เทรนด์ไมโครเผยรายงานความปลอดภัยไตรมาส 3

เทรนด์ไมโครเผยรายงานความปลอดภัยไตรมาส 3
วิเคราะห์ช่องโหว่และผลกระทบจากปัญหาข้อมูลรั่วไหล

เน้นย้ำปัญหาการเจาะระบบโมบายล์ อุปกรณ์เชื่อมต่ออินเทอร์เน็ต และโครงสร้างพื้นฐานเครือข่าย

กรุงเทพฯ, 26 พฤศจิกายน 2558 – ความเชื่อมโยงของเทคโนโลยีนำไปสู่จุดที่อุปกรณ์ต่างๆมีความเสี่ยงในการใช้งาน และในช่วงไตรมาสที่สามผลกระทบของการโจมตีทางไซเบอร์เริ่มปรากฏให้เห็นอย่างชัดเจน และวันนี้ บริษัท เทรนด์ไมโคร (Trend Micro Incorporated) (TYO: 4704; TSE: 4704) เปิดเผยรายงานสรุปด้านความปลอดภัยที่มีชื่อว่า “Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks” (ภัยคุกคามที่รออยู่: ช่องโหว่ที่พบจะเป็นต้นเหตุของการโจมตี) รายงานดังกล่าววิเคราะห์ช่องโหว่และการโจมตีที่เกิดขึ้นในช่วงไตรมาสที่แล้ว รวมถึงผลกระทบของการเจาะระบบรักษาความปลอดภัย ช่องโหว่ที่พบบนแพลตฟอร์มโมบายล์ และจุดอ่อนที่ก่อให้เกิดความเสี่ยงต่อความเป็นส่วนตัวและความปลอดภัยในทางกายภาพของผู้ใช้ นอกจากนั้น ช่องว่างด้านความปลอดภัยเหล่านี้ยังนำไปสู่เหตุการณ์สำคัญๆ ที่เทรนด์ไมโครเชื่อว่าจะส่งผลกระทบอย่างมากในช่วงปี 2559

“วิวัฒนาการของการโจมตีเริ่มที่จะส่งผลกระทบอย่างเป็นรูปธรรมต่อผลประกอบการขององค์กร รวมถึงชีวิตของผู้คน” ไรมันด์ จีนส์ ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีของเทรนด์ไมโคร กล่าว “การค้นพบช่องโหว่มากมายและปัญหาข้อมูลรั่วไหลที่เกิดขึ้นในช่วงไตรมาสนี้ จะทำให้ข้อมูลลับถูกเปิดเผยมากขึ้น และสร้างความเสียหายต่อประชาชนทั่วไป และข้อมูลดังกล่าวจะถูกขายให้แก่ผู้ที่เสนอยอดประมูลสูงสุดในตลาดมืด หรือ Deep Web”

กรณีข้อมูลรั่วไหลที่เกิดขึ้นในช่วงไตรมาสที่แล้ว เช่น การเจาะเว็บไซต์หาคู่ Ashley Madison ก่อให้เกิดการโจมตีมากมาย และทำให้ข้อมูลลับถูกเปิดเผยในที่สาธารณะจนสร้างความเสื่อมเสียต่อผู้ที่ตกเป็นเหยื่อ และสร้างความเสียหายเป็นวงกว้างและร้ายแรงเกินกว่าการหยุดชะงักของธุรกิจทั่วไป อาชญากรไซเบอร์ซึ่งใช้ประโยชน์จากข้อมูลที่รั่วไหล เพื่อดำเนินการโจมตีและแบล็คเมล์ผู้ใช้ สร้างความเสียหายอย่างรุนแรงต่อ Avid Life Media ซึ่งเป็นเจ้าของเว็บไซต์ รวมไปถึงผู้ใช้ของ Ashley Madison กว่า 30 ล้านคน โดยการโจมตีครั้งนี้ส่งผลให้เหยื่อผู้เคราะห์ร้ายหลายรายตัดสินใจฆ่าตัวตาย

