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

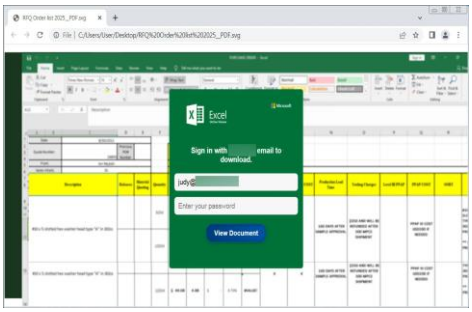
แจ้งเตือน กรณีผู้ไม่หวังดี นำไฟล์ SVG มาใช้ในการหลอกลวงเหยื่อเพิ่มมากขึ้น

วันที่แจ้งเตือน 19 พฤศจิกายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

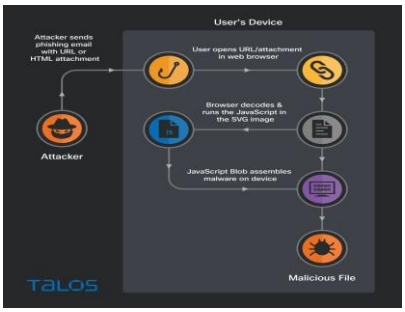
เว็บไซต์ Bleeping Computer รายงานพบผู้ไม่หวังดีนิยมใช้ไฟล์ Scalable Vector Graphics: SVG* เพื่อ Phishing หลอกลวงเหยื่อเพิ่มมากขึ้น โดยอาศัยความสามารถของ SVG ที่รองรับการฝังไฟล์ HTML ไว้ข้างในด้วยแท็ก พร้อมยกตัวอย่างกรณีที่ผู้ไม่หวังดีนำ SVG มาใช้ประโยชน์ เช่น (1) กรณีที่สร้างไฟล์แนบ SVG ที่แสดงรูปเอกสาร Excel ปลอม หลอกให้เหยื่อกรอกข้อมูลเข้าสู่ระบบ โดยข้อมูลดังกล่าวจะถูกส่งไปยังผู้ไม่หวังดี เพื่อขโมยข้อมูลบัญชีของเหยื่อ (ภาพที่ 1) (2) กรณีปลอมเอกสารให้คล้ายของทางราชการเพื่อขอข้อมูลเพิ่มเติม และเมื่อเหยื่อคลิกเปิดหรือดาวน์โหลดจะทำให้มัลแวร์เข้าสู่ระบบ (ภาพที่ 2) และ (3) การใช้งานรูปแบบอื่น เช่น สร้างไฟล์แนบ SVG ที่มีการฝังโค้ด JavaScript ไว้เพื่อเปลี่ยนเส้นทางเบราว์เซอร์ไปยังเว็บไซต์ของผู้ไม่หวังดีโดยอัตโนมัติเมื่อเปิดรูปภาพ (ภาพที่ 3) เป็นต้น

ภาพที่ 1



ภาพที่ 2

ภาพที่ 3



Bleeping Computer ระบุว่ารูปแบบการใช้ประโยชน์จาก SVG เป็นการใช้งานในลักษณะการแสดงข้อความของรูปภาพ (textual representations of images) ซึ่งมักจะส่งผลให้ซอฟต์แวร์รักษาความปลอดภัยไม่สามารถตรวจพบได้ อย่างไรก็ดี การส่งอีเมลโดยแนบไฟล์ SVG นั้นไม่ใช่เรื่องปกติที่บุคคลทั่วไปปฏิบัติกัน หน่วยงานจึงควรพิจารณาตั้งเป็นข้อสังเกตเพื่อการเฝ้าระวังทันที โดยพิจารณาลบอีเมลดังกล่าว หรือ ดำเนินการกักกันอีเมลหรือข้อมูลทันที รวมถึงควรพิจารณาเพิ่มความตระหนักรู้ในลักษณะภัยคุกคามดังกล่าว เพื่อลดผลกระทบที่อาจทำให้ระบบงานสำคัญไม่สามารถใช้งานและให้บริการได้

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

* ไฟล์ SVG เป็นรูปแบบไฟล์เวกเตอร์ที่เก็บข้อมูลรูปภาพโดยใช้ข้อความที่อธิบายไว้ในสูตรทางคณิตศาสตร์ที่เป็นข้อความในโค้ด ที่อิงกับจุดและเส้นบนตารางซึ่งต่างจากไฟล์ประเภท JPEG หรือ PNG ที่สร้างรูปภาพขึ้นจากพิกเซล โดยSVG เขียนขึ้นด้วยโค้ด XML ซึ่งทำให้สามารถเก็บข้อมูลข้อความในรูปแบบตัวอักษรจริงได้ ซึ่ง SVG นิยมใช้งานบนเว็บไซต์ เนื่องจากสามารถปรับขนาดได้อัตโนมัติโดยไม่สูญเสียคุณภาพของภาพหรือรูปร่าง ทำให้เหมาะสำหรับใช้ในเบราว์เซอร์ที่อาจมีความละเอียดแตกต่างกัน

ข้อมูลอ้างอิง

1) https://www.bleepingcomputer.com/news/security/phishing-emails-increasingly-use-svg-attachments-to-evade-detection/
2) https://www.adobe.com/th_th/creativecloud/file-types/image/vector/svg-file.html
3) https://www.bleepingcomputer.com/news/security/attackers-use-svg-files-to-smuggle-qbot-malware-onto-windows-systems/