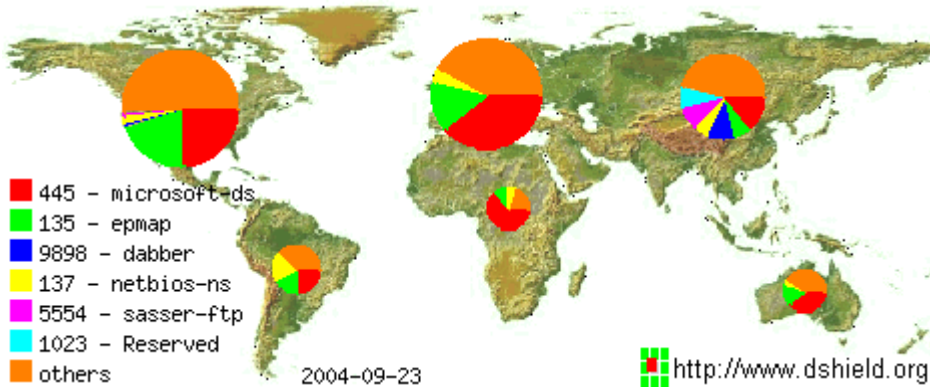
อันตรายจากการต่ออินเทอร์เน็ตโดยผ่านทางโมเด็ม

อำนาจ สุคนเขตร์ *

เครื่องคอมพิวเตอร์ที่ใช้งานอินเทอร์เน็ตโดยต่อผ่านโมเด็มหรือต่อผ่านเครือข่ายขององค์กร นับได้ว่าเป็นเป้าหมายอันดับต้น ๆ ของเหล่าบรรดาแฮกเกอร์ แครกเกอร์ หรือผู้ไม่ประสงค์ดีทั้งหลาย ซึ่งเรียกได้อีกอย่างหนึ่งว่า "ผู้บุกรุก" เหตุที่เป็นเช่นนี้เนื่องจากผู้บุกรุกต้องการข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ที่ท่านใช้งานอยู่ เช่น รหัสผ่านในระบบต่าง ๆ ข้อมูลในอีเมลล์ ข้อมูลขององค์กรหรือหน่วยงาน ข้อมูลส่วนตัว หลายเลขบัตรเครดิต หลายเลขบัญชีธนาคาร และข้อมูลอื่น ๆ ที่ผู้บุกรุกสามารถนำไปใช้แสวงหาผลประโยชน์ให้กับตัวเองได้ นอกจากข้อมูลต่าง ๆ ในเครื่องคอมพิวเตอร์ที่ท่านใช้งานแล้ว อีกสิ่งหนึ่งที่ผู้บุกรุกต้องการครอบครอง คือ ทรัพยากรต่าง ๆ ของเครื่องคอมพิวเตอร์ อาทิเช่น พื้นที่ว่างในฮาร์ดดิสค์ ช่องทางการเชื่อมต่อสู่อินเทอร์เน็ต การใช้เครื่องคอมพิวเตอร์ที่เราใช้งานอยู่ประมวลผลหรือทำงานต่าง ๆ หรือแม้กระทั่งใช้เครื่องคอมพิวเตอร์ที่ท่านใช้งานอยู่ "โจมตี" เครื่องคอมพิวเตอร์เครื่องอื่น ๆ ที่เชื่อมต่ออยู่บนอินเทอร์เน็ต

