มติชน
ปีที่ 27 ฉบับที่ 9484 26 กุมภาพันธ์ พุทธศักราช 2547
หน้า 33

ก5640

มหันตภัย ไวรัส กลายพันธุ์

ต้องป้องกันอย่างไร?

ทุกวันนี้นักล่าไวรัสคอมพิวเตอร์พยายามสอดส่องไปทั่วโลกเพื่อตรวจสอบและหาข้อมูลเกี่ยวกับสถานที่ที่เกิดความเสียหายจากไวรัสตัวใหม่ๆ ที่เกิดขึ้น รวมไปถึงความสามารถในการแพร่กระจายของมัน เป็นเวลานานมาแล้วที่ **Virus, Worm** และ **Trojan** ทั้งหลายไม่มีประสิทธิภาพที่สมบูรณ์เพียงพอ แต่วันนี้ผู้เชี่ยวชาญหลายๆ ฝ่ายได้ออกมาย้ำเตือนให้ระวังถึงภัยที่จะเกิดขึ้นจากการรุกรานอันรวดเร็วของผู้บุกรุกที่มีความเข้มแข็งมากกว่าเดิมหลายเท่า

ปีที่ผ่านมาเราต้องประสบกับเหตุการณ์ที่เลวร้ายที่สุดในประวัติศาสตร์เรื่องความปลอดภัยของระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์นับล้านเครื่องไม่สามารถทำงานได้ บริษัทหลายบริษัทต้องหยุดชะงัก, ข้อมูลที่มีอยู่ไม่มีความปลอดภัยเพียงพอ, เมล์บ็อกซ์เต็มไปด้วยจดหมายขยะ, ไวรัส และเวิร์มถูกส่งออกมาแพร่กระจายไปทั่วโลก ฯลฯ

จากเหตุการณ์ดังกล่าวได้มีการประเมินค่าความเสียหายไว้สูงถึงหลักหมื่นล้านเหรียญเดียว ซึ่งนับวันตัวอันตรายเหล่านี้ก็ยิ่งทวีความรุนแรงมากขึ้นเรื่อยๆ โดยในช่วงครึ่งปีแรกของปีที่ผ่านมาได้มีการค้นพบไวรัสชนิดใหม่ถึง 994 ชนิด จากรายงานของ Symantec พบว่าโดยเฉลี่ยแล้วใน 1 อาทิตย์ จะมีการบุกรุกเข้าไปในระบบของบริษัทต่างๆ ถึง 38 ครั้ง

คริสทอฟ ฟิสเชอร์ ผู้เชี่ยวชาญทางด้านไวรัสคอมพิวเตอร์จากเมืองคาร์ลสรูห์ ได้กล่าวเตือนว่า *"ในยุคต่อไปนี้ ไวรัสและเวิร์มจะกลายเป็นหัวข้อเรื่องที่ต้องมีการกล่าวถึงกันมากยิ่งขึ้นซึ่ง Blaster และ Slammer ที่ออกมาปรากฏโฉมให้เห็นเป็นเพียงแค่ตัวเรียกน้ำย่อยเท่านั้น"* เป็นการยากที่จะจัดประเภทของโปรแกรมทำลายล้างรุ่นใหม่ๆ ที่ถูกปล่อยมาแพร่ระบาดโดยทั่วไปให้เป็นหมวดหมู่ได้ เพราะพวกมันถูกสร้างขึ้นมาให้มีความสมบูรณ์ในตัวเอง โดยให้มีกลไกหลายๆ อย่างประกอบอยู่ในตัว

● ความตื่นตระหนกเมื่อไวรัสและสแปมทำงานร่วมกัน

โปรแกรมเมอร์ที่เขียนไวรัสออกมาต่างก็ต้องการที่จะได้รับผลตอบแทนสำหรับผลงานของตนเช่นเดียวกัน ผู้เชี่ยวชาญต่างหวาดระแวงถึงการประสานงานกันของไวรัส และสแปมที่นับวันจะสูงขึ้นเรื่อยๆ ฟิสเชอร์ได้บรรยายไว้ว่า *"จากจุดเริ่มต้นในความพยายามทุกวิถีทางเพื่อป้องกันไม่ให้มีสแปมหลุดรอดเข้ามาในระบบ แต่ผลที่ตามมาก็คือ Spammer พยายามเสี่ยงหาหนทางอื่นเพื่อทำงานให้บรรลุเป้าหมายน่าห่วงว่าในอนาคตไวรัสอาจจะกลายเป็นสื่อกลางที่ใช้ในการขนส่งสแปมก็เป็นได้"*

จุดมุ่งหมายของไวรัสก็คือเข้าไปควบคุมเครื่องคอมพิวเตอร์

และใช้งานในลักษณะที่ต้องการ ซึ่งรูปแบบการรวมตัวกันของไวรัสและสแปมสามารถอธิบายได้คร่าวๆ คือ ผู้สร้างไวรัสจะนำโปรแกรมที่เรียกว่า **"Ratware"** ซึ่งก่อนหน้านี้ใช้ในการส่งสแปมมาใช้เพื่อทำให้การแพร่กระจายของไวรัสเป็นไปอย่างมีประสิทธิภาพมากยิ่งขึ้นในทำนองเดียวกัน **Spammer** ก็จะส่ง อี-เมล์ขยะ (Junk Mail) ที่ประกอบไปด้วยโทรจันหรือลิงก์ที่จะเปิดไปสู่หน้าเว็บไซต์ลามกโดยอัตโนมัติซึ่งเป็นเหตุให้คุณต้องเสียเงินโดยไม่รู้ตัว

