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

แจ้งเตือนกรณีผู้ไม่หวังดีใช้เครื่องมือประเภท Remote Monitoring and Management (RMM) เพื่อควบคุมระบบ

วันที่แจ้งเตือน 12 มิถุนายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร์กรณีผู้ไม่หวังดีใช้เครื่องมือประเภท Remote Monitoring and Management (RMM) เพื่อควบคุมระบบเพิ่มขึ้น โดยมีรายละเอียดดังนี้

การโจมตี	รายละเอียด	ผลกระทบ
ผู้ไม่หวังดีมีแนวโน้มในการนำเครื่องมือประเภท Remote Monitoring and Management (RMM) ที่ใช้สำหรับบริหารจัดการและควบคุมเครื่อคอมพิวเตอร์มากขึ้น โดยอาจมีการกำหนดค่าให้เชื่อมต่อกลับไปยังเซิร์ฟเวอร์ที่ควบคุมโดยผู้ไม่หวังดี (C2 server) เพื่อใช้โอนย้ายไฟล์ ควบคุมหน้าจอ สำรวจระบบ หรือคงสิทธิการเข้าถึงระบบอย่างต่อเนื่อง	• ผู้ไม่หวังดีสามารถควบคุมเครื่องได้โดยไม่ได้รับอนุญาต • ผู้ไม่หวังดีสามารถสั่งรันคำสั่ง สำรวจระบบ และเคลื่อนย้ายภายในเครือข่าย • มีการติดตั้งเครื่องมือเพิ่มเติม เช่น network scanner, credential tool หรือ malware • ขโมยข้อมูลหรือถ่ายโอนไฟล์ออกจากระบบ • เป็นช่องทาง persistence เพื่อกลับเข้าระบบซ้ำแม้แก้ไขช่องทางโจมตีแรกแล้ว • ตรวจจับยากขึ้น เนื่องจากพฤติกรรมคล้ายการทำงานของผู้ดูแลระบบ • อาจถูกใช้เป็นส่วนหนึ่งของการโจมตี ransomware ขโมยข้อมูลก่อนเข้ารหัสไฟล์ • กระทบต่อระบบสำคัญ ระบบให้บริการ ระบบฐานข้อมูล หรือระบบภายในขององค์กร	ผลิตภัณฑ์ที่ได้รับผลกระทบระบบที่ควรตรวจสอบและเฝ้าระวัง ได้แก่ • เครื่องคอมพิวเตอร์ที่มีการติดตั้งเครื่องมือประเภท RMM หรือ Remote Access Tool โดยไม่ได้รับอนุญาต เช่น MeshAgent, AnyDesk, TeamViewer, ScreenConnect และ SimpleHelp เป็นต้น • เครื่องมือ Remote Desktop, Remote Shell, File Transfer หรือ Remote Support อื่น ๆ ที่มีลักษณะคล้ายกัน

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 9 มิ.ย. 2569
2. https://www.intel471.com/blog/understanding-and-threat-hunting-for-rmm-software-misuse
3. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3277084/nsa-cisa-and-ms-isac-release-guidance-for-securing-remote-monitoring-and-manage/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