ก 5458

กรุงเทพธุรกิจ ปีที่ 17 ฉ.ที่ 5,558 11 พฤศจิกายน 2546 หน้า 5

เตือนอันตราย! หน้าเวบแฝงไวรัสร้าย

นักวิเคราะห์เตือนภัยไวรัสเอชทีเอ็มแอล เพิ่มอัตราโจมตีเครือข่าย เผยเทคนิคแฝงตัวในเนื้อหาอีเมล และหน้าเวบปลอม พร้อมอาศัยรูโหว่ซอฟต์แวร์ไออี ติดตั้งโปรแกรมอันตรายลงเครื่องเหยื่อ แนะผู้ใช้อัพเดทเบราเซอร์สม่ำเสมอ ขณะเชื่อไม่มีทางแก้ไข

ผู้ใช้คอมพิวเตอร์ส่วนใหญ่ มักได้รับคำแนะนำในการป้องกันไวรัสที่คล้ายๆ กัน คือ อย่าเปิดไฟล์แนบที่ไม่รู้จัก และลบอีเมลเหล่านั้นทิ้งไปซะ

วิธีที่ว่านี้ อาจใช้ได้ผลดีสำหรับไวรัส หรือเวิร์มทั่วไป แต่แท้จริงแล้ว ยังมีไวรัสอีกรูปแบบหนึ่ง ที่สามารถเข้าโจมตีคอมพิวเตอร์ได้ทันที เมื่อผู้ใช้เพียงแค่อ่านข้อความบนอินเทอร์เน็ต หรือเยี่ยมชมเวบที่บรรจุไวรัสเอาไว้เท่านั้น ซึ่งผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยได้ทำนายว่า ไวรัสประเภทนี้ จะมีการแพร่ระบาดเพิ่มมากขึ้นในอนาคต

ไวรัสเหล่านี้ อาศัยรูโหว่ในเบราเซอร์อินเทอร์เน็ต เอ็กซ์พลอเรอร์ (IE) ของไมโครซอฟท์ และอาจแฝงมาในรูปของอีเมลจากธนาคารออนไลน์ ที่หลอกให้ผู้รับเปิดเผยข้อมูลส่วนตัว หรือเชื่อมต่อไปยังเวบไซต์ปลอม

นายรัส คูปเปอร์ หัวหน้าทีมนักวิทยาศาสตร์ บริษัทรักษาความปลอดภัยเครือข่าย ทรู ซีเคียวร์ กล่าวเตือนว่า รูปแบบการโจมตีเช่นนี้ จะเพิ่มมากขึ้นเรื่อยๆ ตราบใดที่มีผู้เขียนอีเมลด้วยภาษาฟอร์แมต เอชทีเอ็มแอล (HTML) ซึ่งเป็นภาษาที่โดยปกติแล้ว จะใช้ในการสร้างหน้าเวบมากกว่า

แฝงตัวโจมตี

นายคูเปอร์ กล่าวว่า อันตรายจากภาษาเอชทีเอ็มแอลนั้น กำลังเพิ่มสูงขึ้นทุกที และมีผู้ใช้ภาษาดังกล่าวในการโจมตีคอมพิวเตอร์ ก่อกวนเครือข่าย หรือขโมยข้อมูลลับของผู้ใช้เป็นจำนวนมาก

"การโจมตีเช่นนี้ อาศัยอีเมลที่เขียนด้วยภาษาเอชทีเอ็มแอล และธรรมชาติของภาษานี้ก็คือ เราจะไม่รู้ว่ามีอะไรซ่อนอยู่ภายใน" เขากล่าว

รหัสเอชทีเอ็มแอลที่ออกแบบขึ้นสำหรับโจมตีคอมพิวเตอร์ อาจอยู่ในอีเมล หรืออาจซ่อนอยู่ตามเนื้อหาบนเวบไซต์ต่างๆ ที่ทำให้ดูเหมือนกับเป็นเวบไซต์ที่ถูกต้องตามกฎหมายก็ได้ และอีเมลที่บรรจุรหัสอันตรายเหล่านี้ไว้ก็อาจมาได้ทั้งในรูปของจดหมายจากบริษัท ที่เต็มไปด้วยภาพกราฟิก ไปจนถึงลิงค์ที่เชื่อมต่อไปยังเวบไซต์ต่างๆ

เนื่องจากรหัสร้ายพวกนี้ไม่ได้อยู่ในไฟล์แนบ จึงทำให้ผู้ใช้คอมพิวเตอร์ทั่วไปไม่สามารถดำเนินการป้องกันอะไรได้มากนัก นอกจากจะมีโปรแกรมอีเมลรุ่นล่าสุด ที่สามารถปิดกั้นสคริปท์เหล่านี้ได้ หรือนอกจากจะสามารถตรวจสอบรหัสอีเมลได้เอง ทำให้คาดว่า ไวรัสเอชทีเอ็มแอลดังเช่นกรณีของไวรัส คิวโฮสท์ (Qhost) จะมีอัตราแพร่ระบาดสูงขึ้นเรื่อยๆ

