เทรนด์ไมโครตรวจสอบสถานการณ์ความปลอดภัยไตรมาสแรก ปี 2558

ข่าวประชาสัมพันธ์

เทรนด์ไมโครตรวจสอบสถานการณ์ความปลอดภัยไตรมาสแรก ปี 2558
พบวิธีการโจมตีแบบเดิมๆ ในรูปโฉมใหม่
การโจมตีด้วยมัลแวร์และช่องโหว่ใหม่พุ่งเป้าไปที่ iOS, Adobe, PoS และธุรกิจเฮลท์แคร์

กรุงเทพฯ, 5 มิถุนายน 2558 – สถานการณ์ด้านความปลอดภัยทางไซเบอร์ หรือไซเบอร์ซีเคียวริตี้ ในช่วงไตรมาสแรกของปี 2558 ประกอบด้วยภัยคุกคามทั้งแบบเก่าและแบบใหม่ ไม่ว่าจะเป็น มัลแวร์ที่แฝงตัวในโฆษณา (Malvertising) การโจมตีช่องโหว่ใหม่ๆ มัลแวร์ “รุ่นเก่า” ที่ใช้มาโคร และช่องโหว่ FREAK ซึ่งมีอายุเก่าแก่กว่าหนึ่งทศวรรษ เป็นเพียงตัวอย่างส่วนหนึ่งของไฮไลต์ที่ระบุอยู่ในรายงานฉบับใหม่ของเทรนด์ไมโคร (TYO: 4704; TSE: 4704) “มัลแวร์ที่แฝงตัวในโฆษณาและช่องโหว่ที่เพิ่งค้นพบ: ภัยคุกคามใหม่ๆ ท้าทายความน่าเชื่อถือในระบบซัพพลายเชนและแนวทางปฏิบัติที่เหมาะสม” (Bad Ads and Zero-Days: Reemerging Threats Challenge Trust in Supply Chains and Best Practices) จากมุมมองของอุตสาหกรรม ระบบชำระเงินในธุรกิจค้าปลีกและเฮลท์แคร์ยังพบเจอกับภัยคุกคามที่เพิ่มสูงขึ้น รายงานดังกล่าวเน้นย้ำว่าความไว้วางใจของผู้ใช้อาจก่อให้เกิดความเสี่ยงทางด้านไซเบอร์ซีเคียวริตี้อย่างมากในยุคที่ความผิดพลาดแม้เพียงเล็กน้อยก็อาจก่อให้เกิดปัญหาร้ายแรงได้

“แม้ว่าเราจะอยู่ในช่วงต้นปี แต่ก็เห็นได้อย่างชัดเจนว่าปี 2558 จะเป็นช่วงเวลาสำคัญในแง่ของปริมาณการโจมตี รวมไปถึงความฉลาดหลักแหลม และความซับซ้อนของการโจมตี” ไรมันด์ จีนส์ ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) ของเทรนด์ไมโคร กล่าว “การโจมตีที่เพิ่มขึ้นต่อธุรกิจการดูแลสุขภาพ และการเพิ่มขึ้นของมัลแวร์ที่แฝงมากับโฆษณา แสดงให้เห็นว่าผู้ใช้เทคโนโลยีกำลังถูกโจมตีจากทุกด้าน แน่นอนว่าองค์กรธุรกิจและผู้ใช้ทั่วไปจะต้องดำเนินการเชิงรุกมากขึ้นเพื่อป้องกันภัยคุกคาม ในฐานะองค์กรธุรกิจ นโยบายความปลอดภัยด้านไอทีของคุณเป็นอย่างไรในสภาพแวดล้อมที่ปราศจากความน่าเชื่อถือ (Zero Trust Environment)? แนวทางการรักษาความปลอดภัยที่แตกต่างและจริงจังจึงมีความสำคัญอย่างยิ่งต่อการปกป้องทรัพย์สินด้านการเงิน ทรัพย์สินส่วนตัว และทรัพย์สินทางปัญญาให้ปลอดภัย”
นอกจากนี้ แอดแวร์ (Adware) ยังครองอันดับสูงสุดในบรรดาภัยคุกคามบนระบบโมบายล์ โดยเทรนด์ไมโครตรวจพบภัยคุกคามบน Android มากกว่า 5 ล้านชนิดจนถึงปัจจุบัน หรือเท่ากับเกือบครึ่งหนึ่งของยอดรวม 8 ล้านที่คาด

การณ์ไว้ภายในสิ้นปี 2558 ที่จริงแล้ว แอพอันตรายและแอพความเสี่ยงสูงที่ถูกเทรนด์ไมโครบล็อกไว้โดยมากมีสาเหตุเกี่ยวข้องกับแอดแวร์

นักวิจัยของเทรนด์ไมโครยังตรวจพบการใช้ช่องโหว่ใหม่ๆ เพื่อโจมตีซอฟต์แวร์ของอะโดบี (Adobe) โดยใช้มัลแวร์ที่แฝงตัวในโฆษณา ซึ่งสามารถทำงานได้ถึงแม้เหยื่อไม่ได้เยี่ยมชมหรือโต้ตอบกับเว็บไซต์อันตรายก็ตาม