การเชื่อมต่อเข้ากับอินเทอร์เน็ตโดยตรงผ่านโมเด็มนั้นจะแตกต่างจากการเชื่อมต่อโดยผ่านเครือข่ายขององค์กรก็ตรงที่การเชื่อมต่อโดยตรงผ่านโมเด็มนั้นแบนด์วิธต่ำและไม่มี IP Address ที่ตายตัว ส่วนคุณสมบัติอื่น ๆ เหมือนกันทุกประการ การเชื่อมต่อโดยตรงผ่านโมเด็มนั้นก็ใช่ว่าจะมีความปลอดภัยเหนือกว่าการเชื่อมต่อแบบอื่น ยิ่งมีผู้ใช้ส่วนใหญ่เข้าใจว่าการเชื่อมต่อโดยตรงผ่านทางโมเด็มนั้นปลอดภัยเพราะข้อมูลไม่เกี่ยวข้องกับคนอื่นและไม่เป็นที่น่าสนใจกับเหล่าบรรดาผู้บุกรุก จริงอยู่ที่ผู้บุกรุกมักสนใจที่จะเจาะเข้าไปยังเซิร์ฟเวอร์ใหญ่ ๆ แต่การเจาะเข้าไปยังเครื่องคอมพิวเตอร์ที่ท่านใช้งานอยู่นั้นก็มีอยู่อย่างต่อเนื่อง เพียงแต่ไม่ค่อยเป็นข่าวให้รับรู้ อาจเป็นเพราะผู้ไม่ทราบหรือความเสียหายไม่มากก็เป็นได้ นอกจากจะเป็นเหตุการณ์สำคัญที่มีจำนวนผู้เสียหายมาก ๆ เช่น ถูกเจาะโดยเวิร์มที่เจาะเข้าไปยังเครื่องคอมพิวเตอร์ของผู้ใช้นับล้านเครื่องพร้อม ๆ กัน

* **นักวิชาการอุดมศึกษา** กลุ่มงานพัฒนาและเผยแพร่นวัตกรรมเทคโนโลยีการศึกษา
ฝ่ายเทคโนโลยีทางการศึกษา สำนักวิทยบริการ
มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี



รูปที่ 1 จำนวนเครื่องคอมพิวเตอร์ที่ถูกโจมตีสำหรับเครื่องที่ต่อผ่านโมเด็ม

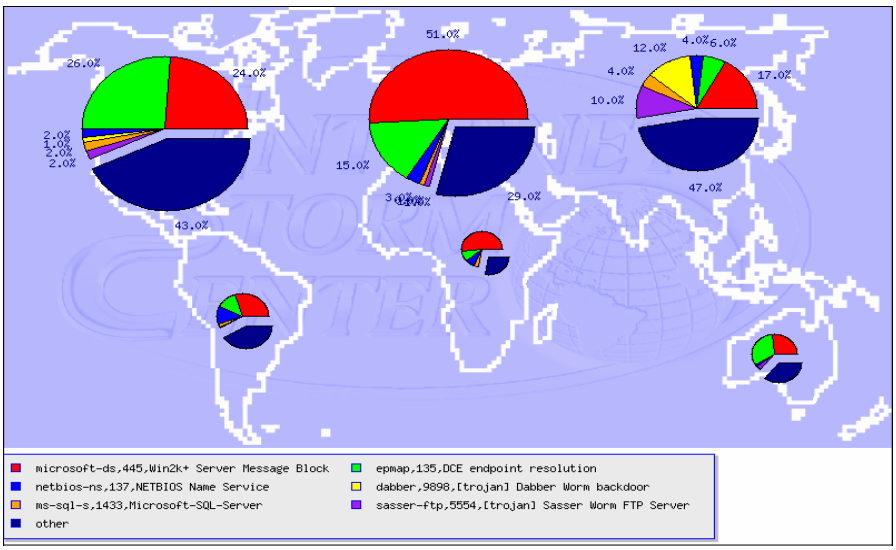
ประเภทของอันตรายจากการต่ออินเทอร์เน็ตโดยผ่านทางโมเด็ม

1. ความบกพร่องของระบบปฏิบัติการ สำหรับเครื่องคอมพิวเตอร์ที่ติดตั้งระบบปฏิบัติการตระกูลไมโครซอฟท์ ไม่ว่าจะเป็น Microsoft Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP หรือแม้กระทั่ง Windows 2003 ต่างก็เป็นช่องทางให้กับผู้บุกรุกเจาะเข้ามายังเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ต ไม่เฉพาะระบบปฏิบัติการตระกูลไมโครซอฟท์เท่านั้นที่มีปัญหาในการรักษาความปลอดภัย ระบบปฏิบัติการตระกูลลีนุกซ์เองก็ใช่ว่าจะมีความปลอดภัยมากนัก เนื่องจากว่ามีผู้ใช้งานไม่แพร่หลายเหมือนตระกูลวินโดวส์ปัญหาจึงไม่ค่อยโด่งดังมากนัก สำหรับปัญหาในหัวข้อนี้มักเรียกว่า ช่องโหว่ สามารถแก้ไขได้โดยติดตั้งโปรแกรมสำหรับอุดช่องโหว่จากเว็ปไซต์ของผู้ผลิต

