วันที่ 10 มิถุนายน 2569

## กลุ่มแฮกเกอร์ที่มีความเชื่อมโยงกับรัสเซีย ใช้ช่องโหว่ WinRAR แพร่มัลแวร์ขโมยข้อมูลในยูเครน

แคมเปญโจมตีทางไซเบอร์ 2 รายการที่มีความเชื่อมโยงกับรัสเซีย ยังคงใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัยใน WinRAR เพื่อโจมตีองค์กรต่างๆ ในยูเครน แม้ว่าจะผ่านไปเกือบหนึ่งปีแล้วหลังจากที่มีการออกแพตช์แก้ไขช่องโหว่นี้

กิจกรรมดังกล่าวถูกระบุโดย Trend Micro ว่าเกี่ยวข้องกับกลุ่ม Earth Dahu (หรือที่รู้จักในชื่อGamaredon) และ SHADOW-EARTH-066 (หรือที่รู้จักในชื่อUAC-0226) โดยอาศัยการโจมตีผ่านช่องโหว่ CVE-2025-8088ซึ่งเป็นช่องโหว่ประเภท Path Traversal ที่เปิดโอกาสให้ผู้โจมตีสามารถเขียนไฟล์ออกไปนอกโฟลเดอร์ที่ใช้แตกไฟล์ได้ ผ่านการใช้ NTFS Alternate Data Streams (ADS) ช่องโหว่นี้ได้รับการแก้ไขโดยWinRAR ตั้งแต่เดือนกรกฎาคม 2025 แล้ว

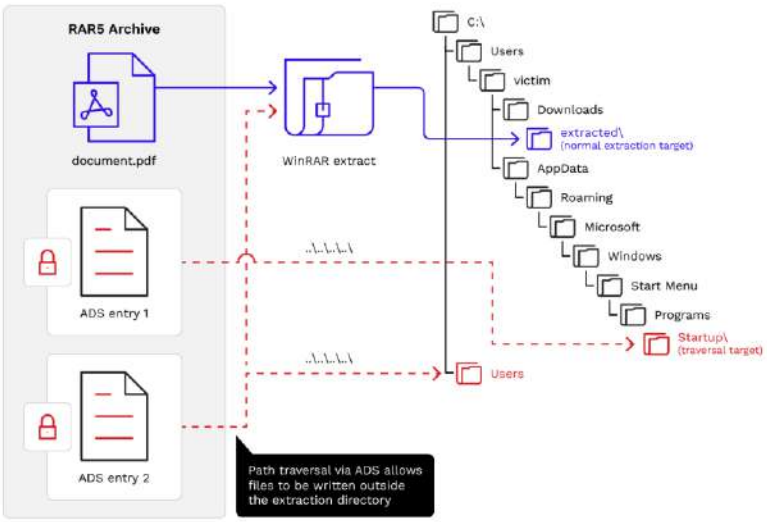
ผลการวิเคราะห์แสดงให้เห็นว่า ซอฟต์แวร์ที่ไม่ได้รับการอัปเดตยังคงเปิดช่องทางให้ผู้โจมตีใช้ประโยชน์ได้ต่อไป แม้ว่าจะมีการออกแพตช์แก้ไขแล้วก็ตาม นักวิจัยของ Trend Micro ได้แก่ Hiroyuki Kakara และ Feike Hacquebordกล่าวไว้ในรายงานที่เผยแพร่เมื่อวันจันทร์

### รูปแบบการโจมตีของกลุ่ม SHADOW-EARTH-066

รูปแบบการโจมตีผ่านช่องโหว่ WinRAR ที่ถูกใช้โดย SHADOW-EARTH-066 ถือเป็นการเปลี่ยนแปลงจากวิธีเดิมที่เคยใช้ไฟล์Excel ที่มีมาโครเป็นตัวปล่อยมัลแวร์ เพื่อส่งมัลแวร์ขโมยข้อมูลที่ชื่อ GIFTEDCROOK เวอร์ชันล่าสุดนี้ใช้ไฟล์RAR ที่ถูกสร้างขึ้นเป็นพิเศษ ภายในมีเอกสาร PDF ลวงตาและเพย์โหลด ADS ที่ซ่อนอยู่ 3 รายการ ซึ่งถูกวางไว้นอกโฟลเดอร์สำหรับแตกไฟล์ เพื่อเริ่มต้นกระบวนการติดเชื้อ

