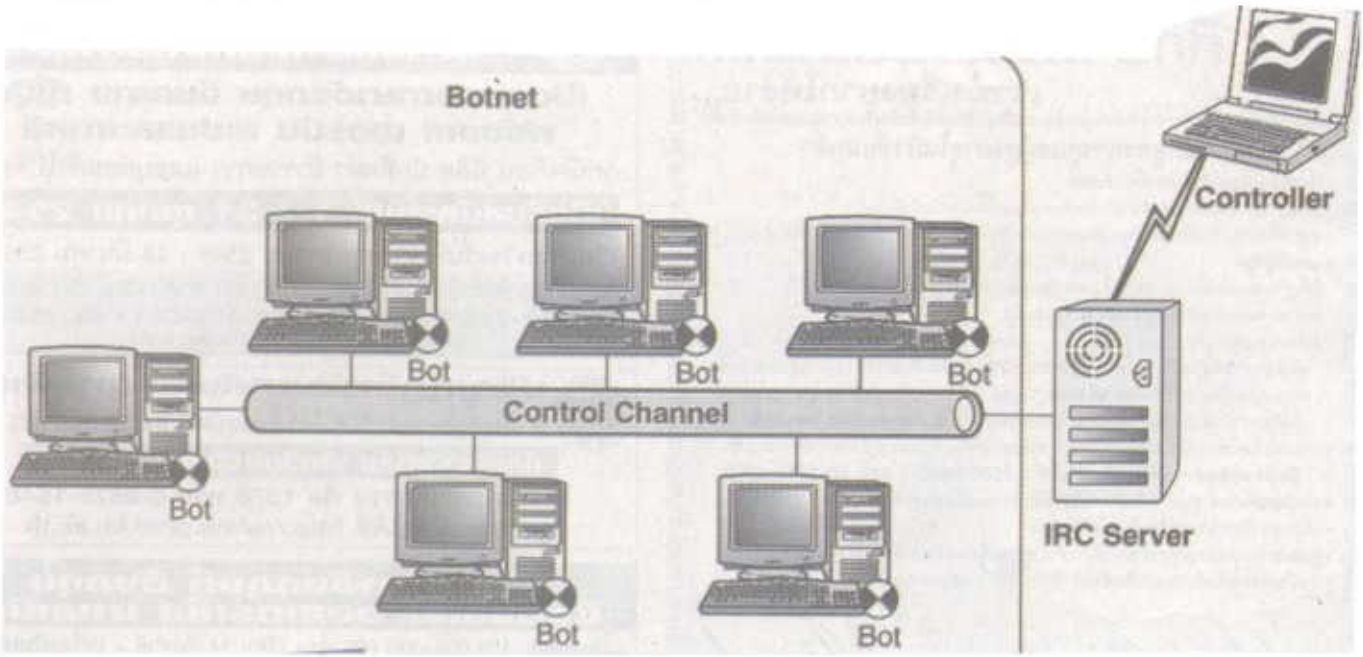
ก 7109

มติชน

ปีที่ 29 ฉบับที่ 10421 วันพฤหัสบดีที่ 21 กันยายน พุทธศักราช 2549 หน้า 32

รู้วิธีปกป้อง...คอมพิวเตอร์ ไม่ให้ถูกโจมตีจาก...บ็อตเน็ตส์



ปัจจุบัน นอกจากมัลแวร์ใหม่สามารถเขียนขึ้นมาได้อย่างง่ายดายแล้ว เจ้าหนอนร้ายยังสามารถแพร่พันธุ์ผ่านเครือข่ายคอมพิวเตอร์ ซอมบี้ ที่เรียกว่า **เครือข่ายบ็อต** (bot networks) หรือ **บ็อตเน็ตส์** (botnets) โดยหนอนที่เปิดใช้งานบ็อตมักจะมีชื่อเล่นว่า **บ็อต**

ความง่ายดายของการเขียนมัลแวร์ใหม่ยังไม่ร้ายเท่ากับความสามารถล่าสุดของหนอนสายพันธุ์ใหม่ที่สามารถแพร่ระบาดผ่านทางเครือข่ายคอมพิวเตอร์ "ซอมบี้" ที่มีการติดเชื้อร้ายโดยที่ผู้ใช้ไม่รู้ตัว

