

ภัยคุกคามจาก ผู้ประสงค์ร้าย (ไวรัส)



จุดประสงค์การเรียนรู้

- นักเรียนบอกความหมายของไวรัสคอมพิวเตอร์ได้
- นักเรียนบอกประเภทของไวรัสคอมพิวเตอร์ได้
- นักเรียนสามารถจำแนกลักษณะของประเภทไวรัสคอมพิวเตอร์ได้
- นักเรียนบอกอาการของเครื่องคอมพิวเตอร์ที่ติดไวรัสคอมพิวเตอร์ได้
- นักเรียนสามารถตรวจหาและบอกวิธีในการป้องกันไวรัสคอมพิวเตอร์ได้



ไวรัสคอมพิวเตอร์คืออะไร

ไวรัสคอมพิวเตอร์ คือ โปรแกรมคอมพิวเตอร์หรือชุดคำสั่งเล็กๆ ที่เขียนขึ้นเพื่อให้รบกวนการทำงาน หรือทำลายไฟล์ข้อมูล ตลอดจนไฟล์โปรแกรมต่างๆ ในระบบคอมพิวเตอร์

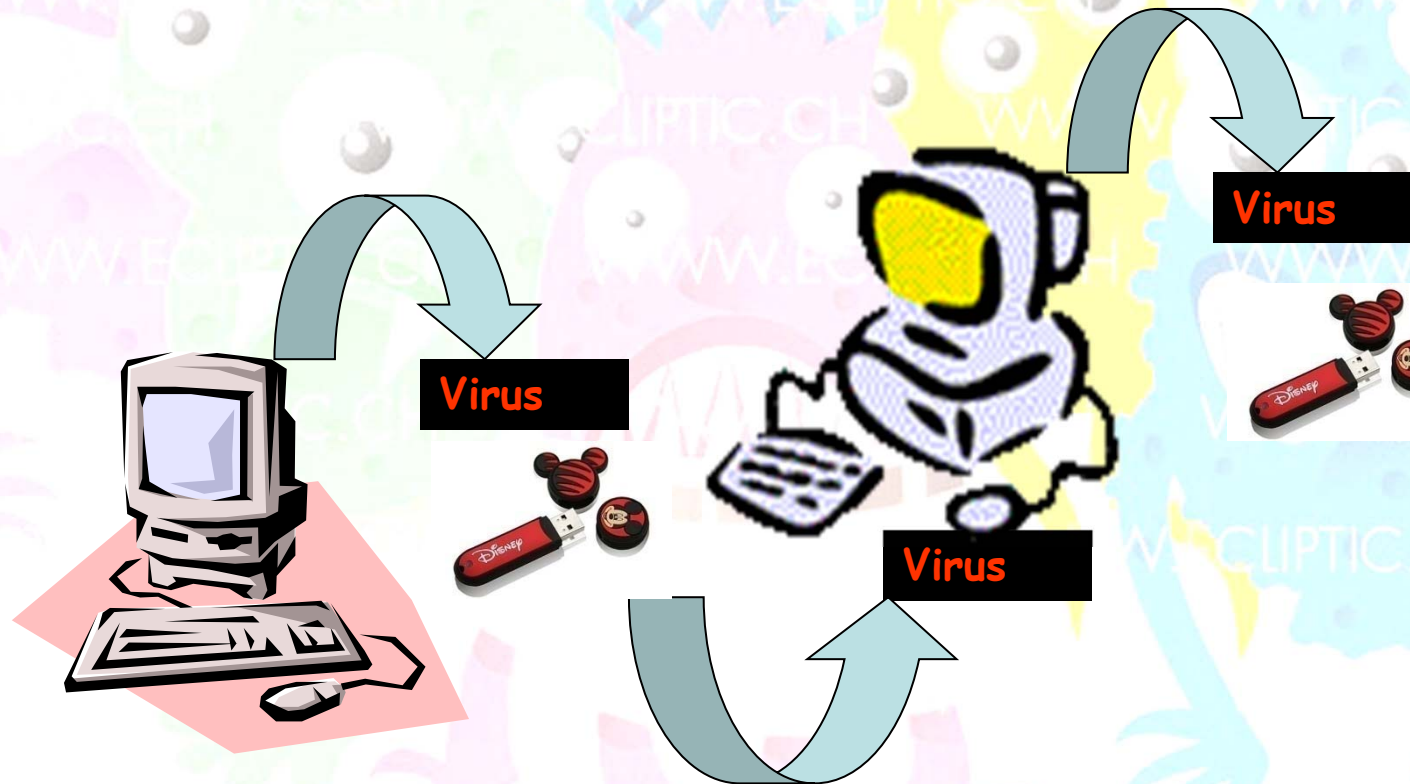
คุณสมบัติพิเศษของไวรัสคอมพิวเตอร์ก็คือ ไวรัสคอมพิวเตอร์สามารถหลบหลีกซ่อนตัวอยู่ในเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง และสำเนาคัดลอกเพื่อแพร่กระจายตัวเองไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ได้



