วันที่ 1 กันยายน 2568

Transparent Tribe ใช้ไฟล์ช็อตคัตบนเดสก์ท็อปโจมตีหน่วยงานรัฐบาลอินเดียผ่านการฟิชชิ่ง

นักวิจัยด้านความปลอดภัยไซเบอร์ได้ออกมาเตือนเกี่ยวกับกลุ่มผู้โจมตีขั้นสูง (APT) ที่รู้จักกันในชื่อ Transparent Tribe ซึ่งพบว่ากำลังโจมตีทั้งระบบปฏิบัติการ Windows และ BOSS (Bharat Operating System Solutions) Linux ด้วยไฟล์ช็อตคัตอันตราย โดยมีเป้าหมายคือหน่วยงานรัฐบาลของอินเดีย

“การเข้าถึงครั้งแรกเกิดขึ้นผ่านอีเมลฟิชชิ่งแบบเจาะจงตัวบุคคล” บริษัท CYFIRMA ระบุ “สภาพแวดล้อมที่ใช้ Linux BOSS จะถูกโจมตีผ่านไฟล์ช็อตคัต .desktop ที่ถูกฝังโค้ดอันตราย เมื่อเปิดขึ้นมาจะดาวน์โหลดและรันเพย์โหลดอันตราย”

Transparent Tribe หรือที่รู้จักอีกชื่อว่า APT36 ถูกประเมินว่ามีต้นกำเนิดจากปากีสถาน กลุ่มนี้รวมถึงกลุ่มย่อยชื่อ SideCopy มีประวัติยาวนานในการเจาะเข้าไปในหน่วยงานรัฐบาลอินเดียด้วยมัลแวร์ประเภท Remote Access Trojan (RATs) ที่หลากหลาย ความสามารถในการโจมตีข้ามแพลตฟอร์มในครั้งนี้แสดงให้เห็นถึงความซับซ้อนที่เพิ่มขึ้นของกลุ่ม ทำให้พวกเขาสามารถขยายการโจมตีและมั่นใจได้ว่าจะเข้าถึงเครื่องเป้าหมายที่ถูกบุกรุกได้มากขึ้น

กลไกการโจมตีและมัลแวร์ Poseidon

ขั้นตอนการโจมตีเริ่มจากอีเมลฟิชชิ่งที่แนบไฟล์ซึ่งทำทีว่าเป็นหนังสือเชิญประชุม แต่จริงๆ แล้วเป็นไฟล์ช็อตคัตของ Linux (“Meeting_Ltr_ID1543ops.pdf.desktop”) ไฟล์เหล่านี้ถูกทำให้ดูเหมือนเป็นไฟล์ PDF เพื่อหลอกให้เหยื่อเปิดใช้งาน และเมื่อเปิดขึ้นมาก็จะรัน สคริปต์เชลล์ ทันที

สคริปต์เชลล์ทำหน้าที่เป็น ดรอปเปอร์ โดยไปดาวน์โหลดไฟล์ที่ถูกเข้ารหัสแบบ hex จากเซิร์ฟเวอร์ที่ผู้โจมตีควบคุม (securestore[.]cv) และบันทึกเป็นไฟล์ ELF binary ลงในเครื่อง ขณะเดียวกันก็เปิดไฟล์ PDF หลอกที่เก็บไว้บน Google Drive ผ่าน Firefox เพื่อเบี่ยงความสนใจ จากนั้นตัวไฟล์ ELF ที่ถูกพัฒนาด้วยภาษา Go จะเชื่อมต่อกับเซิร์ฟเวอร์สั่งการ (C2) ที่ถูกฝังไว้ล่วงหน้า (modgovindia[.]space:4000) เพื่อรับคำสั่ง ดาวน์โหลดเพย์โหลดเพิ่มเติม และขโมยข้อมูล มัลแวร์ยังตั้งค่าให้ทำงานซ้ำได้โดยการเพิ่ม cron job เพื่อให้รันเพย์โหลดหลักโดยอัตโนมัติทุกครั้งที่รีบูตระบบหรือเมื่อกระบวนการถูกปิด

