วันที่ 25 มิถุนายน 2568

Water Curse ใช้บัญชี GitHub 76 บัญชี เป็นฐานปล่อยมัลแวร์หลายขั้นตอน

นักวิจัยด้านความปลอดภัยไซเบอร์ได้เปิดโปงกลุ่มผู้ก่อภัยคุกคามหน้าใหม่ชื่อ Water Curse ที่กำลังใช้แพลตฟอร์ม GitHub เป็นช่องทางหลักในการแพร่กระจายมัลแวร์หลายขั้นตอนอย่างแนบเนียน

มัลแวร์ชุดนี้มีความสามารถร้ายกาจในการ ขโมยข้อมูลสำคัญ เช่น รหัสผ่าน, ข้อมูลเบราว์เซอร์, และโทเคนเซสชัน นอกจากนี้ยังเปิดช่องทางให้ผู้ไม่หวังดีสามารถ เข้าควบคุมระบบจากระยะไกล และ ฝังตัวเพื่อคงอยู่ในเครื่องเป้าหมายได้ยาวนาน ข้อมูลนี้อ้างอิงจากรายงานวิเคราะห์ล่าสุดของทีมวิจัย Trend Micro ซึ่งประกอบด้วย Jovit Samaniego, Aira Marcelo, Mohamed Fahmy และ Gabriel Nicoleta

กลยุทธ์การโจมตีของ Water Curse

แคมเปญที่มีลักษณะ "กว้างและต่อเนื่อง" นี้ถูกตรวจพบครั้งแรกเมื่อเดือนที่ผ่านมา โดยกลุ่มผู้ก่อเหตุได้สร้าง repository บน GitHub ที่ดูเหมือนเป็นเครื่องมือเจาะระบบทั่วไป แต่ซ่อน payload อันตรายไว้ภายในไฟล์ตั้งค่าโปรเจกต์ของ Visual Studio เช่น SMTP email bomber และ Sakura-RAT

ชุดเครื่องมือของ Water Curse ครอบคลุมหลายภาษาโปรแกรมและมีเครื่องมือหลากหลายประเภท สะท้อนถึงความสามารถด้านการพัฒนาที่รอบด้าน เพื่อใช้เจาะโจมตี ห่วงโซ่อุปทาน (supply chain) ผ่านมัลแวร์ขโมยข้อมูลซึ่งพรางตัวเป็นเครื่องมือสำหรับนักทดสอบระบบโดยเฉพาะ

เมื่อรันไฟล์ มัลแวร์จะเริ่มกระบวนการติดเชื้อหลายขั้นตอน โดยใช้สคริปต์ Visual Basic Script (VBS) และ PowerShell ที่ถูกเข้ารหัสอย่างซับซ้อน จากนั้นดาวน์โหลดไฟล์บีบอัดที่เข้ารหัส แตกไฟล์แอปพลิเคชันที่สร้างด้วย Electron และดำเนินการสอดแนมระบบอย่างละเอียด ทีมวิจัยกล่าวเสริม

นอกจากนี้ กลุ่มนี้ยังใช้เทคนิค ต่อต้านการดีบั๊ก ยกระดับสิทธิ์ผู้ใช้ และติดตั้งกลไกคงอยู่ในเครื่องเป้าหมาย รวมถึงใช้ PowerShell ปิดการป้องกันระบบและขัดขวางกระบวนการกู้คืนข้อมูล