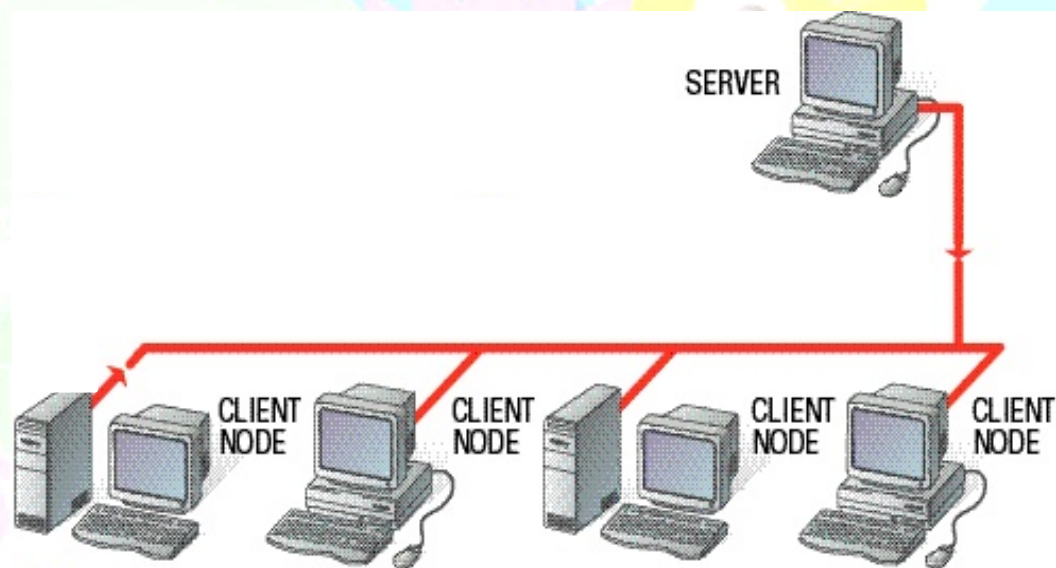
ช่องทางในการแพร่กระจายไวรัส

คอมพิวเตอร์

1. หน่วยความจำสำรอง



2. ระบบเครือข่าย



ประเภทของไวรัส

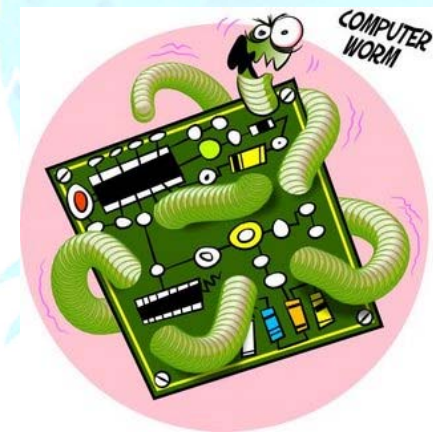
1. หนอนอินเทอร์เน็ต (Worm)
2. บูตเซกเตอร์ไวรัส (Boot Sector Viruses)
3. ไฟล์ไวรัส (File Viruses)
4. ม้าโทรจัน (Trojan Horse)
5. สคริปต์ไวรัส (Scripts Viruses)
6. สปแอมเมล (Spam Mail)
7. มาโครไวรัส (Macro virus)



1. หนอนอินเทอร์เน็ต (Worm)

หนอน (Worm) เป็นรูปแบบหนึ่งของไวรัส มีความสามารถในการทำลายระบบในเครื่องคอมพิวเตอร์สูงที่สุดในบรรดาไวรัสทั้งหมด สามารถกระจายตัวได้รวดเร็ว ผ่านทางระบบอินเทอร์เน็ต

สาเหตุที่เรียกว่าหนอนนั้น คงจะเป็นลักษณะของการกระจายและทำลาย ที่คล้ายกับหนอนกินผลไม้ ที่สามารถกระจายตัวได้มากมาย รวดเร็ว ระดับการทำลายล้างยิ่งสูงขึ้น



2. บูตเซกเตอร์ไวรัส (Boot Sector Viruses)

