งทุกครั้งที่มีการบูตระบบข้อมูลที่เก็บอยู่ในส่วนนี้จะถูกอ่านไปเก็บไว้ในหน่วยความจำเสมอ และไวรัสที่แฝงอยู่ก็จะทำงานด้วยเช่นกัน บูตไวรัสสามารถทำงานได้กับระบบไฟล์ของ DOS, Windows 3.X, Windows9X, Windows NT, หรือ Novell Netware นอกจากนี้การกำจัดไวรัสประเภทนี้อาจทำให้ระบบไม่สามารถบู๊ตระบบกลับมาทำงานได้อีกด้วย

2.3.3 ไวรัสมาโคร (Macro Viruses) ไวรัสประเภทใหม่นี้ สามารถติดไปกับไฟล์ต่างๆ ที่มีความสามารถในการใช้งานมาโครได้ เช่น เอกสารไมโครซอฟท์เวิร์ด มีความสามารถในการสร้างเทมเพลตได้ มาโครไวรัสจะแฝงตัวเข้ากับเทมเพลต ไวรัสชนิดนี้สามารถกระจายผ่านการดาวน์โหลดข้อมูลบนอินเตอร์เนต การแชร์ข้อมูล และการแนบเอกสารไปกับ E-Mail

เมื่อไวรัสคอมพิวเตอร์ทั้ง 3 ประเภทถูกสร้างขึ้นมาจะมีการนำเอาเทคนิคต่างๆ ที่ได้กล่าวไว้ตอนต้นมาผสมผสานเข้าไป ทำให้ไวรัสในปัจจุบันมีลักษณะเด่นหลายรูปแบบในตัวเอง ใช้เทคนิคหลายแบบในแต่ละส่วนของโค้ดไวรัส ทำให้ยากแก่การตรวจสอบและทำลาย

3. ก้าวต่อไปของไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ จัดเป็นรูปแบบหนึ่งของการคุกคามข้อมูล และความปลอดภัยของระบบ ในปัจจุบันนี้เทคโนโลยีของไวรัสมีการพัฒนารูปแบบที่แตกต่างมาก เมื่อไวรัสตัวหนึ่งประสบความสำเร็จในการทำลายระบบไวรัสตัวนั้นก็จะกลายมาเป็นแม่แบบ ของไวรัสรุ่นต่อๆ ไปและพัฒนาความรุนแรงเพิ่มขึ้นทำให้เกิดปัญหาของไวรัสมากยิ่งขึ้น และวิธีการที่จะนำเสนอต่อไปนี้จะถูกใช้มากขึ้นในอนาคต

3.1 เครื่องมือสำหรับการพัฒนาไวรัส (Virus Authoring Tools) วิธีการนี้ถูกนำมาช่วยในการสร้างไวรัสอย่างแพร่หลายในปัจจุบัน เครื่องมือเหล่านี้มีลักษณะเป็นโปรแกรมช่วยสร้างที่ง่ายต่อการใช้งาน มีส่วนเชื่อมต่อกับผู้ใช้ (User Interface) แบบง่ายๆ ผู้สร้างไม่จำเป็นต้องรู้เรื่องระบบคอมพิวเตอร์มากนักเพียงทำตามคำแนะนำก็สามารถสร้างไวรัสขึ้นมาได้ โดยตัวโปรแกรมจะมีโครงสร้างหลัก (Engine) ที่ใช้เทคนิค Polymophic Virus โดยภายในอาจมีโครงสร้างแบบ MtE หรือ TPE ไวรัส นอกจากนี้ยังเปิดโอกาสให้ผู้สร้างใส่รหัสโปรแกรม และนำโปรแกรมต้นแบบ (Source Program) มาดัดแปลงเพิ่มเติมได้ เครื่องมือที่ช่วยในการพัฒนาไวรัสลักษณะนี้ทำให้จำนวนไวรัสเพิ่มมากขึ้น แต่ไวรัสที่สร้างโดยวิธีนี้มักจะถูกตรวจพบได้ง่ายๆ เพราะรูปแบบการทำงานไม่ซับซ้อนมาก อย่างไรก็ตามหากผู้พัฒนามีความรู้เกี่ยวกับระบบ จะสามารถดัดแปลงให้ตรวจจับยากขึ้น และการทำลายสูงขึ้นด้วย เครื่องมือเหล่านี้สามารถหาได้ง่ายจากระบบอินเทอร์เน็ตในปัจจุบัน และยังเป็นที่นิยมในหมู่นักเรียนนักศึกษาบางกลุ่ม นอกจากนี้ยังมีการแจกจ่ายและแลกเปลี่ยนไวรัสกันระหว่างกลุ่ม

