เทรนด์ไมโครเผยรายงานสรุปด้านความปลอดภัยไตรมาสสอง พบภัยคุกคามมือถือเพิ่มขึ้นต่อเนื่องและช่องโหว่ในอุปกรณ์สร้างความเสี่ยงสูง

ศูนย์วิจัยเทรนด์แล็บส์ บริษัท เทรนด์ไมโคร อิงค์ เผยรายงานสรุปด้านความปลอดภัยไตรมาสสองพบว่าภัยคุกคามที่มีต่อแพลตฟอร์มมือถือ อุปกรณ์มือถือ และแอพพลิเคชั่นมือถือกำลังขยายตัวเพิ่มมากขึ้นในช่วงปีที่ ผ่านมา และดูเหมือนว่าไตรมาสนี้จะเดินหน้าโจมตีอย่างเต็มพิกัด โดยอาชญากรไซเบอร์ใช้วิธีที่ซับซ้อนกว่าเดิมในการเลี่ยงผ่านระบบรักษาความปลอดภัยสำหรับมือถือ ซึ่งไม่ได้จำกัดเฉพาะแอพพลิเคชั่นที่เป็นอันตรายอีกต่อไป

ผู้ใช้แอนดรอยด์เสี่ยงกับภัยคุกคามจากช่องโหว่ที่ร้ายแรง

เป็นที่ทราบกันดีว่าขณะนี้ช่องโหว่ “Master Key” ในระบบปฏิบัติการแอนดรอยด์ กำลังถูกอาชญากรไซเบอร์จำนวนมากนำไปใช้หาประโยชน์ให้กับตนเอง ด้วยการปรับปรุงแอพต้นฉบับให้กลายเป็นแอพอันตราย ขณะที่มัลแวร์ชื่อ OBAD ก็ได้ใช้ประโยชน์จากช่องโหว่ด้านการดูแลระบบในการเรียกใช้ชุดคำสั่งการแพร่กระจายและการขโมยข้อมูลในระดับที่ซับซ้อนกว่าเดิม ซึ่งช่องโหว่ร้ายแรงเหล่านี้ชี้ให้เห็นว่าการอัพเดตที่ล่าช้ากำลังกลายเป็นปัญหาสำคัญ และมีส่วนทำให้การส่งโปรแกรมซ่อมแซมระบบรักษาความปลอดภัยผ่านทางนักพัฒนาเป็นไปอย่างล่าช้ากว่าจะมาถึงมือผู้ใช้งาน

และแอพแอนดรอยด์ที่เป็นอันตรายและมีความเสี่ยงสูงยังคงพุ่งเป้าโจมตีผู้ใช้งานเพิ่มขึ้น โดยในไตรมาสนี้ตรวจพบการโจมตีถึง 718,000 ครั้ง ด้วยเหตุนี้จึงไม่แปลกที่ผู้ใช้ระบบปฏิบัติการแอนดรอยด์จะพบว่าอาชญากร ไซเบอร์ยังคงทำการโจมตีอย่างต่อเนื่อง โดยในระยะเวลาเพียงหกเดือนแอพมัลแวร์ได้เพิ่มจำนวนขึ้นประมาณ 350,000 รายการ ซึ่งก่อนหน้านี้เชื่อกันว่าจำนวนรวมดังกล่าวจะเกิดขึ้นได้ต้องใช้เวลานานถึงสามปี

ภัยคุกคามรูปแบบใหม่ๆ และมัลแวร์ออนไลน์แบงกิ้งขยายตัวเพิ่มมากขึ้น

จำนวนภัยคุกคามระบบออนไลน์แบงกิ้งในไตรมาสนี้เพิ่มขึ้นเกือบ 1 ใน 3 เมื่อเทียบกับไตรมาสที่แล้ว โดยที่เหยื่อส่วนใหญ่จะอยู่ในประเทศสหรัฐอเมริกา บราซิล ออสเตรเลีย และฝรั่งเศส ในขณะที่จำนวนรวมของภัยคุกคามทั้งหมดที่เทรนด์ไมโคร สมาร์ท โพรเท็คชั่น เน็ตเวิร์คบล็อกไว้ได้นั้นมีจำนวนเพิ่มขึ้นประมาณ 13% เมื่อเทียบกับไตรมาสที่แล้ว โดยหนอน DOWNAD/Conficker ยังคงเป็นมัลแวร์ยอดนิยม ขณะที่ปริมาณของแอดแวร์ก็เพิ่ม

