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

มัลแวร์ msaRAT เชื่อมโยงกับกลุ่ม Chaos Ransomware และมัลแวร์ Dolphin X ใช้ AI ในการวิเคราะห์พฤติกรรมเป้าหมาย

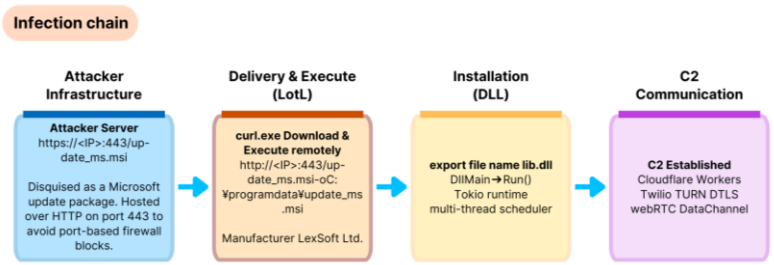
วันที่แจ้งเตือน 24 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบการรายงานของหน่วยงานวิจัยเกี่ยวกับ มัลแวร์ msaRAT มีความเชื่อมโยงกับกลุ่ม Chaos Ransomware และมัลแวร์ Dolphin X ซึ่งใช้ AI ในการวิเคราะห์พฤติกรรมเป้าหมาย โดยมีรายละเอียดดังนี้

1. **มัลแวร์ msaRAT** เป็น Trojan ควบคุมเครื่องจากระยะไกล (Remote Access Trojan) มีความเชื่อมโยงกับกลุ่ม Chaos Ransomware (อาศัยเบราว์เซอร์เพื่อสร้างช่องทาง C2 แบบลับ (C2 tunneling)) โดยมัลแวร์ใช้เทคนิคหลบเลี่ยงการตรวจจับด้วยการใช้ Google Chrome หรือ Microsoft Edge ในการสื่อสารกับ C2 Server ของกลุ่มผู้ไม่หวังดีผ่าน Chrome DevTools Protocol แทนการเชื่อมต่อจากมัลแวร์โดยตรง ทำให้ Traffic มีลักษณะเป็นการใช้งานปกติ ทำให้หลบเลี่ยงการตรวจจับจากไฟร์วอลล์และระบบเฝ้าระวังเครือข่ายได้ เมื่อผู้ไม่หวังดีเข้าถึงเครื่องคอมพิวเตอร์เป้าหมายได้แล้ว Choas Ransomware จะเริ่มเข้ารหัสข้อมูลและดำเนินการเรียกค่าไถ่

ทั้งนี้ ผู้ประกอบธุรกิจ ควรเพิ่มการเฝ้าระวัง หมั่นตรวจสอบการใช้งานเครือข่ายและดำเนินการเมื่อพบพฤติกรรมที่น่าสงสัย เพื่อลดความเสี่ยงที่อาจกระทบต่อระบบและข้อมูลขององค์กร



2. **มัลแวร์ Dolphin X** เป็น Trojan ควบคุมเครื่องจากระยะไกล (Remote Access Trojan) ที่ออกแบบมาเพื่อเจาะระบบ Windows โดยเฉพาะ ซึ่งมีความสามารถในการขโมยข้อมูล Credential พร้อมทั้งใช้ AI Profiler ในการวิเคราะห์พฤติกรรมของผู้ใช้งานและจัดอันดับเหยื่อ เพื่อเลือกเป้าหมายที่มีข้อมูลหรือสิทธิในการเข้าถึงระดับสูงจากรายงานระบุว่า Dolphin X สามารถโจมตีแอปพลิเคชันได้กว่า 300 รายการ รวมถึงขโมยข้อมูลสำคัญ เช่น ข้อมูลการเข้าสู่ระบบของเว็บเบราว์เซอร์ กระเป๋าเงินคริปโตเคอร์เรนซี กุญแจ SSH และ Cloud Tokens เป็นต้น โดยทั้งหมดจะถูกรวบรวมไว้ในไฟล์เดียวก่อนส่งกลับไปยังผู้ไม่หวังดี

ทั้งนี้ ผู้ประกอบธุรกิจ ควรเพิ่มการบริหารจัดการสิทธิให้มั่นคงปลอดภัย เพื่อไม่ให้ข้อมูล Credential รั่วไหล เฝ้าระวัง หมั่นตรวจสอบและดำเนินการเมื่อพบพฤติกรรมที่น่าสงสัย (Behavior-based Detection) เพื่อลดความเสี่ยงที่อาจกระทบต่อระบบและข้อมูลขององค์กร

ข้อมูลอ้างอิง msaRAT

1. https://blog.talosintelligence.com/chaos-msarat-living-off-the-browser-to-build-covert-c2-channel/
2. https://securityaffairs.com/195876/malware/chaos-ransomware-deploys-browser-based-msarat-to-evade-network-detection.html

ข้อมูลอ้างอิง Dolphin X

1. https://www.varonis.com/blog/dolphin-x-stealer
2. https://www.infosecurity-magazine.com/news/new-dolphin-x-stealer-ai-targets/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