สุดยอดทริปเกี่ยวกับคอมพิวเตอร์ โดยทีมงาน Com 7#

ครบเครื่องเรื่อง

ไวรัส Trojan

เรียนรู้ต้นกำเนิด เทคนิควิธีการ
ในการกำจัดเจ้าไวรัส Trojan
พร้อมทั้งวิธีป้องกันสุดเจ๋ง

วิชา [237211-2554 COMPUTER NETWORKING FOR EDUCATION]

คำนำ

สมุดเล่มนี้ นำเสนอในเรื่องราวของไวรัสคอมพิวเตอร์เป็นไวรัสม้าโทรจัน ซึ่งประกอบไปด้วยความเป็นมา การทำงาน , วิธีตรวจสอบ , ประเภทของไวรัสม้าโทรจัน และวิธีการกำจัดไวรัสม้าโทรจัน ซึ่งสมุดเล่มนี้เป็นส่วนหนึ่งของรายวิชา 237211 COMPUTER NETWORKING FOR EDUCATION ทางคณะผู้จัดทำขอขอบคุณท่าน อ.ดร.จารุณี ซามาตย์ เป็นอย่างสูงที่ได้ให้คำปรึกษาในการจัดทำสมุดเล่มนี้

หากมีข้อผิดพลาดประการใดทางคณะผู้จัดทำก็ต้องขอโทษขออภัยมา ณ ที่นี้ด้วย

คณะผู้จัดทำ

สารบัญ

ม้าโทรจัน Trojan Horses

ม้าโทรจันเป็นนิยายกรีก คือมีสงครามระหว่างเมือง
สองเมืองเมืองโทรจันกับเมืองทรอยสู้รบกันยืดเยื้อยาวนาน
สุดท้ายเมืองโทรจันจึงวางแผน สร้างม้าไม้ขึ้นมาตัวหนึ่ง
ให้ทหารเข้าไปอยู่ในม้า แล้วเอาม้าไปวางหน้าประตู
เมืองทรอย ทหารเมืองทรอยก็สงสัยว่าม้าอะไร
จึงลากม้าเข้าเมือง แล้วทหารที่อยู่ในม้าก็แอบออกมาเปิด
ประตูเมือง ทำให้ทหารเมืองโทรจันบุกเข้าไปยึดเมือง
ทรอยได้

Trojan = เกี่ยวกับเมืองทรอย (Troy) หรือชาวเมืองทรอย

โดยส่วนใหญ่แฮคเกอร์จะส่งโปรแกรม "ม้าโทรจัน" เข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบ และเพื่อโจมตีคอมพิวเตอร์เซิร์ฟเวอร์ ระบบเครือข่ายอีกที ซึ่งเป็นที่รู้จักกันในชื่อการโจมตีเพื่อ "ปฏิเสธการให้บริการ" (Denied of Services)

โปรแกรมม้าโทรจัน ถือเป็นโปรแกรมที่สอดคล้องกับการทำงานของคอมพิวเตอร์ ไม่มีคำสั่งหรือการปฏิบัติการที่เป็นอันตรายต่อคอมพิวเตอร์ พูดง่ายๆมันไม่ใช่ "ไวรัสซึ่งถูกถือเป็นเชื้อโรค" แต่ม้าโทรจันเป็นโปรแกรมธรรมดาที่โปรแกรมตรวจสอบไวรัสไม่สามารถตรวจจับพฤติกรรมร้ายๆได้ แต่วัตถุประสงค์ของโปรแกรมม้าโทรจันนั้นกลับเป็นการทำงานเพื่อละเมิด

ม้าโทรจันในคอมพิวเตอร์ทำงานอย่างไร

อย่างที่กล่าวแล้วว่า ม้าโทรจันแตกต่างจากไวรัสที่การทำงาน ไวรัสทำงานโดยทำลายคอมพิวเตอร์ ทั้งฮาร์ดแวร์และซอฟต์แวร์อย่างแท้จริงไวรัสบางตัวอย่าง Love BUG ทำลายไฟล์โดยการเปลี่ยน-แปลงรายละเอียดในไฟล์ ไวรัส CIH ทำให้ไบออสของคอมพิวเตอร์เสีย และเข้าถึงข้อมูลในฮาร์ดดิสก์ไม่ได้ แต่ "ม้าโทรจัน" ไม่ทำอะไรกับคอมพิวเตอร์ ม้าโทรจันไม่มีคำสั่งหรือพฤติกรรมการทำลายคอมพิวเตอร์เหมือนไวรัส ม้าโทรจันเหมือนโปรแกรมทั่วไปในคอมพิวเตอร์