2. ความตื่นตัวของผู้ใช้ในด้านความปลอดภัยค่อนข้างต่ำ ผู้ใช้งานเครื่องคอมพิวเตอร์นั้นมีหลายระดับ และผู้ใช้ส่วนใหญ่ไม่ได้เป็นผู้เชี่ยวชาญทางด้านคอมพิวเตอร์แต่อย่างใด ต่างกับเครื่องที่ทำหน้าที่เป็นเซิร์ฟเวอร์ซึ่งจะต้องใช้ผู้ดูแลระบบที่มีความชำนาญ อย่างน้อยที่สุดต้องมีความรู้ด้านคอมพิวเตอร์เป็นอย่างดีมาดูแลรักษาเซิร์ฟเวอร์ ดังนั้นเมื่อผู้ใช้ไม่ค่อยมีความรู้ทางด้านคอมพิวเตอร์มากนักย่อมเปิดโอกาสที่จะทำให้เครื่องคอมพิวเตอร์ที่ใช้งานอยู่ไม่ปลอดภัยขึ้นมาโดยไม่ตั้งใจ เช่น การเปิดใช้งานแฟ้มข้อมูลร่วมกัน (File Sharing) โดยไม่ระมัดระวังและไม่มีการจำกัดผู้ใช้เพราะคิดว่าเป็นการใช้ข้อมูลเฉพาะภายในสำนักงานเท่านั้นเอง แต่เมื่อนำเครื่องคอมพิวเตอร์นั้นไปเชื่อมต่อเข้ากับอินเทอร์เน็ต แฟ้มข้อมูลที่เปิดไว้นั้นได้เปิดเผยให้แก่คนทั้งโลกที่เชื่อมต่ออินเทอร์เน็ตอยู่ในขณะนั้น หากเพียงแต่มีผู้ใดมาเจอก็สามารถนำแฟ้มข้อมูลเหล่านั้นไปอ่านได้ทันที หรือแม้กระทั่งนำแฟ้มข้อมูลอื่นไปเก็บไว้ในเครื่องคอมพิวเตอร์ที่ท่านใช้งานอยู่โดยที่ท่านไม่รู้ตัว กรณีนี้เป็นกรณีที่เกิดขึ้นสูงมากและพบอยู่เสมอ ผู้บุกรุกมีโปรแกรมที่ทำหน้าที่ค้นหาเฉพาะเครื่องคอมพิวเตอร์ที่มีการเปิดใช้งานแฟ้มข้อมูลร่วมกันเหล่านี้ทิ้งไว้ในขณะที่ต่อกับอินเทอร์เน็ต เมื่อ

พบเข้าก็จะสามารถขโมยข้อมูลของท่านได้ทันที ถึงแม้ว่าจะมีการป้องกันโดยการถามชื่อผู้ใช้และรหัสผ่านแล้วก็ตามผู้บุกรุกจะมีโปรแกรมที่ทำหน้าที่ถอดชื่อผู้ใช้และรหัสผ่านโดยเฉพาะ (Dictionary Attack)