3.2 การโจมตีระบบป้องกัน เป้าหมายของการโจมตีของไวรัสคอมพิวเตอร์ในปัจจุบันได้เปลี่ยนแปลงรูปแบบต่างไปจากเดิมที่มุ่งการสร้างความเสียหายต่อไฟล์ข้อมูล และไฟล์ระบบ ซึ่งจะทำให้ถูกตรวจจับจากระบบป้องกันได้โดยง่าย เนื่องจากเทคโนโลยีการป้องกันไวรัสในปัจจุบันมักมีการตรวจจับพฤติกรรมของไวรัสในแบบเดิมได้ดี ปัจจุบันไวรัสจะยกเลิกการทำงานของตัวป้องกันไวรัสก่อนแล้วจึงเริ่มทำงานการโจมตีไฟล์ และแพร่กระจาย

3.3 ไวรัสบนเครือข่าย ไวรัสบนระบบเครือข่ายเป็นอีกรูปแบบหนึ่งของการแพร่กระจาย สามารถแพร่กระจายผ่านการสื่อสารข้อมูลภายในเครือข่ายทั้งภายใน และภายนอก รวมทั้งการดาวน์โหลดข้อมูลโปรแกรมจากสถานที่ต่างๆ และการสนทนาบนระบบเครือข่าย โดยทั่วไปไวรัสมักจะมีลักษณะเป็นหลุมพราง (Trojan Horse) โดยค้นหาข้อมูลที่สำคัญจากเครื่องเป้าหมายเพื่อเป็นประตูนำไปสู่การเข้าโจมตีระบบ หรือการควบคุมระบบในภายหลัง [การเจาะระบบจากนักเจาะระบบ Hacker และการโจมตีจากเครือข่ายระยะไกลแบบ Command – Bomber]

3.4 Multi - Platform เนื่องจากเทคนิคการพัฒนารูปแบบของโปรแกรมที่ไม่ยึดติดกับระบบในปัจจุบันที่นิยม

กันอย่างแพร่หลาย เพราะมีความยืดหยุ่นในการทำงานสูง แต่จุดนี้ทำให้ผู้พัฒนาไวรัส อาศัยช่องว่างการทำงานของระบบมาพัฒนาโปรแกรมไวรัสในลักษณะที่ไม่ขึ้นกับระบบออกมา ซึ่งอาศัยเทคนิคการเขียนโปรแกรมโดยใช้ java และ Active X มากขึ้น

3.5 Hardware - Level จากแนวคิดแบบเก่าที่ว่า "ไวรัสคอมพิวเตอร์เป็นโปรแกรม (ซอฟต์แวร์) ชนิดหนึ่งที่ทำงานบนระบบคอมพิวเตอร์ จะไม่สามารถสร้างความเสียหายต่อระบบฮาร์ดแวร์ได้" ได้ถูกท้าทายโดยไวรัสชนิดใหม่ๆ ที่พัฒนาขึ้นมาโดยไม่ได้มุ่งเน้นที่การทำลายข้อมูลอย่างเดียว แต่เปลี่ยนเป็นการมุ่งเน้นการทำลายข้อมูลถาวรในระดับฮาร์ดแวร์ การเข้าควบคุมในระดับฮาร์ดแวร์จะทำให้การทำลายสูงขึ้น การเข้าไปแก้ไขข้อมูลที่สำคัญของระบบใน CMOS หรือการทำลายข้อมูล BIOS ของระบบที่ใช้เทคโนโลยี Flash BIOS การเพิ่มความสามารถของไวรัสในการเข้าโจมตีจุดอ่อนของระบบแบบนี้ก่อให้เกิดความเสียหายในระดับที่รุนแรง (ไวรัสเชอร์โนบิล CIH มีความสามารถดังกล่าว)

3.6 ไวรัสที่พัฒนาโดยภาษาระดับสูง ไวรัสในปัจจุบันไม่ได้มีการพัฒนามาจากภาษาภาษาระดับล่างที่เป็นแอสเซมบลี (Assembly Language) แต่เพียงอย่างเดียว แต่ยังมีการนำเอาภาษาระดับสูงมาใช้มากขึ้น ทำให้ความง่ายในการพัฒนามีมากขึ้น นอกจากนี้การนำเอาความสามารถของภาษาระดับสูงมาใช้เพิ่มความสามารถให้กับไวรัส การที่ไวรัสสามารถยกระดับความสามารถของตัวเอง ผ่านการสื่อสารทางอินเทอร์เน็ต เมื่อตัวไวรัสตรวจพบว่ามีการ Up – Date Code และฟังก์ชั่นใหม่ๆ ได้ โดยเทคนิคนี้เป็นการเลียนแบบการทำงานของโปรแกรมป้องกันไวรัสในการ Up – Date ฐานข้อมูลไวรัส และรหัสใหม่ๆ ของไวรัส (Virus Signature)