คือไวรัสคอมพิวเตอร์ที่แพร่เข้าสู่เป้าหมายในระหว่างเริ่มทำการบูตเครื่อง ส่วนมาก มันจะติดต่อเข้าสู่ Flash Drive, CD, DVD, ระหว่างกำลังสั่งปิดเครื่อง เมื่อนำแผ่นที่ติดไวรัสนี้ไปใช้กับเครื่องคอมพิวเตอร์เครื่องอื่นๆ ไวรัสก็จะเข้าสู่เครื่องคอมพิวเตอร์ตอนเริ่มทำงานทันที

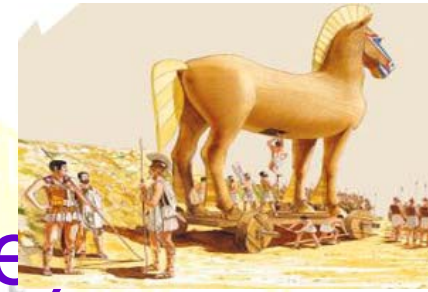


3. ไฟล์ไวรัส (File Viruses)

- ไวรัสอีกประเภทหนึ่งที่มีมักจะระบาดด้วยการติดไปกับไฟล์โปรแกรมที่มีนามสกุลเป็น com, exe, sys, dll
- ไฟล์โปรแกรมจะมีขนาดที่โตขึ้นจากเดิม
- บางชนิดอาจจะสำเนาตัวเองไปทับบางส่วนของโปรแกรม
- ตัวอย่าง Jerusalem, Die Hard II



4. ม้าโทรจัน (Trojan Horse)



- เป็นไวรัสประเภทสปาย (SPY) ที่จะคอยล้วงความลับจากเครื่องของเรา ส่งไปให้ผู้เขียนโปรแกรม
- ระบาดกันมากบนอินเทอร์เน็ต ความลับที่ม้าโทรจันจะส่งกลับไปยังผู้เขียนโปรแกรมได้แก่ Username, Password หรือเลขที่บัตรเครดิต

	Description
TROJ_APS.216576	
TROJ_BACKDOOR.AC	
TROJ_BEARDED	
TROJ_BLEEM	
TROJ_BO2K.PLUG	
TROJ_BOCLIENT	
TROJ_BUDDY.B	
TROJ_BUDDY.C	Virus Name: TROJ_BUDDY.C
TROJ_CATFOD.A	Virus Type: Trojan
TROJ_CINDY	Alias: TROJ_AOL.BUDDY.C, TROJ_BUDDY.D, BUDDY.C
TROJ_CLICK	Language: English
TROJ_DA_RIPPER	Platform: Windows
	Size of Virus: 236,544 bytes
	Seen in the Wild: Yes
	Detected by Scan Engine#: 2,080
	Detected by Pattern File#: 580
	Trigger Date: Any Day
	Payload: Others(steals password)
	Payload: Modifies Files
	Payload: Displays Graphics
	Payload: Displays Message

5) สคริปต์ไวรัส (Scripts Viruses)

- ไวรัสสายพันธุ์นี้เขียนขึ้นมาจากภาษาที่ใช้ในการเขียนโปรแกรม เช่น VBScript, JavaScript
- ไวรัสคอมพิวเตอร์เหล่านี้จะทำงานเมื่อผู้ใช้เปิดหรือเรียกใช้งานไฟล์นามสกุล .vbs, .js ที่เป็นไวรัส ซึ่งอาจจะติดมาจากการเรียกดูไฟล์ HTML ในหน้าเว็บเพจบนเครือข่ายอินเทอร์เน็ต



6. สปแอมเมล (Spam Mail)

คือ จดหมายอิเล็กทรอนิกส์ (E-Mail) ที่เราไม่พึงประสงค์ หรือ
เพื่อประโยชน์อย่างใดอย่างหนึ่ง

จุดมุ่งหมาย เพื่อก่อกวนทำให้เกิดความรำคาญ และ เสียเวลา
ซึ่งการส่งสปแอมเมลนั้นอาจมีวัตถุประสงค์ในการโฆษณาสินค้า
หรืออื่น ๆ



7. มาโครไวรัส (macro virus)

คือไวรัสที่ติดไฟล์เอกสารชนิดต่างๆ ซึ่งมีความสามารถในการใส่คำสั่งมาโครสำหรับทำงานอัตโนมัติในไฟล์เอกสารด้วย ตัวอย่างเอกสารที่สามารถติดไวรัสได้ เช่น ไฟล์ไมโครซอฟท์เวิร์ด ไมโครซอฟท์เอ็กเซล เป็นต้น



