แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนกลุ่ม Ransomware ใช้เทคนิค BYOVD หลบเลี่ยงการตรวจจับเพื่อโจมตี

วันที่แจ้งเตือน 17 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์กรณีกลุ่มแรนซัมแวร์ Qilin และ Warlock ใช้เทคนิค Bring Your Own Vulnerable Driver (BYOVD) โดยนำไดรเวอร์ที่มีช่องโหว่มาใช้งานบนระบบที่ถูกเจาะแล้ว เพื่อปิดการทำงานของระบบตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคาม Endpoint Detection and Response: EDR และหลบเลี่ยงระบบการตรวจจับ ก่อนดำเนินการโจมตีในขั้นถัดไป

ลักษณะการโจมตี:

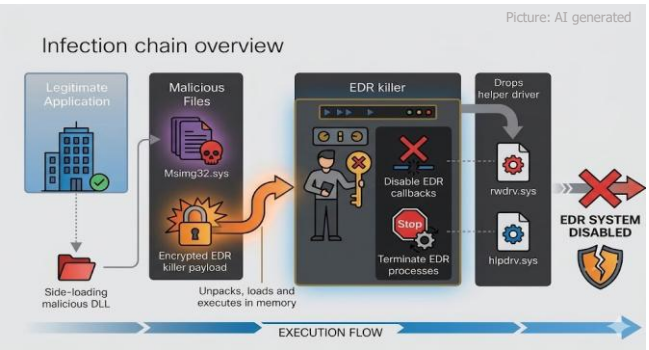
1. กลุ่ม Qilin ใช้ไดรเวอร์ที่มีช่องโหว่เพื่อช่วยให้มัลแวร์เข้าถึงระบบในระดับสูง และใช้ปิดการทำงานของ EDR ก่อนรันเพย์โหลดหลัก โดยจุดเริ่มต้นของกระบวนการ มีการใช้ไฟล์ DLL ร่วมกับการใช้การโจมตีหลายขั้นตอนเพื่อปิดการทำงานของระบบ EDR โดยไฟล์ดังกล่าวถูกใช้ผ่านเทคนิค DLL side-loading และ ใช้วิธีหลบการตรวจจับหลายรูปแบบ เช่น ลดการบันทึกเหตุการณ์ (Logging) ของระบบ และรันเพย์โหลดอยู่ในหน่วยความจำเพื่อให้ตรวจจับได้ยากขึ้น
2. กลุ่ม Warlock ใช้ไดรเวอร์ที่มีช่องโหว่ เพื่อยุติการทำงานของผลิตภัณฑ์ความปลอดภัยระดับเคอร์เนลและยังใช้เครื่องมืออื่นร่วมด้วยเพื่อเคลื่อนย้ายภายในเครือข่าย ควบคุมระบบ และดึงข้อมูลออก

พฤติกรรมสำคัญที่ควรเฝ้าระวัง:

ผู้โจมตีมักไม่รีบเข้ารหัสข้อมูลทันทีหลังเจาะระบบ แต่จะใช้เวลาอยู่ในระบบเพื่อขยายการควบคุมก่อน โดยพบการรันแรนซัมแวร์อาจเกิดขึ้นหลังการเจาะระบบครั้งแรกหลายวัน ในช่วงดังกล่าวควรเฝ้าระวังความผิดปกติ เช่น การทำงานของระบบป้องกันถูกปิดหรือหยุดทำงานโดยไม่ทราบสาเหตุ การพบไฟล์หรือไดรเวอร์ที่ไม่คุ้นเคยในระบบ รวมถึงการใช้งานเครื่องมือที่เกี่ยวข้องกับการเข้าควบคุมหรือเคลื่อนย้ายภายในเครือข่ายอย่างผิดปกติ

แนวทางป้องกัน:

1. อนุญาตเฉพาะไดรเวอร์ที่เชื่อถือได้ และควบคุมการติดตั้งไดรเวอร์อย่างเข้มงวด
2. เฝ้าระวังและตรวจสอบเหตุการณ์ที่เกี่ยวข้องกับการติดตั้งไดรเวอร์
3. อัปเดตแพตช์ระบบและซอฟต์แวร์ด้านความปลอดภัยอย่างสม่ำเสมอ
4. ใช้การป้องกันหลายชั้น และติดตามพฤติกรรมผิดปกติในระบบอย่างต่อเนื่อง



สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 17 เม.ย.. 2569
2. https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html?
3. https://blog.talosintelligence.com/qilin-edr-killer/?