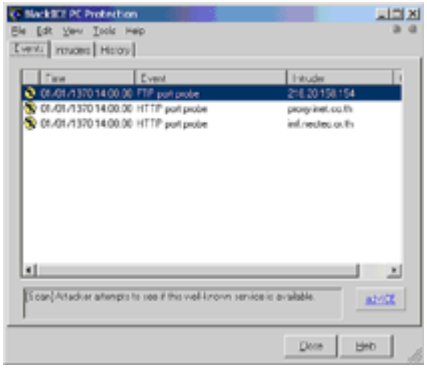
เรียนรู้วิธีป้องกัน PC ด้วยโปรแกรมประเภท Personal Firewalls , SteathWare Finders/Removers และ SPAM Fighters

by A.Pinya Hom-anek, CISSP

"หยุดไวรัส , กำจัดโปรแกรมแฮกเกอร์ , ต่อต้านสแปมเมอร์ " เรามักได้ยินคำกล่าวเหล่านี้บ่อยๆ จากคนที่ใช้ PC หรือ Personal Computer อยู่เป็นประจำ ทุกวันนี้ไม่มีใครปฏิเสธได้ว่า PC ได้เข้ามามีบทบาทกับการทำงานและการดำเนินชีวิตของเรา ในหนึ่งวันเราต้องอยู่หน้าคอมพิวเตอร์ PC เพื่อการทำงาน การรับส่งเมล์ ท่องเว็บ ค้นหาข้อมูล เขียนเว็บบอร์ด หรืออ่านข่าวสารต่างๆจาก Magazine Online เครื่องคอมพิวเตอร์ PC แทบทุกเครื่องในปัจจุบันนี้ จะต้องมีโมเด็ม (Modem) มากับเครื่องเพื่อต่อเชื่อมกับโลกอินเทอร์เน็ต เรียกว่าโมเด็มได้กลายมาเป็นอุปกรณ์มาตรฐานของเครื่องคอมพิวเตอร์ PC ไปแล้วก็ว่าได้ ดังนั้นเครื่องคอมพิวเตอร์ PC ไม่ได้ทำงานแบบเครื่องเดียว (Stand alone) อีกต่อไป เพราะเราต้องการเชื่อมต่อ PC ของเราเข้ากับเครือข่ายที่ใหญ่ที่สุดในโลกก็คืออินเทอร์เน็ตกันแทบทุกวัน ซึ่งในปัจจุบันนี้ ภัยจากแฮกเกอร์และไวรัสคอมพิวเตอร์ ที่อยู่ในอินเทอร์เน็ตนั้นมีมากมายเหลือประมาณ ไม่เหมือนกับช่วง 2-3 ปีก่อน ดูตัวอย่างรูปที่ 1 Events Screen ของโปรแกรม Personal Firewall ชื่อ "BlackICE PC Protection" (http://www.iss.net /products/networkice/eval) แสดงรายงานให้เราดูว่า เพียงแค่เราต่อโมเด็มเล่นอินเทอร์เน็ต 1 ถึง 2 ชั่วโมงก็พบว่ามี IP Address ที่แปลกๆ เข้ามาติดต่อเครื่องเราเป็นว่าเล่น อาทิ เข้ามาตรวจพอร์ต Web Server ของเรา (HTTP Port Probe) ทั้งๆที่เราไม่ได้เป็น Web Server มักมาจากจีนบ้าง , เกาหลีบ้าง ไต้หวันก็มีครับ



Picture 1 : BlackICE events screen

วิธีการจะดูว่า IP Address นั้นมาจากไหนให้เข้าไปหาในเว็บไซต์ http://combat.uxn.com แล้วเติม IP Address เข้าไปในช่อง IP Address ดังรูปที่ 2