ม้าโทรจันนั้นเป็นเครื่องมือของแฮคเกอร์ในการเจาะระบบ ว่ากันว่าบรรดาแฮคเกอร์นั้นมีสังคมเฉพาะที่แจกจ่าย เผยแพร่ม้าโทรจันออกไปใช้งาน โดยส่วนใหญ่ม้าโทรจันซึ่งปัจจุบันมีอยู่นับพันโปรแกรม ถูกพัฒนาโดยพวกนักศึกษาแฮคเกอร์ และมือสมัครเล่นอีกหลายคน เพราะม้าโทรจันนั้นคือโปรแกรมที่เขียนขึ้นเพื่อบันทึกว่าแป้นคีย์บอร์ดแป้นไหนถูกกดบ้าง ด้วยวิธีการนี้ก็จะได้ข้อมูลของUser ID, Password หลังจากนั้นโปรแกรมม้าโทรจันจะบันทึกข้อมูลลงไปใน RAM , CMOS หรือ Hidden Directory ในฮาร์ดดิสก์ แล้วก็หาโอกาสที่จะอัพโหลดตัวเองไปยังแห่งที่ผู้เขียนม้าโทรจันกำหนด หรือบางทีแฮคเกอร์อาจจะใช้วิธีการเก็บไฟล์ดังกล่าวไปด้วยวิธีอื่น

ประเภทต่างๆของม้าโทรจัน

ม้าโทรจันนั้นไม่มีเพียงประเภทเดียว แต่มีการแบ่งออกเป็นหลายประเภท ตามลักษณะการคุกคามและการทำงาน

-Client / server ม้าโทรจันแบบนี้จะส่งจากเซิร์ฟเวอร์ไปไว้ที่ไคลเอ็นต์ โดยสั่งเปิดพอร์ตที่ไคลเอ็นท์แล้วให้เครื่องไคลเอ็นต์อีกเครื่องไปควบคุม

- DDOS Distributed Denial of Service แฮคเกอร์จส่งโทรจันไปไว้ที่เครื่องไคลเอ็นต์หลายๆเครื่อง หลังจากนั้นจะใช้เครื่องไคลเอนต์เหล่านั้นโจมตีเว็บไซต์เป้าหมายพร้อมๆกันเพื่อให้หยุดบริการอย่างที่ได้ยินกันในเดือนมิถุนายน 2543 ที่ผ่านมา

- Password Stealer ตัวขโมยรหัสผ่าน โดยขโมยรหัสผ่านของ ICQ , e-mail , ระบบคอมพิวเตอร์,การต่อเชื่อม ISP แล้วเก็บรหัสผ่านนั้นไว้ในไฟล์หนึ่ง แล้วเอาม้าโทรจันอีกตัวมาอัพโหลดไฟล์นั้นไปยังปลายทาง

- Remote Flooder ทำงานเหมือนกับ DDOS คือส่งโทรจันไปที่เครื่องปลายทาง (รีโมท) แล้วสั่งจากเครื่องมาสเตอร์ให้เครื่องปลายทาง (รีโมท) โจมตีเป้าหมายอีกทีหนึ่ง

- Telnet ม้าโทรจันตัวนี้จะยึดเครื่องรีโมทเป็นอาวุธโจมตีเครื่องปลายทาง โดยผ่าน Telnet ใช้คำร้องขอบริการ Telnet เพื่อจัดการกับเครื่องเหยื่อ

วิธีตรวจสอบว่าม้า Trojan เข้ามาในเครื่องคุณหรือไม่

1. ให้ตรวจสอบการทำงานของเครื่องท่านโดยการกด ปุ่มstart > All programs > Accessories > MS-Dos Prompt (หรือ Command promt นั่นเอง)

2. แล้วพิมพ์ netstat -an

การป้องกัน-กำจัดม้าโทรจัน

ป้องกัน-กำจัดม้าโทรจันสำหรับสำนักงาน

นับวันม้าโทรจันจะยิ่งมีโอกาสในการแพร่ระบาดสูงขึ้น เพราะพัฒนาการของของเทคโนโลยีพีซี จากยุคเก่าที่มีเพียงเครื่องมินิคอมพิวเตอร์หรือเมนเฟรม 1 เครื่อง และ Dumb Terminal ที่Dumb Terminal นั้นไม่มีดิสก์เก็ต ดังนั้นโอกาสที่ม้าโทรจันจะถูกโหลดผ่านดิสก์เก็ตย่อมไม่มี แต่หลังจากนั้น Dumb Terminalถูกแทนที่โดยThin Client ซึ่งอาจจะมีดิสก์เก็ตและมีฮาร์ดดิสก์ ทำให้ง่ายต่อการแพร่ระบาดของม้าโทรจัน นอกจากนี้ การที่อินเตอร์เน็ตถูกนำเข้าเป็นส่วนหนึ่งของระบบคอมพิวเตอร์ ก็ทำให้การแพร่ระบาดของม้าโทรจันง่ายขึ้นดังนั้นการวางแผนและกำหนดนโยบายเกี่ยวกับระบบรักษาความปลอดภัยที่รัดกุมจะช่วยป้องกันม้าโทรจันได้

