ภัยคุกคามการรักษาความปลอดภัยระบบสารสนเทศ

ปัจจุบันเราใช้คอมพิวเตอร์ในการจัดเก็บข้อมูลหรือสารสนเทศ ติดต่อสื่อสาร รวมทั้งใช้ในการถ่ายโอนข้อมูลระหว่างคอมพิวเตอร์โดยอาศัยการทำงานผ่านระบบเครือข่าย แต่ก็ยังมีคงมีความเสี่ยงอยู่มากถ้ายังไม่มีการควบคุมหรือป้องกันที่ดี อาจถูกผู้ไม่หวังดีเข้าโจมตีระบบคอมพิวเตอร์หรือระบบเครือข่าย และทำความเสียหายต่อระบบสารสนเทศได้

การโจมตีหรือการบุกรุกเครือข่าย

หมายถึง ความพยายามที่จะเข้าไปในระบบ การแก้ไขข้อมูลหรือเปลี่ยนแปลงระบบ การทำให้ระบบไม่สามารถใช้งานได้ และการทำให้ข้อมูลเป็นเท็จ สำหรับการกระทำที่อาจก่อให้เกิดความเสียหายดังกล่าวจะเรียกว่า การโจมตี (Attack)

ผู้ที่เป็นเหตุให้เกิดเหตุการณ์ดังกล่าวเกิดขึ้นจะเรียกว่าผู้โจมตี (Attacker) หรือบางที่จะเรียกว่าแฮคเกอร์ (Hacker) หรือแคร็คเกอร์ (Cracker) ก็ได้โดยบุคคลทั่วไปเข้าใจเป็นความหมายเดียวกันแต่ความเป็นจริงแล้วคำสองคำดังกล่าวมีความแตกต่างกันอย่างมาก

ภัยคุกคาม (Threat)

หมายถึง สิ่งที่อาจก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน อาจเกิดจากธรรมชาติหรือตัวบุคคลผู้เกี่ยวข้องไม่ว่าจะเกิดด้วยความตั้งใจหรือไม่ก็ตาม

ภัยคุกคามนั้นอาจไม่เกิดขึ้นเลยก็ได้ถ้ามีการป้องกันที่ดี หรือถ้าเรามีการเตรียมการที่ดีเมื่อมีเหตุการณ์เกิดขึ้นก็จะช่วยลดความเสียหายได้ การรักษาความปลอดภัยของคุณสมบัติข้อมูลหรือสารสนเทศ ทั้ง 3 ด้าน ที่กล่าวมาแล้วในบทที่ 1 จะเป็นสิ่งที่ช่วยต้านภัยคุกคามที่อาจเกิดขึ้น

ประเภทของภัยคุกคาม

แบ่งประเภทของภัยคุกคามออกเป็น 2 ลักษณะ

1. ภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย
   - ภัยคุกคามทางตรรกะ (Logical)
   - ภัยคุกคามทางกายภาพ (Physical)

2. ภัยคุกคามที่เกิดขึ้นกับข้อมูลหรือสารสนเทศ

ประเภทของภัยคุกคาม

1. ภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย

- ระบบคอมพิวเตอร์และระบบเครือข่าย เป็นเทคโนโลยีที่มีความทันสมัยและพัฒนาอยู่เสมอ อีกทั้งยังมีราคาแพง
- ที่สำคัญที่สุดระบบดังกล่าวใช้เป็นเป็นสถานที่เก็บข้อมูลหรือสารสนเทศของ
- จำเป็นต้องดูแลรักษาระบบให้เป็นอย่างดี หากเกิดปัญหาขึ้นจะทำให้ข้อมูลหรือสารสนเทศของเราเสียหายตามไปด้วย
- สามารถแบ่งประเภทของภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายนั้น ได้ 2 ประเภท

ประเภทของภัยคุกคาม

1. ภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย

1. ภัยคุกคามทางตรรกะ (Logical)

ภัยคุกคามที่เกิดขึ้นนั้นจะมุ่งเน้นไปทางด้านข้อมูลหรือสารสนเทศ ไม่ว่าจะเป็นการเข้าใช้ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือขัดขวางไม่ให้ระบบคอมพิวเตอร์ทำงานได้ตามปกติ และอาจเข้าใช้ข้อมูล ลบข้อมูล และแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ซึ่งการกระทำดังกล่าวนั้น ส่วนใหญ่เกิดจากฝีมือของผู้ใช้งานคอมพิวเตอร์แทบทั้งสิ้น

