ฟอร์ทิเน็ตเตือนภัยW32/Bagle.CJ-mm

ซันนีเวล แคลิฟอร์เนีย ■ ฟอร์ทิเน็ตเผยโฉมม้าโทรจัน W32/Bagle.CJ-mm ภัยคุกคามล่าสุดที่รู้จักในชื่อของ W32/Mitglieder.FE โดยติดมากับเอกสารแนบที่ส่งมาทางอีเมล์ในรูปของ .exe หรือ .zip ซึ่งจะเข้าไปฝังตัวใน Windows Explorer และอาศัยในหน่วยความจำของระบบการดำเนินการ แนะอย่าเปิด

ฟอร์ทิเน็ต ผู้นำด้านระบบรักษาความปลอดภัยบนเครือข่ายสมบูรณ์แบบ (Unified Threat Management) เพียงผู้เดียวบน ASIC-powered ที่ครอบคลุมทั้งไฟล์วอลล์และระบบป้องกันไวรัสแบบเรียลไทม์ได้ประกาศถึงความสามารถของ FortiGate ซึ่งเป็นการผสมผสานระหว่างอุปกรณ์รักษาความปลอดภัย, ระบบรักษาความปลอดภัยทางอีเมล์ FortiMail และ FortiClient เข้าด้วยกัน โดยซอฟต์แวร์ระบบรักษาความปลอดภัยจะป้องกันม้าโทรจัน W32/Bagle.CJ-mm หรือที่รู้จักในชื่อของ W32/Mitglieder.FE ไม่ให้เข้าสู่ระบบได้

ม้าโทรจัน W32/Bagle.CJ-mm ถือว่าเป็นสแปมอย่างหนึ่งที่ไม่สามารถแพร่กระจายได้ด้วยตัวเอง แต่ขึ้นอยู่กับการเปิดเอกสารแนบ (attachment) ซึ่งม้าโทรจันนี้จะไปหยุดการทำงานของระบบ firewall, antivirus ในแอพพลิเคชั่นและระบบรักษาความปลอดภัยอื่นๆ ที่เกี่ยวข้อง, การเปลี่ยนชื่อไฟล์, กระบวนการการลบไฟล์ต่างๆ รวมถึงลดระดับการรักษาความปลอดภัยโดยรวม และโทรจันตัวล่าสุดนี้ส่งผลกระทบกับผู้ใช้งานทั่วโลก ซึ่งฟอร์ทิเน็ตได้จัดลำดับความรุนแรงของ W32/Bagle.CJ-mm อยู่ที่ระดับ 4 ซึ่งถือว่าเป็นภัยคุกคามที่มีแนวโน้มที่กลายเป็นสแปมที่มีจำนวนมากขึ้น

เพื่อการป้องกันม้าโทรจัน W32/Bagle.CJ-mm ทางฟอร์ทิเน็ตแนะนำผู้ใช้ไม่ให้เปิดข้อความในอีเมล์ง่ายเกินไป โดยเฉพาะอย่างยิ่งในไฟล์ที่เป็น .exe หรือ .zip และเช่นเดียวกับเอกสารแนบในอีเมล์จากผู้ส่งที่ไม่เคยรู้จักมาก่อน ตัวอย่างที่ทางฟอร์ทิเน็ตแนะนำให้ระวังไม่ให้เปิดอีเมล์ ที่มีลักษณะดังต่อไปนี้ : Subject : new price, Body : price และ Attachment : price.zip

ระบบฟอร์ทิเกตทั้งหมดทั่วโลกจะเก็บข้อมูลอย่างทันท่วงทีอย่างอัตโนมัติ โดยเครือข่าย FortiGuard ของฟอร์ทิเน็ตได้มีการจัดเตรียมการปรับปรุงข้อมูลอย่างต่อเนื่องและตลอดเวลา เพื่อให้มั่นใจว่าผู้ใช้งานจะปลอดภัยจากการคุกคามที่สามารถเกิดขึ้นได้ทั่วโลก และตลอดเวลา และเพื่อเป็นการป้องกันลูกค้าจากม้าโทรจัน W32/Bagle.CJ-mm ทางฟอร์ทิเน็ตจึงจัดทำฐานข้อมูล antivirus V6.066 สำหรับระบบ FortiGate ภายใน 2 ชั่วโมงที่ได้รับตัวอย่างการตรวจพบครั้งแรก และในฐานข้อมูล antivirus ครั้งล่าสุด ระบบ Forti Gate สามารถหยุดการคุกคามของโทรจันตัวนี้ได้ รวมถึงสามารถป้องกันการคุกคามอื่นๆ ได้จากทางเข้าเครือข่ายของลูกค้าตั้งแต่แรกอีกด้วย