4. เทคนิคในการตรวจจับไวรัส

เทคนิคในการตรวจจับ และวิเคราะห์การทำงานของไวรัสคอมพิวเตอร์ที่นิยมใช้กันอย่างแพร่หลายในโปรแกรมสำหรับป้องกันไวรัสที่สำคัญและจะกล่าวถึงในบทความนี้ 2 วิธีคือ

4.1 วิธีการวิเคราะห์พฤติกรรม เทคนิคนี้ใช้วิธีการวิเคราะห์การทำงานของโปรแกรมต่างๆ ที่ถูกโหลดขึ้นมาทำงาน โดยโปรแกรมป้องกันไวรัสจะทำหน้าที่ตรวจจับพฤติกรรมการทำงานต่างๆ ที่เป็นรูปแบบเฉพาะของไวรัส เช่น ตรวจสอบการพยายามฝังตัวของโปรแกรมลงในหน่วยความจำ (Memory Resident Program) การตรวจจับโปรแกรมที่พยายามจะเข้าแก้ไขข้อมูลในส่วนของบูตเรคคอร์ดของฮาร์ดดิสก์ ซึ่งเมื่อตรวจจับพฤติกรรมที่เข้าข่ายที่ระบุได้ว่าเป็นไวรัสโปรแกรมป้องกันก็จะแจ้งเตือน

4.2 วิธีการเปรียบเทียบข้อมูลในระดับไบนารี่ เทคนิคนี้เป็นเทคนิคที่ใช้เปรียบเทียบข้อมูลของไฟล์หรือโปรแกรมในระดับไบนารี่ โดยจะนำเอาข้อมูลไวรัสจากฐานข้อมูลที่เก็บรหัสรายเซ็นของไวรัสมาทำการเปรียบเทียบกับชุดของข้อมูลในไฟล์ต่างๆ ซึ่งวิธีการนี้จะต้องอาศัยการ Up-date ฐานข้อมูลรหัสลายเซ็นไวรัสอย่างสม่ำเสมอเพื่อที่จะทำให้โปรแกรมป้องกันไวรัสสามารถรู้จักไวรัสชนิดใหม่ๆ และวิธีการนี้จะใช้ไม่ได้ผลกับไวรัสที่เป็น Stealth และ Polymorphic นอกจากนี้วิธีการนี้จะทำได้ช้า

เทคนิคที่กล่าวข้างต้นเป็นเทคนิคพื้นฐานในการตรวจสอบและวิเคราะห์การทำงานของโปรแกรมต้องสงสัย เทคนิคแบบผสมผสานจึงถูกนำมาใช้มากขึ้น นอกจากนี้ผู้พัฒนาโปรแกรมป้องกันไวรัสแต่ละราย ก็จะมีเทคนิคพิเศษเฉพาะตัวในการเพิ่มประสิทธิภาพในการค้นหาไวรัส ความเร็วในการทำงานของโปรแกรม การกำจัดไวรัส และการค้นคืนข้อมูลที่เกิดความเสียหายจากไวรัส และการทำสำเนาข้อมูลที่สำคัญของระบบเก็บสำรองไว้ใช้ในกรณีฉุกเฉินเป็นต้น

5. ผลกระทบต่อสังคม

ไวรัสคอมพิวเตอร์ ได้ก่อให้เกิดปัญหาและความเสียหายต่อสังคมทั้งทางด้านเศรษฐกิจ และทางด้านจริยธรรม ความเสียหายที่เกิดจากนักพัฒนาโปรแกรมที่มีความสามารถสูงแต่ขาดความรับผิดชอบต่อสังคม จากข่าวการทำลายระบบของ ไวรัสที่ผ่านมามีมูลค่าความเสียหายต่อธุรกิจโดยรวมสูง เช่น *ไวรัสเชอร์โนบิลได้*

สร้างความเสียหายต่อระบบคอมพิวเตอร์เฉพาะในเอเชียมากกว่า 100,000 เครื่อง ไวรัสเมริสสา ได้สร้างความเสียหายในอเมริกามากกว่า 200,000 เครื่อง [4] นอกจากความเสียหายที่เกิดขึ้นแล้ว เหตุการณ์ลักษณะนี้ ก็มีส่วนเป็นแรงกระตุ้นให้แก่ผู้ที่มีแนวคิด และนักพัฒนาไวรัสรุ่นใหม่ๆ เกิดตามมาอีกอย่างหลีกเลี่ยงไม่ได้ แนวทางการป้องกันดูจะเป็นทางออกอย่างหนึ่งในการป้องกันความเสียหายที่เกิดจากการคุกคามโดยไวรัสคอมพิวเตอร์ นักพัฒนาระบบความปลอดภัย และนักวางแผนไอที จะต้องลงทุนในส่วนรักษาความปลอดภัยเป็นมูลค่าที่สูงขึ้นและการทุ่มงบประมาณในการพัฒนา การวิจัย แม้ว่าระบบป้องกันจะมีการพัฒนาไปมากขึ้นแต่นักพัฒนาก็พยายามพัฒนาไวรัสเพื่อที่จะผ่านแนวป้องกันให้ได้เช่นกัน

