# เทรนด์ไมโคร เผยถึงรายงาน อัตราการโจมตีแบบ Fileless สูงถึง 265%


เทรนด์ไมโคร (TYO: 4704; TSE: 4704) ผู้นำระดับโลกด้านโซลูชั่นความปลอดภัยทางไซเบอร์ ได้ออกรายงานสรุปเหตุการณ์ในช่วงครึ่งปีแรกของ 2019 ที่เผยให้เห็นถึงอัตราการเติบโตของการโจมตีแบบ Fileless ที่พุ่งขึ้นอย่างรุนแรง ซึ่งเป็นการโจมตีที่เน้นปกปิดหลบซ่อนกิจกรรมที่เป็นอันตราย โดยผลการตรวจพบอันตรายลักษณะเดียวเพียงอย่างเดียวพุ่งขึ้นมากถึง 265% เมื่อเทียบกับครึ่งปีแรกของปี 2018 เลยทีเดียว

การค้นพบที่เกิดขึ้นในปี 2019 ที่ผ่านมานั้นได้ยืนยันผลการพยากรณ์ที่ทางเทรนด์ไมโครคาดการณ์ไว้ในปีที่แล้วมากมาย มองภาพรวมได้ว่า เหล่าผู้โจมตีต่างฉลาดมากขึ้น และพุ่งเป้าไปยังธุรกิจและสภาพแวดล้อมการทำงานที่มีโอกาสได้ผลตอบแทนมากที่สุด

“เรียกว่าภาพของเวทีของความท้าทายด้านความปลอดภัยทางไซเบอร์เป็นเรื่องของคำว่า ซับซ้อน และ ซ่อนเร้น เป็นส่วนใหญ่ อันเนื่องมาจากทั้งเทคโนโลยีของบริษัทต่าง ๆ รวมทั้งการโจมตีของอาชญากรต่างมีการเชื่อมต่อระหว่างกัน และมีความอัจฉริยะมากขึ้น” Jon Clay ผู้อำนวยการด้านการสื่อสารข้อมูลเกี่ยวกับอันตรายทั่วโลกจากเทรนด์ไมโครกล่าว “จากมุมของผู้โจมตีนั้น เราเห็นการโจมตีทั้งที่มีจุดประสงค์ชัดเจน เจาะจงเป้าหมาย และมีการออกแบบวางแผนเป็นอย่างดี ทำให้สามารถหาผลประโยชน์ได้อย่างเงียบ ๆ จากทั้งผู้คน กระบวนการทำงานต่าง ๆ และเทคโนโลยี อย่างไรก็ดี ในด้านของธุรกิจนั้น การปฏิวัติทางดิจิตอลและการย้ายขึ้นมาอยู่บนคลาวด์ต่างกำลังได้

รับความนิยม ทำให้รูปแบบการโจมตีทางไซเบอร์เปลี่ยนไปด้วย เพื่อที่จะไล่ตามความเสี่ยงใหม่เหล่านี้ ธุรกิจทั้งหลายจำเป็นต้องมีพาร์ทเนอร์ทางเทคโนโลยีที่สามารถผสานความเชี่ยวชาญของมนุษย์เข้ากับเทคโนโลยีความปลอดภัยชั้นสูง เพื่อให้สามารถทำงานได้ดีขึ้นทั้งการตรวจจับ โยงความสัมพันธ์ ตอบสนอง และแก้ไขอันตรายต่าง ๆ”

จากอัตราการเติบโตของอันตรายแบบ Fileless ที่พุ่งสูงในช่วงครึ่งปีแรกนี้ ชี้ให้เห็นว่าผู้โจมตีหันมาใช้เทคนิคที่ตัดคัดกรองอันตรายหรือระบบความปลอดภัยแบบเดิมมองไม่เห็นกันมากขึ้น ทั้งนี้เพราะการโจมตีลักษณะดังกล่าวสามารถรันบนหน่วยความจำของระบบ ฝังตัวอยู่ในรีจิสตรี้ หรือแม้แต่ใช้ทูลที่มีอยู่อย่างถูกต้องบนระบบอยู่แล้วในทางที่ผิด นอกจากนี้ยังมีแนวโน้มการแบ่งปันชุดโจมตีสำเร็จรูปหรือ Exploit Kit มากขึ้น ด้วยจำนวนมากขึ้นกว่า 136% เมื่อเทียบกับช่วงเวลาเดียวกันของปีที่แล้ว

ส่วนมัลแวร์ขุดเหมืองบิทคอยน์ก็ยังเป็นอันตรายที่โดนตรวจพบมากที่สุดในช่วงครึ่งปีแรกของปี 2019 จากที่ผู้โจมตีมีการใช้มัลแวร์ดังกล่าวไปฝังตามเซิร์ฟเวอร์และระบบคลาวด์กันมากขึ้น นอกจากนี้ยังมีเหตุการณ์ที่สอดคล้องกับการพยากรณ์ล่วงหน้าอีก ไม่ว่าจะเป็นจำนวนเราเตอร์ที่มีความเสี่ยงโดนโจมตีจากภายนอกพุ่งขึ้นถึง 64% เมื่อเทียบกับครึ่งปีแรกของปี 2018 โดยจะเป็นการใช้สายพันธุ์ที่พัฒนาจาก Miraiในการค้นหาอุปกรณ์ที่เปิดช่องโหว่

นอกจากนี้ การเรียกค่าไถ่เพื่อกู้ข้อมูลทางดิจิตอลก็พุ่งสูงกว่า 319% เมื่อเทียบกับช่วงครึ่งปีหลังของ 2018 ซึ่งสอดคล้องกับการคาดการณ์ก่อนหน้านี้ ส่วนการโจมตีผ่านอีเมล์เพื่อหลอกลวงทางธุรกิจหรือ BEC ก็ยังเป็นอันตรายสำคัญ ที่ตรวจพบมากขึ้นกว่า 52% เมื่อเทียบกับช่วง 6 เดือนก่อนหน้า รวมทั้งยังพบไฟล์ อีเมล์ และ URL ที่เกี่ยวข้องกับแรนซั่มแวร์เพิ่มจำนวนมากขึ้น 77% เมื่อเทียบกับช่วงเวลาเดียวกันของปีที่แล้ว

กล่าวโดยสรุปแล้ว เทรนด์ไมโครได้สกัดกั้นอันตรายจำนวนมากกว่า 26.8 พันล้านรายการในช่วงครึ่งปีแรกของปี 2019 ซึ่งมากกว่าช่วงเวลาเดียวกันของปีที่แล้วมากกว่า 6 พันล้านรายการ ซึ่งเป็นที่น่าสังเกตว่า 91% ของอันตรายเหล่านี้เข้ามายังเครือข่ายของบริษัทผ่านทางอีเมล์ ดังนั้น การสกัดกั้นอันตรายชั้นสูงเหล่านี้จำเป็นต้องใช้ระบบป้องกันอัจฉริยะที่เจาะลึก และโยงความสัมพันธ์ของข้อมูลจากแหล่งต่าง ๆ ไม่ว่าจะเป็นเกตเวย์, เครือข่าย, เซิร์ฟเวอร์, และเอนด์พอยต์ เพื่อให้สามารถระบุและหยุดยั้งการโจมตีได้ดีที่สุด

ท่านสามารถอ่านรายงานฉบับสมบูรณ์Evasive Threats, Pervasive Effects: 2019 Midyear Security Roundupได้ที่
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/evasive-threats-pervasive-effects