เทรนด์ไมโครคาดเทคโนโลยีเกิดใหม่ทำให้เกิดภัยคุกคามใหม่ๆ ในปี 2560

เทรนด์ไมโครคาดเทคโนโลยีเกิดใหม่ทำให้เกิดภัยคุกคามใหม่ๆ ในปี 2560
การโจมตีจะกระจายมากขึ้นและปรับเปลี่ยนรูปแบบเพื่อเจาะช่องโหว่ใหม่ๆ

กรุงเทพฯ, 13 ธันวาคม 2559 – บริษัท เทรนด์ไมโคร (TYO: 4704; TSE: 4704) ผู้นำระดับโลกด้านโซลูชั่นไซเบอร์ซีเคียวริตี้ เปิดเผยรายงานคาดการณ์ประจำปีเกี่ยวกับสถานการณ์ความปลอดภัยภายใต้ชื่อ “พัฒนาการขั้นถัดไป – ข้อมูลคาดการณ์เรื่องความปลอดภัย 8 ข้อสำหรับปี 2560” (The Next Tier – 8 Security Predictions for 2017) โดยในปีหน้า คาดว่าการโจมตีจะมีลักษณะขยายขอบเขตเป็นวงกว้างและเจาะลึกมากขึ้น ขณะที่รูปแบบภัยคุกคามที่อันตรายจะใช้วิธีการที่แตกต่างออกไปเพื่อใช้ประโยชน์จากสภาพแวดล้อมทางเทคโนโลยีที่กำลังเปลี่ยนแปลง

นายไรมันด์ จีนส์ ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีของเทรนด์ไมโคร กล่าวว่า “ในช่วงปีหน้า อุตสาหกรรมไซเบอร์ซีเคียวริตี้จะก้าวเข้าสู่ยุคใหม่หลังจากที่สถานการณ์ภัยคุกคามในช่วงปี 2559 อาชญากรไซเบอร์ใช้รูปแบบตรวจสอบช่องโหว่เพื่อการโจมตีและใช้ช่องทางการโจมตีที่หลากหลายมากขึ้น เราคาดการณ์ว่ากฎระเบียบว่าด้วยการปกป้องข้อมูลทั่วไป (General Data Protection Regulation – GDPR) ส่งผลให้เกิดการเปลี่ยนแปลงการจัดการข้อมูลในบริษัทต่างๆ ทั่วโลก ขณะที่วิธีการโจมตีใหม่ๆ สร้างภัยคุกคามต่อองค์กรต่างๆ รูปแบบมัลแวร์เรียกค่าไถ่ (Ransomware) มีความหลากหลายมากขึ้นส่งผลกระทบต่ออุปกรณ์ต่างๆ รวมไปถึงการโฆษณาชวนเชื่อทางไซเบอร์ที่มีอิทธิพลต่อความคิดของประชาชนทั่วไป”

ในช่วงปี 2559 ช่องโหว่บนแพลตฟอร์มของ Apple® เพิ่มจำนวนขึ้นอย่างมาก โดยมีรายงานราว 50 รายการ พร้อมด้วยบั๊ก 135 รายการในโปรแกรมของ Adobe และอีก 76 รายการที่ส่งผลกระทบต่อแพลตฟอร์มของ Microsoft การโจมตีช่องโหว่ซอฟต์แวร์ที่เพิ่มขึ้นอย่างมากนี้จะยังคงดำเนินต่อไปในช่วงปี 2560 ขณะที่ Microsoft พยายามปรับปรุงมาตรการป้องกัน และระบบปฏิบัติการของ Apple จะได้รับความนิยมเพิ่มขึ้นอย่างต่อเนื่อง