(ต่อหน้าหลัง) ...→

• อนุสัญญาความร่วมมือเพื่อต่อสู้กับอาชญากรรมบนอินเตอร์เน็ต

ผู้ที่ส่งไวรัสหรือสแปมออกมาแพร่ระบาดต่างก็พยายามที่จะหลบหนีการติดตามให้พ้นโดยการหลบหนีไปยังประเทศอื่นๆ ไม่ว่าจะเป็นประเทศในแถบเอเชีย, ยุโรปตะวันออก, อเมริกาใต้ หรือเกาะที่ไม่ค่อยมีใครรู้จัก แต่บ่อยครั้งที่เบาะแสทางข้อมูลดิจิตอลสามารถนำไปสู่ต้นตอของการก่ออาชญากรรมออนไลน์ได้หากมีการติดตามสืบเสาะไปจนถึงจุดเริ่มต้นที่แท้จริง ซึ่งจะทำให้สามารถจับกุมผู้ที่ลักลอบส่งรูปภาพอนาจารของเด็ก หรือทำการแพร่เชื้อไวรัส รวมไปถึงผู้ที่มีพฤติกรรมฉ้อโกงผ่านทางระบบออนไลน์ทุกชนิดได้

แม้ว่าผู้เชี่ยวชาญส่วนใหญ่จะมีประสบการณ์มากมายเกี่ยวกับการโจมตีของไวรัสแต่บางครั้งก็ต้องอาศัยโชคเพื่อจะพบตัวผู้บุกรุกที่เข้ามาวนเวียนอยู่ในระบบอย่างทันท่วงที ซึ่งเป็นสาเหตุสำคัญที่จะต้องมีการตรวจสอบเป็นระยะๆ เพราะเมื่อหนอนไวรัสตัวหนึ่งแพร่กระจายไปอย่างรวดเร็ว ดังตัวอย่างเช่น **SQL-Slammer** ที่จะเพิ่มจำนวนเป็น 2 เท่าทุกๆ 8.5 วินาที ย่อมเป็นไปไม่ได้ที่จะแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้นได้ทันท่วงที

ไวรัสชนิดใหม่ๆ ที่เกิดขึ้นมาโดยส่วนใหญ่ จะเป็นไวรัสที่ได้รับการปรับปรุงความสามารถจากไวรัสรุ่นเก่าๆ ที่เคยมีมาแล้วให้อยู่ในรูปแบบที่ใหม่ขึ้น โดยจะมีการเปลี่ยนแปลง Text-Line เพียงเล็กน้อย หรือแก้ไขให้สามารถถูกตรวจพบได้ยากขึ้นเท่านั้น ถ้ามีการลิสต์รูปแบบทั้งหมดของไวรัสออกมาจะพบได้ว่าในปัจจุบันมีไวรัสที่เป็นที่รู้จักประมาณ 90,000 ชนิด

ไวรัส มีความสามารถในการทำลายหรือขโมยข้อมูลทางด้านอุตสาหกรรมได้ เมื่อมันเริ่มทำงาน มันจะส่งข้อมูลของบริษัทที่ถูกเก็บเอาไว้ออกมาภายนอก หรือทำให้การทำงานทั้งหมดหยุดชะงัก โดยเฉพาะไวรัสประเภทที่มีวิธีการทำงานที่ไม่ได้เปิดเผยตัวออกมาอย่างเด่นชัดจะยิ่งอันตรายเป็นพิเศษ ในขณะที่ความเสียหายที่ปรากฏออกมาสามารถใช้การแบ็กอัพช่วยแก้ปัญหาได้ แต่ความเสียหายจากการที่ข้อมูลถูกเปลี่ยนแปลงไปเป็นระยะเวลานานนับเดือนถือเป็นความเสียหายที่มีความรุนแรงมากกว่าอย่างเปรียบเทียบกันไม่ได้

วิธีที่จะแก้ปัญหาเรื่องไวรัสให้หมดสิ้นไปมีทางเดียวคือเปลี่ยนแปลงโครงสร้างของเครื่องคอมพิวเตอร์ให้อยู่ในรูปแบบใหม่ทั้งหมด ซึ่ง Fischer กล่าวว่า "โดยหลักการแล้วเราเปลี่ยนมาใช้ระบบใหม่แทนระบบ Windows, Unix รวมไปถึง Linux ที่มีใช้กันอยู่เดิมให้หมดสิ้น" ซึ่งทุกคนต่างก็รู้กันดีอยู่แล้วว่าเป็นไปไม่ได้ เพราะการลงทุนในเรื่องดังกล่าวต้องเสียค่าใช้จ่ายมากมายมหาศาลอย่างมิอาจประเมินได้

เพื่อให้รู้เท่าทันมหันตภัยไวรัสที่กำลังกลายพันธุ์ และหาทางป้องกันไม่ให้มันแพร่กระจายสร้างความเดือดร้อนอีกต่อไป ก็สามารถหาอ่านข้อมูลอื่นๆ นอกเหนือจากนี้ได้จากนิตยสาร CHIP ฉบับกุมภาพันธ์ จะได้ไม่ตกหลุมพรางของเจ้าตัวร้ายได้ง่ายๆ อีกต่อไป