

3อันตราย ..ระวังไว้ดีกว่าแก้

นำเสนอเมื่อ : 24 มี.ค. 2552

อันตราย 3 ประการที่คุณไม่รู้จัก

แฮกเกอร์จะแอบเข้ามาในเครื่องของคุณ โดยสามารถที่จะผ่านแม้แต่ระบบป้องกันที่ดีที่สุดเข้า มาจนได้ แล้วก็เริ่มก่อความเสียหายให้ในที่สุด

แฮกเกอร์ทั้งหลายนั้นเริ่มใช้วิธีการที่ก้าวร้าวและอันตรายมากขึ้นเรื่อยๆ พวกเขาจะมีหนทางใหม่ ๆ อยู่เสมอในการที่จะแพร่โปรแกรมร้ายเข้าไปในเครื่องของคุณ และถ้าใครที่คิดว่าแค่ Update ล่าสุด โปรแกรมป้องกันไวรัสที่ดีที่สุด และไฟร์วอลล์ที่แกร่งที่สุด จะทำให้เครื่องของคุณปลอดภัยได้

บอกได้เลยว่าคิดผิดแล้ว

กรรมวิธีใหม่ ๆ

ของแฮกเกอร์และมาเฟียอินเทอร์เน็ตทั้งหลายนั้นได้สร้างปัญหาให้กับผู้เชี่ยวชาญด้านความปลอดภัยต่าง ๆ ไม่น้อยเลยทีเดียว แต่อย่างน้อยคุณก็สามารถที่จะลดอัตราความเสี่ยงลงได้ CHIP จะแนะนำให้คุณรู้จักกับอันตราย 10 ประการ ที่เราเชื่อว่าหลายคนคงแทบจะไม่เคยได้ยินมันมาก่อน พร้อมทั้งแนะนำวิธีที่ดีที่สุดในการต่อกรกับพวกมันอีก กตวย

1. ช่องว่างในระบบรักษาความปลอดภัยของ Security Suite

ไฟร์วอลล์ โปรแกรมป้องกันไวรัส และโปรแกรมป้องกันสแปมเมล เป็นสิ่งที่มีอยู่ในคำแนะนำด้านความปลอดภัยสำหรับ บเครื่องพีซีที่ซื้อมาได้ว่าเป็นระบบปฏิบัติการ แต่ในขณะที่เดียวกันพวกมันก็เป็นเสมือนกับบัตรเชิญไปยัง มาเฟียอินเทอร์เน็ตทั้งหลายด้วย เพราะในโปรแกรมเหล่านี้จะมีบั๊ก (Bug) อยู่ภายในเช่นเดียวกับในโปรแกรมอื่นๆ ทั่วไป ซึ่งจะกลายเป็นช่องโหว่ให้เจตตัวร้ายรายต่างๆ สามารถเข้ามาสู่เครื่องของคุณได้ในทันทีที่มีการต่อเชื่อมอินเทอร์เน็ต เช่นเพื่อการอัปเดต

จากตัวอย่างของ Blackice Firewall จะเห็นได้อย่างชัดเจนถึงความร้ายแรงของข้อผิดพลาดนี้ เมื่อแฮกเกอร์พบช่องโหว่ในระบบรักษาความปลอดภัย พวกเขาจะใช้มันให้เป็นประโยชน์ทันที โดยส่งไวรัส "Witty" เขาไปยัง Blackice Firewall ต่างๆ ทั่วโลก ภายในเวลาแค่ไม่ถึงชั่วโมงมันจะเข้าไปทำลายข้อมูลที่ทั้งหมดที่มีอยู่บนฮาร์ดดิสก์ของผู้เคราะห์ร้าย

แม้แต่บริษัทใหญ่ๆ อย่าง Symantec ก็ต้องประสบกับปัญหานี้เช่นกัน อย่างที่แฮกเกอร์คนหนึ่งได้แสดงให้เห็นว่า สามารถนำข้อผิดพลาดใน Symantec Antivirus Corporate Edition ไปใช้ได้อย่างไร แค่ชั่วพริบตาเขาก็สามารถที่จะเข้าไปในเครื่องที่ดู เหมือนจะมีการป้องกันเอาไว้อย่างสมบูรณ์แบบได้อย่าง ยาดาย