ประเภทของภัยคุกคาม

1. ภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย

2. ภัยคุกคามทางกายภาพ (Physical)

ภัยคุกคามลักษณะนี้มุ่งสร้างเน้นอุปกรณ์ประเภทฮาร์ดแวร์ที่ใช้ในระบบคอมพิวเตอร์และระบบเครือข่าย เช่น ทำให้ฮาร์ดดิสก์เสีย ทำให้คอมพิวเตอร์ทำงานผิดพลาด โดยส่วนใหญ่แล้วจะเกิดภัยจากธรรมชาติ อาจเป็นน้ำท่วม ไฟไหม้ ฟ้าฝ่า เป็นต้น และบางครั้งเกิดจากการกระทำของมนุษย์ที่ทำความเสียหายให้กับตัวเครื่องและอุปกรณ์ ทั้งโดยเจตนาหรือไม่เจตนา

ประเภทของภัยคุกคาม

2. ภัยคุกคามที่เกิดขึ้นกับข้อมูลหรือสารสนเทศ

ผู้ใช้คอมพิวเตอร์ไม่ว่าจะเป็นบุคคลธรรมดา หรือบุคคลผู้ใช้งานในองค์กร ต่างก็มีข้อมูลหรือสารสนเทศที่จำเป็นต้องเก็บรักษาไว้ ซึ่งมีทั้งข้อมูลที่สามารถเปิดเผยและข้อมูลที่ ไม่สามารถเปิดเผยได้ถือเป็นความลับของตัวผู้ใช้งานเองหรือองค์กรดังกล่าว จำเป็นอย่างยิ่งที่ต้องมีการป้องกันรักษาความปลอดภัยของข้อมูลดังกล่าวไว้ อย่างไรก็ตามเราไม่สามารถแน่ใจได้เลยว่าข้อมูลของเราจะปลอดภัยร้อยเปอร์เซ็นต์ได้ตลอดไป

1. แฮคเกอร์ (Hacker)

- บุคคลที่มีความสนใจใคร่รู้ลึกลงไปในความลับและความซับซ้อนของการทำงานของคอมพิวเตอร์ โดยเฉพาะระบบปฏิบัติการและซอฟต์แวร์
- ส่วนใหญ่จะเป็นโปรแกรมเมอร์ฝีมือดีด้วย
- เป็นผู้มีความรูลึกซึ้งในเรื่องระบบปฏิบัติการและการเขียนโปรแกรม รู้ช่องโหว่ต่างๆ และรู้ไปถึงต้นเหตุของช่องโหว่เหล่านั้นในระบบ
- แฮกเกอร์คือผู้ที่ใฝ่หาความรู้อยู่ตลอดเวลา และยินดีถ่ายทอดความรู้ที่มีอยู่อย่างไม่หวง

http://www.fm100cmu.com/blog/ITWave/uploads/Hacker_d70focus_3.gif

1. แฮคเกอร์ (Hacker)

- ไม่มีเจตนาทำความเสียหายให้กับข้อมูลหรือระบบ
- แฮกเกอร์มักจะแอบเข้าใช้งานระบบคอมพิวเตอร์หรือข้อมูลของหน่วยงานหรือองค์กรอื่นโดยไม่ได้รับอนุญาต ส่วนใหญ่เหตุผลที่ทำเช่นนั้นเป็นเพราะต้องการทดสอบความรู้ความสามารถของตนเองเป็นสำคัญ

www.darknightmarket.com/filebase/hacker_2012.gif

2. แครกเกอร์ (Cracker)

- มีความรู้ในเรื่องของฮาร์ดแวร์และซอฟต์แวร์ ดี
- มีความสามารถด้านการเขียนโปรแกรม และการใช้โปรแกรมประยุกต์ต่างๆ ได้ดี
- บุคคลที่นำความรู้ที่ได้ไปใช้ในทางที่ไม่ถูกต้อง โดยการแอบเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต โดยมีจุดประสงค์ร้ายแอบแฝงอยู่
- ไม่ว่าจะเป็นการขโมยข้อมูล การทำลายข้อมูล การทำให้ผู้อื่นไม่สามารถใช้งานระบบคอมพิวเตอร์ได้ และการสร้างปัญหาอื่นๆ ให้เกิดขึ้นในระบบคอมพิวเตอร์และระบบเครือข่าย
- สร้างความเดือนร้อนให้กับผู้เกี่ยวข้อง

