

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

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



แจ้งเตือนการใช้ 2CLoader แพร่กระจายมัลแวร์ เพื่อควบคุมเครื่องและขโมยข้อมูลสำคัญ

วันที่แจ้งเตือน 14 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช.ได้ติดตามสถานการณ์ภัยคุกคามทางไซเบอร์พบรายงานการใช้มัลแวร์ 2CLoader สำหรับนำส่งมัลแวร์ Xworm รวมถึงมัลแวร์ขโมยข้อมูล เช่น Vidar และ Remus เป็นต้น ไปยังเครื่องเป้าหมาย ทำให้โปรแกรมเสียหาย (crash) หยุดทำงาน (Denial of Service) และ ทำให้ข้อมูลในหน่วยความจำ Heap รั่วไหล นำไปสู่การเปิดเผยข้อมูลสำคัญได้ ดังนี้

รายละเอียด	ผลกระทบ
2CLoader เป็นไฟล์ Loader สำหรับนำมัลแวร์เข้าสู่เครื่องเป้าหมาย โดยมีการซ่อน Payload ไว้ภายในไฟล์และถอดรหัสเฉพาะตอนรัน ทำให้ตรวจจับได้ยาก โดย Payload ที่พบ ได้แก่ Vidar Stealer, Remus Stealer เพื่อขโมยข้อมูลบัญชีและข้อมูลสำคัญ และ Xworm RAT ซึ่งเป็น Remote Access Trojan เพื่อใช้สำหรับควบคุมเครื่องเป้าหมาย 2CLoader ใช้เทคนิค AES-GCM Encryption, Rolling XOR และ Indirect Syscall (Hell's Gate) เพื่อหลบเลี่ยงการตรวจจับจาก EDR / Anti Virus 2CLoader สามารถติดต่อกับ Command & Control (C2) ผ่าน HTTP และส่งข้อมูลของเครื่องเหยื่อกลับไปหาผู้ไม่หวังดี เช่น ข้อมูลเวอร์ชันระบบปฏิบัติการ, Process ID, ระดับสิทธิ์ (Privilege), จำนวน CPU, หน่วยความจำ, Locale, Path ของ Malware เพื่อให้ผู้ไม่หวังดีสามารถติดตามสถานะของเหยื่อได้	- XWorm เป็นมัลแวร์แบบ Modular RAT ที่รองรับการควบคุมเครื่อง รวมถึงการขโมยข้อมูล เช่น รหัสผ่านและข้อมูลทางการเงิน เป็นต้น การติดตั้งมัลแวร์เพิ่มเติม รวมถึงสามารถถูกนำไปใช้ร่วมกับ Spyware หรือ Ransomware ได้ - โดยมีรายงานช่องทางการแพร่กระจาย Xworm หลายรูปแบบ เช่น Phishing, Malicious Attachment, Drive-by Download, Exploit Kit, อุปกรณ์ USB และการเข้าถึงผ่าน Remote Desktop Protocol เป็นต้น
คำแนะนำด้านความปลอดภัย: - ตรวจสอบเครื่องที่มีการเชื่อมต่อกับ C2 หรือมีพฤติกรรมผิดปกติ ให้แยกเครื่องออกจากเครือข่ายเพื่อป้องกันการติดต่อกับ C2 และการดาวน์โหลดมัลแวร์เพิ่มเติม - ตรวจสอบ Firewall, Proxy, DNS และ EDR Log ย้อนหลัง เพื่อค้นหาการเชื่อมต่อไปยัง IP Address, Domain หรือพอร์ตที่เกี่ยวข้องกับ 2CLoader และ Xworm - ตรวจสอบ Registry Run/RunOnce, Startup Folder, Scheduled Tasks และ กลไก Persistence อื่นโดยเฉพาะรายการที่ถูกสร้างขึ้นใหม่หรือไปยังไฟล์ที่ไม่รู้จัก - ตรวจสอบ Process Tree และ EDR เพื่อค้นหาการทำการ Process Injection การเรียกใช้ Payload ใน Memory หรือพฤติกรรมผิดปกติของ dllhost.exe, explorer.exe และ Process ที่ไม่รู้จัก - อัปเดต Antivirus, EDR, Firewall และระบบตรวจจับภัยคุกคามให้เป็นเวอร์ชันล่าสุด พร้อมนำ IoCs ที่เกี่ยวข้องไปใช้ในการ Threat Hunting และเฝ้าระวังภัยคุกคามทางไซเบอร์ (อ้างอิง2)	- หากตรวจพบมัลแวร์ ควรเปลี่ยนรหัสผ่าน, ยกเลิก Session หรือ Token ที่ใช้งานอยู่ และเปิดใช้งาน MFA สำหรับบัญชีที่เกี่ยวข้อง - หลีกเลี่ยงการเปิด RDP จากอินเทอร์เน็ตโดยตรง ควรใช้งานผ่าน VPN หรือ Secure Remote Access พร้อมเปิดใช้งาน MFA และจำกัดสิทธิ์ตามหลัก Least Privilege - ใช้ Application Control หรือ Allow listing เพื่อจำกัดการเรียกใช้ Executable และ Script จากแหล่งที่ไม่ได้รับอนุญาต โดยเฉพาะไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ต - เฝ้าระวัง URL และไฟล์แนบจากแหล่งที่ไม่รู้จัก พร้อมแนะนำผู้ใช้งานไม่เปิดไฟล์หรือคลิกลิงก์ที่ไม่สามารถยืนยันแหล่งที่มาได้ - สำรองข้อมูลสำคัญอย่างสม่ำเสมอ และแยก Backup ออกจากระบบ Production เพื่อลดผลกระทบหากมีการติดตั้ง Ransomware หรือมัลแวร์

ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 13 ต.ค. 2569
- <https://cyberint.com/blog/dark-web/xworm-malware-worming-its-way-from-entry-to-exploitation/>
- <https://cybersecuritynews.com/new-2cloder-malware/>