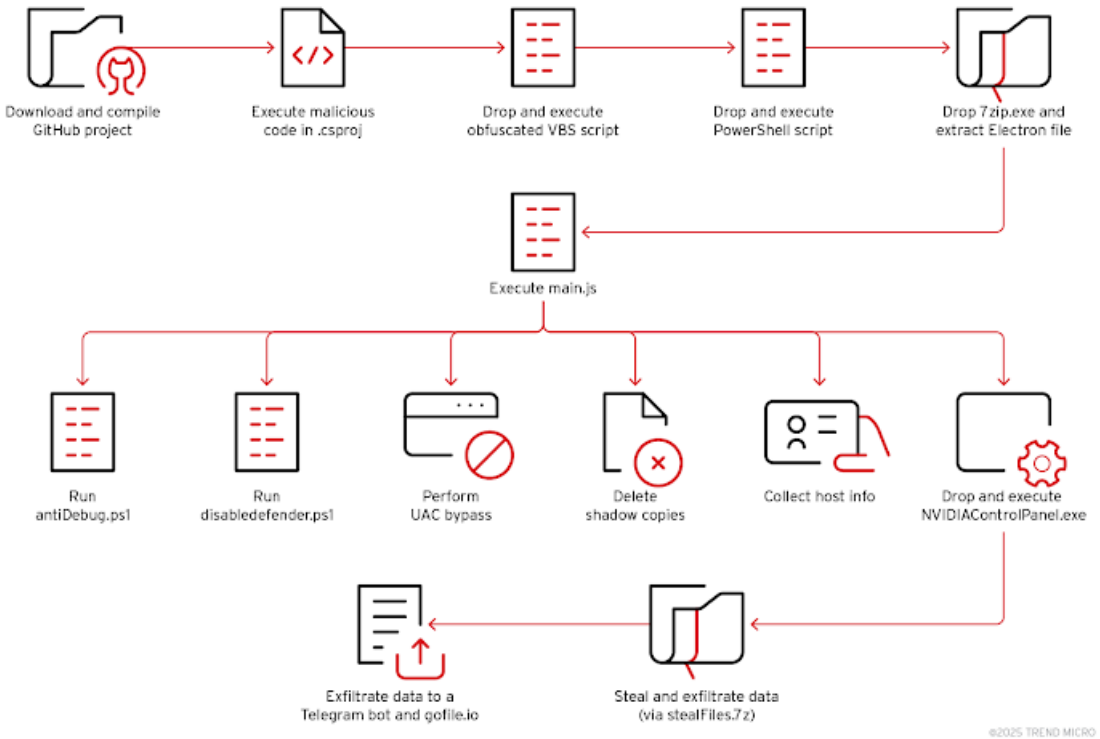
แรงจูงใจและการเชื่อมโยง

Water Curse ถูกจัดเป็นกลุ่มที่มี แรงจูงใจทางการเงิน มุ่งเน้นขโมยข้อมูลรับรอง, เก็บข้อมูลเซสชัน, และขายสิทธิ์เข้าถึงระบบที่ได้มาโดยมิชอบ ปัจจุบันพบว่ามีบัญชี GitHub ที่เชื่อมโยงกับแคมเปญนี้แล้วอย่างน้อย 76 บัญชี และมีหลักฐานบ่งชี้ว่ากิจกรรมอาจเริ่มมาตั้งแต่เดือนมีนาคม 2023

แม้ว่าการใช้ GitHub เพื่อกระจายมัลแวร์จะไม่ใช่เรื่องใหม่ แต่การสร้างเครือข่ายบัญชีเพื่อเผยแพร่ repository อันตรายลักษณะนี้ คล้ายกับวิธีการของบริการแจกมัลแวร์แบบ as-a-service ที่มีชื่อว่า Stargazers Ghost Network

ทาง Check Point Research ให้ข้อมูลกับ The Hacker News ว่า "ไม่สามารถยืนยันหรือปฏิเสธได้ว่ากิจกรรมเหล่านี้เกี่ยวข้องกับ Stargazers Ghost Network หรือไม่ เนื่องจากข้อมูลยังมีจำกัด" แต่ยอมรับว่าเทคนิคโจมตีแบบ <PreBuildEvent> เคยถูกใช้ในแคมเปญของ Stargazers Ghost Network มาก่อนหน้านี้แล้ว