Note :

ไม่ว่าจะเป็นแฮกเกอร์ (Hacker) หรือ แคร็กเกอร์ (Cracker) ถ้ามีการแอบเข้าใช้งานระบบคอมพิวเตอร์เครือข่ายของผู้อื่นโดยไม่ได้รับอนุญาต แม้ว่าจะไม่ประสงค์ร้ายก็ถือว่าเป็นการกระทำที่ไม่ดีทั้งสิ้น เพราะขาดจริยธรรมด้านคอมพิวเตอร์

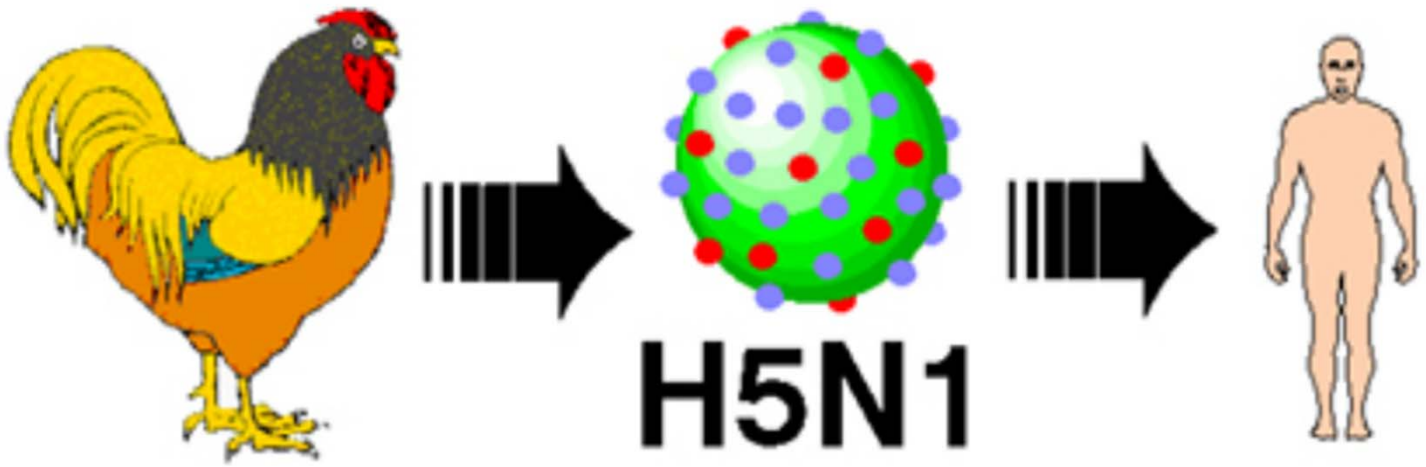
ตัวอย่าง

ในครั้งแรกที่เกิดอาชญากรขึ้น ได้มีการละเมิดลิขสิทธ์ทาง web page ในกรณีนี้ผู้ต้องหาถูกสอบสวนโดย SPA ผู้ซึ่งควบคุม ดูแล web page โดย SPA ได้รวบรวมเหตุการณ์ที่บุคคลอื่นกระจายโปรแกรมลิขสิทธ์ และรูปภาพโดยปราศจากการอนุมัติของผู้ประกาศ หรือผู้ก่อตั้ง ผู้ต้องหาได้รับการตัดสินให้ถูกภาคทัณฑ์ เป็นเวลา 24 เดือน และถูกบังคับให้อยู่แต่ในบ้านเป็นเวลา 6 เดือน

