รายงานภัยคุกคามจากฟอร์ติเน็ตแจ้งแอดแวร์บนแอนดรอยด์พุ่งสูง Zitmo อาจกลายเป็นบอทเน็ท แฮกเกอร์จากโรมาเนียสแกนหาช่องโหว่บนเว็ป

แคลิฟอร์เนีย, 10 ตุลาคม 2555 – Fortinet® (NASDAQ: FTNT) ฟอร์ติเน็ตผู้บุกเบิกและผู้ให้บริการชั้นนำด้านโซลูชั่นความปลอดภัยเครือข่ายทรงประสิทธิภาพ – ได้ประกาศถึงผลการวิจัยด้านภัยคุกคามประจำไตรมาส 3 ปี คศ. 2012 (ระหว่าง 1 กรกฎาคม – 30 กันยายน) ว่านักวิจัยของฟอร์ติการ์ดแล็ปส์พบว่ามีแอดแวร์บนแอนดรอยด์ (Android adware) พุ่งสูง และมีหลักฐานชี้นำว่า Zitmo (Zeus-in-the-Mobile) โทรจันบนโมบายแบ็งค์กิ้งมีแนวโน้มจะพัฒนากลายเป็นบอทเน็ทได้ และยังพบแฮกเกอร์จากโรมาเนียสแกนหาช่องโหว่บนเว็ปทั่วโลก

แอดแวร์บนแอนดรอยด์พุ่งสูง

ในช่วง 3 เดือนที่ผ่านมา นักวิจัยของฟอร์ติการ์ดแล็ปส์รายงานว่าพบแอดแวร์บนระบบปฏิบัติการแอนดรอยด์พุ่งสูงเกือบเท่า Netsky.PP ตัวผลิตสแปมที่เคยทำให้วงการอินเตอร์เน็ตเคยปั่นป่วนมาแล้ว ทั้งนี้ ระบบการตรวจสอบจากฟอร์ติการ์ดพบตัวแอดแวร์แวริเอนท์ใหม่ 2 ชนิด คือ Android/NewyearL และ Android/Plankton ในปริมาณสูงเกือบถึง 1% ในภูมิภาคเอเชียแปซิฟิคและยุโรป ตะวันออกกลางและแอฟริกา (EMEA) และเกือบ 4% ในอเมริกา แอดแวร์แวริเอนท์ใหม่ 2 ชนิดนี้ทำงานในด้านแอปพลิเคชั่นหลายอย่าง รวมถึงจะฝังทูลส์เพื่อแสดงโฆษณาที่ผู้ใช้ไม่ต้องการที่บาร์แสดงสถานะบนมือถือ และยังสอดแนมดูเบอร์อีมี่ (International Mobile Equipment Identity – IMEI) และฝังไอคอนบนเดสท้อปของเครื่อง

กีโยม โลเว่ ผู้จัดการอาวุโสฝ่าย ทีมรับมือภัยคุกคามของฟอร์ติการ์ดแล็ปส์ กล่าวว่า “แอดแวร์บนแอนดรอยด์นี้จะมีแนวโน้มให้ผู้ใช้งานติดตั้งแอปพลิเคชั่นที่ถูกต้องตามกฎหมายแต่มีรหัสแอดแวร์ฝังตัวอยู่ไปด้วย และเมื่อแอดแวร์เริ่มทำงานแล้วจะสร้างรายได้ให้ผู้ที่สร้างมากโขจากโปรแกรมโฆษณาหลอกลวงนี้”

แอปพลิเคชั่นประเภทนี้มักถามขอสิทธิที่ไม่จำเป็นมากมายจากผู้ใช้งานมากกว่าแอปพลิเคชั่นธรรมดาๆ โปรแกรมหนึ่งควรจะถาม ดังนั้น จึงเป็นการส่อให้เห็นว่ามีวัตถุประสงค์ที่ซ่อนเร้น เช่น การขอข้อมูลเพื่อเข้าใช้เครื่องในส่วนอื่นๆ ทั้งที่ไม่เกี่ยวกับแอปพลิเคชั่นนั้นๆ รวมทั้งการเข้าถึงประวัติเบราว์เซอร์ของอุปกรณ์ ข้อมูลที่อยู่ติดต่อ บันทึก

โทรศัพท์ ไฟล์บันทึกการเข้าสู่ระบบและข้อมูลส่วนตัวต่างๆ

แอปพลิเคชั่นด้านล่างนี้พบภายใต้ชื่อทั่วไปว่า “ Android/Plankton” เป็นตัวอย่างของแอปพลิเคชั่นแอดแวร์บนมือถือประเภทแอนดรอยด์นี้ที่มักถามหาข้อมูลที่ไม่จำเป็นของผู้ใช้และเครื่อง:

ฟอร์ติการ์ดแล็ปส์แนะนำว่า ท่านควรให้เพิ่มความสนใจให้มากขึ้นเดิม เมื่อโดนขอสิทธิในขณะที่ท่านกำลังติดตั้งแอปพลิเคชั่นใดๆ อยู่ ยิ่งไปกว่านั้น ท่านควรพิจารณาดาวน์โหลดแอปพลิเคชั่นมือถือที่ได้รับการจัดอันดับสูงและมีการวิเคราะห์อย่างดีแล้วเท่านั้น

ซิทโมเริ่มซับซ้อนมากขึ้น

ในช่วงไตรมาสสุดท้าย นักวิจัยค้นพบว่ามัลแวร์ Zitmo หรือ Zeus-in-the-mobile ใหม่ที่เน้นการโจมตีผู้ใช้งานแอนดรอยด์และแบล็คเบอรี่รุ่นใหม่ๆ มีแนวโน้มพัฒนาเป็นภัยคุกคามที่ซับซ้อนมากขึ้น

ซิทโมเป็นมัลแวร์มือถือที่ฉาวโฉ่ของโทรจันด้านแบ็งคกิ้ง “เซอุส” ที่ทำความเสียหายให้การรับรองการเข้าใช้งานทางด้านแบ็งค์กิ้ง 2 ครั้ง (Two-factor authentication) ซึ่งส่วนใหญ่เป็นการยืนยันจากเอสเอ็มเอส โดยจะสกัดไม่ให้ได้รับเอสเอ็มเอสที่ผู้ใช้รออยู่ ทั้งนี้ ซิทโมรุ่นใหม่ๆ สำหรับแอนดรอยด์และแบล็คเบอรี่มีคุณสมบัติใหม่ที่คล้ายบอทเน็ท เช่น เริ่มมีสามารถเปิดให้อาชญากรไซเบอร์ควบคุมโทรจันผ่านทางคำสั่งเอสเอ็มเอสได้

“ซิทโมรุ่นใหม่ๆ แพร่กระจายไปทั่วยุโรปและเอเชีย ถึงแม้ว่าเรายังพบมัลแวร์น้อยประเภทในภูมิภาคเหล่านั้น แต่ก็ชวนให้เราเชื่อว่าผู้ที่สร้างมันขึ้นมากำลังทดสอบโค้ดอยู่ หรือจะมีการนำไปใช้ในการโจมตีประเภทที่ระบุเป้าหมายชัดเจน” โลเว่กล่าวเสริม

ในขณะที่ ทางธนาคารและร้านค้าออนไลน์ต่างพากันเสริมความปลอดภัยให้ใช้การรับรองตนเมื่อจะเข้าใช้งานถึงสองครั้ง เช่น มักจะใช้รหัสเอสเอ็มเอสโค้ดแจ้งวิธีการตรวจสอบครั้งที่สองและใช้ยืนยันการทำรายการนั้น ทั้งนี้ ผู้ใช้แอนดรอยด์และแบล็คเบอรี่ได้ควรระวังเมื่อสถาบันการเงินของท่านขอให้ท่านติดตั้งซอฟต์แวร์ลงบนอุปกรณ์คอมพิวเตอร์ของท่าน ซึ่งจริงๆ แล้ว ทางธนาคารไม่ค่อยขอให้ลูกค้าทำเช่นนี้ สำหรับการรักษาความปลอดภัยที่สูงสุด ฟอร์ติการ์ดแล็ปส์แนะนำให้ใช้บริการออนไลน์แบ็งค์กิ้งจากซีดีระบบปฏิบัติการอันเดิม แต่ถ้าไม่มีออปชั่นเช่นนั้น

ผู้ใช้ควรติดตั้งโปรแกรมป้องกันไวรัสบนโทรศัพท์และคอมพิวเตอร์ และควรแน่ใจว่ามีการปรับปรุงด้วยแพทช์ล่าสุดอยู่เสมอ

แฮกเกอร์จากโรมาเนียสแกนหาช่องโหว่ phpMyAdmin บนเว็ป

ในช่วงสามเดือนที่ผ่านมา ฟอร์ติการ์ดแล็ปส์ได้ตรวจพบการสแกนขนาดใหญ่หาช่องโหว่ ซึ่งการสแกนเหล่านี้ได้กระทำการผ่านเครื่องมือที่พัฒนาโดยแฮกเกอร์ในโรมาเนียที่มองหาเว็บเซิร์ฟเวอร์ที่ใช้ซอฟแวร์ MySQL ประเภทการบริหาร (phpMyAdmin) โดยมีวัตถุประสงค์จะควบคุมเซิร์ฟเวอร์