นายโจ สาร์ดแมนน์ ผู้อำนวยการกลุ่มวิจัยด้านการป้องกันไวรัส บริษัท เทรนด์ ไมโคร เปิดเผยว่า ขณะนี้มีสายพันธุ์บ็อตจำนวนมากที่เกิดขึ้นจากผู้เขียนมัลแวร์หลายคน ในฤดูใบไม้ผลิ เราพบบ็อต 6 สายพันธุ์ จากมัลแวร์ 4 ตระกูล ทั้งหมดใช้โค้ดเหมือนกัน บ็อตทั้ง 6 สายพันธุ์ มีฟังก์ชันการทำงานหลักๆ เหมือนกัน แต่มีบางสายพันธุ์ที่ได้เพิ่มฟังก์ชันใหม่ลงไปด้วย เช่น การส่งจดหมายปริมาณมาก (mass mailer) ส่งผลให้มีการเพิ่มจำนวนหนอนร้ายไปทั่วโลกอย่างรวดเร็ว

บรรดาผู้เชี่ยวชาญด้านความปลอดภัยเพิ่มเติมว่า กลุ่มผู้เขียนมัลแวร์มักจะนำเทคนิคนี้ไปใช้กันอยู่บ่อยครั้ง โดยเริ่มจากมีคนเขียนโค้ดร้ายขึ้น และนำไปประกาศไปยังไซต์อินเตอร์เน็ตสาธารณะ จากนั้นผู้เขียนมัลแวร์รายอื่นๆ ก็จะผนวกฟังก์ชันใช้งานเพิ่มเติมเช่น เทคนิคการกระจายและแพร่พันธุ์ในขั้นที่สูงขึ้น เพื่อทำให้มัลแวร์ตัวนี้แพร่กระจายและมีขีดความสามารถเพิ่มขึ้น

ทั้งนี้ ความเร็วก็เป็นสิ่งจำเป็นอย่างที่สุดต่อความสำเร็จของการโจมตีด้วยบ็อต สืบเนื่องจากเหตุผล 2 ประการ นั่นคือประการแรกเป็นเรื่องของโอกาสของความสำเร็จที่โดยทั่วไปแล้วจะมีเพียง 30 - 90 วันเท่านั้น เพราะช่วงเวลาดังกล่าวเป็นการประกาศช่องโหว่ และคอมพิวเตอร์ส่วนใหญ่ต้องได้รับการซ่อมแซมช่องโหว่นั้น เพื่อไม่ให้ระบบสามารถติดเชื้อร้ายได้อีก

ประการที่สอง เป็นการแข่งกันสร้างเครือข่ายบ็อตเน็ตของตัวเองของกลุ่มผู้เขียนหนอนจำนวนหนึ่ง โดยพวกเขาจะรู้กันดีว่า เวลาเป็นสิ่งสำคัญ เนื่องจากต่างแข่งกันทำให้ระบบของผู้ใช้จำนวนมากติดเชื้อให้มากที่สุด เพื่อสร้างบ็อตเน็ตและขัดขวางกลุ่มอื่นไม่ให้ใช้ระบบเดียวกันนี้สร้างบ็อตเน็ตของตัวเองขึ้นมา

[ต่อด้านหลัง]

ผลคือ เมื่อมีการประกาศช่องโหว่ออกมา เป็นการจูงใจให้บรรดาผู้เขียนมัลแวร์พากันสร้างโค้ดร้าย และปล่อยโค้ดนั้นให้แพร่กระจายให้รวดเร็วที่สุดเท่าที่จะเป็นไปได้เพื่อให้การโจมตีนั้นมีประสิทธิภาพมากที่สุด

นายนรุช สิวส์ วิศวกรอาวุโสฝ่ายวิจัยเทรนด์ ไมโคร กล่าวว่า บ๊อตส่วนใหญ่จะใช้ประโยชน์จากช่องโหว่เดียวกันอย่างต่อเนื่อง เมื่อบริษัทหนึ่งติดเชื้อ พวกเขาจะแก้ด้วยการซ่อมแซมระบบที่มีช่องโหว่ และเชื่อว่าจะไม่มีการติดเชื้อร้ายได้อีก แล้วจะมีช่องโหว่ใหม่ที่ทำให้พวกเขาตกเป็นเป้าหมายได้อีกครั้ง