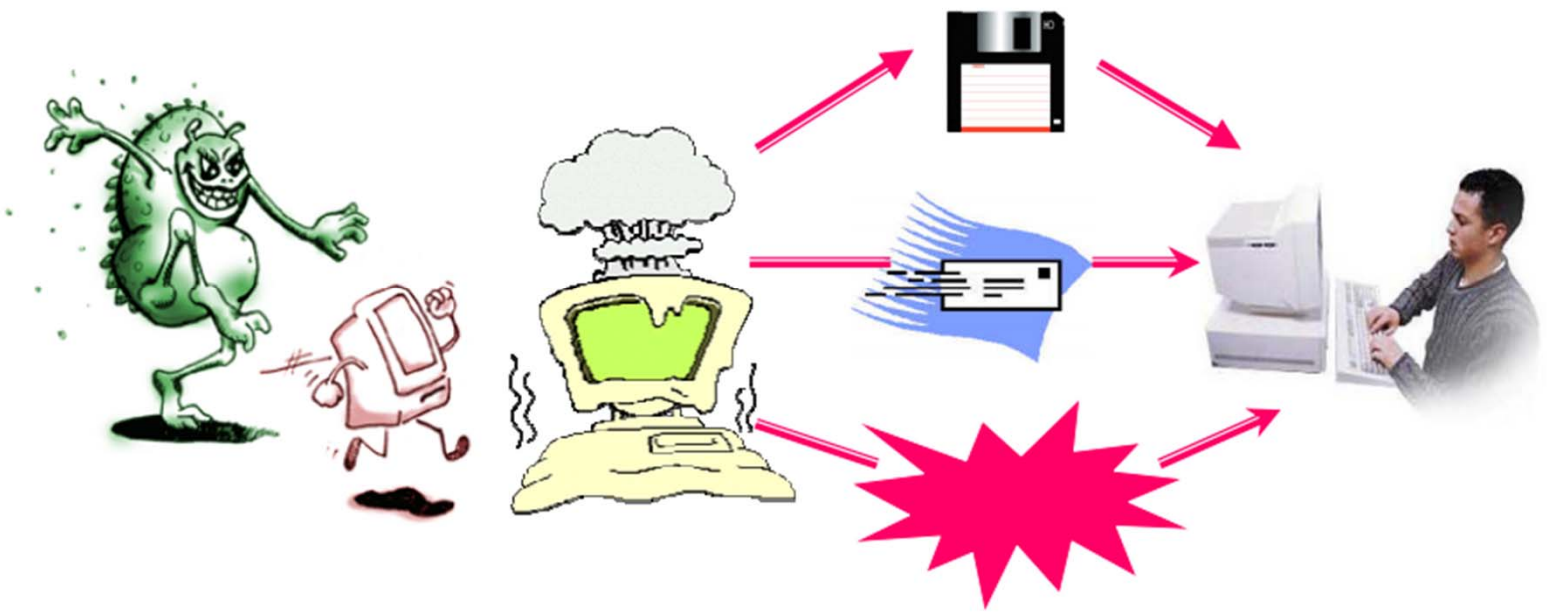
ตัวอย่าง

Cracker เข้าไปใน webside สถานฑูต America ในจีน เพื่อไปลบ home page ของสถานฑูต และใส่ข้อความที่ต่อต้านรัฐบาลอเมริกาเข้าไปแทน ซึ่งกลุ่มบุคคลที่ก่อกวน และแก้ไขระบบมีชื่อว่า Level Seven Crew ถูกเรียกร้อง (claim)ให้รับผิดชอบกับการกระทำดังกล่าวที่พวกเขาก่อขึ้น แต่ FBI ก็ไม่สามารถทำอะไรกับกลุ่มบุคคลนี้ได้เพราะไม่มีหลักฐานที่จะฟ้องร้องได้ ซึ่งกลุ่ม Level Seven Crew นี้ได้ไป cracking web site ต่าง ๆมากกว่า 24 web โดยมี web ที่สำคัญ ๆด้วย เช่น web ของ NASA

ไวรัส (Virus)



ไวรัสคอมพิวเตอร์ (Computer Virus)



3. ไวรัสคอมพิวเตอร์ (Computer Viruses)

- โปรแกรมคอมพิวเตอร์ที่เขียนขึ้นโดยความตั้งใจของโปรแกรมเมอร์ ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่ง ไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์
- ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์ หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้าๆ
- ไวรัสจะไม่สามารถแพร่กระจายตัวเองจากเครื่องหนึ่งไปยังเครื่องอื่นๆได้ด้วยตัวมันเอง ต้องมีพาหะนำไป
- การติดไวรัสทั่วไปแล้วจะเกิดจากการที่ผู้ใช้งานใช้สื่อจัดเก็บข้อมูลที่ติดไวรัส เมื่อนำไปใช้กับเครื่องอื่นและมีการเปิดไฟล์ข้อมูลที่ติดไวรัสนั้น ก็จะทำให้เครื่องดังกล่าวติดไวรัสไปด้วย