นอกจากนี้ ยังมีการพบการละเมิดระบบรักษาความปลอดภัยจำนวนมากที่ส่งผลกระทบต่อแวดวงการแพทย์ เช่น การโจมตีระบบสุขภาพ UCLA ซึ่งส่งผลให้ข้อมูลเวชระเบียนของผู้ป่วยราว 4.5 ล้านคนเกิดรั่วไหล ที่จริงแล้ว ข้อมูลด้านสุขภาพที่สามารถระบุตัวบุคคลเป็นข้อมูลที่ถูกโจรกรรมมากที่สุดเป็นอันดับที่สอง เมื่อเทียบกับการรั่วไหลของ

ข้อมูลประเภทอื่นๆ ทั้งหมด กรณีเหล่านี้ตอกย้ำเหตุผลว่าทำไมแวดวงการแพทย์จึงตกเป็นเป้าหมายหลักสำหรับอาชญากรไซเบอร์อย่างต่อเนื่อง

ผู้โจมตียังคงพุ่งเป้าไปที่ผู้ใช้อุปกรณ์พกพา โดยใช้ประโยชน์จากช่องว่างในระบบรักษาความปลอดภัยบนแพลตฟอร์ม iOS และ Android การค้นพบช่องโหว่ใน Android ตอกย้ำถึงความจำเป็นในการปรับใช้กลยุทธ์ด้านความปลอดภัยอย่างครบวงจร ขณะที่เครื่องมือสร้างแอพที่ถูกดัดแปลงก็หักล้างความเชื่อที่ว่า แนวทางแบบระบบปิดของ iOS ในเรื่องของความปลอดภัยจะช่วยให้แพลตฟอร์มดังกล่าวรอดพ้นจากการโจมตี

“นักวิเคราะห์ของเทรนด์ไมโครพบว่า ไซเบอร์สเปซมีอันตรายเพิ่มมากขึ้น และการโจมตีไม่ได้เกิดขึ้นในลักษณะแยกออกจากกันอีกต่อไป” ทอม เคลเลอร์มานน์ ประธานเจ้าหน้าที่ฝ่ายไซเบอร์ซีเคียวริตี้ของเทรนด์ไมโคร กล่าว “เพื่อป้องกันการเจาะระบบและลดความเสี่ยงที่จะเกิดขึ้นในอนาคต องค์กรต่างๆ จะต้องมุ่งเน้นการป้องปรามการบุกรุก และรับมือกับการแพร่กระจายระยะที่สอง (Downloader) การติดตั้งระบบตรวจจับการละเมิดถือเป็นมาตรการสำคัญที่จะช่วยลดระยะเวลาที่แฮ็กเกอร์แอบแฝงอยู่ในเครือข่ายขององค์กร การคาดการณ์ที่จะถูกโจมตีและการอยู่รอดจากการโจมตีจะเป็นหัวข้อหลักที่คุณต้องเตรียมตัวนับจากนี้จนถึงปลายปี 2559

ต่อไปนี้คือประเด็นสำคัญที่ระบุไว้ในรายงานในเรื่องที่เกี่ยวกับกิจกรรมต่างๆ ที่เกิดขึ้นในช่วงไตรมาสที่ 3:

 ข้อมูลที่รั่วไหลถูกใช้ในการโจมตีและการขู่กรรโชกครั้งต่อๆไป การโจมตี The Hacking Team และ Ashley Madison ส่งผลกระทบอย่างมากต่ออุตสาหกรรมคอมพิวเตอร์และการรักษาความปลอดภัย
 การค้นพบจุดอ่อนบนแพลตฟอร์มโมบายล์เน้นย้ำถึงปัญหาที่มีอยู่ในทั้งสองระบบ และจากเหตุการณ์ที่เกิดขึ้นบนระบบ Android กูเกิลได้แจ้งว่าจะทำการอัพเดตด้านความปลอดภัยอย่างสม่ำเสมอ
 อาชญากรไซเบอร์ใช้ “แนวทางแบบเหวี่ยงแห” สำหรับการโจมตีด้วยมัลแวร์ PoS ซึ่งส่งผลกระทบต่อธุรกิจขนาดเล็กเป็นหลัก การโจมตีที่ปรากฏให้เห็นในช่วงไตรมาส 3 เกี่ยวข้องกับมัลแวร์ PoS ที่ใช้เทคนิคแบบ “เก่า” เช่น สแปม รวมถึงเครื่องมือต่างๆ เช่น มัลแวร์มาโคร ชุดเครื่องมือเจาะระบบ และบ็อตเน็ต
 บุคคลสำคัญทางการเมืองตกเป็นเป้าหมายการจารกรรมข้อมูลอย่างต่อเนื่อง จากการวิเคราะห์ข้อมูลล่าสุด พบว่าปฏิบัติการ Pawn Storm ได้ขยายเป้าหมายจากองค์กรของสหรัฐฯ ไปสู่องค์กรของรัสเซียเพิ่มมากขึ้น
 Angler Exploit Kit ยังคงเป็นเครื่องมือที่ถูกใช้งานอย่างกว้างขวาง โดยมีการเข้าใช้งานเพิ่มขึ้น 34 เปอร์เซ็นต์ ผู้สร้าง Angler Exploit Kit ได้อัพเดตเครื่องมือโจมตีในช่วงไตรมาสที่ผ่านมา ส่งผลให้คนร้ายใช้เครื่องมือดังกล่าวเพื่อเผยแพร่มัลแวร์ใหม่ๆ กันอย่างกว้างขวาง
 ผลวิจัยล่าสุดระบุปัญหาเรื่องความปลอดภัยของอุปกรณ์ที่รองรับอินเทอร์เน็ต ผู้โจมตีกำลังปรับเปลี่ยนกลยุทธ์การเจาะข้อมูลระดับสูง ซึ่งในท้ายที่สุดแล้วอาจสร้างความเสียหายอย่างร้ายแรงต่อประชาชนทั่วไป

ดูรายงานฉบับเต็มได้ที่:
http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/vulnerabilities-prelude-impending-attacks

เกี่ยวกับเทรนด์ ไมโคร

บริษัท เทรนด์ ไมโคร ผู้นำระดับโลกในด้านซอฟต์แวร์ความปลอดภัย มุ่งมั่นที่จะสร้างโลกที่ปลอดภัยสำหรับการแลกเปลี่ยนข้อมูลดิจิตอล จากประสบการณ์มากกว่า 25 ปีของเรา โซลูชั่นของเราได้ให้บริการทั้งสำหรับผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยในการปกป้องข้อมูลแบบแบ่งระดับชั้น [Layered content security] ในอุปกรณ์พกพา อุปกรณ์ลูกข่าย เกตเวย์ เซิร์ฟเวอร์ และระบบคลาวด์ โซลูชั่นทั้งหมดของเราขับเคลื่อนด้วย Trend Micro™ Smart Protection Network™ ซึ่งเป็นเครือข่ายข้อมูลเกี่ยวกับภัยคุกคามทั่วโลกบนระบบคลาวด์ พร้อมการสนับสนุนจากผู้เชี่ยวชาญด้านภัยคุกคามกว่า 1,200 คนทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th

###

ติดต่อข้อมูลประชาสัมพันธ์

จารุวรรณ ฤกษ์พิชญโยธิน

บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด
+662 646 1968,
jaruwan_r@trendmicro.com

วราวอง จงรักษ์

ดุษฎี เย็นสุดใจ

บริษัท เอฟเอคิว จำกัด: +662 971 3700
Trendmicrothpr@faq.co.th