การเกิดขึ้นของกลุ่ม Water Curse จึงถือเป็นอีกตัวอย่างที่สะท้อนถึงวิธีการที่แฮกเกอร์ใช้ประโยชน์จากความน่าเชื่อถือของแพลตฟอร์มชื่อดังอย่าง GitHub ในการแพร่กระจายมัลแวร์ และมุ่งโจมตีห่วงโซ่อุปทานของซอฟต์แวร์อย่างแยบยล

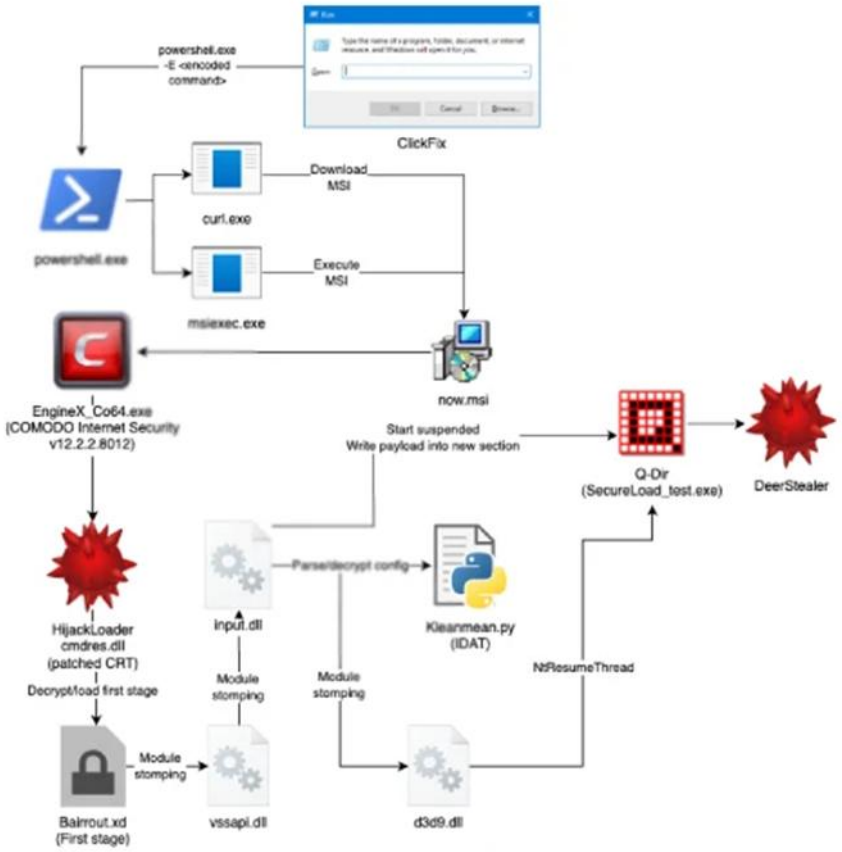


"Repository ของพวกเขาประกอบไปด้วยมัลแวร์, เครื่องมือหลบเลี่ยงการตรวจจับ, เครื่องมือจัดการกระเป๋าเงินคริปโต, โปรแกรมขูดข้อมูล OSINT, บอทสำหรับ spam และตัวขโมยรหัสผ่าน ซึ่งทั้งหมดนี้สะท้อนให้เห็นถึงกลยุทธ์โจมตีที่หลากหลายผสมผสานการโจมตีทางไซเบอร์กับการหาผลประโยชน์เชิงพาณิชย์แบบฉวยโอกาสได้อย่างแนบเนียน" Trend Micro ระบุ

"โครงสร้างพื้นฐานและพฤติกรรมของกลุ่มนี้บ่งชี้ชัดว่าเน้นการพรางตัว การทำงานแบบอัตโนมัติ และสามารถขยายการโจมตีได้ง่าย พร้อมกับมีช่องทางส่งออกข้อมูลที่ขโมยมาได้ผ่าน Telegram และบริการฝากไฟล์สาธารณะต่างๆ"