นอกจากความเร็วของการเขียนโค้ดร้ายแล้ว ผู้เขียนมัลแวร์ยังนิยมใช้โค้ดแบบโมดูลดาร์ หรือที่เรียกว่าโปรแกรมย่อยที่ทำงานอย่างอิสระด้วยเช่นตัวอย่างความสำเร็จของ WORM_SASSER และ WORM_BLASTER ที่เหมือนกับการติดเชื้อ ZOTOB หนอนร้ายตัวล่าสุด ความสามารถเหล่านี้ถูกเพิ่มลงในบ๊อตที่มีอยู่แล้วอย่างรวดเร็ว หลังจากที่มีการประกาศช่องโหว่ แม้ว่าสายพันธุ์แรกจะประสบความสำเร็จไม่มากนัก แต่สิวส์เตือนว่าสายพันธุ์ต่อๆ มาจะมีความสำเร็จมากยิ่งขึ้นไปอีก

ผู้เชี่ยวชาญด้านความปลอดภัย จึงเตือนว่าอาจมีการโจมตีโดยใช้ช่องโหว่เหล่านี้มากขึ้น และแนวทางป้องกันที่ดีที่สุดคือ ความระแวดระวังของผู้ใช้ระดับต่าง ๆ ซึ่งรวมถึงการหมั่นปรับปรุงโปรแกรมซ่อมแซม (patch) ล่าสุดของไมโครซอฟท์ และคอยดูแลให้ Antivirus Definition เป็นปัจจุบันอยู่เสมอ.

หากต้องการป้องกันภัยคุกคามชนิดนี้ ผู้เชี่ยวชาญด้านความปลอดภัยของเทรนด์ ไมโคร มีข้อแนะนำดังนี้

- ตรวจสอบให้แน่ใจว่าระบบได้รับการซ่อมแซมจากโปรแกรมการปรับปรุงระบบล่าสุด
- ตรวจสอบให้แน่ใจว่า Antivirus Definition ทันสมัย โดยทั่วไปบริษัทป้องกันไวรัสส่วนใหญ่จะให้ตัวเลือกการปรับปรุงอัตโนมัติภายในผลิตภัณฑ์ด้านความปลอดภัยอยู่แล้ว
- เพิ่มการตั้งค่าความปลอดภัยของคุณบนโปรแกรมบราวเซอร์ให้สูงขึ้น เพื่อให้ผู้โจมตีมีโอกาสกระทำการได้สำเร็จน้อยลง
- จำกัดสิทธิผู้ใช้ของคุณเมื่อออนไลน์ ผู้ใช้ประสงค์ร้ายมักจะได้รับสิทธิในระดับเดียวกับผู้ใช้ที่ถูกต้องในองค์กร ดังนั้น ถ้าผู้ใช้ที่ถูกต้องเข้าสู่ระบบด้วยสิทธิผู้ใช้มาตรฐาน ผู้ใช้ประสงค์ร้ายจะสามารถได้รับสิทธิเดียวกันนี้ด้วย ในทางตรงข้าม ถ้าผู้ใช้เข้าสู่ระบบด้วยสิทธิของผู้ดูแลระบบ ผู้ใช้ประสงค์ร้ายก็สามารถได้รับสิทธิควบคุมระบบของผู้ใช้ได้อย่างเต็มที่เช่นกัน
- เปลี่ยนการกำหนดลักษณะอี-เมลของคุณให้เป็นแบบปิดใช้งานการดาวน์โหลดอัตโนมัติ เมื่อแสดงตัวอย่างข้อความ และบล็อครูปภาพและเนื้อหาอินเตอร์เน็ตอื่นๆ จากการดาวน์โหลดลงในคอมพิวเตอร์โดยอัตโนมัติด้วย
- ใช้อี-เมลอย่างปลอดภัย รวมถึงละเว้นจากการคลิกลิงค์ฝังตัวใดๆ
- หลีกเลี่ยงการเปิดสิ่งที่แนบมาที่ปรากฏเป็นรูปภาพหรือไฟล์อื่นๆ จากแหล่งที่มาที่ไม่รู้จักกับสิ่งที่แนบมา หากสงสัยให้สอบถามผู้ที่รู้จักว่าส่งสิ่งใดมาให้หรือไม่ ก่อนเปิดสิ่งที่แนบมาใดๆ
- **เทรนด์ ไมโคร เปิด housecall เพื่อให้บริการสแกนไวรัสฟรี ที่เว็บไซต์ http://housecall.trendmicro.com**