ผู้เชี่ยวชาญ เผยว่า ไวรัสคิวโฮสท์ อาศัยรูโหว่ในเบราเซอร์ไมโครซอฟท์ ที่ช่วยให้ตนสามารถติดตั้งรหัสอันตรายลงบนคอมพิวเตอร์เหยื่อได้ เมื่อผู้ใช้เข้าไปยังหน้าเวบอันตรายบางแห่ง ก็เท่ากับเปิดทางให้โฆษณาประเภทป๊อป-อัพ เข้าไปรันอยู่ใต้หน้าต่างเบราเซอร์หลักของเครื่องโดยไม่รู้ตัว ซึ่งจะทำให้เครื่องปล่อยโฆษณาป๊อป-อัพออกมา รวมทั้งมีการติดตั้งโปรแกรมอันตรายลงบนเครื่องด้วย

การเปลี่ยนแปลงครั้งใหญ่

สำหรับผู้เชี่ยวชาญบางรายแล้ว ไวรัสคิวโฮสท์ แสดงถึงการเปลี่ยนแปลงครั้งสำคัญจากไวรัสที่ทำให้ระบบชำรุด และสร้างความปั่นป่วนบนเครื่องข่าย

อย่างไรก็ตาม นายเกรแฮม คลูลี่ย์ นักวิเคราะห์บริษัทโซฟอส เผยว่า รูปแบบการโจมตีเช่นนี้ ยังสามารถป้องกันได้โดยการอัพเดทโปรแกรมอินเทอร์เน็ต เอ็กซ์พลอเรอร์ในเครื่องอย่างสม่ำเสมอ

"บริษัทผลิตซอฟต์แวร์ต้านไวรัสเริ่มหันมาจัดกลุ่มให้อีเมลเอชทีเอ็มแอล เป็นรูปแบบการสื่อสารที่อาจมีอันตราย และผู้ที่ดำเนินธุรกิจโฆษณาผ่านอีเมล อย่างถูกต้องตามกฎหมาย ก็เริ่มมองเห็นข้อบกพร่องเหล่านี้ และเริ่มต่อต้านการใช้เอชทีเอ็มแอลกันแล้ว" เขา กล่าว

แม้ว่ารูโหว่ในโปรแกรมเบราเซอร์จะแก้ไขได้ ด้วยการดาว์นโหลดซอฟต์แวร์ซ่อมแซม แต่นายคูเปอร์ให้ความเห็นว่า บรรดาแฮคเกอร์ที่เป็นตัวปล่อยไวรัส ก็จะหาวิธีอื่นๆ ในการโจมตีคอมพิวเตอร์อยู่ดี และทำให้ต้องตามผลิตโปรแกรมซ่อมแซมไปเรื่อยๆ

ซ่อนแผนโจมตี

นอกจากนี้ ยังมีการโจมตีของไวรัสเอชทีเอ็มแอล ที่พุ่งเป้าไปยังลูกค้าของธนาคารออนไลน์โดยเฉพาะ ในกรณีเหล่านี้ แฮคเกอร์จะส่งอีเมลไปยังลูกค้า และบอกให้ไปยังเวบไซต์ของธนาคาร เพื่อตรวจสอบรหัสผ่าน และข้อมูลสำคัญหลายๆอย่าง

แต่ตัวการปล่อยไวรัสเหล่านี้ มักไม่รู้ว่าลูกค้าใช้บริการธนาคารอะไร ซึ่งนายคลูลีย์แนะนำว่า ผู้ใช้ไม่ควรเปิดดูอีเมลที่มาจากธนาคาร และตรวจสอบข้อเท็จจริงกับทางธนาคารผ่านทางโทรศัพท์แทน หรืออาจบันทึกลิงค์เวบไซต์ธนาคารออนไลน์ของตนไว้ในเครื่อง

"แต่คนที่เรารู้จัก ก็มักส่งอีเมลเอชทีเอ็มแอลมาด้วยเช่นกัน และการตั้งกฎว่าต้องลบอีเมลที่เขียนด้วยภาษานี้เสมอ คงเป็นวิธีที่ไม่ถูกต้องนัก" นายคลูลีย์ กล่าว

พร้อมทิ้งท้ายว่า "ไมโครซอฟท์ ยังคงวิ่งไล่งับหางตัวเอง โดยหวังว่าจะสามารถทำให้อีเมลเอชทีเอ็มแอล มีความปลอดภัยได้ แต่พวกเราคิดว่า ปัญหาเช่นนี้ จะยิ่งเพิ่มมากขึ้นในอนาคตมากกว่า"