การโจมตีอื่นๆ ที่กำลังระบาด

การเปิดโปงครั้งนี้เกิดขึ้นในช่วงที่มีหลายแคมเปญเริ่มนำกลยุทธ์ ClickFix มาใช้ติดตั้งมัลแวร์หลากหลายตระกูล ไม่ว่าจะเป็น AsyncRAT, DeerStealer (ผ่าน Hijack Loader), Filch Stealer, LightPerlGirl และ SectopRAT



AsyncRAT ถือเป็นหนึ่งใน RAT (Remote Access Trojan) ที่หาได้ง่าย และถูกกลุ่มแฮกเกอร์นิรนามนำมาใช้โจมตีองค์กรนับพันแห่งทั่วโลกมาตั้งแต่ต้นปี 2024 โดยมีรายงานบางส่วนจาก Forcepoint ในเดือนสิงหาคม 2024 และมกราคม 2025

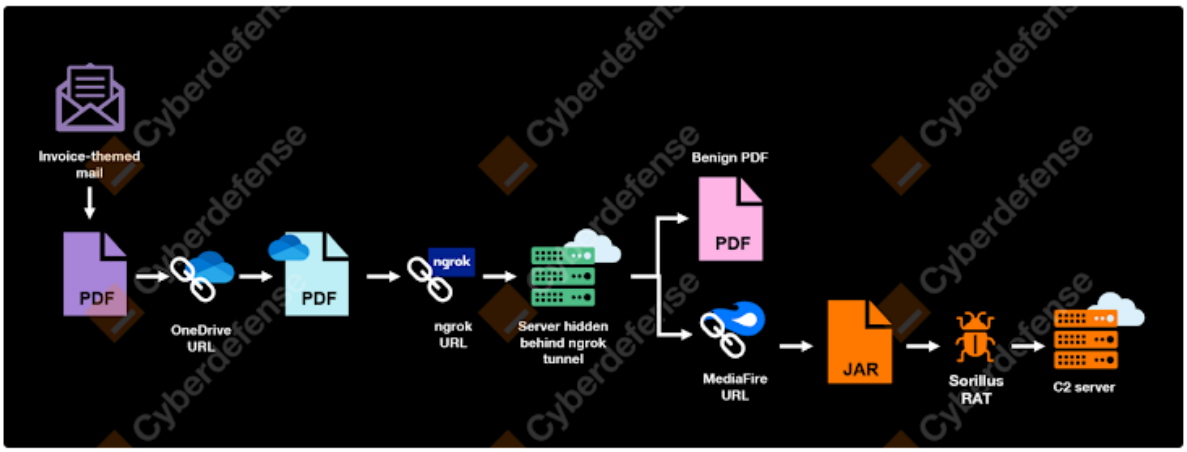
"กลวิธีนี้ช่วยให้มัลแวร์เลี่ยงระบบป้องกันรอบนอกได้ โดยอาศัยการสร้าง Cloudflare Temporary Tunnels เพื่อปล่อย payload ผ่านโครงสร้างพื้นฐานที่ดูน่าเชื่อถือ" Halcyon ระบุเพิ่มเติม "การสร้างโดเมนย่อยชั่วคราวซึ่งไม่มีข้อมูลทะเบียนล่วงหน้า ทำให้ระบบความปลอดภัยตรวจจับได้ยาก และป้องกันล่วงหน้าได้ยากยิ่งขึ้น" เนื่องจากโครงสร้างพื้นฐานนี้ถูกสร้างขึ้นแบบชั่วคราวผ่านบริการที่ถูกต้องตามกฎหมาย ฝ่ายป้องกันจึงตรวจสอบได้ยากว่าการใช้งานดังกล่าวเป็นงาน DevOps ปกติ หรือเป็นการรันมัลแวร์แฝง เทคนิคนี้จึงเปิดทางให้แฮกเกอร์ปล่อย payload ได้โดยไม่ต้องพึ่งพาเซิร์ฟเวอร์ที่ถูกแฮกหรือ hosting เถื่อน ทำให้สามารถขยายขอบเขตการโจมตีและพรางตัวได้อย่างมีประสิทธิภาพมากขึ้น