ในบางประเทศมีการแจ้งข้อมูลความเสียหายที่เกิดจากไวรัสคอมพิวเตอร์ ลักษณะการทำลาย และการฝ่าเข้าสู่แนวป้องกัน ต่อหน่วยงานที่ดูแลด้านความปลอดภัยของระบบคอมพิวเตอร์โดยรวม เพื่อใช้เป็นบทเรียนกับหน่วยงานอื่น สำหรับบางประเทศทำในสิ่งที่ตรงกันข้าม คือ การปกปิดข้อมูลที่เกิดขึ้น เพื่อเหตุผลที่ต้องการรักษาชื่อเสียง ของหน่วยงาน หรือผู้รับผิดชอบดูแลระบบความปลอดภัย ทำให้การสร้างความเข้าใจ และการแบ่งปันประสบการณ์เกี่ยวกับไวรัส และพฤติกรรมการแพร่ระบาดต่างๆ ทำได้น้อยลง ส่งผลให้ การแก้ไขและป้องกันทำได้ยากยิ่งขึ้น

6. บทสรุป

จากข้อมูลที่นำเสนอข้างต้น ไวรัสคอมพิวเตอร์เกิดขึ้นมาจากการพัฒนาเทคนิคในการเขียนโปรแกรมเพื่อการทำงานในลักษณะของการทำลาย สร้างความเสียหาย แต่เทคโนโลยีบางส่วนของไวรัส เป็นเทคนิคที่มีประโยชน์สามารถนำไปพัฒนาโปรแกรมทั่วไปให้มีความสามารถในการฝังตัวเองในหน่วยความจำ การป้องกันการลบ เป็นต้น นอกจากนี้จุดที่ไวรัสคอมพิวเตอร์ใช้ เพื่ออาศัยเป็นช่องทางเข้าสู่การโจมตีระบบคือการอาศัยผู้ใช้เป็นพาหะ หากผู้ใช้คอมพิวเตอร์ทุกคนมีวินัยที่ดีในการใช้เครื่องคอมพิวเตอร์ และมีวินัยที่ดีในการทำงานกับระบบ แล้วไวรัสคอมพิวเตอร์ก็ไม่สามารถสร้างความเสียหายต่อผู้ใช้ สังคม และเศรษฐกิจ

ทางหนึ่งในการสร้างวินัยที่ดีในการใช้ระบบคอมพิวเตอร์ คือการปรับเปลี่ยนพฤติกรรมที่เสี่ยงต่อการนำเอาไวรัสคอมพิวเตอร์เข้าสู่ระบบ เช่น การเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการทำงานของไวรัส การฝึกอบรมการใช้งานระบบพื้นฐานการฝึกนิสัยที่ดีในการใช้งานแผ่นดิสก์เก็ต หรือไฟล์ต่างๆ ที่นำมาจากที่อื่น ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือการดาวน์โหลดจากอินเตอร์เน็ต ควรทำการสแกนตรวจหาไวรัสก่อนการใช้งานทุกครั้ง การหมั่น Up-date เพิ่มความสามารถของโปรแกรมป้องกันไวรัสตามคำแนะนำของโปรแกรม สิ่งเหล่านี้จะเป็นเกราะป้องกันไวรัสคอมพิวเตอร์เข้าคุกคามระบบคอมพิวเตอร์ได้

เอกสารอ้างอิง

[1] Vesselin Bontchev *"Future Trends in Virus Writing"*, Virus Test Center, University of Hamburg
[2] Tarkan Yetiser *"Polymophic Viruses Implementation, Detection and Protection"* VDS Advanced Research Group, Baltimore us. (1993)
[3] VIRUS Reference Document Symantec Corp. http://www.symantec.com
[4] CERT Coordination Center
http://www.cert.org

Sanya Klongnaivai (Research Assistant) : received his B.Eng. in Technical Education in Computer Technology from King Mongkut's Institute of Technology North Bangkok, in 1996. He was a student trainee at CTL, NECTEC, in 1994. After graduated in 1995, he started working at CTL, NECTEC, as a research assistant. His main research areas are developing the electronics and Control unit in photovoltaic system and fuzzy controller for consumer products. He is also working in PC's performance testing project in the IND department, NECTEC and Implement algorithms for Y2K Checker Program in Y2K Project. His interests are Computer Architecture, PC Technology and Computer Virus Technology.