Picture 2 : IP address WHOIS information from http://combat.uxn.com

ก็จะทราบได้ทันทีว่าต้นทางของ IP Address นั้นมาจากที่ใด โปรแกรม Personal firewall จะรายงานให้เราทราบถึงผู้บุกรุกที่ไม่ได้รับเชิญ และช่วยแกะรอยให้เราว่ามาจาก Host ชื่ออะไร (ทำ DNS Reverse Lookup Query) จะเห็นได้ว่าโปรแกรมประเภทนี้ นั้นมีประโยชน์หลายอย่าง นอกจากจะเตือนให้เราทราบถึงการเข้าถึง PC ของเราแบบแปลกๆ แล้วยังช่วยให้เรารู้ว่าเราโดนจู่โจจากที่ไหน โปรแกรม Personal Firewall ตัวเด่นที่ผมอยากจะแนะนำให้ลองดูได้แก่ "Sygate Personal Firewall" (http://soho.sygate.com) ซึ่งแจกฟรีสำหรับใช้ส่วนบุคคล หรือ "Zonelabs ZoneAlarm" (http://www.zonelabs.com) แจกฟรีสำหรับ Basic Version ยกตัวอย่าง ZoneAlarm นั้น สามารถป้องกันได้ทั้งข้อมูลที่เข้ามาโจมตี PC เราและข้อมูลที่ถูกส่งออกไปจาก PC เราโดยโปรแกรมพวกม้าโทรจัน (Trojan Horse) ถ้ามีการเปิดโปรแกรม Backdoor ไว้ที่เครื่องเราเพื่อแฮกเกอร์จะได้เข้ามาควบคุมเครื่องเราแบบ Remote Control โปรแกรมก็จะ pop-up แสดงให้เราทราบถึงความเคลื่อนไหวในแบบ Real Time และยังบล็อก (Block) การจู่โจมของพวก Virus ตระกูล NIMDA ที่ชอบเข้ามาทางพอร์ต HTTP (Web Server) เป็นต้น โปรแกรมจะปิดพอร์ตสำคัญๆให้กับ PC ของเราโดยอัตโนมัติ เช่น พอร์ต HTTP, พอร์ต NetBIOS ซึ่งโดยปกติแล้ว แฮกเกอร์จะเข้ามาสำรวจข้อมูลเครื่องเราโดยผ่านทางช่องโหว่ Null Session ของ NetBIOS ซึ่งโปรแกรม Personal Firewall ทั้งหลายก็จะทำการปิดพอร์ตตระกูล NetBIOS ให้เราโดยอัตโนมัติ ทำให้คนอื่นไม่สามารถมาถึงข้อมูลจากเครื่องเราโดยการ Map Network Drive ตามปกติได้ พูดง่ายๆ ว่าปิด Share ในเครื่องเราทันทีที่โปรแกรมทำงาน แต่เราก็สามารถสั่งให้เปิดได้ถ้าต้องการเปิดให้เฉพาะคนบางคนเท่านั้น รูปที่ 3 แสดงถึงหน้าจอ Alert เตือนเราเวลามีคนมาติดต่อกับ PC เราผ่านทาง NetBIOS โดย

จะแสดง IP Address พร้อมวันและเวลาที่มีเหตุการณ์เกิดขึ้นจากนั้นก็จะบันทึกลงใน Log File เพื่อพิมพ์รายงานในภายหลัง โปรแกรมจะมี Link ไปยัง WHOIS Search เพื่อระบุว่า IP Address นี้มาจากที่ใดในโลก โดยจะระบุเป็นชื่อ ISP ที่ดูแล IP Address นั้นๆอยู่

Picture 3 : ZoneAlarm Pro Alert Screen

ขณะนี้โปรแกรม Personal Firewall ดังกล่าวมาในตอนต้นนั้น ในความเห็นของผม ผมคิดว่าเป็นสิ่งที่จำเป็นที่ต้องอยู่คู่กับ PC ของเรา เปรียบเสมือนตอนนี้ถ้าใครไม่มีโปรแกรมประเภท Anti-virus บนเครื่องก็ถือว่าค่อนข้างอันตรายพอสมควร เพราะภัยจากอินเทอร์เน็ตเข้ามาจู่โจมเราได้หลายแบบ ไม่ว่าจะเป็นไวรัส หรือพวกแฮกเกอร์ ที่สแกนมาเจอ IP Address ของเครื่องเราพอดี ดูจากรูปจะเห็นว่า IP Address ส่วนใหญ่มาจากต่างประเทศครับ