ปัจจุบันมีผลิตภัณฑ์ Firewall ใหม่หลายตัว ที่ถูกพัฒนาขึ้นมาเพื่อป้องกันการโจมตีของม้าโทรจันโดยเฉพาะ โดยผนวกเอาคุณสมบัติการป้องกันม้าโทรจันเข้าไปในผลิตภัณฑ์ Firewall ทั้งฮาร์ดแวร์และซอฟต์แวร์ นอกจากนี้ยังเพิ่มฟังก์ชันในการตรวจสอบว่าระบบถูกการโจมตีแบบ DDOS หรือไม่ด้วย

สำหรับสำนักงานแล้ว ดูเหมือนเป็นหน้าที่ของฝ่ายไอที ในการตรวจสอบ (Audit) ระบบ เพื่อดูว่ามีความเสี่ยงต่อการถูกโทรจันหรือไม่ เพราะแต่ละองค์กรมีความเสี่ยงเรื่องการถูกโทรจันไม่เท่ากัน เช่นองค์กรที่เคยใช้คอมพิวเตอร์เฉพาะในองค์กรเท่านั้น และมีการควบคุมที่ดี ย่อมเสี่ยงต่อมาโทรจันน้อย แต่ต่อมา ถ้าหากองค์กรนั้นต่อเชื่อมระบบเครือข่ายของตัวเองเข้ากับอินเตอร์เน็ต

ป้องกัน-กำจัดม้าโทรจันสำหรับคอมพิวเตอร์ที่บ้าน

ส่วนการใช้งานคอมพิวเตอร์ภายในบ้าน โดยการออนไลน์ปกติโดยการต่อเชื่อมอินเตอร์เน็ตจากคอมพิวเตอร์ภายในบ้านที่ใช้ Dial Up Network โดยการต่อเชื่อมผ่านโมเด็มนั้น เสี่ยงต่อม้าโทรจันเช่นกัน ผมเคยถูกม้าโทรจันหลายๆ ตัวโจมตีภายในเดือนเดียวกัน 5 ครั้ง วิธีการป้องกันได้แก่ การติดตั้งโปรแกรม อย่าง NetBUS Detective จะคอยตรวจจับม้าโทรจันพวก Netbus ,BO Orifice , หรือโปรแกรม NukeNubber ก็ป้องกันระบบ โดยการตรวจสอบพอร์ตต่างๆของ TCP/IP ถึง 50 พอร์ต

นโยบายการป้องกันม้าโทรจันนั้น แตกต่างกันไปในแต่ละที่ โดยส่วนใหญ่จะต้องใช้วิธีการ กันไว้ดีกว่าแก้ โดยการติดตั้ง Firewall ไว้ก่อนเลยในชั้นแรก แต่ถ้าหากวันหนึ่งเกิดสงสัยว่าในระบบคอมพิวเตอร์นั้นมีม้าโทรจันถูกส่งมาหรือไม่ ก็ต้องใช้ซอฟต์แวร์ในการตรวจจับ

ซอฟต์แวร์สำหรับการตรวจจับและทำลายโทรจัน

กรณีที่ต้องการตรวจจับและทำลายม้าโทรจัน ซอฟต์แวร์กำจัดไวรัสทั่วไปอย่าง Norton Antivirus , Mcafee Virus SCAN นั้นสามารถตรวจจับและกำจัดม้าโทรจันได้บ้างบางตัว แต่ไม่ครอบคลุมทั้งหมด ทั้งนี้เพราะซอตฟ์แวร์ป้องกันกำจัดไวรัสนั้นมุ่งจะกำจัดไวรัส (โปรแกรมคอมพิวเตอร์ที่มีอันตรายต่อคอมพิวเตอร์) มากกว่าจะตรวจจับและทำลายโทรจัน วิธีการส่งเข้ามาในคอมพิวเตอร์ และพฤติกรรมการทำงานของโทรจันนั้นแตกต่างจากไวรัส เครื่องมือในการตรวจจับ การป้องกันจึงแตกต่างจากไวรัสด้วย