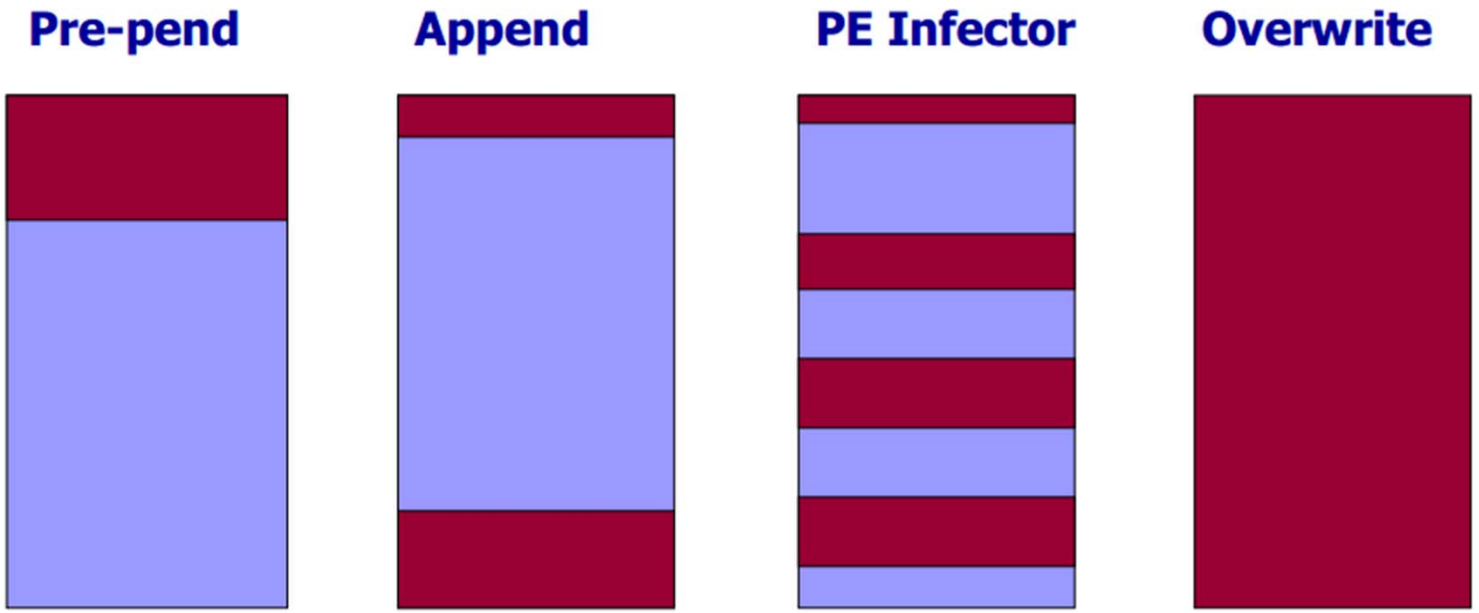
3. ไวรัสคอมพิวเตอร์ (Computer Viruses)

- ไฟล์ไวรัสอาจแนบมากับไฟล์ข้อมูลทางจดหมายอิเล็กทรอนิกส์
- ทำความเสียหาย ตั้งแต่ลบไฟล์ข้อมูลทั้งหมดที่อยู่ในฮาร์ดดิสก์ หรือแค่สร้างความรำคาญให้กับผู้ใช้งาน

คุณสมบัติที่สำคัญของไวรัส

- การทำสำเนาตัวเอง
- โดยต้องอาศัยพาหะ (host)
- ต้องได้รับการเอ็กซิคิวต์
- อาจก่อให้เกิดอาการหรือความเสียหาย (payload)