ทางแกั การแก้ไขปัญหานี้เป็นหน้าที่ของผู้ผลิตโปรแกรมรักษาความปลอดภัยที่ต้องตอบสนองได้อย่างรวดเร็วและถูกต้องของโ หวเหล่านั้นได้อย่างทันท่วงที แต่อย่างไรก็ตามคุณไม่ควรที่จะปิดฟังก์ชัน Online Update ของชุดโปรแกรมรักษาความปลอดภัย (Security Suite) ของคุณโดยเด็ดขาด เพราะไม่เช่นนั้นก็จะไม่สามารถแก้ไขข้อผิดพลาดอื่นๆ ที่อาจจะร้ายแรงกว่าได้ ในขณะที่เรากำลังปิดต้นฉบับอยู่นี้ Symantec ก็ได้ทำการกำจัดบั๊กที่แอสแกเกอร์ไตสาคิตให้เราดูออกไป เรียบร้อยแล้ว แต่ถึงอย่างไรการป้องกันแบบ 100% นั้นก็คงยังไม่สามารถทำได้อย่างแน่นอน

2. เครื่องพิมพ์อันตรายในระบบเครือข่ายของบริษัท

แอสแกเกอร์ยังคงค้นหาจุดอ่อนใหม่ๆ ในระบบเครือข่ายอยู่ตลอดเวลา ดังนั้นผู้ดูแลระบบ (Administrator) ที่ดีจึงไม่ควรที่จะเพิ่มระบบป้องกันแต่เฉพาะบนเซิร์ฟเวอร์และตัวไฟร์วอลล์เท่านั้น แต่ควรจะรวมไปถึงเครื่องไคลเอนท์ต่างๆ ให้ได้มากที่สุดด้วย แต่จุดอ่อนสำคัญอย่างหนึ่งที่มีมักจะถูกมองข้ามไปได้แก่ เครื่องพิมพ์ โดยเครื่องพิมพ์ที่สามารถใช้ในระบบเครือข่ายได้นั้นก็ จะเป็นเหมือนเซิร์ฟเวอร์ตัวหนึ่งด้วยเหมือนกัน นั่นหมายความว่า ถ้าใครที่ต้องการจะโจมตีระบบของคุณ ก็สามารถที่จะเข้าไปเปลี่ยนแปลงการตั้งค่าต่างๆ หรือแม้แต่เข้ายึดครองระบบปฏิบัติการของเครื่องพิมพ์ อย่างสมบูรณ์แบบเลยก็ได้

เมื่อหลายปีที่ผ่านมา Hacker FX จากกลุ่ม Hacker Phenoelit ได้นำข้อมูลและเครื่องมือที่สามารถนำไปใช้เปิดช่องโหว่ของเครื่องพิมพ์ยี่ห้อ HP ได้ออกมาเผยแพร่ และในปีนี้ออสแกเกอร์อีกคนก็ได้แสดงให้เราเห็นถึงพริ้น เซิร์ฟเวอร์ที่ได้รับการดัดแปลงมา ซึ่งบนนั้นจะมี Hacker Tool บางตัวทำงานอยู่แล้วด้วยซ้ำ

ซึ่งช่วยให้แอสแกเกอร์ทำงานได้ง่ายขึ้นไปอีก เครื่องพิมพ์ที่ถูกดัดแปลงแล้วนี้จะสามารถส่งข้อมูลส่วนตัวของผู้ใช้ อย่างเช่น ข้อมูลบัญชีธนาคาร หลักฐานเงินเดือน

หรือแม้แต่ पासเวิร์ดกลับไปให้แอสแกเกอร์ได้อย่างง่ายดายตา ยทุกครั้งที่ยึดต้องการพิมพ์ข้อมูลลงบนกระดาษ

