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

ผู้ไม่หวังดีใช้ซอฟต์แวร์ VPN ปลอม หลอกขโมย Credential

วันที่แจ้งเตือน 15 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงานเกี่ยวกับแคมเปญการโจมตีที่ผู้ไม่หวังดีเผยแพร่ซอฟต์แวร์ VPN ปลอม เพื่อขโมยข้อมูลผู้ใช้งาน โดยกลุ่มผู้ไม่หวังดี Storm-2561 ได้ปลอมแปลงเว็บไซต์ของผู้ผลิตซอฟต์แวร์ VPN รายสำคัญ เพื่อหลอกให้ผู้ใช้งานดาวน์โหลดโปรแกรม VPN ปลอม

ผู้ไม่หวังดีใช้เทคนิค Search Engine Optimization (SEO) poisoning เพื่อบิดเบือนผลการค้นหา เมื่อผู้ใช้งานค้นหาเกี่ยวกับการดาวน์โหลดโปรแกรม VPN โดยลิงก์ที่ได้จะถูกเปลี่ยนเส้นทางไปยังเว็บไซต์ปลอมที่มีลักษณะคล้ายกับเว็บไซต์ของผู้ผลิตซอฟต์แวร์จริง ซึ่งเว็บไซต์ดังกล่าวเชื่อมโยงไปยังไฟล์ติดตั้ง VPN ปลอม เมื่อผู้ใช้งานดาวน์โหลดและติดตั้งไฟล์ดังกล่าว ระบบจะติดตั้งโปรแกรม Pulse.exe ลงในเครื่อง พร้อมทั้งวางไฟล์ loader และมัลแวร์ประเภท infostealer ลงในระบบ จากนั้นโปรแกรม VPN ปลอมจะแสดงหน้าจอเข้าสู่ระบบที่มีลักษณะเหมือนซอฟต์แวร์จริง เพื่อหลอกลวงให้ผู้ใช้งานกรอกข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยข้อมูลดังกล่าวจะถูกดักจับและส่งออกไปยังผู้ไม่หวังดี

มาตรการป้องกันและแนวทางปฏิบัติ เพื่อป้องกันภัยคุกคาม สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบ พิจารณาดำเนินแจ้งเตือนผู้ใช้งานภายในองค์กรให้ดาวน์โหลดซอฟต์แวร์ VPN จากเว็บไซต์ของผู้ผลิตหรือแหล่งที่เชื่อถือได้ หรือที่องค์กรจัดเตรียมให้เท่านั้น พร้อมทั้งตรวจสอบความถูกต้องของเว็บไซต์ก่อนทำการดาวน์โหลดซอฟต์แวร์ และดำเนินการเฝ้าระวังบันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง เพื่อให้สามารถตรวจจับและตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันท่วงที

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/fake-enterprise-vpn-downloads-used-to-steal-company-credentials/

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