1. The Cleaner 3.1 จาก Moosoft เป็นซอฟต์แวร์ที่ทำหน้าที่ทั้ง ป้องกัน ตรวจจับ และกำจัดไวรัสที่ได้รับความนิยมมากตัวหนึ่ง เพราะทาง ZDNet ,Tucows และอีกหลายๆสื่อออนไลน์ที่ได้รีวิวซอฟต์แวร์ตัวนี้ต่างก็โหวดให้ประสิทธิภาพของการทำงาน "ยอดเยี่ยม" ทั้งหมด พูดได้ว่า The Cleaner เป็นซอฟต์แวร์ในการกำจัดโทรจันที่เป็นที่รู้จักกันดีและได้รับความนิยม ประสิทธิภาพของ The Cleaner นั้นมีฐานข้อมูลโทรจันที่ตรวจสอบและกำจัดได้กว่า 3000 ตัว และยังมีการอัพเดททุกๆ เดือน การตรวจจับความเร็วสูง สนับสนุนการตรวจสอบไฟล์ที่บีบอัดไว้ (Compress Files) OS ที่ The Cleaner สนับสนุนคือ Windows 95/98/ME , NT 4.0 Server , 4.0

2. Trojan Remover เป็นซอฟต์แวร์ที่ทำหน้าที่ตรวจสอบและกำจัดโทรจันอีกตัวหนึ่งที่ได้รับการพัฒนาอย่างต่อเนื่อง ปัจจุบันพัฒนาถึงเวอร์ชัน 4.0.4 แล้ว Trojan Remover ได้รับความนิยมเช่นกัน ถึงแม้ว่า OS ที่ Trojan Remover สนับสนุนจะมีเพียง 95/98/ME เท่านั้นเอง TrojanRemover ทำงานไม่แตกต่างจาก The Cleaner คือ ถ้าหากตรวจสอบพบว่าไฟล์ระบบหรือไฟล์ข้อมูลได้มีโทรจันแฝงตัวอยู่ Trojan Remover จะดำเนินการแก้ไขไฟล์นั้นให้เข้าสู่สภาพปกติ รวมไปถึงการแก้ไข Registry ของวินโดวส์ด้วย นอกจากนี้สำหรับโทรจันที่แฝงตัวในหน่วยความจำ Trojan Remover ก็มีวิธีการที่ชาญฉลาดในการจัดการโดยใช้กระบวนการ REMOVE all traces

3. Anti-Trojan 5ซอฟต์แวร์จากเยอรมัน เป็นซอฟต์แวร์สำหรับจัดการกับ Trojan อีกตัวที่น่าสนใจ Anti-Trojan มีขนาดไฟล์สำหรับติดตั้ง 4.8 เมกะไบต์ มากกว่า Trojan Remover และ The Cleaner การพัฒนาอย่างต่อเนื่องจนถึงเวอร์ชัน 5.0 น่าจะประกันได้ว่าซอฟต์แวร์ป้องกันโทรจันตัวนี้น่าสนใจไม่น้อย การทำงานของ Anti-Trojan ทำงานในการตรวจสอบโทรจันโดยการสแกนพอร์ต (เพราะโทรจันโดยส่วนใหญ่จะเล็ดลอดเข้ามาและเปิดพอร์ตต่างๆ) สแกน Registy และสแกนฮาร์ดดิสก์ การค้นหาและตรวจจับไวรัสใช้ Signature ของโทรจัน การสแกนในไฟล์รวมถึงการสแกนไฟล์บีบอัดด้วย คุณสมบัติเด่นของ Anti-Trojan คือ รู้จัก Trojan มากกว่า

