วันที่ 1 เมษายน 2569

Silver Fox ขยายแคมเปญโจมตีไซเบอร์ในเอเชีย ใช้ AtlasCross RAT และโดเมนปลอม

ผู้ใช้งานที่ใช้ภาษาจีนกำลังตกเป็นเป้าหมายหลักในแคมเปญการโจมตีที่ยังคงดำเนินอยู่ โดยกลุ่มผู้โจมตีได้ใช้วิธี Typosquatting เพื่อปลอมตัวเป็นซอฟต์แวร์แบรนด์ดัง และใช้เป็นช่องทางในการปล่อยโทรจันควบคุมเครื่องระยะไกล ตัวใหม่ที่ไม่เคยถูกค้นพบมาก่อนชื่อ "AtlasCross RAT" บริษัทความปลอดภัยทางไซเบอร์จากเยอรมนี Hexastrike ระบุในรายงานว่า ปฏิบัติการครั้งนี้ครอบคลุมซอฟต์แวร์หลายประเภท เช่นโปรแกรม VPN แอปส่งข้อความแบบเข้ารหัส เครื่องมือประชุมออนไลน์ โปรแกรมติดตามคริปโต และแอปอีคอมเมิร์ซ โดยพบโดเมนที่ใช้แพร่มัลแวร์อย่างน้อย 11 โดเมน ซึ่งปลอมเป็นแบรนด์ดัง เช่น Surfshark VPN, Signal, Telegram, Zoom และ Microsoft Teams

เบื้องหลังการโจมตีจากกลุ่ม Silver Fox

กิจกรรมทั้งหมดนี้ถูกเชื่อมโยงกับกลุ่มอาชญากรไซเบอร์จากประเทศจีนที่ชื่อว่า Silver Fox ซึ่งยังถูกติดตามภายใต้ชื่ออื่นๆ เช่น SwimSnake, The Great Thief of Valley (หรือ Valley Thief), UTG-Q-1000 และ Void Arachne ทาง Knownsec 404 บริษัทความปลอดภัยจีน Knownsec 404 ระบุว่า Silver Fox เป็นหนึ่งในภัยคุกคามไซเบอร์ที่เคลื่อนไหวมากที่สุดในช่วงไม่กี่ปีที่ผ่านมา โดยมักโจมตีพนักงานระดับผู้จัดการและฝ่ายการเงินผ่าน WeChat, QQ อีเมลฟิชชิง และเว็บไซต์เครื่องมือปลอม เป้าหมายของการติดมัลแวร์คือเพื่อให้ผู้โจมตีสามารถควบคุมเครื่องจากระยะไกล ขโมยข้อมูลสำคัญ และดำเนินการฉ้อโกงทางการเงิน การพบ AtlasCross RAT ครั้งนี้แสดงให้เห็นว่ากลุ่มผู้โจมตีได้พัฒนาเครื่องมือของตนจากตระกูล Gh0st RAT เดิม เช่น ValleyRAT (หรือ Winos 4.0), Gh0stCringe และ HoldingHands RAT (หรือ Gh0stBins)

ขั้นตอนการทำงานแนบเนียนผ่านเว็บไซต์ปลอม

การโจมตีมีการวางแผนมาอย่างเป็นระบบ เริ่มต้นจากการหลอกให้เหยื่อดาวน์โหลดไฟล์ ZIP จากเว็บไซต์ปลอม ซึ่งแท้จริงแล้วแฝงมัลแวร์ไว้ โดยตัวติดตั้งจะปล่อยไฟล์โปรแกรมของ Autodesk ถูกดัดแปลง พร้อมกับแอปตัวจริงที่ใช้เป็นตัวหลอก ตัวติดตั้ง Autodesk ที่ถูกฝังมัลแวร์จะเปิดตัวโหลดเชลล์โค้ด shellcode loader เพื่อถอดรหัสการตั้งค่าของ Gh0st RAT ที่ซ่อนอยู่ แล้วดึงข้อมูลเซิร์ฟเวอร์ควบคุม (C2) จากนั้นระบบจะทำการดาวน์โหลดเพย์โหลดระยะที่สองจากโดเมน bifa668[.]com ผ่านการเชื่อมต่อเครือข่าย TCP พอร์ต 9899 ก่อนจะรัน AtlasCross RAT ฝังลงในหน่วยความจำของเครื่องโดยตรง

นักวิจัยยังพบว่าเว็บไซต์ปลอมส่วนใหญ่ถูกจดทะเบียนภายในวันเดียวกัน คือวันที่ 27 ตุลาคม 2025 ซึ่งบ่งชี้ว่าการโจมตีครั้งนี้มีการวางแผนมาอย่างตั้งใจ

รายชื่อโดเมนที่ยืนยันแล้วว่าใช้กระจายมัลแวร์มีดังนี้

- app-zoom.com (Zoom)
- eyy-eyy.com (ไม่ทราบชื่อบริการ)
- kefubao-pc.com (KeFuBao ซอฟต์แวร์บริการลูกค้าอีคอมเมิร์ซของจีน)
- quickq-quickq.com (QuickQ VPN)
- signal-signal.com (Signal)
- telegrtam.com.cn (Telegram)
- trezor-trezor.com (Trezor)
- ultraviewer-cn.com (UltraViewer)
- wwtalk-app.com (WangWang)
- www-surfshark.com (Surfshark VPN)
- www-teams.com (Microsoft Teams)

ไฟล์ติดตั้งเหล่านี้จะใช้ใบรับรองดิจิทัลแบบ Extended Validation (EV) ที่ซึ่งออกให้กับบริษัท DUC FABULOUS CO., LTD ในกรุงฮานอย ประเทศเวียดนาม ทำให้มัลแวร์ดูเหมือนซอฟต์แวร์ที่เชื่อถือได้และหลบเลี่ยงการตรวจจับของระบบความปลอดภัย

