แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กรณีแคมเปญ Mirai Botnet มุ่งเป้าการโจมตีไปที่ช่องโหว่ของเราเตอร์และอุปกรณ์ IoT

วันที่แจ้งเตือน 26 มกราคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามเกี่ยวกับการโจมตีทางไซเบอร์รูปแบบใหม่ที่มีความรุนแรงและซับซ้อน โดยมีการตรวจพบแคมเปญ Mirai Botnet มุ่งเป้าการโจมตีไปที่ช่องโหว่ของ router และอุปกรณ์ IoT โดยมัลแวร์ดังกล่าวถูกตรวจพบครั้งแรกในเดือนกุมภาพันธ์ 2567 และได้พัฒนาขีดความสามารถอย่างต่อเนื่อง โดยใช้ช่องโหว่มากกว่า 20 รายการ รวมถึงช่องโหว่ Zero-day ของอุปกรณ์เป้าหมาย ในการแพร่กระจาย ปัจจุบันทั่วโลกมีเครื่องที่ติดมัลแวร์แล้วประมาณ 15,000 เครื่อง

Routers และอุปกรณ์ IoT ที่มีความเสี่ยง เช่น

- Routers : ASUS, Huawei, Neterbit, LB-Link และ Four-Faith Industrial Routers
- กล้องวงจรปิด : PZT
- เครื่องบันทึกภาพ DVR : Kguard, Lilin และแบรนด์ทั่วไป
- อุปกรณ์สมาร์ทโฮม : Vimar
- อุปกรณ์ 5G/LTE ที่มี misconfigurations หรือ weak credentials เป็นต้น

มัลแวร์นี้ถูกใช้ในการโจมตีแบบ DDoS เพื่อสร้างความเสียหายต่อระบบเครือข่าย โดยการโจมตีแต่ละครั้งมีระยะเวลา 10-30 วินาที และมีการโจมตีขนาดใหญ่สูงถึง 100 Gbps ซึ่งอาจสามารถสร้างความเสียหายอย่างมากต่อระบบ รวมถึงโครงสร้างพื้นฐานที่มีความแข็งแกร่ง รวมทั้ง การโจมตีมีการใช้เทคนิค Brute-force เพื่อเจาะระบบผ่านรหัสผ่าน Telnet ที่ไม่แข็งแกร่งและอาจส่งผลให้ระบบงานสำคัญหยุดชะงัก เกิดการรั่วไหลของข้อมูล สูญเสียความน่าเชื่อถือ และเกิดความเสียหายทางการเงิน โดยเฉพาะอย่างยิ่งในภาคการเงินและตลาดทุนที่ต้องให้บริการอย่างต่อเนื่อง

ทั้งนี้ อาจมีผู้ประกอบธุรกิจอนุญาตให้พนักงานทำงานจากที่บ้าน (Work From Home) หรือ Remote Working จากระยะไกล การตรวจสอบช่องโหว่ของอุปกรณ์เครือข่ายอย่างสม่ำเสมอจึงมีความจำเป็นอย่างมาก เพื่อลดกระทบต่ออุปกรณ์ข้างต้น ผู้ประกอบธุรกิจจึงควรพิจารณาดำเนินการตรวจสอบและปรับปรุงความปลอดภัยของระบบ ติดตั้งการอัพเดทซอฟต์แวร์ล่าสุดจากผู้ผลิต ปิดการเข้าถึงระบบจากระยะไกลที่ไม่จำเป็น เปลี่ยนรหัสผ่านเริ่มต้นของอุปกรณ์ให้มีความซับซ้อน และตรวจสอบช่องโหว่ในระบบเครือข่ายอย่างสม่ำเสมอ รวมทั้งพิจารณาแจ้งเตือนพนักงาน เพื่อลดกระทบที่อาจเกิดขึ้นกับการใช้งานอุปกรณ์ดังกล่าว

สำนักงาน ก.ล.ต. และ TCM-CERTเล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 24 มกราคม 2568
2. https://www.bleepingcomputer.com/news/security/new-mirai-botnet-targets-industrial-routers-with-zero-day-exploits/
3. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-002