แบบฝึกหัด

ให้เติมคำว่า "ถูก" หน้าข้อความที่ถูกและคำว่า "ผิด" หน้าข้อความที่ผิด

_____ 1. โปรแกรมม้าโทรจันเป็นโปรแกรมที่สอดคล้องกับการทำงานของคอมพิวเตอร์

_____ 2. ม้าโทรจันเป็นเครื่องมือในการเจาะระบบ

_____ 3. ม้าโทรจันนั้นมีเพียงประเภทเดียวเท่านั้น

_____ 4. การกำจัดม้าโทรจัน ส่วนมากจะเน้นการป้องกันมากกว่าการแก้

_____ 5. ม้าโทรจันไม่สามารถแฝงตัวในหน่วยความจำได้

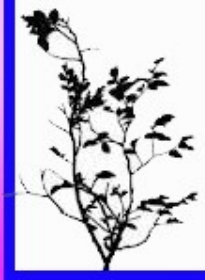
เฉลย :1.ถูก 2.ถูก 3.ผิด 4.ถูก 5.ผิด

อ้างอิง

http://www.sorncomputer.com/index.php/topic,41.0.html

http://antivirus.nabia10.com/virus-t/Trojan_p.html

http://www.missladyboys.com/webboard/index.php?showtopic=5215



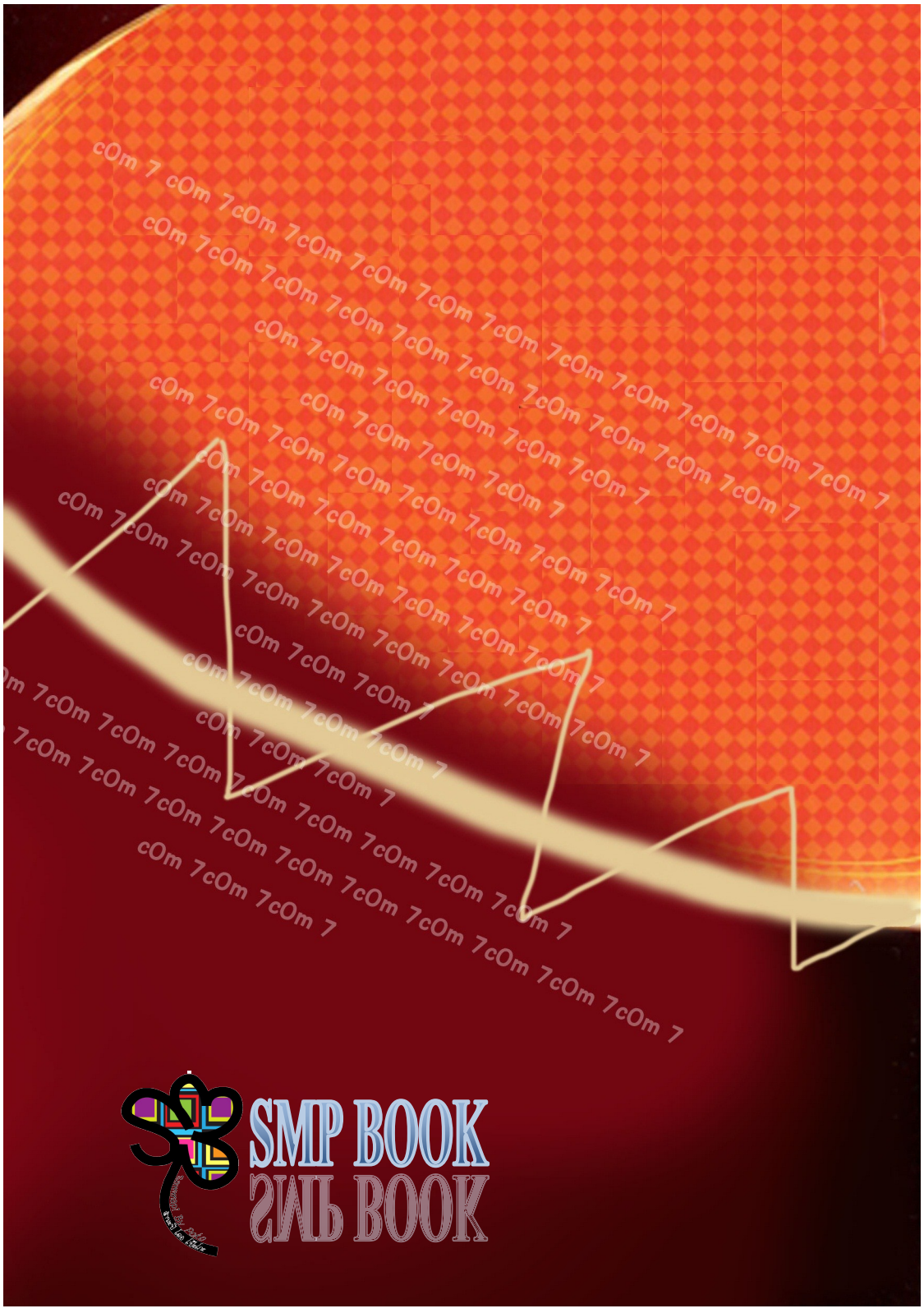
โดย SMP BOOK

222/2 หอพักนพรัตน์ มหาวิทยาลัยขอนแก่น

อ.เมืองขอนแก่น จ.ขอนแก่น 40002

THAILAND โทร: 0874222606

E-Mail : Panna_rai@hotmail.com


SMP BOOK