นอกเหนือจาก iOS™ และระบบชำระเงิน (Point-of-Sale – PoS) ที่ตกเป็นเป้าหมายการโจมตีอย่างต่อเนื่องแล้ว ธุรกิจเฮลท์แคร์ตกเป็นเป้าหมายใหม่ที่ต้องเผชิญกับการโจมตีทางไซเบอร์ที่เพิ่มขึ้นอย่างมาก เนื่องจากการโจมตีในธุรกิจนี้อยู่ในช่วงเริ่มแรกมานานหลายปี ดังนั้นนักวิจัยจึงเชื่อว่าการเพิ่มขึ้นนี้เป็นผลมาจากการขาดความพร้อม ซึ่งนับเป็นปัญหาสำคัญที่จำเป็นต้องได้รับการจัดการดูแลอย่างจริงจัง

“ประเด็นที่เราต้องตั้งคำถามก็คือ ‘เราดำเนินการอย่างเพียงพอแล้วหรือยังเพื่อที่จะปกป้องตัวเราเองจากภัยคุกคามด้านความปลอดภัย?’” จีนส์กล่าวเพิ่มเติม “เราจำเป็นที่จะต้องอัพเดตระบบเพื่อป้องกันภัยคุกคามใหม่ๆ อย่างไรก็ตามไตรมาสแรกของปี 2558 แสดงให้เห็นอย่างชัดเจนว่าเราจะต้องระวังภัยคุกคามเดิมๆ ด้วยเช่นกัน โดยครอบคลุมทุกระบบและทุกกลุ่มอุตสาหกรรมอย่างไม่มีข้อยกเว้น”

ประเด็นสำคัญที่ระบุไว้ในรายงานมีดังนี้:

• ธุรกิจเฮลท์แคร์ถูกโจมตีอย่างหนัก: ผู้ให้บริการด้านเฮลท์แคร์หลายราย เช่น Premera Blue Cross และ Anthem ประสบปัญหาข้อมูลรั่วไหล ส่งผลให้ข้อมูลด้านการเงินและการแพทย์ของลูกค้าหลายล้านรายถูกเปิดเผย

• มีการพบภัยคุกคามเก่าๆ โดยใช้เครื่องมือและกระบวนการใหม่สำหรับการโจมตีแบบเจาะจงเป้าหมาย: Rocket Kitten และผู้ที่อยู่เบื้องหลังการโจมตี Operation Pawn Storm เบนเข็มไปสู่เป้าหมายใหม่ๆ ซึ่งแสดงให้เห็นว่าการโจมตีแบบเจาะจงเป้าหมายกำลังพัฒนาเปลี่ยนแปลงอย่างต่อเนื่อง

• ชุดเครื่องมือสำหรับการเจาะระบบมีความก้าวล้ำเพิ่มมากขึ้น: ชุดเครื่องมือสำหรับการเจาะระบบมีการเพิ่มเติมช่องโหว่ใหม่ๆ และเพิ่มความน่าสนใจสำหรับผู้โจมตีที่เป็นทั้งมือใหม่และระดับผู้เชี่ยวชาญ

• มัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูล (Crypto-Ransomware) มีปริมาณเพิ่มขึ้นอย่างมาก และขยายเข้าสู่องค์กร: มัลแวร์เรียกค่าไถ่แบบเข้ารหัสข้อมูลขยายฐานเป้าหมายไปสู่ผู้ใช้ในองค์กร โดยไม่ได้ติดตามผู้บริโภคอีกต่อไป

• มัลแวร์รุ่นเก่าในรูปแบบมาโครยังคงมีประสิทธิภาพ: การกลับมาอีกครั้งของมัลแวร์ในรูปแบบมาโครแสดงให้เห็นว่าอาชญากรไซเบอร์กำลังใช้ประโยชน์จากความไว้วางใจที่ผู้ใช้มีต่อค่าดีฟอลต์ของ Microsoft Office®

• ช่องโหว่ FREAK ซึ่งมีอายุราวสิบปีก่อให้เกิดปัญหาท้าทายต่อการจัดการแพตช์: เนื่องจากมีช่องโหว่ใหม่ๆ เกิดขึ้นในระบบปฏิบัติการและโปรแกรมโอเพ่นซอร์ส ดังนั้นผู้ดูแลระบบไอทีจึงประสบปัญหาเพิ่มมากขึ้นในการป้องกันความเสี่ยง

รายงานฉบับสมบูรณ์มีอยู่ที่: http://www.trendmicro.com/vinfo/us/security/roundup/

ดูบล็อกโพสต์เกี่ยวกับรายงานดังกล่าวได้ที่นี่: http://blog.trendmicro.com/1q-2015-security-roundup/

เกี่ยวกับเทรนด์ ไมโคร

บริษัท เทรนด์ ไมโคร ผู้นำระดับโลกในด้านซอฟต์แวร์ความปลอดภัย มุ่งมั่นที่จะปกป้องโลกให้ปลอดภัยเพื่อรองรับ

การแลกเปลี่ยนข้อมูลดิจิตอล นวัตกรรมโซลูชั่นของเราให้บริการสำหรับผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยในการปกป้องข้อมูลแบบแบ่งระดับชั้น (Layered content security) ในอุปกรณ์พกพา อุปกรณ์ปลายทาง เกตเวย์ เซิร์ฟเวอร์ และระบบคลาวด์ โซลูชั่นทั้งหมดของเราขับเคลื่อนด้วย Trend Micro™ Smart Protection Network™ ซึ่งเป็นเครือข่ายข้อมูลเกี่ยวกับภัยคุกคามทั่วโลกบนระบบคลาวด์ พร้อมการสนับสนุนจากผู้เชี่ยวชาญด้านภัยคุกคามกว่า 1,200 คนทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.com

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