Ensures virus executes before original executable

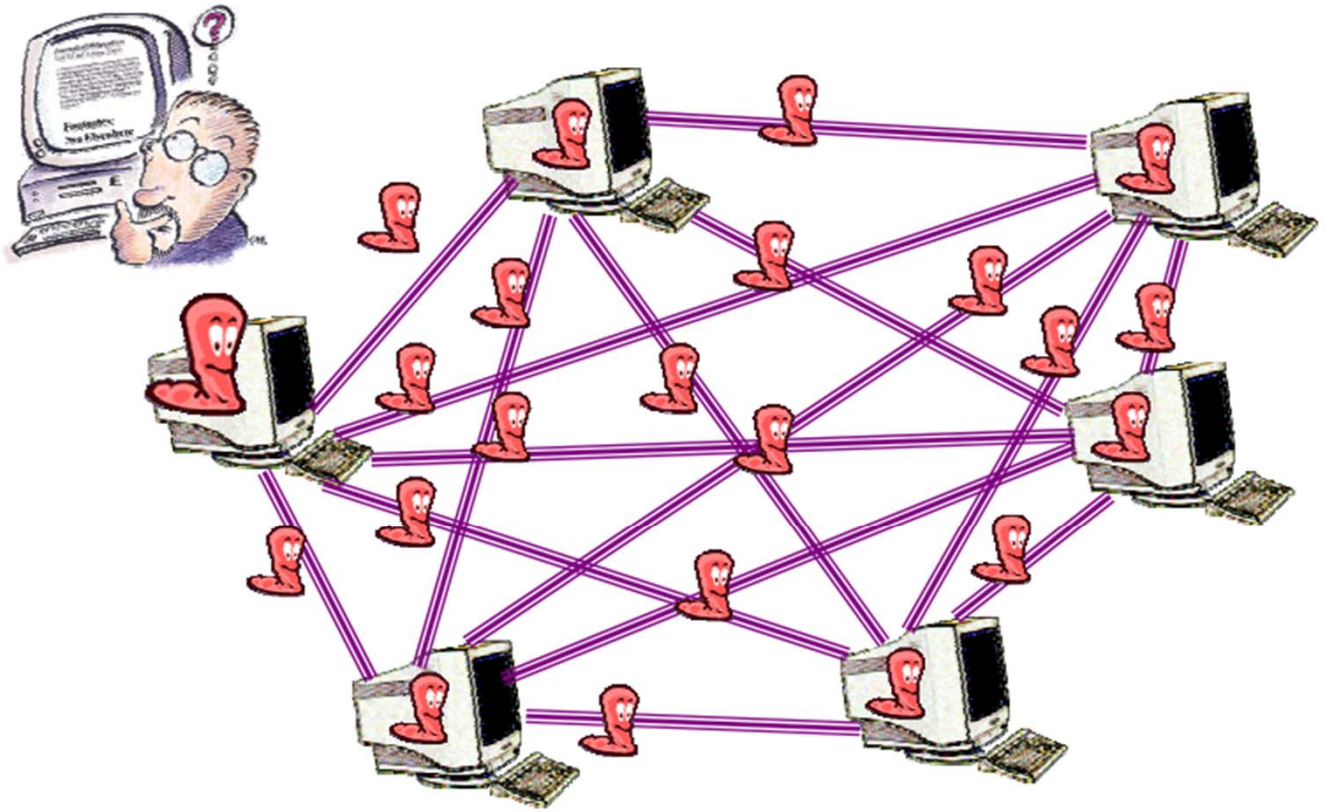


กระบวนการของการติดไวรัส

ไวรัส - ตัวอย่าง

VBS.Redlof.A

- ถูกพัฒนาด้วย VB Script
- พยายามแพร่กระจายไปยังไฟล์ที่มีนามสกุล .html .htm .jsp .asp .php และ .vbs
- สามารถแพร่กระจายไปยังไฟล์ Kernel.dll



4. หนอนอินเทอร์เน็ต (Worms)

- มีอันตรายต่อระบบมาก ทำความเสียหายต่อระบบได้จากภายใน เหมือนกับหนอนที่กัดกินผลไม้จากภายใน
- หนอนร้ายเป็นโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์เครื่องอื่นๆ ที่อยู่ในระบบเครือข่าย
- หนอนอินเตอร์เน็ตจะใช้ประโยชน์จากแอพพลิเคชันที่รับส่งไฟล์โดยอัตโนมัติ ไม่ต้องอาศัยผู้ใช้งานคอมพิวเตอร์
- การแพร่กระจายทำได้ด้วยตัวของมันเองอย่างรวดเร็วและรุนแรงกว่าไวรัส

4. หนอนอินเทอร์เน็ต (Worms)

- เช่นการแชร์ไฟล์ข้อมูลผ่านระบบเครือข่าย เมื่อนั้นหนอนอินเตอร์เน็ต ก็กระจายตัวเองไปยังเครื่องคอมพิวเตอร์อื่นๆที่อยู่ภายในเครือข่ายโดยไม่ต้องรอให้ผู้ใช้งานเปิดไฟล์ที่ติดหนอนอินเตอร์เน็ต เหมือนไวรัสคอมพิวเตอร์

