ฟอร์ติเน็ตรายงาน 4 มัลแวร์ที่ควรจับตาในปี 2013 ฟอร์ติการ์ดแลปส์ยังพบมัลแวร์โฆษณาบนมือถือและการสแกนเว็ปเซิร์ฟเวอร์มากขึ้น

ซันนี่เวลล์ แคลิฟอร์เนีย, 26 กุมภาพันธ์ 2556– Fortinet® (NASDAQ: FTNT) – ฟอร์ติเน็ตผู้นำด้านความปลอดภัยเครือข่ายทรงประสิทธิภาพสูงประกาศผลรายงานประจำไตรมาส 4 – 2012 ของฟอร์ติการ์ดแลปส์ซึ่งพบตัวอย่างของภัยคุกคามมัลแวร์ที่ล่อลวงเหยื่อให้เสียหายและเสียเงินมากถึง 4 ประเภทด้วยกัน นอกจากนี้ ยังพบว่ามีมัลแวร์โฆษณาบนมือถือของ Android Plankton ad kit และการสแกนหาช่องโหว่บนเว็ปเซิร์ฟเวอร์เพื่อโจมตีมากขึ้น ซึ่งคาดว่าภัยคุกคามดังกล่าวยังจะระบาดมากขึ้นในปี 2013 นี้

มัลแวร์ที่ทำให้เหยื่อเสียเงิน 4 ประเภทที่ควรจับตามองในปี 2013 ได้แก่

1. Simda.B: คือมัลแวร์ที่แฝงตัวมากับการอัปเดท Flash หลอกให้เหยื่ออนุญาตให้ติดตั้ง เมื่อเหยื่ออนุญาต มัลแวร์จะขโมยพาสเวิร์ดไป และอาชญากรจะเข้าใช้อีเมล์และบัญชีโซเชี่ยลเน็ทเวิร์คในการแพร่กระจายสแปมและมัลแวร์ แม้กระทั่งใช้บัญชีของผู้ดูแลเว็ปเพื่อเข้าไปขโมยเงินในระบบชำระเงินออนไลน์ได้

1. FakeAlert.D: มัลแวร์ที่เป็นแอนตี้ไวรัสปลอม จะส่งข้อความป๊อปอัฟหลอกว่าเครื่องของเหยื่อติดไวรัส และล่อให้เหยื่อจ่ายค่าเอาไวรัสนั้นออก

1. Ransom.BE78: รู้จักกันในวงกว้างว่า “โปรแกรมเรียกค่าไถ่” โดยจะเริ่มจากโจรไฮเทคใจร้ายใช้โปรแกรมเข้ารหัส “ล็อค” ไฟล์เอกสาร ทำให้เหยื่อไม่สามารถเข้าใช้ไฟล์ได้ จากนั้นจะทิ้งข้อความเกี่ยวกับจำนวนเงินเรียกค่าไถ่พร้อมกับอีเมลแอดเดรสติดต่อกลับ เมื่อได้รับเงินแล้วจึงจะส่งโปรแกรมปลดล็อคมาให้ทางอีเมล

1. Zbot.ANQ: เป็นโทรจันที่เป็นส่วนประกอบหนึ่งของมัลแวร์ Zitmo หรือ Zeus-in-the-mobile ที่เน้นการโจมตีผู้ใช้งานแอนดรอยด์และแบล็คเบอรี่รุ่นใหม่ๆ มันจะโผล่ขึ้นมาเมื่อเหยื่อกำลังล็อคอินเข้าใช้งานออนไลน์

แบ๊งค์กิ้ง และจะหลอกให้เหยื่อติดตั้งมัลแวร์โมบายบนสมาร์ทโฟนของเหยื่อ หลังจากนั้น จะขัดขวางการรับ SMS จากธนาคารที่คอนเฟิร์มธุรกรรม และกลับโอนเงินนั้นเข้าบัญชีปลอมที่ตั้งไว้

แอดแวร์บนแอนดรอยด์พุ่งสูง

ในช่วง 3 เดือนที่ผ่านมา นักวิจัยของฟอร์ติการ์ดแล็ปส์รายงานว่าพบแอดแวร์บนระบบปฏิบัติการแอนดรอยด์ (Android Plankton ad kit) แอดแวร์นี้จะฝังทูลส์เพื่อแสดงโฆษณาที่ผู้ใช้ไม่ต้องการที่บาร์แสดงสถานะบนมือถือ และยังสอดแนมดูเบอร์อีมี่ (International Mobile Equipment Identity – IMEI) และฝังไอคอนบนเดสท้อปของเครื่องเพื่อกระทำการใดๆ ในอนาคต ทั้งนี้ ผู้ใช้สามารถปกป้องตัวเองโดยให้ความสนใจในข้อความสิทธิที่แจ้งมาในตอนการติดตั้งนั้น และควรดาวน์โหลดโปรแกรมมือถือที่ได้รับการศึกษาและการจัดอันดับสูงไว้แล้วเท่านั้น

แฮกเกอร์ Hacktivist สแกนหาช่องโหว่ phpMyAdmin บนเว็ปเซิร์ฟเวอร์

ในช่วงกลางปี 2012 ที่ผ่านมา ฟอร์ติการ์ดแล็ปส์ได้ตรวจพบทูลส์ ZmEu เป็นการสแกนขนาดใหญ่หาช่องโหว่บนที่สร้างโดยแฮกเกอร์ชาวโรมาเนีย ซึ่งจะมองหาเว็บเซิร์ฟเวอร์ที่ใช้ซอฟแวร์ phpMyAdmin บน MySQL โดยมีวัตถุประสงค์จะควบคุมเซิร์ฟเวอร์ และตั้งแต่เดือนกันยายนที่ผ่านมาพบการสแกนนี้สูงขึ้นมาถึง 9 เท่าตัว และน่าจะแพร่กระจายไปทั่ว ทั้งนี้ ฟอร์ติการ์ตแล็ปส์แนะนำให้อัปเดท PhPMyAdmin เวอร์ชั่นล่าสุด

นายพีระพงศ์ จงวิบูลย์ ผู้จัดการประจำประเทศไทยแห่งฟอร์ติเน็ตกล่าวว่า “ในปัจจุบันภัยคุกคามมักเข้ามาจากหลากหลายรูปแบบ จึงทำให้องค์กรเกิดความต้องการอุปกรณ์รักษาความปลอดภัยที่ทำหน้าที่ได้หลายประเภท (Multi-function) เพื่อให้แน่ใจว่าจะสามารถตรวจจับและเห็นภัยหลายรูปแบบที่เข้ามา และองค์กรยังต้องการอุปกรณ์ที่ทำงานได้รวดเร็วมีประสิทธิภาพในราคาการลงทุนที่เหมาะสมทั้งที่เป็นค่าใช้จ่ายเบื้องต้นและตลอดอายุของอุปกรณ์นั้นด้วย”