Internet of Things (IoT) และ Industrial Internet of Things (IIoT) จะมีบทบาทสำคัญเพิ่มมากขึ้นในการโจมตีแบบเจาะจงเป้าหมายในช่วงปี 2560 โดยการโจมตีเหล่านี้จะใช้ประโยชน์จากจำนวนอุปกรณ์ต่อเชื่อมที่แพร่หลายเพิ่มขึ้น โดยจะอาศัยช่องโหว่และระบบที่ขาดการป้องกันเพื่อทำให้การดำเนินธุรกิจหยุดชะงัก ดังเช่นกรณีของมัลแวร์ Mirai มีการใช้งานอุปกรณ์พกพาเพิ่มสูงขึ้นเพื่อตรวจสอบระบบควบคุมในโรงงานอุตสาหกรรม ผนวกกับปริมาณช่องโหว่จำนวนมากที่ตรวจพบในระบบเหล่านี้ จะเป็นจุดที่สร้างภัยคุกคามต่อองค์กรต่างๆ

อีเมล์หลอกลวง (Business Email Compromise – BEC) และระบบธุรกิจถูกปรับเปลี่ยน (Business Process Compromise – BPC) จะยังเพิ่มขึ้นอย่างต่อเนื่อง เพราะเป็นวิธีการหลอกลวงที่ง่ายและมีค่าใช้จ่ายน้อยมาก การโจมตีด้วยวิธีการ BEC นี้อาจสร้างรายได้ให้แก่คนร้ายมากถึง 140,000 ดอลลาร์ ด้วยการล่อหลอกให้พนักงานโอนเงินไปยังบัญชีของคนร้าย ส่วนการเจาะเข้าสู่ระบบธุรกรรมทางการเงินโดยตรง ซึ่งเป็นวิธีการที่ยากกว่าจะสร้างรายได้เป็นกอบเป็นกำให้แก่คนร้ายโดยอาจสูงถึง 81 ล้านดอลลาร์เลยทีเดียว

นายเอ็ด คาเบรร่า ประธานเจ้าหน้าที่ฝ่ายรักษาความปลอดภัยของเทรนด์ไมโคร กล่าวว่า “เราพบว่าอาชญากรไซเบอร์พัฒนาตามเทคโนโลยีที่เปลี่ยนไป แม้ว่ามัลแวร์เรียกค่าไถ่รุ่นใหม่ๆ มีจำนวนเพิ่มขึ้นอย่างมากในช่วงปี 2559 แต่การเติบโตนั้นก็ไม่ยั่งยืนอีกต่อไป ด้วยเหตุนี้ คาดว่าอาชญากรไซเบอร์จะมองหาหนทางใหม่ๆ ในการใช้มัลแวร์ที่มีอยู่ และในขณะเดียวกัน ความเปลี่ยนแปลงที่เกิดขึ้นใน IoT จะก่อให้เกิดช่องทางใหม่ๆ สำหรับการโจมตี และการเปลี่ยนแปลงในส่วนของซอฟต์แวร์จะผลักดันให้คนร้ายค้นหาจุดอ่อนในรูปแบบที่ต่างออกไป”

ประเด็นสำคัญจากรายงานคาดการณ์ประจำปี 2560 มีดังนี้:

• จำนวนมัลแวร์เรียกค่าไถ่รุ่นใหม่ๆ คาดว่าจะปรับตัว เพิ่มขึ้นเล็กน้อยเพียง 25 เปอร์เซ็นต์ แต่จะขยายขอบเขตไปสู่อุปกรณ์ IoT และอุปกรณ์ประมวลผลที่ไม่ใช่เดสก์ท็อป เช่น เครื่องคิดเงิน (PoS) หรือตู้เอทีเอ็ม

• ผู้ผลิตจะไม่สามารถป้องกันอุปกรณ์ IoT และ IIoT ได้ทันเวลา เพื่อป้องกันการโจมตีแบบ Denial of Service และการโจมตีแบบอื่นๆ

• จะยังคงมีการตรวจพบช่องโหว่ใหม่ๆ ในซอฟต์แวร์ของ Apple และ Adobe ซึ่งจะถูกใช้เป็นช่องทางสำหรับการโจมตีเพิ่มเติม