ความสามารถทางเทคนิคที่อันตรายของมัลแวร์

Hexastrike อธิบายเพิ่มเติมว่า RAT ตัวนี้มีการฝังเฟรมเวิร์ก PowerChell ซึ่งเป็นเอนจินรันคำสั่ง PowerShell ที่เขียนด้วย C/C++ ทำให้สามารถฝัง .NET CLR ลงในโปรเซสของมัลแวร์ได้โดยตรง พร้อมทั้งปิดระบบป้องกันอย่าง AMSI, ETW, Constrained Language Mode และ ScriptBlock logging ก่อนจะรันคำสั่งต่างๆ การสื่อสารกับเซิร์ฟเวอร์ควบคุม (C2) ถูกเข้ารหัสด้วย ChaCha20 โดยใช้คีย์แบบสุ่มสำหรับแต่ละแพ็กเก็ต ซึ่งสร้างจากฮาร์ดแวร์ RNG เช่น

- ฉีด DLL เข้าไปในโปรเซสของ WeChat
- แฮกหรือยึดเซสชัน RDP
- ตัดการเชื่อมต่อระดับ TCP จากซอฟต์แวร์ความปลอดภัยของจีน เช่น 360 Safe, Huorong, Kingsoft และ QQ PC Manager
- จัดการไฟล์และรันคำสั่งเชลล์
- สร้าง Scheduled Task เพื่อให้มัลแวร์ทำงานต่อเนื่องในระบบ

Hexastrike ระบุเพิ่มเติมว่า AtlasAgent หรือ AtlasCross RATถือเป็นวิวัฒนาการล่าสุดของเครื่องมือในกลุ่มนี้ โดยยังคงใช้พื้นฐานโปรโตคอลของ Gh0st RAT แบบเดียวกับ ValleyRAT และ Winos 4.0 แต่มีการเพิ่มเฟรมเวิร์ก PowerChell และชุดเทคนิคหลบเลี่ยงระบบความปลอดภัยที่ซับซ้อนมากขึ้น

ผู้โจมตียังใช้หลายเทคนิคพร้อมกัน เช่น

- การสร้างโดเมนสะกดคล้ายของจริง (typosquatting)
- การยึดครองโดเมน
- การปรับแต่งหรือบิดเบือน DNS

ทั้งหมดนี้เพื่อสร้างภาพลักษณ์ว่าเป็นบริการที่ถูกต้องตามปกติ

แคมเปญโจมตีล่าสุดยังพบว่ากลุ่มนี้เปลี่ยนวิธีการหลายครั้ง เช่น

- ใช้ ValleyRAT ผ่านไฟล์ PDF อันตรายในอีเมลฟิชชิงที่โจมตีองค์กรในไต้หวัน
- ใช้เครื่องมือ RMM ของจีนชื่อ SyncFuture TSM ที่ตั้งค่าผิดพลาด

ปล่อยมัลแวร์ขโมยข้อมูลที่เขียนด้วย Python โดยปลอมเป็นแอป WhatsApp

การขยายเป้าหมายครอบคลุมทั่วเอเชีย

ตั้งแต่เดือนธันวาคม 2025 เป็นต้นมา การโจมตีได้ขยายไปยังองค์กรในญี่ปุ่น มาเลเซีย ฟิลิปปินส์ ไทย อินโดนีเซีย สิงคโปร์ และอินเดีย โดยก่อนหน้านี้พบการใช้เนื้อหาเรื่องภาษีหลอกผู้ใช้ในอินเดียให้ติดมัลแวร์ Blackmoon

บริษัทความปลอดภัย Sekoia กลุ่มนี้ใช้โมเดลสองแนวทาง คือเปิดแคมเปญโจมตีวงกว้างควบคู่กับปฏิบัติการที่ซับซ้อนกว่า โดยพัฒนาเครื่องมือของตนอย่างต่อเนื่อง อย่างไรก็ตาม แคมเปญที่ใช้เครื่องมือ RMM และมัลแวร์ขโมยข้อมูลแบบ Python ดูจะมีลักษณะใกล้เคียงกับอาชญากรรมไซเบอร์ทั่วไปมากกว่าปฏิบัติการระดับ APT

นอกจากนี้ ในช่วงสัปดาห์ที่ผ่านมา กลุ่มแฮกเกอร์ดังกล่าวยังถูกเชื่อมโยงกับแคมเปญ spear-phishing ที่ใช้เนื้อหาหลอกลวงเกี่ยวกับ

- การตรวจสอบการปฏิบัติตามกฎหมายภาษี
- การปรับเงินเดือน
- การเปลี่ยนตำแหน่งงาน
- แผนการถือหุ้นของพนักงาน

เพื่อเจาะจงโจมตีบริษัทผู้ผลิตในญี่ปุ่นและองค์กรธุรกิจอื่นๆ ด้วยมัลแวร์ ValleyRAT

บริษัท ESET ระบุว่า เมื่อ ValleyRAT ถูกติดตั้งสำเร็จ ผู้โจมตีจะสามารถควบคุมเครื่องจากระยะไกล ดึงข้อมูลสำคัญ เฝ้าติดตามพฤติกรรมผู้ใช้ และสร้างการคงอยู่ในระบบได้ ซึ่งทำให้ผู้โจมตีสามารถแทรกตัวลึกเข้าไปในเครือข่าย ขโมยข้อมูลลับ หรือเตรียมขั้นตอนการโจมตีเพิ่มเติมในอนาคตได้

ข้อมูลอ้างอิง

Mar 31, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/silver-fox-expands-asia-cyber-campaign.html