ยังมีโปรแกรมอีกประเภทหนึ่งเรียกว่า "STEATHWARE" มาแอบซ่อนอยู่ใน PC ของเรา โดยเราเคยคิดไหมว่ามีคนกำลังแอบดูหน้าจอเครื่องของเราอยู่แบบรีโมต (Remote) หรือบางครั้งเราไม่ได้ทำอะไรเลยขณะที่เรา online อยู่ แต่ก็มีสัญญาณไฟของโมเด็มกระพริบแสดงข้อมูลลงเข้าออกจากเครื่องเราอยู่ตลอดเวลา แถมยังอยู่ดีๆ ก็มี pop-up โฆษณาต่างๆโผล่ขึ้นมาบนจอภาพของเรา โปรแกรมพวกนี้บางที่เราเรียกว่า "SPYWARE" หรือ "ADWARE" ซึ่งเราต้องหมั่นตรวจสอบ โดยการสแกนเครื่อง PC ของเราว่ามีโปรแกรม SPY พวกนี้อยู่ในเครื่องเราหรือไม่ ผมแนะนำโปรแกรม LAVASOFT AD-AWARE PLUS 5 จาก http://www.lavasoftusa.com เป็นโปรแกรมที่จะช่วยตรวจและลบโปรแกรม STEATHWARE ทั้งหลายออกจากเครื่อง PC ของเรา ผมแนะนำให้ลอง download มาใช้ดูจะทำให้เราเข้าใจโปรแกรมประเภทนี้มากขึ้น

เคยมีคนถามผมว่าแล้ว Microsoft เองไม่มีโปรแกรม Personal Firewall ติดมากับ OS เลยหรือ คำตอบก็คือมีครับ ใน Microsoft Windows XP นั้น จะมี Internet Connection Firewall อยู่ แต่คุณสมบัติจะสู้โปรแกรมจาก

3rd Party ไม่ได้ อาทิ ไม่มีการเตือนเวลาถูกบุกรุก หรือการเก็บ Log File ก็อาจจะยากที่จะเข้าใจและเข้าถึง แต่ก็เป็นนิมิตหมายที่ดีนะครับที่ Microsoft ได้ติดตั้งคุณสมบัติ Personal Firewall ให้กับ Microsoft Windows XP มาระดับหนึ่ง (ก็ดีกว่าไม่มีครับ) สำหรับโปรแกรมประเภทสุดท้ายก็คือโปรแกรมจัดการกับ SPAM ทั้งหลาย ก็ขอแนะนำ "SpamKiller" ของ www.mcafee.com ซึ่งจะใช้ได้กับ POP3 mail และ Microsoft Exchange โปรแกรมนี้ใช้ฟรีอย่างเต็ม Feature 30 วันครับ

จะเห็นได้ว่าตอนนี้ เราต้องมีทั้ง Personal Firewalls, STEATHWARE Finders and Removers และ SPAM Fighters ในเครื่อง PC ของเรา ถึงจะปลอดภัยจากภัยอินเทอร์เน็ตได้พอสมควร ถึงแม้แต่จะไม่เกิดขึ้นก็ตาม นี่ยังไม่รวมโปรแกรมกลุ่ม Anti-virus อีกนะครับ โปรแกรมเหล่านี้เป็นสิ่งจำเป็นที่เราเห็นทีจะหลีกเลี่ยงไม่ได้เสียแล้ว แต่ถ้าเรามีงบประมาณจำกัด ผมก็ขอแนะนำให้ใช้ Free Version ของแต่ละโปรแกรมดังทีแนะนำมาก็ยังดีกว่าปล่อยเครื่อง PC เราไว้โดยไม่ป้องกันอะไรเลยนะครับ

ต้องการทราบข้อมูลเพิ่มเติมไปดูได้ที่ www.acisonline.net หรือติดต่อผมได้ที่ prinya@acisonline.net
พบกันใหม่ฉบับหน้าครับ.....

จาก : หนังสือ eLeader Thailand
ปีที่14 ฉบับที่161 ประจำเดือน กรกฎาคม 2545
Update Information : 4 กรกฎาคม 2545