ทางแกั

ความจริงแล้ววิธีการป้องกันในเรื่องนี้นั้นง่ายมาก แค่กำหนดรหัสผ่าน (Password) ที่แข็งแกร่งขึ้นมาใน Configuration Console ของเครื่องพิมพ์หรือการจำกัดสิทธิในการใช้งานก็มักจะ เพียงพอแล้ว

ที่สำคัญอีกอย่างหนึ่งก็คือ การมองออกไปให้ไกลกว่านั้นอีก เช่น มีอุปกรณ์ใดบ้างที่ต่อเชื่อมกับระบบเครือข่ายของคุณ เพราะทั้งกล่องเว็บแคม เราเตอร์ไร้สาย และอุปกรณ์ต่างๆ ก็ล้วนแล้วแต่เป็นเป้าหมายของแอสแกเกอร์ด้วยทั้งนั้น

3. แค้ไตรพัสตักก็สามารถเข้ายึดพีซีได้ทุกเครื่อง

ผู้เชี่ยวชาญด้านความปลอดภัยทุกคนรู้ว่าถ้าแอสแกเกอร์ มาถึงหน้าเครื่องแล้ว แม้แต่การป้องกันที่ดีที่สุดก็ยังไม่สามารถช่วยอะไรได้ อีกต่อไป ดังนั้น Terminal สารณะต่างๆ อย่างเช่นเครื่องคอมพิวเตอร์ในห้องสมุด หรือในซูเปอร์มาร์เก็ตจึงมีการปิดกั้นการรับข้อมูลจาก ภายนอกทั้งหมด เว้นแต่คีย์บอร์ด เม้าส์ และจอมอนิเตอร์เท่านั้น แต่แค่นั้นก็มากเกินไปแล้ว

มีจุดเปราะที่่เกิดจากความผิดพลาด (Error Source) อยู่ 2 ประการที่จะเป็นประโยชน์ต่อแฮกเกอร์ได้ ประการแรกคือในซอฟต์แวร์ทุกตัวซึ่งรวมทั้งวินโดวส์ด้วย จะมี Keyboard Combination (การกดปุ่มบนคีย์บอร์ดเป็นชุด เช่น Ctrl + Alt + Del) อยู่จำนวนหนึ่งที่ไม่มีการจดบันทึกไว้ ซึ่งเป็นการเปิดช่องให้ผู้บุกรุกทำอะไรได้หลายๆ อย่างเช่น เปิดรันไดอะล็อกซ์ของวินโดวส์ขึ้นมา หรือที่ยิ่งอันตรายไปกว่านั้นก็คือ Buffer OverFlow ในไดรเวอร์ Plug & Play

ในงานนิทรรศการ Hacker DefCon ที่ Las Vegas เราได้ให้ทดลองโจมตีเครื่องโน้ตบุ๊กของเราดู ซึ่งการสาธิตนั้นใช้เวลาไปแค่ไม่กี่วินาที แค่อแฮกเกอร์นำไดรฟ์สติ๊กยูเอสบีที่สร้างขึ้นมาจากตัวเองมา สียบเข้ากับเครื่องของเรา จากนั้นในชั่วแค่ไฟกระพริบนิดเดียว วินโดวส์ก็จะหยุดทำงานและปรากฏลูสกรีนขึ้นมาทันที ซึ่งถ้านี่ไม่ใช่แค่การทดสอบ เครื่องของเราก็คงจะมีโทรจันติดมาแล้ว

ทางแก้

ทางป้องกันที่ดีที่สุดคือปิดหรือถอดพอร์ตที่ไม่ได้ใช้ ออกเสีย แต่นั้นก็ไม่สามารถที่จะป้องกันการแอบเชื่อมกับคีย์บอร์ดชั่วคราวขณะของแฮกเกอร์ได้อยู่ดี ดังนั้นวิธีที่ดีกว่านั้นคือใช้โปรแกรมอย่างเช่น Device Wall ของ Contennial Software คอยเฝ้าระวังพอร์ตยูเอสบีทั้งหมด แต่ก็ยังคงต้องรอทดสอบจากการใช้งานจริงต่อไปอีกว่า มันจะใช้ได้ผลมากน้อยเพียงใด

ข้อมูลจาก : thaigaming.com