แจ้งเตือน Alert	ผลกระทบทางธุรกิจ	ผลกระทบต่อระบบ	TLP Color : CLEAR
	☒ Financial Damage ☒ Reputation Damage ☒ Non-compliance ☒ Privacy Violation	☒ Loss of Confidentiality ☒ Loss of Integrity ☒ Loss of Availability	ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กลุ่ม Akira Ransomware มุ่งเป้าโจมตีผลิตภัณฑ์ Microsoft Defender และ SonicWall VPNs

วันที่แจ้งเตือน 11 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานกรณีกลุ่ม Akira Ransomware ได้พัฒนาวิธีในการหลบหลีกการตรวจจับจากโปรแกรม Microsoft Defender โดยใช้กลยุทธที่เรียกว่า "Bring Your Own Vulnerable Driver: BYOVD”

โดยผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่ไดรเวอร์ของแอปพลิเคชัน ThrottleStop* (rwdrv.sys) ซึ่งเป็นไดรเวอร์ที่ถูกต้องจากผู้ผลิตเพื่อเข้าถึงระบบจากระยะไกล (Remote access) แล้วจึงทำการติดตั้งไดรเวอร์อันตราย (hlpdrv.sys) เพื่อทำการยกระดับสิทธิ (ระดับ kernel) และทำการปิดการทำงานของโปรแกรม Microsoft Defender โดยผู้ไม่หวังดีสามารถ Run โปรแกรมอันตรายอื่น ๆ โดยที่ Microsoft Defender ไม่สามารถตรวจพบได้ การโจมตีลักษณะดังกล่าวเริ่มพบตั้งแต่ เดือนกรกฎาคม 2568 และปัจจุบันมีการนำไปใช้ในการโจมตีกรณีที่เชื่อมโยงกับเหตุการณ์โจมตีอุปกรณ์ VPN ของ SonicWall โดยอาศัยช่องโหว่ CVE-2024-40766 อีกด้วย

*ThrottleStop คือโปรแกรมปรับแต่งประสิทธิภาพ (tuning software) สำหรับซีพียู (CPU)

แนวทางการป้องกันและลดผลกระทบ	
- ใช้ Antivirus Software ที่มีประสิทธิภาพ	- ดาวน์โหลดซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น
- จำกัดการเข้าถึง VPN	- อัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด
- ลดความเสี่ยง เลี่ยงเว็บที่ไม่น่าไว้ใจ, ไม่เปิด email attachment ที่ไม่รู้จัก	- เปิด Two-Factor Authentication (2FA)

Indicators of Compromise:

IoCs	Type	Value
hlpdrv.sys	SHA256	bd1f381e5a3db22e88776b7873d4d2835e9a1ec620571d2b1da0c58f81c84a56
rwdrv.sys	SHA256	16f83f056177c4ec24c7e99d01ca9d9d6713bd0497eeedb777a3ffefa99c97f0
file path for hlpdrv.sys	File Path	Users\REDACTED\AppData\Local\Temp\hlpdrv.sys
file path for rwdrv.sys	File Path	Users\REDACTED\AppData\Local\Temp\rwdrv.sys
Service creation for rwdrv.sys	Service	Service “mgdsrv” registered – C:\Users\REDACTED\AppData\Local\Temp\rwdrv.sys
Service creation for hlpdrv.sys	Service	Service “KMHLPSVC” registered – C:\Users\REDACTED\AppData\Local\Temp\hlpdrv.sys

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 10 ก.ย. 2568
2) https://cyberguy.com/security/hackers-found-way-turn-windows-defender-remotely/
3) https://www.guidepointsecurity.com/blog/gritrep-akira-sonicwall/
4) https://www.bleepingcomputer.com/news/security/akira-ransomware-abuses-cpu-tuning-tool-to-disable-microsoft-defender/