วันที่ 17 ตุลาคม 2568

มัลแวร์ธนาคาร Astaroth ใช้ประโยชน์จาก GitHub เพื่อคงการทำงานต่อได้หลังถูกปิดระบบ

นักวิจัยด้านความปลอดภัยทางไซเบอร์ได้ออกมาเตือนถึงแคมเปญใหม่ที่แพร่กระจาย ‘มัลแวร์ธนาคารชื่อ Astaroth’ ซึ่งสร้างความกังวลอย่างยิ่ง เนื่องจากมันใช้ GitHub เป็นโครงสร้างพื้นฐานหลักในการดำเนินงาน กลยุทธ์นี้ทำให้มัลแวร์สามารถคงการทำงานได้ แม้ถูกเจ้าหน้าที่หรือผู้เชี่ยวชาญด้านความปลอดภัยปิดระบบเซิร์ฟเวอร์หลักลงก็ตาม

Harshil Patel และ Prabudh Chakravorty นักวิจัยจาก McAfee Labs กล่าวในรายงานว่า “แทนที่จะพึ่งพาเพียงเซิร์ฟเวอร์ Command-and-Control (C2) แบบเดิมที่สามารถถูกปิดได้ง่าย กลุ่มผู้โจมตีเลือกใช้ GitHub ในการโฮสต์ค่าการตั้งค่าของมัลแวร์แทน” พวกเขาย้ำว่า “เมื่อโครงสร้างพื้นฐาน C2 ถูกปิดโดยเจ้าหน้าที่หรือผู้เชี่ยวชาญ Astaroth ก็สามารถดึงค่าการตั้งค่าใหม่จาก GitHub และทำงานต่อได้ทันที”

เป้าหมายหลัก: ละตินอเมริกาโดยเฉพาะบราซิล

กิจกรรมดังกล่าวของ Astaroth มุ่งเป้าไปที่ประเทศบราซิลเป็นหลัก ซึ่งสอดคล้องกับพฤติกรรมในอดีต แม้ว่ามัลแวร์ธนาคารชนิดนี้จะเคยแพร่กระจายไปยังประเทศต่าง ๆ ในละตินอเมริกา เช่น เม็กซิโก อุรุกวัย อาร์เจนตินา ปารากวัย ชิลี โบลิเวีย เปรู เอกวาดอร์ โคลอมเบีย เวเนซุเอลา และปานามา

นี่ไม่ใช่ครั้งแรกที่ Astaroth มุ่งเป้าไปยังบราซิล ก่อนหน้านี้ในเดือนกรกฎาคมและตุลาคม 2024 ทั้ง Google และ Trend Micro เคยเตือนถึงกลุ่มแฮ็กเกอร์ที่ใช้ชื่อว่า PINEAPPLE และ Water Makara ซึ่งส่งมัลแวร์ผ่านอีเมลฟิชชิ่ง

เส้นทางติดเชื้อ: จาก DocuSign ปลอมสู่ System Shell

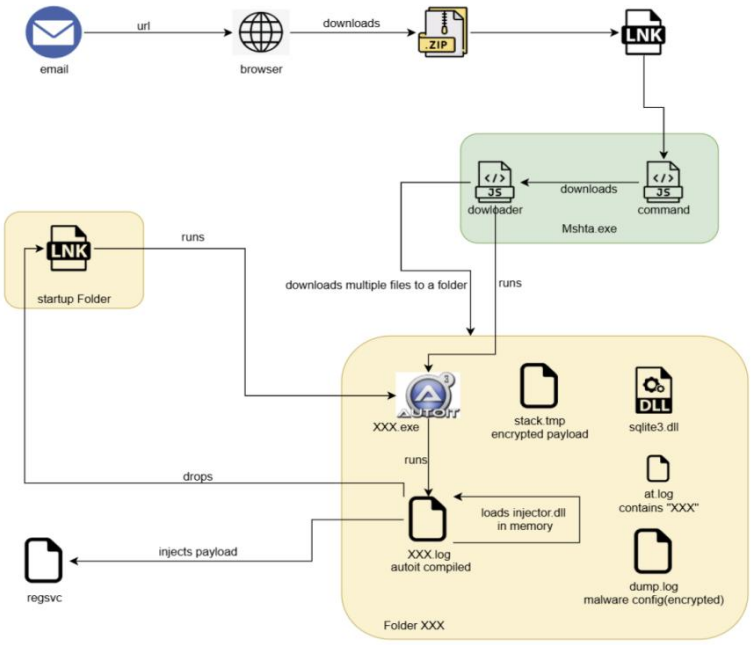
แคมเปญล่าสุดใช้วิธีคล้ายกัน โดยเริ่มจากอีเมลฟิชชิ่งที่ปลอมเป็นข้อความจาก DocuSign ซึ่งมีลิงก์ให้ดาวน์โหลดไฟล์ ZIP ที่ภายในมี ไฟล์ทางลัด Windows (.lnk) เมื่อเหยื่อเปิดไฟล์นี้ กระบวนการติดตั้ง Astaroth จะเริ่มต้นขึ้น:

1. ไฟล์ .LNK มีโค้ด JavaScript ที่ถูกทำให้ซับซ้อน (obfuscated)
2. โค้ดจะดาวน์โหลดโค้ด JavaScript เพิ่มเติมจากเซิร์ฟเวอร์ภายนอก
3. โค้ดที่ดาวน์โหลดมาจะสั่งให้โหลดไฟล์หลายไฟล์จากเซิร์ฟเวอร์ที่ถูกสุ่มเลือก ซึ่งรวมถึงสคริปต์ AutoIt
4. สคริปต์ AutoIt จะถูกรันต่อโดยโค้ด JavaScript
5. จากนั้นจะโหลดและรัน shellcode ซึ่งจะนำไปสู่การโหลด DLL ที่เขียนด้วย Delphi เพื่อถอดรหัสและฉีดมัลแวร์ Astaroth เข้าไปในโปรเซส RegSvc.exe ที่ถูกสร้างขึ้นใหม่

Astaroth: มัลแวร์ Delphi ที่จ้องขโมยข้อมูลธนาคาร

Astaroth เป็นมัลแวร์ที่พัฒนาโดยใช้ภาษา Delphi ออกแบบมาเพื่อดักจับข้อมูลขณะเหยื่อเข้าใช้งานเว็บไซต์ธนาคารหรือคริปโทเคอร์เรนซี และขโมยข้อมูลเข้าสู่ระบบผ่านการบันทึกคีย์ (keylogging) ข้อมูลที่ได้จะถูกส่งกลับไปยังผู้โจมตีผ่านบริการพร็อกซีแบบย้อนกลับชื่อ Ngrok

มัลแวร์จะตรวจสอบหน้าต่างโปรแกรมเบราว์เซอร์ที่กำลังใช้งานอยู่ ทุกวินาที และหากพบว่าเป็นเว็บไซต์ที่เกี่ยวข้องกับธนาคาร มันจะเริ่มบันทึกการกดแป้นพิมพ์ทันที



เว็บไซต์เป้าหมายหลัก ได้แก่:

- **ธนาคาร/การเงิน:** caixa.gov[.]br, safra.com[.]br, itau.com[.]br, bancooriginal.com[.]br, santandernet.com[.]br, btgpactual[.]com

- **คริปโทเคอร์เรนซี:** etherscan[.]io, binance[.]com, bitcointrade.com[.]br, metamask[.]io, foxbit.com[.]br, localbitcoins[.]com

การซ่อนตัวใน GitHub และการป้องกันการวิเคราะห์

นี่คือหัวใจสำคัญของแคมเปญ:

- คงอยู่ในระบบ: มัลแวร์จะสร้างความคงอยู่ในระบบโดยวางไฟล์ .LNK ไว้ในโฟลเดอร์ Startup ของ Windows เพื่อให้สคริปต์ AutoIt ถูกเรียกใช้อัตโนมัติเมื่อเครื่องรีบูต
- Steganography บน GitHub: McAfee ระบุว่า “Astaroth ใช้ GitHub ในการอัปเดตค่าการตั้งค่าเมื่อเซิร์ฟเวอร์ C2 ไม่สามารถเข้าถึงได้ โดยซ่อนข้อมูลเหล่านี้ไว้ในภาพที่อัปโหลดบน GitHub ผ่าน เทคนิคการซ่อนข้อมูล (steganography)” ด้วยวิธีนี้มัลแวร์จึงใช้แพลตฟอร์มที่ถูกต้องตามกฎหมายเป็นพื้นที่สำรองในการเก็บค่าการตั้งค่า ทำให้ระบบยังทำงานได้แม้โครงสร้างหลักจะถูกปิด
- การต่อต้านการวิเคราะห์: Astaroth จะปิดการทำงานทันทีหากตรวจพบว่าอยู่ในสภาพแวดล้อมของ emulator หรือเครื่องมือวิเคราะห์ เช่น QEMU Guest Agent, HookExplorer, IDA Pro, ImmunityDebugger, PE Tools, WinDbg และ Wireshark
- การจำกัดพื้นที่: URL ที่ถูกเรียกจาก JavaScript ภายในไฟล์ .LNK ยังถูกจำกัดให้ใช้งานได้เฉพาะในพื้นที่ที่กำหนด และมัลแวร์ยังตรวจสอบไม่ให้ทำงานบนเครื่องที่ตั้งค่าภาษาเป็นภาษาอังกฤษหรืออยู่ในภูมิภาคสหรัฐฯ

บริษัท McAfee กล่าวเพิ่มเติมว่า ได้ร่วมมือกับ GitHub ซึ่งเป็นบริษัทในเครือของ Microsoft เพื่อลบ repository เหล่านั้นออก ช่วยยุติการทำงานของแคมเปญนี้ได้ชั่วคราว แต่ผู้ใช้ยังคงต้องระมัดระวังอีเมลฟิชชิ่งที่ปลอมแปลงมาในรูปแบบเอกสารสำคัญอย่าง DocuSign อย่างเข้มงวดต่อไป

ข้อมูลอ้างอิง

Oct 13, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/10/astaroth-banking-trojan-abuses-github.html