ขึ้นอย่างเห็นได้ชัดเนื่องจากมีผู้ใช้จำนวนมากขึ้นจากภาคส่วนต่างๆ ถูกลวงให้ดาวน์โหลดแอดแวร์ซึ่งเป็นส่วนหนึ่งของซอฟต์แวร์ฟรี ทั้งนี้อาชญากรไซเบอร์ไม่ได้สร้างภัยคุกคามรูปแบบใหม่ขึ้นมา แต่ได้รวมภัยคุกคามรูปแบบเดิมๆ มาไว้ในแพคเกจใหม่ และเราพบแนวโน้มที่น่าสนใจหลายอย่างในภัยคุกคามที่เกิดขึ้นกับระบบออนไลน์แบงกิ้งในช่วง ไตรมาสนี้ ซึ่งเป็นเหตุที่ทำให้ปริมาณของติดเชื้อมัลแวร์ในประเภทนี้เพิ่มขึ้นถึง 29%

ภัยคุกคามทางสังคมใช้ประโยชน์จากแพลตฟอร์มที่หลากหลาย

ปัจจุบันผู้ใช้จำนวนมากกำลังให้ความสำคัญมากขึ้นกับการบริหารจัดการบัญชีออนไลน์ของตนที่มีอยู่ด้วยกันหลายบัญชี ทำให้อาชญากรไซเบอร์เริ่มมองเห็นช่องทางที่จะใช้ประโยชน์จากแนวโน้มดังกล่าว โดยอาชญากรจะใช้ไซต์บล็อกยอดนิยม เช่น Tumblr, WordPress และ Blogger เพื่อโฮสต์ไซต์สตรีมมิ่งปลอมของภาพยนตร์ยอดนิยมในช่วงซัมเมอร์ ซึ่งรวมถึงภาพยนตร์เรื่อง Man of Steel, Fast and Furious 6 และ Iron Man 3 ขณะที่ Apple ID และแพลตฟอร์มการรับส่งข้อความด่วน (IM) แบบหลายโปรโตคอล เช่น Digsby ก็ตกเป็นเป้าหมายของการโจมตีด้วยเช่นกัน จะเห็นได้ว่าการโจมตีเหล่านี้ใช้ประโยชน์จาก SSO (การลงชื่อเข้าระบบครั้งเดียว) ซึ่งผู้ใช้ควรทราบข้อมูลนี้ไว้เพื่อป้องกันบัญชีออนไลน์และหลีกเลี่ยงการใช้รหัสผ่านที่คาดเดาได้ง่าย

นอกจากนี้ ผู้ใช้ยังจะพบกับเทคนิคด้านวิศวกรรมสังคมที่คุ้นเคยซึ่งยังคงเดินหน้าใช้ประโยชน์จากเหตุการณ์ต่างๆ ล่อลวงเหยื่ออยู่ ซึ่งรวมถึงเหตุระเบิดในการแข่งวิ่งมาราธอนประจำปีของเมืองบอสตัน พายุทอร์นาโดพัดถล่มที่มลรัฐโอกลาโฮม่า และการระเบิดของโรงงานปุ๋ยในเท็กซัส

และหลังจากเกิดกรณีช่องโหว่ซีโร่เดย์จำนวนมากในไตรมาสที่แล้ว บริษัท ออราเคิล จึงได้ปรับใช้ขั้นตอนหลายอย่างเพื่อปรับปรุงระบบรักษาความปลอดภัยของ Java ให้ดียิ่งขึ้น ซึ่งรวมถึงการออกโปรแกรมปรับปรุงประจำไตรมาส การทดสอบระบบรักษาความปลอดภัยอัตโนมัติ และไม่อนุญาตให้ใช้แอพที่ไม่มีการลงนามหรือที่ลงนามด้วยตนเองกับซอฟต์แวร์ Java ที่ใช้ในเบราว์เซอร์

ประเด็นเรื่องการจัดการช่องโหว่ถือเป็นหัวข้อยอดฮิตในไตรมาสนี้ โดยเฉพาะเมื่อกูเกิลได้ประกาศนโยบายจัดการช่องโหว่ให้ได้ภายใน 7 วันออกมา และ**ไรมันด์ จีนส์ ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี บริษัท เทรนด์ ไมโคร อิงค์** แนะนำว่าควรมีการพูดคุยเกี่ยวกับวิธีการรายงานช่องโหว่ต่างๆ ให้ชัดเจนมากยิ่งขึ้น