3. การแพร่กระจายของไวรัส เวิร์ม โทรจันและแบ็คออริฟิซ เครื่องคอมพิวเตอร์ส่วนบุคคลที่ทำหน้าที่เป็นไคลเอนต์ปกติจะสามารถติดตั้งโปรแกรมต่าง ๆ ให้ทำงานได้อย่างหลากหลาย ซึ่งต่างจากเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเซิร์ฟเวอร์ เนื่องจากต้องติดตั้งเพียงโปรแกรมที่ทำงานในหน้าที่นั้นเฉพาะอย่าง เช่น เว็บเซิร์ฟเวอร์ก็ติดตั้งโปรแกรมที่ทำหน้าที่สำหรับให้บริการเว็บเพียงอย่างเดียว การเปิดโอกาสให้สามารถเปิดโปรแกรมขึ้นมาทำงานได้นั้นเป็นช่องทางให้โปรแกรมประเภทมุ่งร้ายสามารถทำงานได้ ดังนั้นจึงพบได้ว่าเครื่องคอมพิวเตอร์ส่วนบุคคลจำนวนมากมีโปรแกรมประเภทมุ่งร้ายทำงานในเครื่อง การที่มีโปรแกรมประเภทดังกล่าวทำงานอยู่จะส่งผลเสียหายได้มากมายเป็นทวีคูณ คือ นอกจากความเสียหายที่เกิดขึ้นจากตัวโปรแกรมเองแล้ว ยังมีความเสียหายอันเกิดจากโปรแกรมที่มุ่งร้ายเหล่านั้นได้เปิดช่องทางให้ผู้บุกรุกสามารถเข้ามาในเครื่องได้โดยผ่านทางอินเทอร์เน็ตที่ผู้ใช้ต่อไว้นั้นเอง เช่น โปรแกรม NetBus ซึ่งเป็นโปรแกรมประเภท Back Door ชนิดหนึ่งซึ่งมีอันตรายมาก หากโปรแกรมนี้ติดตั้งไว้ในเครื่องใดก็ตามผู้บุกรุกจะสามารถควบคุมเครื่องคอมพิวเตอร์ของท่านผ่านทางอินเทอร์เน็ตได้โดยเปรียบเสมือนว่ามานั่งอยู่หน้าเครื่องคอมพิวเตอร์ของท่าน สามารถทำงานได้ทุกอย่างไม่ว่าจะเป็นการเปิดโปรแกรมต่าง ๆ เปิดดูแฟ้มข้อมูลต่าง ๆ อ่านคีย์บอร์ด เลื่อนเม้าส์ ควบคุมซีดีเพลย์เยอร์หรือแม้กระทั่งปิดเครื่องคอมพิวเตอร์ของท่าน



รูปที่ 2 จำนวนเครื่องคอมพิวเตอร์ที่เสียหายจากไวรัส เวิร์ม โทรจันและแบ็คออริฟิซ

4. โปรแกรมสื่อสารประเภท ICQ การทำงานของอินเทอร์เน็ตจะเป็นไปในลักษณะของไคลเอนต์กับเซิร์ฟเวอร์เป็นหลัก โดยที่ไคลเอนต์คือเครื่องคอมพิวเตอร์ที่อยู่ในฝั่งผู้ใช้งานอินเทอร์เน็ตกับอีกฝั่งหนึ่งคือเซิร์ฟเวอร์ ซึ่งเซิร์ฟเวอร์จะเป็นเครื่องคอมพิวเตอร์ที่ทำหน้าที่คอยส่งข้อมูลตอบกลับมายังฝั่งเครื่องไคลเอนต์ อาทิเช่น เว็ปเซิร์ฟเวอร์ เมลล์เซิร์ฟเวอร์ เอฟทีพีเซิร์ฟเวอร์ เป็นต้น แต่มีโปรแกรมบางประเภทที่สามารถทำให้เครื่องไคลเอนต์ติดต่อสื่อสารกันได้โดยตรงโดยไม่ผ่านเซิร์ฟเวอร์ อาทิเช่น ICQ ,QQ ทำให้ผู้ใช้งานทั้งสองฝั่งคือผู้ใช้งาน ICQ ไม่ทราบว่าผู้ที่กำลังสื่อสารอยู่ด้วยนั้นคือใคร การสื่อสารประเภทนี้เครื่องไคลเอนต์จะต้องมีช่องทาง (Port) ของการสื่อสารโดยตรง ช่องทาง (Port) นี้เองที่เป็นจุดอ่อนให้ผู้บุกรุกสามารถแอบส่งข้อมูลหรือติดตั้งโปรแกรมเข้ามายังเครื่องคอมพิวเตอร์ที่ใช้งาน ICQ ได้ด้วย สำหรับโปรแกรมประเภทนี้เรียกว่า ICQ Hack ซึ่งจะทำหน้าที่เจาะเครื่องคอมพิวเตอร์ที่เป็นคู่สนทนาโดยเฉพาะและมีเป้าหมายเป็นเครื่องคอมพิวเตอร์ที่เชื่อมต่อผ่านทางโมเด็มเป็นหลัก

