แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

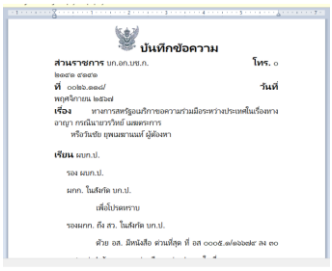
แจ้งเตือน มัลแวร์ Yokai มุ่งเป้าโจมตีหน่วยงานในประเทศไทย เพื่อเข้าถึงข้อมูลสำคัญ

วันที่แจ้งเตือน 26 ธันวาคม 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สำนักงาคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เผยแพร่ข่าวแจ้งเตือนมัลแวร์ Yokai มุ่งเป้าโจมตีหน่วยงานในประเทศไทยเพื่อเข้าถึงข้อมูลสำคัญ ซึ่งการโจมตีทางไซเบอร์นี้ใช้เทคนิคที่เรียกว่า DLL side-loading* เพื่อส่งมัลแวร์ Yokai backdoor ซึ่งมีความสามารถในการเข้าควบคุมระบบ และรับคำสั่งจากผู้ไม่หวังดีผ่าน Command and Control Server (C2 Server) เพื่อทำการขโมยข้อมูลสำคัญขององค์กร รวมทั้งผู้ไม่หวังดีสามารถทำการเชื่อมต่อจากระยะไกล และ ส่งคำสั่งที่เป็นอันตรายเข้าสู่ระบบได้

การทำงานของมัลแวร์ดังกล่าวเริ่มต้นจากไฟล์ RAR ที่แนบมากับอีเมลซึ่งภายในจะมี LNK shortcut 2 ไฟล์ ชื่อว่า “กระทรวงยุติธรรมสหรัฐ.pdf” และ “ด่วนที่สุด ทางการสหรัฐอเมริกาขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา.docx” เมื่อเหยื่อทำการคลิก LNK shortcut ดังกล่าวเพื่อเปิดเอกสาร ระบบจะทำการ copy ข้อมูลที่เป็นอันตรายจาก ADS** เพื่อนำไปสร้าง executable file “file.exe” เพื่อใช้ในการสร้างไฟล์อันตราย 3 ไฟล์ ได้แก่ IdrInit.exe, ProductStatistics3.dll และ IdrInit.exe.data ที่ใช้ในการโจมตีแบบ DLL side-loading (สามารถดูข้อมูล IoC ได้จากข้อมูลอ้างอิง 4)



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

* DLL side-loading: เทคนิคการโจมตีโดยการโหลดไฟล์ DLL (Dynamic Link Library) ที่เป็นอันตราย โดยใช้ประโยชน์จากกลไกในลำดับการค้นหา และเรียกใช้งาน DLL ไฟล์บน Windows เพื่อวางไฟล์ DLL ที่เป็นอันตรายด้วยชื่อเดียวกันกับไฟล์ DLL ที่ถูกต้อง เพื่อทำให้เมื่อแอปพลิเคชันพยายามโหลดไฟล์ DLL แอปพลิเคชันจะโหลดไฟล์ DLL ที่เป็นอันตรายไปแทน ซึ่ง DLL ที่เป็นอันตราย สามารถให้สิทธิสูงแก่ผู้ไม่หวังดี หรือเรียกใช้คำสั่งบนเครื่องเหยื่อ โดยใช้แอปพลิเคชันที่กำลังรันคำสั่งอยู่ เมื่อผู้ใช้งานทำการติดตั้งแอปพลิเคชันอันตรายสำเร็จ จะสร้าง shortcut บนเดสก์ท็อป และ startup ระบบ ซึ่งเมื่อเหยื่อทำการเรียกใช้ desktop shortcut แอปดังกล่าว จะเป็นการส่งคำสั่งเพื่อเรียกใช้งานโค้ด และเปิดใช้งานแอปพลิเคชันที่เป็นอันตรายต่อไป

** Alternate Data Stream (ADS) เป็นคุณสมบัติของระบบไฟล์ NTFS บน Windows ที่อนุญาตให้ไฟล์หรือโฟลเดอร์สามารถเก็บข้อมูลที่ซ่อนอยู่โดยใช้ชื่อ stream เช่น file.txt:<stream-name> ทำให้ไฟล์ NTFS สามารถมีหลาย stream ที่ถูกเชื่อมโยงไว้กับไฟล์เดียวกันโดยไม่ส่งผลต่อเนื้อหาหลักของไฟล์หรือแสดงให้เห็นในขนาดไฟล์ปกติเมื่อดูผ่าน File Explorer ทั้งนี้ ADS ออกแบบมาเพื่อประโยชน์ของการเก็บสถานะหรือข้อมูลเพิ่มเติม แต่ก็สามารถถูกใช้งานในทางที่ไม่พึงประสงค์ เช่น ซ่อนมัลแวร์

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 25 ธ.ค. 2567
2) https://thehackernews.com/2024/12/thai-officials-targeted-in-yokai.html
3) https://www.netskope.com/blog/new-yokai-side-loaded-backdoor-targets-thai-officials
4) https://github.com/netskopeoss/NetskopeThreatLabsIOCs/tree/main/Malware/Yokai/IOCs