บริษัท CloudSEK ที่ตรวจสอบเหตุการณ์นี้เช่นกันรายงานว่า มัลแวร์สามารถเก็บข้อมูลระบบ และยังใส่เทคนิคตบตา เช่น ตรวจจับการดีบักหรือการรันใน sandbox เพื่อหลอกการวิเคราะห์แบบอัตโนมัติ นอกจากนี้ ผลการวิเคราะห์จาก Hunt.io ยังเผยว่า การโจมตีครั้งนี้มีเป้าหมายเพื่อปล่อยแบ็กดอร์ที่กลุ่ม Transparent Tribe ใช้มานานแล้วชื่อ Poseidon ซึ่งช่วยให้ขโมยข้อมูล เข้าถึงระบบในระยะยาว เก็บรหัสผ่าน และอาจเคลื่อนย้ายไปยังระบบอื่นๆ ได้

เทคนิคฟิชชิ่งและการเลียนแบบระบบรัฐบาล

“ความสามารถของ APT36 ที่ปรับกลไกการส่งมัลแวร์ตามระบบปฏิบัติการของเหยื่อ ทำให้โอกาสในการโจมตีสำเร็จสูงขึ้น ขณะเดียวกันก็ยังคงเข้าถึงระบบสำคัญของรัฐบาลได้อย่างต่อเนื่อง และหลบเลี่ยงการตรวจจับแบบเดิมๆ ได้” CYFIRMA กล่าว

การเปิดเผยครั้งนี้เกิดขึ้นไม่กี่สัปดาห์หลังจาก Transparent Tribe ถูกพบว่าโจมตีองค์กรด้านกลาโหมและหน่วยงานรัฐบาลอินเดีย โดยใช้โดเมนปลอมเพื่อขโมยบัญชีผู้ใช้และรหัสยืนยันตัวตนสองขั้นตอน (2FA) ซึ่งคาดว่าผู้ใช้จะถูกล่อให้กดลิงก์ผ่านอีเมลฟิชชิ่ง

“เมื่อผู้ใช้กรอกอีเมลที่ถูกต้องในหน้าฟิชชิ่งแรกและกด ‘Next’ จะถูกเปลี่ยนหน้าไปยังอีกเพจหนึ่งที่หลอกให้กรอกรหัสผ่านอีเมลและรหัสยืนยัน Kavach” CYFIRMA กล่าว ควรสังเกตว่า การเจาะระบบเพื่อขโมยรหัสยืนยัน Kavach ซึ่งเป็นระบบ 2FA ของหน่วยงานรัฐบาลอินเดีย เป็นเทคนิคที่ Transparent Tribe และ SideCopy ใช้มาอย่างต่อเนื่องตั้งแต่ต้นปี 2022

“การใช้โดเมนที่สะกดใกล้เคียงกับของจริง รวมถึงโครงสร้างพื้นฐานที่โฮสต์บนเซิร์ฟเวอร์ในปากีสถานนั้น สอดคล้องกับวิธีการที่กลุ่มนี้ใช้มาโดยตลอด” บริษัทกล่าวเสริม

นอกจากนี้ ยังมีการค้นพบอีกแคมเปญหนึ่งโดยกลุ่ม APT ในเอเชียใต้ที่โจมตีบังกลาเทศ, เนปาล, ปากีสถาน, ศรีลังกา และตุรกี ผ่านอีเมลฟิชชิ่งที่ออกแบบมาเพื่อขโมยข้อมูลบัญชี โดยใช้หน้าเว็บเลียนแบบที่โฮสต์บน Netlify และ Pages.dev

“การโจมตีเหล่านี้ปลอมตัวเป็นการสื่อสารอย่างเป็นทางการเพื่อหลอกให้เหยื่อกรอกรหัสผ่านในหน้าเข้าสู่ระบบปลอม” Hunt.io กล่าว “หน้า Zimbra และ Secure Portal ปลอมเหล่านี้ถูกทำให้เหมือนกับระบบอีเมลภาครัฐ บริการแชร์ไฟล์ หรือระบบอัปโหลดเอกสารอย่างเป็นทางการ เพื่อหลอกให้เหยื่อกรอกข้อมูลผ่านช่องเข้าสู่ระบบปลอม”

ข้อมูลอ้างอิง

Aug 25, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/08/transparent-tribe-targets-indian-govt.html