แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กลุ่ม Mustang Panda ใช้มัลแวร์โจมตี IP ในประเทศ ก่อนติดตั้ง Backdoor

วันที่แจ้งเตือน 7 ตุลาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารเกี่ยวกับการโจมตีทางไซเบอร์ และได้รับรายงานจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. เกี่ยวกับกรณีกลุ่มผู้โจมตี APT Mustang Panda ติดตั้ง SnakeDisk USB Worm เจาะจง IP ในประเทศ ก่อนติดตั้ง Yokai Backdoor

มัลแวร์ชุดนี้ถูกออกแบบมาเพื่อแพร่กระจายผ่านสื่อเก็บข้อมูลแบบพกพา (USB Drive) และมุ่งเป้าการโจมตีไปยังเครื่องคอมพิวเตอร์ที่มี IP Address ในประเทศ โดยมีเป้าหมายเพื่อสร้างช่องทางเข้าควบคุมระบบ (backdoor) และดึงข้อมูลสำคัญออกจากเครื่องที่โดนโจมตี โดย SnakeDisk จะทำการคัดลอกไฟล์ภายใน USB และสร้างไฟล์ปลอม (เช่น USB.exe เป็นต้น) เพื่อหลอกให้ผู้ใช้เปิดใช้งาน เมื่อรันไฟล์ดังกล่าว ทั้งนี้ มัลแวร์จะโหลด DLL ของ Yokai Backdoor เข้าสู่ระบบและสร้างการเชื่อมต่อกับเซิร์ฟเวอร์ควบคุม (C2) ผ่านเส้นทาง /kptinfo/import/index.php โดย Backdoor นี้สามารถเปิด reverse shell ให้ผู้ไม่ประสงค์ดีควบคุมเครื่องจากระยะไกล และตั้ง Scheduled Task (“MicrosoftEdgeAcModuleUpdateTask”) เพื่อให้รันซ้ำทุก 5 นาที ทำให้มัลแวร์คงอยู่ในระบบอย่างถาวร

เพื่อป้องกันและลดความเสี่ยงจากมัลแวร์ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินการดังนี้

- หลีกเลี่ยงการใช้ USB Drive หรืออุปกรณ์สื่อสารข้อมูลจากแหล่งที่ไม่เชื่อถือ และห้ามเปิดไฟล์ที่ไม่ทราบที่มา
- ตรวจจับและบล็อกพฤติกรรม DLL Sideloading โดยตรวจสอบการเรียกใช้งานไฟล์ที่ลงนาม (Signed Executable) ซึ่งเปิด cmd.exe ด้วย argument ผิดปกติ เช่น -Embedding หรือ -project-mod
- เฝ้าระวังการสร้าง Scheduled Task ที่ไม่ปกติ โดยเฉพาะ Task ชื่อ “MicrosoftEdgeAcModuleUpdateTask”
- จำกัดสิทธิ์การอ่าน - เขียนไฟล์จากสื่อ USB และใช้นโยบาย Data Loss Prevention (DLP) หรือ Endpoint Detection and Response (EDR) เพื่อสแกนและบล็อกไฟล์ที่น่าสงสัย
- ตรวจสอบการเชื่อมต่อออกภายนอก (outbound connection) โดยเฉพาะการส่งข้อมูลไปยังโดเมนหรือ IP ดังนี้
  - hxxp://118.174.183[.]89/kptinfo/import/index.php
  - IP: 123.253.34[.]44, 146.70.29[.]229, 188.208.141[.]196
- หากตรวจพบเครื่องที่โดนโจมตี ให้ถอดอุปกรณ์ USB ออกจากระบบทันที และบล็อกการเชื่อมต่อกับโดเมนหรือ IP ของ Command & Control (C2)

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2025/09/mustang-panda-deploys-snakedisk-usb.html
2. https://www.ibm.com/think/x-force/hive0154-drops-updated-toneshell-backdoor
3. รายงานวิเคราะห์มัลแวร์ USB Worm Snakedisk และ Yokai backdoor โดย ThaiCERT (เอกสารแนบ)

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