คุณสมบัติที่สำคัญของหนอนอินเทอร์เน็ต

- อยู่ได้ด้วยตัวเอง
- ไม่ต้องอาศัยตัวกลางในการแพร่กระจาย
- ไม่แพร่กระจายผ่านไฟล์
- แพร่กระจายผ่านทางระบบเครือข่าย

4. หนอนอินเทอร์เน็ต (Worms)

- ความเสียหายของหนอนอินเตอร์เน็ตนั้นจะไม่ทำลายข้อมูลเหมือนไวรัส
- แต่ก็จัดเป็นภัยคุกคามที่ร้ายแรงอยู่ดี เนื่องจากหนอนอินเตอร์เน็ตจะเข้าไปควบคุม และใช้สอยทรัพยากรบนระบบคอมพิวเตอร์และระบบเครือข่ายจนไม่สามารถใช้งานได้ในที่สุด
- วิธีการป้องกันและรักษาความปลอดภัยให้ทำเช่นเดียวกับวิธีการป้องกันไวรัส

หนอนอินเทอร์เน็ต - ตัวอย่าง

W32.Blaster.Worm

- โจมตีช่องโหว่ DCOM RPC ผ่าน Port 135/TCP (MS03-026)
- มีผลกับระบบปฏิบัติการ Windows NT, 2000, XP และ 2003
- เครื่องจะ restart เองโดยอัตโนมัติ

หนอนอินเทอร์เน็ต - ตัวอย่าง

W32.Blaster.Worm

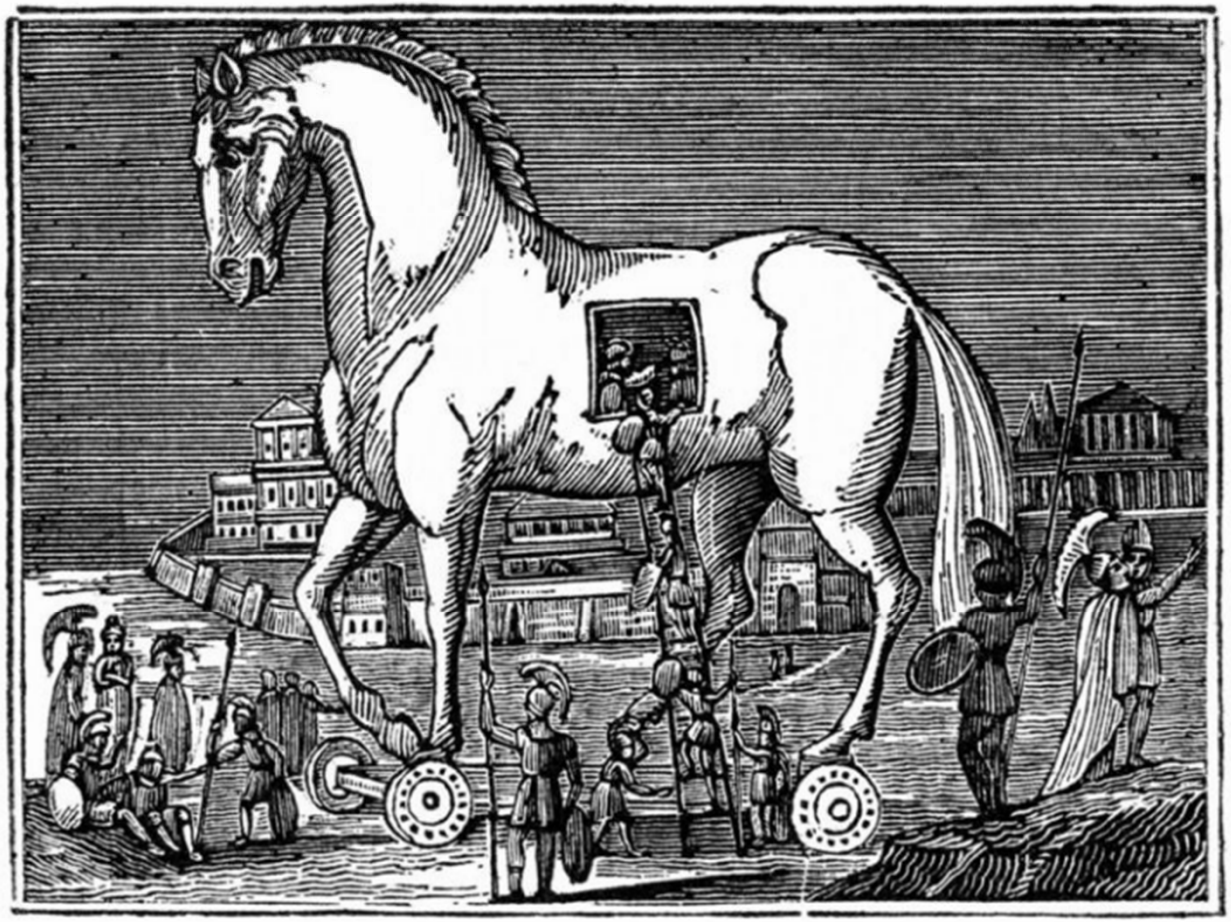
- วิธีแก้ไข ดาวน์โหลดไฟล์ FixBlast.exe จาก