ทั้งนี้ ทูลส์ที่มีชื่อว่า “ZmEu” มีสายรหัสในเพย์โหลดที่เชื่อมโยงถึงการเคลื่อนไหวด้านการแฮครระดับโลกชื่อ “AntiSec” ที่สร้างเมื่อปีที่แล้วโดยกลุ่มพวกที่ไม่ระบุชื่อและ LulzSec ทั้งนี้ เกิดการสแกนขึ้นทั่วโลกในเดือนกันยายน โดยเกือบร้อยละ 25 ของการดักตรวจของฟอร์ติการ์ดแล็ปส์พบเจอการสแกน ซึ่งเป็นการพบการสแกนอย่างน้อย 1 ครั้งต่อวัน

“ยังมีการถกเถียงเรื่องวัตถุประสงค์เบื้องหลังการโจมตีช่องโหว่นี้ แต่ถ้าแฮกเกอร์เหล่านี้เกี่ยวข้องกับ AntiSec จริงแล้ว น่าจะเป็นไปได้ว่าจะเป็นการดักหาข้อมูลที่สำคัญ และอาจจะเข้าควบคุมใช้เซิร์ฟเวอร์นั้นกระทำการปฏิเสธการบริการ (Direct denial of service – DDoS) หรือเปลี่ยนรูปแบบเว็บไซต์ที่ถูกแทรกซึมเข้าไปให้เสียโฉมได้” เพื่อรักษาความปลอดภัยเว็บเซิร์ฟเวอร์ให้พ้นจากภัยคุกคามเหล่านี้ ทางฟอร์ติเน็ตแนะนำในการปรับปรุง phpMyAdmin ให้ล่าสุดอยู่เสมอ

เกี่ยวกับฟอร์ติการ์ดแล็ปส์

ฟอร์ติการ์ดแล็ปส์ทำหน้าที่รวบรวมสถิติและแนวโน้มภัยคุกคามจากข้อมูลที่เก็บรวบรวมจากอุปกร์ฟอร์ติเกท FortiGate ® ซึ่งเป็นอุปกรณ์รักษาความปลอดภัยด้านเครือข่ายที่ใช้งานอยู่ทั่วโลก บริการฟอร์ติการ์ดนำเสนอโซลูชั่นการรักษาความปลอดภัยป้องกันไวรัสรวมทั้งการป้องกันการบุกรุกการกรองเนื้อหาเว็บและความสามารถในการป้องกันสแปม บริการเหล่านี้ช่วยป้องกันภัยคุกคามบนโปรแกรมทและชั้นเครือข่าย บริการฟอร์ติการ์ดมีการปรับปรุงโดยทีมนักค้นคว้าฟอร์ติการ์ดแล็ปส์

เกี่ยวกับฟอร์ติเน็ต (www.fortinet.com)

ฟอร์ติเน็ต (NASDAQ: FTNT) เป็นผู้ให้บริการระดับโลกด้านผลิตภัณฑ์ความปลอดภัยเครือข่ายและเป็นผู้นำตลาดด้านการจัดการภัยคุกคามแบบหลอมรวม หรือที่เรียกว่า Unified Threat Management (UTM) ทั้งนี้ กลุ่ม

ผลิตภัณฑ์และบริการ Subscription จะปกป้องเครือข่ายจากภัยคุกคามต่างๆด้วยการป้องกันแบบรวมที่มีประสิทธิภาพสูงในขณะที่ช่วยปรับโครงสร้างด้านความปลอดภัยด้านความปลอดภัยไอทีให้กลับง่ายขึ้น กลุ่มลูกค้าได้แก่ องค์กร ผู้ให้บริการ ราชการทั่วโลก ซึ่งอยู่ในกลุ่ม The 2009 Fortune Global 100 ทั้งนี้อุปกรณ์ฟอร์ติเกท (FortiGate®) ซึ่งเป็นแพลทฟอร์มความปลอดภัยชั้นนำของฟอร์ติเน็ตจะมอบประสิทธิภาพความปลอดภัยระดับ ASIC และรวมระดับด้านความปลอดภัยต่างๆ ที่ได้รับการออกแบบมาเพื่อช่วยป้องกันการคุกคามระดับเครือข่ายและแอปพลิเคชั่น กลุ่มผลิตภัณฑ์ของฟอร์ติเน็ตมีมากกว่า UTM ที่จะช่วยรักษาความปลอดภัยขององค์กร ตั้งแต่อุปกรณ์ปลายทาง รวมทั้งพารามิเตอร์ และส่วนคอร์ อันได้แก่ ดาต้าเบสและแอปพลิเคชั่น สำนักงานใหญ่ของฟอร์ติเน็ตตั้งอยู่ที่เมืองซันนี่เวล รัฐแคลิฟอร์เนีย ประเทศสหรัฐอเมริกา