นอกจากนี้ ภัยคุกคามแบบมีเป้าหมายยังคงเป็นปัญหาใหญ่สำหรับองค์กร โดยศูนย์วิจัยเทรนด์แล็บส์ยังตรวจพบว่าภัยคุกคามในลักษณะนี้กำลังทำงานอยู่และเกิดขึ้นอย่างต่อเนื่อง การโจมตี Naikon ที่ใช้โทรจันเข้าถึงจากระยะไกลที่ชื่อว่า RARSTONE ถูกตรวจพบในหลายประเทศของภูมิภาคเอเชียแปซิฟิก และการโจมตีนี้พุ่งเป้าไปที่อุตสาหกรรมหลากหลายประเภท เช่น โทรคมนาคม น้ำมันและแก๊ส หน่วยงานภาครัฐ สื่อ และอื่นๆ โดยปกติแล้วจะเริ่มต้นด้วยการโจมตีประเภทสเปียร์ฟิชชิ่งที่มีเป้าหมายเป็นช่องโหว่เฉพาะ ซึ่งมักจะถูกใช้ในการโจมตีอีกรูปแบบที่

เรียกว่า “Safe” ขณะเดียวกันจากการวิจัยของเราเกี่ยวกับการโจมตีแบบ Safe ยังพบด้วยว่าการโจมตีในลักษณะนี้ได้แพร่กระจายครอบคลุมไปแล้วใน 100 ประเทศทั่วโลก

การโจมตีแบบมีเป้าหมายยังใช้ประโยชน์จากเหตุการณ์อันน่าสลดเพื่อแทรกซึมเข้าสู่ในเครือข่ายองค์กรในไตรมาสนี้ด้วย โดยเราตรวจพบอีเมลที่ใช้เหตุระเบิดในการแข่งขันมาราธอนของเมืองบอสตัน ซึ่งเป็นเทคนิควิศวกรรมสังคมที่ล่อลวงให้ผู้ใช้ดาวน์โหลดมัลแวร์ที่จะทำการสื่อสารผ่านระบบ Secure Sockets Layer (SSL)

ขณะที่ Blackhole Exploit Kit (BHEK) ใช้มัลแวร์สายพันธุ์ใหม่ FAREIT ทำหน้าที่ขโมยข้อมูลประจำตัวของโปรโตคอลการถ่ายโอนไฟล์ (FTP) และข้อมูลส่วนตัวอื่นๆ ในเครื่องคอมพิวเตอร์เป้าหมาย รูปแบบการโจมตีแบบมีเป้าหมาย เช่น Safe ยังคงเดินหน้าโจมตีองค์กรอย่างต่อเนื่อง ขณะที่แอพพลิเคชั่นฝั่งเซิร์ฟเวอร์ ได้แก่ Plesk, Ruby on Rails และ ColdFusion® ก็ถูกนำช่องโหว่ไปใช้ประโยชน์ด้วยเช่นกัน และภัยคุกคามในรูปแบบวิศวกรรมสังคมได้ตั้งเป้าโจมตีไปที่บริการเข้าถึงบัญชีผู้ใช้แบบหลายบัญชีในคราวเดียว เช่น Digsby รวมทั้งยังได้ใช้แพลตฟอร์มของการสร้างบล็อกจำนวนมากเป็นฉากหน้าในการสร้างเพจสตรีมมิ่งปลอมขึ้นมาล่อลวงเหยื่ออีกด้วย

บริษัทเทรนด์ไมโครพร้อมให้การปกป้องข้อมูลของผู้ใช้งานด้วยเครือข่ายป้องกันภัยอัจฉริยะหรือเทรนด์ไมโคร สมาร์ท โพรเทคชั่น เน็ตเวิร์ค (Trend Micro™ Smart Protection Network™) ที่สามารถตรวจพบไฟล์ที่เป็นอันตรายและบล็อก URL อันตรายทั้งหมดได้อย่างครอบคลุม

สำหรับข้อมูลรายงานฉบับเต็มสามารถคลิกดูได้ที่

http://about-threats.trendmicro.com/apac/security-roundup/2013/2Q/mobile-threats-in-full-throttle/