ประจำวันอังคารที่ 4 ตุลาคม 2565

กลุ่ม Witchetty APT ใช้ Steganography ในการโจมตีหน่วยงานในตะวันออกกลาง

ทีม Symantec Threat Hunter ของ Broadcom ได้สังเกตเห็นกลุ่มจารกรรมทางไซเบอร์ชื่อ Witchetty ใช้ Steganography เพื่อซ่อนแบ็คดอร์ที่ไม่มีเอกสารในโลโก้ Windows โดยกลุ่มนี้ใช้แบ็คดอร์ในการโจมตีรัฐบาลตะวันออกกลาง

กลุ่มจารกรรมทางไซเบอร์ Witchetty หรือที่รู้จักในชื่อ LookFrog ได้ถูกพบครั้งแรกโดยบริษัทรักษาความปลอดภัยทางไซเบอร์ ESET เมื่อเดือนเมษายน 2022 ซึ่งผู้เชี่ยวชาญยืนยันว่าเป็นกลุ่มย่อยของกลุ่ม TA410 ที่มีความเชื่อมโยงกับจีน (aka APT10, Cicada, Stone Panda และ TA429) โดยกลุ่ม APT ได้ปรับปรุงชุดเครื่องมือเพื่อใช้มัลแวร์ใหม่ในการโจมตีซึ่งมุ่งเป้าไปที่รัฐบาล ภารกิจทางการทูต องค์กรการกุศล และองค์กรอุตสาหกรรม/การผลิตในตะวันออกกลางและแอฟริกา

การทำงานของ Witchetty มีลักษณะเฉพาะโดยใช้มัลแวร์สองขั้นตอน ได้แก่ แบ็คดอร์ขั้นแรกชื่อว่า X4 และมัลแวร์ modular ขั้นที่สองที่ชื่อ LookBack โดยผู้โจมตีใช้ประโยชน์จาก ProxyShell (CVE-2021-34473 , CVE-2021-34523 และ CVE-2021-31207) และ ProxyLogon (CVE-2021-26855 และ CVE-2021-26855) เป็นช่องโหว่ในการปรับใช้เว็บเชลล์บนเซิร์ฟเวอร์สาธารณะก่อนที่จะดำเนินการที่เป็นอันตราย เช่น การขโมยข้อมูลประจำตัว การย้ายข้ามเครือข่ายในแนวขวาง และปล่อยเพย์โหลดที่เป็นอันตรายเพิ่มเติม

โดยการโจมตีเมื่อเร็วๆ นี้ กลุ่มผู้โจมตีได้ใช้ implant track ที่ทำให้ตรวจไม่พบในชื่อ Backdoor.Stegmap เพื่อปกปิดข้อมูลที่เป็นอันตรายในภาพ bitmap ของโลโก้ Microsoft Windows เก่าที่โฮสต์บนที่เก็บ GitHub การซ่อนรหัสที่เป็นอันตรายภายในภาพที่โฮสต์บนบริการที่เชื่อถือได้ทำให้ผู้โจมตีสามารถหลบเลี่ยงการตรวจจับได้

ที่มาของข่าว : https://securityaffairs.co/wordpress/136477/apt/witchetty-apt-steganography.html