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

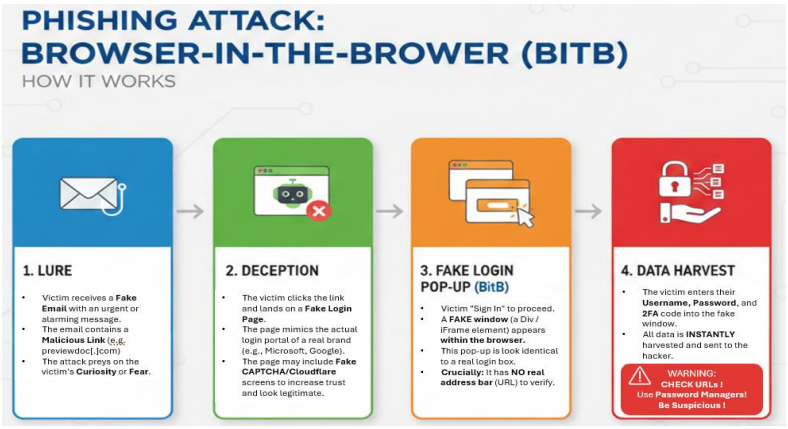
ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

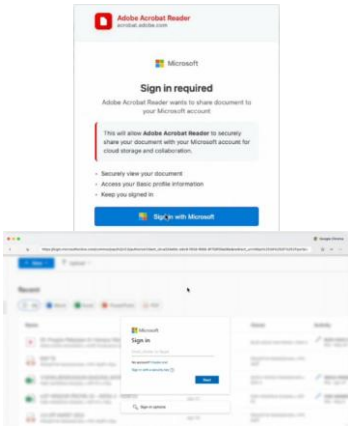
แจ้งเตือนการนำเทคนิค Browser-in-the-Browser (BitB) มาใช้เพื่อมุ่งเป้าขโมยข้อมูลการเข้าสู่ระบบ

วันที่แจ้งเตือน 24 พฤศจิกายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่ข่าวสารภัยคุกคามทางไซเบอร์ กรณีพบการนำเทคนิค Browser-in-the-Browser (BitB) มาใช้ในชุดเครื่องมือโจมตีแบบ Phishing-as-a-Service (PhaaS) ที่ชื่อว่า Sneaky2FA เพื่อมุ่งเป้าขโมยข้อมูลการเข้าสู่ระบบและ Session Token (2FA/MFA) ของผู้ใช้งาน **Microsoft 365** โดยจะมีการสร้างหน้าต่างล็อกอินปลอมที่สามารถปรับเปลี่ยนรูปแบบหน้าตาให้สอดคล้องกับระบบปฏิบัติการและเบราว์เซอร์ของเหยื่อโดยอัตโนมัติ เช่น ปรับให้เหมือน Edge บน Windows หรือ Safari บน macOS ซึ่งช่วยให้ผู้ไม่หวังดีสามารถหลอกลวงเหยื่อได้แนบเนียนขึ้น





รูปแบบการโจมตีของ Sneaky2FA เริ่มจากการหลอกให้เหยื่อคลิกลิงก์เพื่อดูเอกสาร (เช่น บนโดเมน previewdoc[.]com) เมื่อเหยื่อกดปุ่ม Sign in with Microsoft ระบบจะแสดงหน้าต่าง Pop-up ปลอมที่สร้างจาก iframe ขึ้นมาซ้อนทับ โดยหน้าต่างนี้จะมีการเลียนแบบแถบ URL ที่ดูเหมือนโดเมนที่ถูกต้องของ Microsoft (OAuth pop-up) อย่างแนบเนียนจนทำให้เหยื่อหลงเชื่อ และเบื้องหลังการทำงานนี้ Sneaky2FA ยังคงใช้กลยุทธ์ Attacker-in-the-Middle หรือการเป็นตัวกลาง (Reverse Proxy) เพื่อส่งต่อข้อมูลการล็อกอินจริงไปยังเซิร์ฟเวอร์ของ Microsoft ทำให้แฮกเกอร์สามารถดักจับทั้งรหัสผ่านและ Session Token ที่ใช้งานได้พร้อมกัน

แนวทางการป้องกันและลดผลกระทบ:

- หลีกเลี่ยงการกดลิงก์ที่ไม่แน่ใจ โดยเฉพาะอีเมลและข้อความที่ไม่รู้จัก
- ตรวจสอบ URL ทุกครั้งก่อนกรอกข้อมูล และ ทดลองขยับหน้าต่าง POP UP หากไม่สามารถขยับหรือลากออกมาภายนอกเบราว์เซอร์หรือหน้าเว็บได้ ให้พึงระวังว่าเป็นของปลอม
- ไม่ควรอนุญาตให้พนักงานภายในองค์กรท่าน ติดตั้งส่วนขยายเบราว์เซอร์ (Browser Extensions) หรืออนุญาตเฉพาะที่จำเป็นและน่าเชื่อถือเท่านั้น
- ควรสื่อสารให้พนักงานภายในองค์กรท่านทราบถึงความเสี่ยงในประเด็นนี้ เพื่อเป็นการสร้างความตระหนักรู้ และซักซ้อมว่าหากพบความผิดปกติในการเข้าสู่ระบบ ควรรีบแจ้งผู้ดูแลระบบทันที

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

ข้อมูลอ้างอิง

1) ข่าวสารภัยคุกคามทางไซเบอร์ของ ThaiCERT ประจำวันที่ 21 พ.ย. 2568
2) https://www.bleepingcomputer.com/news/security/sneaky2fa-phaas-kit-now-uses-redteamers-browser-in-the-browser-attack/
3) ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล - PDPC Eagle Eye's: https://www.facebook.com/share/p/17eHeMo5ve/