• ปัจจุบัน ราว 46 เปอร์เซ็นต์ของประชากรโลกเชื่อมต่อกับอินเทอร์เน็ต ส่งผลให้มีการโฆษณาชวนเชื่อทางไซเบอร์เพิ่มมากขึ้น ขณะที่ผู้นำคนใหม่ของประเทศต่างๆ ก้าวขึ้นสู่ตำแหน่ง โดยมีจุดมุ่งหมายเพื่อครอบงำความคิดเห็นของประชาชนโดยใช้ข้อมูลที่บิดเบือน

• ดังที่พบเห็นจากกรณีการโจมตีธนาคาร Bangladesh Bank เมื่อช่วงต้นปี 2559 การโจมตีแบบ BPC ทำให้อาชญากรไซเบอร์สามารถปรับเปลี่ยนกระบวนการทางธุรกิจ และได้รับผลกำไรเป็นกอบเป็นกำ ขณะที่การโจมตีแบบ BEC ยังคงมีประโยชน์ในการหลอกลวงองค์กรธุรกิจผ่านทางพนักงานที่ขาดความระมัดระวัง

• กฎระเบียบ GDPR จะส่งผลให้มีการเปลี่ยนแปลงนโยบายและการบริหารจัดการ ซึ่งจะส่งผลกระทบอย่างมากต่อต้นทุนและค่าใช้จ่าย และองค์กรจะต้องดำเนินการตรวจสอบกระบวนการทางด้านข้อมูลอย่างทั่วถึง เพื่อให้มั่นใจว่าสอดคล้องตามกฎระเบียบ

• วิธีใหม่ๆ ในการโจมตีแบบเจาะจงเป้าหมายจะมุ่งเน้นเทคนิคการตรวจจับการบุกรุกที่ทันสมัย ซึ่งจะช่วยให้คนร้าย

สามารถพุ่งเป้าโจมตีองค์กรได้อย่างแตกต่างหลากหลายมากขึ้น

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการคาดการณ์เรื่องภัยคุกคามในปี 2560 ของเทรนด์ไมโคร โปรดดูที่: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017

เกี่ยวกับเทรนด์ไมโคร

เทรนด์ไมโคร อินคอร์ปอเรทเต็ด ผู้นำระดับโลกด้านโซลูชั่นความปลอดภัยไซเบอร์ มุ่งมั่นที่จะช่วยให้การแลกเปลี่ยนข้อมูลดิจิทัลในโลกของเราเป็นไปอย่างปลอดภัย เทรนด์ไมโครมีโซลูชั่นที่ให้บริการผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยหลายระดับให้กับดาต้าเซ็นเตอร์, คลาวด์, เน็ตเวิร์ค และเครื่องลูกข่าย ผลิตภัณฑ์และโซลูชั่นทั้งหมดของเทรนด์ไมโครผสานการทำงานร่วมกันเพื่อให้ข้อมูลเชิงลึกเกี่ยวกับการป้องกันภัยคุกคามอย่างชาญฉลาด และสร้างการป้องกันภัยคุกคามที่เกี่ยวโยงกันหลายส่วน ด้วยการควบคุมและแสดงผลแบบรวมศูนย์ ซึ่งช่วยให้สามารถป้องกันภัยคุกคามได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น เทรนด์ไมโครมีพนักงานมากกว่า 5,000 คนในกว่า 50 ประเทศ มีผลิตภัณฑ์ โซลูชั่น และความเชี่ยวชาญในการป้องกันภัยคุกคามที่ทันสมัยที่สุดในโลก เราช่วยให้องค์กรต่างๆ เดินทางสู่การใช้งานระบบคลาวด์ได้อย่างปลอดภัย ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th , www.trendmicro.com

###

ติดต่อข้อมูลประชาสัมพันธ์

จารุวรรณ ฤกษ์พิชญโยธิน

บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด

+662 646 1968

jaruwan_r@trendmicro.com

ดุษฎี เย็นสุดใจ

บริษัท เอฟเอคิว จำกัด: +662 971 3700

Trendmicrothpr@faq.co.th