  http://securityresponse.symantec.com/avcenter/FixBlast.exe

  1. ปิดทุกโปรแกรมที่กำลังใช้งานอยู่ก่อนรันไฟล์ที่ดาวน์โหลด
  2. ตัดขาดการเชื่อมต่อจากเครือข่ายทุกทาง
  3. ถ้าใช้ระบบปฏิบัติการ Windows XP หรือ ME ให้ทำการ disable System Restore ก่อน
  4. รันไฟล์ FixBlast.exe แล้วกดปุ่ม start

หมายเหตุ ถ้าไม่สามารถรันไฟล์นี้ได้ ให้ทำการรีสตาร์ทเข้าสู่ Safe Mode ก่อน โดยในระบบปฏิบัติการวินโดวส์ 95/2000/XP ให้กด F8 ระหว่างการบูตเครื่อง และระบบปฏิบัติการวินโดวส์ 98/ME ให้กดปุ่ม Ctrl

ภัยคุกคามการรักษาความปลอดภัยระบบสารสนเทศ



Trojans Deceived.

5. ม้าโทรจัน (Trojan horses)

- หรือเรียกว่า โทรจันฮอร์ส
- เป็นโปรแกรมที่เข้าสู่คอมพิวเตอร์ โดยที่แอบแฝงตัวเองมากับโปรแกรมอื่นๆ เช่น เกมส์ ซอฟต์แวร์ ทีให้ดาว์นโหลด
- เมื่อผู้ใช้งานคอมพิวเตอร์เลือกดาว์นโหลดโปรแกรมดังกล่าว และติดตั้งลงสู่เครื่องคอมพิวเตอร์ก็ทำให้ไปรันโปรแกรมม้าโทรจัน โดยอัตโนมัติซึ่งผู้ใช้งานเองไม่รู้ตัว

5. ม้าโทรจัน (Trojan horses)

- อันตรายที่จะเกิดขึ้นคือม้าโทรจันจะเข้าไปรบกวนประสิทธิภาพการใช้งานคอมพิวเตอร์ ลบข้อมูล หรือดักจับข้อมูลที่สำคัญๆ ส่งไปให้ผู้สร้างโปรแกรมม้าโทรจัน เช่น รหัสผ่าน เลขที่บัตรเครดิต เป็นต้น และยังสามารถสร้างแบ็คดอร์ให้กับโปรแกรมอื่นๆ เข้ามาทำลายระบบได้อีกด้วย

5. ม้าโทรจัน (Trojan horses)

คุณสมบัติที่สำคัญของหนอนอินเทอร์เน็ต

- ไม่ทำสำเนาตัวเอง
- เจตนาทำสิ่งที่คาดไม่ถึง
  - ลบไฟล์
  - เปิดประตูลับ หรือ Back Door
  - ขโมยข้อมูลสำคัญ เช่น รหัสผ่าน เลขที่บัตรเครดิต เป็นต้น
  - ทำการเชื่อมต่อสู่ภายนอก

แบ่งกลุ่มทำกิจกรรมในชั้นเรียน

- หาไวรัสคอมพิวเตอร์ และหนอนคอมพิวเตอร์ ที่ติดมากในปัจจุบัน
- บอกอาการและบอกวิธีการแก้ไข