Sorillus RAT และ SambaSpy โจมตีองค์กรยุโรป

อีกหนึ่งแคมเปญที่น่ากังวล คือการส่งอีเมลปลอมในหัวข้อใบแจ้งหนี้ ไปยังองค์กรในสเปน, โปรตุเกส, อิตาลี, ฝรั่งเศส, เบลเยียม และเนเธอร์แลนด์ เพื่อใช้เป็นช่องทางติดตั้ง Sorillus RAT (หรือ Ratty RAT)

ก่อนหน้านี้ กลุ่มผู้โจมตีจะมุ่งเป้าไปที่นักบัญชีและที่ปรึกษาด้านภาษี โดยใช้เอกสารยื่นภาษีปลอม พร้อมใช้เทคนิค HTML smuggling เพื่อซ่อน payload ไม่ให้ถูกตรวจจับได้ง่าย

การโจมตีที่ Orange Cyberdefense พบในครั้งนี้ ใช้อีเมลแนบไฟล์ PDF ที่ฝังลิงก์ OneDrive เมื่อเหยื่อกดปุ่ม "เปิดเอกสาร" จะถูกพาไปยังเซิร์ฟเวอร์อันตราย ซึ่งทำหน้าที่เป็น Traffic Distribution System (TDS) เพื่อประเมินว่าเครื่องของเหยื่อเหมาะสมหรือไม่ หากผ่านเกณฑ์ ระบบจะเปิด PDF ปกติให้เหยื่อดูเพื่อไม่ให้สงสัย ขณะเดียวกันก็แอบดาวน์โหลดไฟล์ JAR เพื่อติดตั้ง Sorillus RAT ลงในเครื่องโดยไม่รู้ตัว



Sorillus RAT เป็นมัลแวร์แบบ Java ที่สามารถทำงานข้ามแพลตฟอร์ม ถูกค้นพบครั้งแรกในปี 2019 โดยมีความสามารถหลากหลาย ไม่ว่าจะเป็นการขโมยข้อมูล, ถ่ายโอนไฟล์, ถ่ายภาพหน้าจอ, บันทึกเสียง, ดักจับการพิมพ์คำสั่ง ไปจนถึงการถอนการติดตั้งตัวเอง อีกทั้งยังมีเวอร์ชันดัดแปลงวางขายตามเว็บใต้ดินอีกจำนวนมาก

การโจมตีนี้ยังมีความเชื่อมโยงกับการปล่อย SambaSpy ในอิตาลี ซึ่งจัดอยู่ในตระกูลเดียวกับ Sorillus โดย Orange Cyberdefense ระบุว่า "ปฏิบัติการนี้ใช้บริการจริง เช่น OneDrive, MediaFire รวมถึงแพลตฟอร์ม tunneling อย่าง Ngrok และ LocaltoNet เพื่อช่วยหลบเลี่ยงการตรวจจับ" นอกจากนี้ payload หลายชุดยังเขียนด้วยภาษาโปรตุเกสบราซิล ซึ่งบ่งชี้ได้ว่าผู้ก่อเหตุอาจเป็นกลุ่มที่ใช้ภาษาโปรตุเกสในบราซิล

ภัยคุกคามไซเบอร์ยังคงพัฒนาและปรับเปลี่ยนกลยุทธ์อย่างต่อเนื่อง การโจมตีผ่านแพลตฟอร์มที่น่าเชื่อถืออย่าง GitHub หรือการใช้บริการคลาวด์ทั่วไปเพื่อซ่อนตัว เป็นสัญญาณว่าองค์กรและผู้ใช้งานต้องเพิ่มความระมัดระวังและปรับปรุงมาตรการป้องกันให้ทันสมัยอยู่เสมอ

ข้อมูลอ้างอิง

Jun 18, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/06/water-curse-hijacks-76-github-accounts.html