วันที่ 5 มิถุนายน 2568

เว็บไซต์ปลอม DocuSign และ Gitcode แพร่มัลแวร์ NetSupport RAT ผ่าน PowerShell

ผู้เชี่ยวชาญด้านความปลอดภัยได้แจ้งเตือนเกี่ยวกับแคมเปญใหม่ที่ใช้เว็บไซต์ปลอม หลอกให้ผู้ใช้เรียกใช้คำสั่ง PowerShell ที่เป็นอันตรายบนเครื่องคอมพิวเตอร์ของตน ซึ่งนำไปสู่การติดมัลแวร์ชื่อ **NetSupport RAT**

ทีม DomainTools Investigations (DTI) ระบุว่าได้พบ **สคริปต์ PowerShell ที่ทำงานแบบหลายขั้นตอนในการดาวน์โหลด (multi-stage downloader)** บนเว็บไซต์ปลอมที่แฝงตัวเป็น Gitcode และ DocuSign และได้กล่าวว่า

“เว็บไซต์เหล่านี้พยายามหลอกให้ผู้ใช้คัดลอกและเรียกใช้สคริปต์ PowerShell ผ่านคำสั่ง Run ของ Windows”

เมื่อผู้ใช้ทำตามคำแนะนำและเรียกใช้สคริปต์ PowerShell ดังกล่าว ระบบจะดาวน์โหลดสคริปต์อีกชุดหนึ่งเพื่อติดตั้งมัลแวร์บนเครื่องโดยอัตโนมัติ ซึ่งในท้ายที่สุดจะทำให้เครื่องของเหยื่อติด **NetSupport RAT** มีความเป็นไปได้ว่าเว็บไซต์ปลอมเหล่านี้ถูกเผยแพร่ผ่านเทคนิค **Social Engineering** เช่น การส่งอีเมล หรือแชร์ผ่านโซเชียลมีเดีย บนเว็บไซต์ปลอมที่แฝงตัวเป็น Gitcode มีสคริปต์ PowerShell ที่จะดาวน์โหลดสคริปต์จากเซิร์ฟเวอร์ภายนอก (tradingviewtool[.]com) เพื่อค่อยๆ ดำเนินการติดตั้ง NetSupport RAT ลงในระบบ

ทาง DomainTools ยังตรวจพบเว็บไซต์ปลอมที่แฝงตัวเป็น DocuSign เช่น docusign.sa[.]com ซึ่งใช้เทคนิคใหม่ในการลวงผู้ใช้ โดยการใช้ **CAPTCHA แบบ ClickFix** เพื่อหลอกให้เหยื่อตรวจสอบว่า "ไม่ใช่หุ่นยนต์" เมื่อผู้ใช้คลิก CAPTCHA ระบบจะคัดลอกคำสั่ง PowerShell ที่ถูกเข้ารหัสไว้ไปยังคลิปบอร์ดของผู้ใช้ **โดยที่ผู้ใช้ไม่รู้ตัว** เทคนิคนี้เรียกว่า **clipboard poisoning** จากนั้นหน้าเว็บจะมีคำแนะนำให้ผู้ใช้กด **Win + R** วางคำสั่ง (Ctrl + V) แล้วกด Enter ซึ่งจะเป็นการเรียกใช้คำสั่งที่เป็นอันตราย

เมื่อคำสั่งดังกล่าวถูกรัน สคริปต์จะดาวน์โหลดไฟล์ wbdims.exe จาก GitHub เพื่อสร้าง **ช่องทางการเข้าถึงเป้าหมายให้คงอยู่เสมอ (persistence)** โดยให้มัลแวร์ทำงานอัตโนมัติทุกครั้งที่ผู้ใช้เข้าสู่ระบบ แม้ว่าในขณะทำการตรวจสอบ ไฟล์ payload ดังกล่าวจะไม่สามารถดาวน์โหลดได้ แต่คาดว่าจะมีการติดต่อไปยังเว็บไซต์ docusign.sa[.]com/verification/c.php และโหลดหน้าเว็บใหม่เพื่อแสดงเนื้อหาจาก docusign.sa[.]com/verification/s.php?an=1

หลังจากนั้นจะมีการส่ง **สคริปต์ PowerShell ขั้นที่สอง** ซึ่งจะดาวน์โหลด **ไฟล์ ZIP** จากเซิร์ฟเวอร์เดิม โดยใช้ **ค่าพารามิเตอร์ใน URL (an=2)** เมื่อแตกไฟล์ ZIP แล้ว จะมีการเรียกใช้ไฟล์ jp2launcher.exe ซึ่งเป็น **ขั้นตอนสุดท้าย** ที่นำไปสู่การติดตั้ง NetSupport RAT ลงในระบบ

การใช้ลำดับขั้นตอนแบบหลายชั้นในการดาวน์โหลดและเรียกใช้สคริปต์ เป็นความพยายามเพื่อ หลีกเลี่ยงการตรวจจับจากซอฟต์แวร์ความปลอดภัย เพิ่มความยืดหยุ่นต่อการตรวจสอบหรือการถูกปิดกั้น

คำแนะนำ (Recommendation)

- อย่าเรียกใช้คำสั่งจากเว็บไซต์ที่ไม่น่าเชื่อถือ
- ระวังเว็บไซต์ที่ขอให้ทำ CAPTCHA แล้วให้กด Win + R หรือ Ctrl + V
- อัปเดตซอฟต์แวร์ป้องกันไวรัสและเปิดใช้ระบบป้องกันแบบ Real-time

ข้อมูลอ้างอิง

- https://thehackernews.com/2025/06/fake-docusign-gitcode-sites-spread.html