อาการของเครื่องที่ติดไวรัส

สามารถสังเกตการทำงานของเครื่องคอมพิวเตอร์ถ้ามีอาการดังต่อไปนี้
อาจเป็นไปได้ว่าได้มีไวรัสเข้าไปติดอยู่ในเครื่องแล้ว อาการที่ว่ามัน
ได้แก่

- ใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
- ขนาดของโปรแกรมใหญ่ขึ้น
- วันเวลาของโปรแกรมเปลี่ยนไป
- ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อยๆ

- เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
- เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้อยู่
- เป็นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
- ขนาดของหน่วยความจำที่เหลือน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
- ไฟล์แสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ๆ ก็หายไป
- เครื่องทำงานช้าลง
- เครื่องบูตตัวเองโดยไม่ได้สั่ง
- ระบบหยุดทำงานโดยไม่ทราบสาเหตุ
- เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้น โดยมีการรายงานว่าจำนวนเซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นกว่าแต่ก่อน โดยที่
- ยังไม่ได้ใช้โปรแกรมใดเข้าไปตรวจหาเลย



การแก้ไขระบบที่ติดไวรัสคอมพิวเตอร์

1. ตรวจสอบไวรัสที่เข้ามาคุกคามระบบว่าเป็นไวรัสอะไร ทำได้ 2 วิธี ดังนี้

- นำเครื่องคอมพิวเตอร์อื่นที่มีซอฟต์แวร์ **Anti-virus** ติดตั้งอยู่และได้รับการ **update**ฐานข้อมูลไวรัสตรวจสอบเสมอ
- ใช้บริการระบบตรวจหาไวรัสคอมพิวเตอร์ผ่านเว็บ (ฟรี) เช่น

<http://housecall.trendmicro.com/housecall/>

หรือ

<http://www.pandasoftware.com/products/activescan/>



2. การจัดหาโปรแกรมสำหรับกำจัดไวรัสคอมพิวเตอร์ตัวนั้นๆ
(Fix Tool) มาใช้กำจัดไวรัสบนระบบ ซึ่งสามารถ
download ได้ฟรีจากเว็บไซต์ต่างๆ เช่น
<http://securityresponse.symantec.com/avcenter/tools.list.html> หรือ
<http://www.pandasoftware.com/download/utilities/> เป็นต้น

3. Update ฐานข้อมูลไวรัสของโปรแกรม Anti-virus
แล้วใช้โปรแกรมทำการตรวจหาไวรัสบนระบบอีกครั้ง

การป้องกันไวรัส

2 วิธีแรกสำคัญที่สุด

1. ติดตั้งโปรแกรม Anti-virus บนระบบ
2. ตรวจสอบและอุดช่องโหว่ของระบบปฏิบัติการอย่างสม่ำเสมอ
3. ปรับแต่งการทำงานของระบบปฏิบัติการและซอฟต์แวร์บนระบบให้มีความปลอดภัยสูง
4. ใช้ความระมัดระวังในการเปิดอ่านอี-เมลล์ และการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ
5. สำรองข้อมูลที่สำคัญบนระบบอยู่เสมอ

โปรแกรมป้องกันไวรัส (**Antivirus software**)

โปรแกรมป้องกันไวรัสมี 2 แบบใหญ่ ๆ คือ

1. แอนติไวรัส เป็นโปรแกรมป้องกันไวรัสทั่วไป จะค้นหาและทำลายไวรัส
2. แอนติสพายแวร์ เป็นโปรแกรมป้องกันการโจรกรรมข้อมูล จากไวรัสสพายแวร์ และจากแฮคเกอร์ รวมถึงการกำจัด Adware ซึ่งเป็นป๊อปอัพโฆษณาอีกด้วย

จงตอบคำถามต่อไปนี้

1. ไวรัสคอมพิวเตอร์หมายถึง.....

.....

2. ไวรัสคอมพิวเตอร์แบ่งได้กี่ประเภท อะไรบ้าง.....

.....

3. จงบอกลักษณะอาการของเครื่องคอมพิวเตอร์ที่แสดงอาการว่าติดไวรัสมา 5 ข้อ

.....

.....

4. ให้นักเรียนบอกการป้องกันไวรัสคอมพิวเตอร์ทำได้อย่างไรบ้าง

.....

.....

5. จงยกตัวอย่างชื่อโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่นักเรียนรู้จักมาอย่างน้อย

3 โปรแกรม.....