แจ้งเตือน

Alert

**ผลกระทบทางธุรกิจ**

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

**ผลกระทบต่อระบบ**

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# กรณี GhostLock เทคนิคใหม่ใช้ Windows API บล็อกการเข้าถึงไฟล์ และกรณีผู้ไม่หวังดีใช้ AI ค้นหาช่องโหว่และพัฒนา Zero-Day Exploit เพื่อใช้โจมตี

**วันที่แจ้งเตือน 13 พฤษภาคม 2569**

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบนักวิจัยรายงานเกี่ยวกับภัยคุกคามไซเบอร์จำนวน 2 เรื่อง ได้แก่ (1) กรณี GhostLock[1] ใช้ประโยชน์จาก Windows API เพื่อบล็อกการเข้าถึงไฟล์ของระบบโดยไม่ต้องใช้การเข้ารหัส ทำให้ไฟล์เป้าหมายอยู่สถานะกำลังใช้งาน (in use) ทำให้โปรแกรมหรือกระบวนการอื่นไม่สามารถเข้าถึงไฟล์ดังกล่าวได้ และ (2) กรณีผู้ไม่หวังดีใช้ AI ค้นหาช่องโหว่และพัฒนา Zero-Day Exploit เพื่อใช้โจมตี [2]

**<u>กรณีที่ 1</u>** รายงานระบุว่า GhostLock อาศัยการทำงานของฟังก์ชัน CreateFileW API ของระบบปฏิบัติการ Windows โดยกำหนดค่า dwShareMode เป็น 0 เพื่อให้สิทธิใช้งานไฟล์เป็น Exclusive Access ทำให้โปรแกรมหรือผู้ใช้งานรายอื่นไม่สามารถเปิดใช้งานไฟล์เดียวกันได้ และอาจปรากฏข้อความ “STATUS_SHARING_VIOLATION” ระหว่างการใช้งาน เพื่อขัดขวางการทำงานการเข้าถึงไฟล์สำคัญ หรือระบบจัดเก็บข้อมูลที่ใช้งานร่วมกันในองค์กร โดยเฉพาะระบบ File Server หรือระบบที่เปิดให้เข้าถึงผ่าน SMB Share ภายในเครือข่าย ผู้ไม่หวังดีจะใช้เทคนิคดังกล่าวร่วมกับการโจมตีประเภทอื่น เพื่อขัดขวางการเข้าถึงข้อมูล ทำให้เกิด Denial-of-Service (DoS) ต่อระบบงานหรือขัดขวางกระบวนการสำรองข้อมูลและการประมวลผลไฟล์ เป็นผลให้ผู้ใช้งานไม่สามารถเข้าถึงไฟล์ได้

**<u>กรณีที่ 2</u>** รายงานระบุว่า google ได้แจ้งเตือนกรณีกลุ่มผู้ไม่หวังดีใช้ AI ในกระบวนการโจมตีหลายขั้นตอน เช่น การรวบรวมข้อมูลเป้าหมาย (Reconnaissance) การวิเคราะห์ช่องโหว่ การสร้างโค้ดอันตราย การจัดทำอีเมล Phishing ที่มีความสมจริง และพัฒนา Zero-Day Exploit จากการตรวจสอบพบบางส่วนของโค้ดและคำอธิบายมีลักษณะรูปแบบใกล้เคียงกับการสร้างโดย Large Language Model (LLM) นอกจากนี้ Google เปิดเผยว่า ได้ตรวจพบกรณีที่ผู้ไม่หวังดีใช้ AI ช่วยพัฒนาเครื่องมือโจมตีช่องโหว่เพื่อหลีกเลี่ยงระบบยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) และพัฒนา Zero-Day Exploit ในลักษณะใช้งานจริง และกลุ่มอาชญากรไซเบอร์ ได้ให้ความสนใจในการใช้ AI เพิ่มขีดความสามารถของปฏิบัติการทางไซเบอร์มีแนวโน้มเพิ่มสูงขึ้น ส่งผลให้ความเสี่ยงต่อองค์กรต่าง ๆ รวมถึงภาคการเงินและโครงสร้างพื้นฐานสำคัญ


**<u>ข้อมูลอ้างอิง 1</u>**

1. https://www.bleepingcomputer.com/news/security/new-ghostlock-tool-abuses-windows-api-to-block-file-access/
2. https://cyberpress.org/hackers-can-exploit-windows-createfilew/
3. https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-createfilew

**<u>ข้อมูลอ้างอิง 2</u>**

1. https://securityaffairs.com/191984/ai/google-warns-artificial-intelligence-is-accelerating-cyberattacks-and-zero-day-exploits.html
2. https://thehackernews.com/2026/05/hackers-used-ai-to-develop-first-known.html
3. https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access