5. การอ่านค่าแอกทีฟคอนเทนต์ (Active Content) ของโปรแกรมบราวเซอร์ โดยพื้นฐานการเรียกดูเว็ปเพจจะเหมือนกับการเรียกดูไฟล์ธรรมดา เพียงแต่มีการจัดรูปแบบข้อมูลภายในเนื้อหานั้นให้น่าสนใจ โดยนำข้อความ รูปภาพ และเสียงมาผสมกันโดยอาศัยภาษา HTML เป็นภาษาที่ใช้ในการสื่อสารกันระหว่างเครื่องไคลเอนต์กับเครื่องเซิร์ฟเวอร์ โดยที่เครื่องไคลเอนต์จะทำหน้าที่เสมือนเป็นผู้แปลภาษา HTML ออกมาแสดงผลให้ผู้ใช้อ่านได้เข้าใจ ส่วนเซิร์ฟเวอร์จะทำหน้าที่จัดเตรียมไฟล์ที่ผู้ใช้ต้องการอ่านส่งมาให้ การแสดงหน้าเว็ปเพจจะเป็นเสมือนการแปลภาษา HTML ออกมาให้เป็นรูปร่างหน้าตาตามที่ผู้เขียนได้สร้างไว้บนเว็ปเซิร์ฟเวอร์ในลักษณะของพาสสีฟคอนเทนต์ (Passive Content) คือ เนื้อหานั้นเป็นเพียงข้อมูลที่อ่านและดูได้อย่างเดียวเท่านั้น ไม่สามารถสั่งงานให้บราวเซอร์ทำงานอย่างหนึ่งอย่างใดได้

ปัจจุบันเทคโนโลยีของเว็ปได้มีการปรับปรุงมาในทิศทางจากพาสสีฟคอนเทนต์มาเป็นแอคทีฟคอนเทนต์ (Active Content) คือเนื้อหาเปลี่ยนแปลงได้ตลอดเพื่อตอบสนองความต้องการของผู้ใช้อาทิเช่น ภาษาจาวา (Java) หรือภาษาวิชวลเบสิค (Visual Basic) ลักษณะการทำงานของแอคทีฟคอนเทนต์คือ เซิร์ฟเวอร์จะส่งชุดคำสั่งที่เตรียมไว้แล้วสำหรับหน้าเว็บนั้นมายังเว็บบราวเซอร์พร้อมกับ HTML โดยที่ HTML จะเป็นเสมือนยูสเซอร์อินเทอร์เฟสของแอพพลิเคชั่น และคำสั่งที่ส่งมาจะเสมือนเป็นส่วนประมวลผลที่เซิร์ฟเวอร์ต้องการให้ไคลเอนต์ทำงาน ซึ่งคำสั่งที่ส่งมาให้ไคลเอนต์ และสามารถสั่งให้บราวเซอร์ทำงานได้เสมือนเซิร์ฟเวอร์

บรรณานุกรม

ปนิวัธน์ ทรัพย์รุ่งเรือง. 2547. **การรักษาความปลอดภัยเครื่องคอมพิวเตอร์ ของท่าน.** กรุงเทพฯ : โปรวิชั่น.

เรืองไกร รังสิตพล. 2544. **เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน.** กรุงเทพฯ : โปรวิชั่น.

เรืองไกร รังสิตพล. 2545. **เปิดโลก Firewall และ Internet Security.** กรุงเทพฯ : โปรวิชั่น.

เรืองไกร รังสิตพล และคณะ. 2545. **เปิดโลก TCP/IP และโปรโตคอลของอินเทอร์เน็ต.** พิมพ์ครั้งที่ 2. กรุงเทพฯ : โปรวิชั่น.

Computer Emergency Response Team. 2004. **CERT/CC Statistics 1988-2004.** [ออนไลน์] สืบค้นได้จาก http://www.cert.org/stats/cert_stats.htm l [20 สิงหาคม 2547]

Distributed Intrusion Detection System. 2004. **Reports and Database Summaries.** [ออนไลน์] สืบค้นได้จาก http://www.dshield.org/report.php [23 กันยายน 2547]

Sys Admin Audit Network Security. 2004. **Internet Storm Center Reports.** [ออนไลน์] สืบค้นได้จาก http://www.isc.sans.org/large_map.php [23 กันยายน 2547]

****