หนึ่งในไฟล์ดังกล่าวคือไฟล์ Windows Shortcut (LNK) ที่ถูกวางไว้ในโฟลเดอร์ Startup ทำให้ถูกเรียกใช้งานโดยอัตโนมัติทุกครั้งที่ผู้ใช้เข้าสู่ระบบ จากนั้นไฟล์ดังกล่าวจะเรียกใช้งาน PowerShell Loader ผ่าน "cmd.exe" ก่อนใช้เทคนิคโหลด DLL เข้าไปในหน่วยความจำโดยตรง เพื่อเปิดใช้งาน GIFTEDCROOK เวอร์ชันปรับปรุงใหม่ ("result.dll") ในที่สุด

มัลแวร์ตัวนี้มุ่งเป้าไปที่การขโมยรหัสผ่านและคุกกี้จากเบราว์เซอร์ที่ใช้ Chromium ได้แก่ Google Chrome, Microsoft Edge และ Opera รวมถึง Mozilla Firefox นอกจากนี้ยังรวบรวมเอกสารที่มีนามสกุลไฟล์ตามที่กำหนดจากเครื่องของเหยื่อด้วย หลังจากส่งข้อมูลออกไปยังเซิร์ฟเวอร์ภายนอกแล้ว ไฟล์และร่องรอยที่เป็นอันตรายทั้งหมดจะถูกลบออก เพื่อปกปิดหลักฐานการโจมตี




**การเปลี่ยนแปลงช่องทางการส่งข้อมูล**

อีกหนึ่งการเปลี่ยนแปลงที่น่าสนใจคือ การเปลี่ยนจากการใช้ Telegram เป็นช่องทางส่งข้อมูลที่ขโมยมา ไปสู่การใช้เซิร์ฟเวอร์ควบคุมและสั่งการ (C2) โดยเฉพาะ ซึ่งน่าจะสอดคล้องกับการที่รัสเซียสั่งบล็อกแพลตฟอร์ม Telegram ภายในประเทศเมื่อต้นเดือนกุมภาพันธ์ที่ผ่านมา

**กลยุทธ์การโจมตีของกลุ่ม Earth Dahu และมัลแวร์ตระกูล Gamma**

กลุ่มแฮกเกอร์ที่มีความเชื่อมโยงกับรัสเซียอีกกลุ่มหนึ่งที่นำ CVE-2025-8088 มาใช้ในการโจมตีคือ Earth Dahu โดยได้เพิ่มช่องโหว่นี้เข้าไปในชุดเครื่องมือของตนอย่างน้อยตั้งแต่เดือนกันยายน2025 กลุ่มดังกล่าวเป็นที่รู้จักจากความพยายามในระดับอุตสาหกรรมเพื่อรักษาการเข้าถึงองค์กรที่ถูกเจาะระบบไว้ในระยะยาว

"Earth Dahu ใช้ช่องโหว่นี้ร่วมกับกระบวนการติดเชื้อแบบ HTA-to-VBScriptเพื่อส่งมอบโมดูลจารกรรมข้อมูล" Trend Micro ระบุ "จากการวิเคราะห์เวลาที่บันทึกไว้ภายในไฟล์ RAR และรูปแบบการตั้งชื่อไฟล์ พบว่ากระบวนการโจมตีดังกล่าวยังคงถูกใช้งานอย่างต่อเนื่องอย่างน้อยจนถึงวันที่ 10เมษายน 2026"

การโจมตีเหล่านี้ ซึ่ง Sekoia ได้เผยแพร่รายละเอียดเพิ่มเติมไว้เมื่อสัปดาห์ที่ผ่านมา จะนำไปสู่การติดตั้ง GammaPhish ซึ่งเป็นไฟล์ประเภท HTML Application (HTA) จากนั้นจะถูกใช้เพื่อดาวน์โหลดตัวดาวน์โหลด VBScriptที่ชื่อ GammaLoad โดยจะทำหน้าที่ส่งมอบโมดูลเพิ่มเติม เช่น GammaSteel

Sekoia อธิบายว่า GammaLoad เป็น "ชุดของ VBScript ที่ถูกออกแบบมาเพื่อรักษาการเข้าถึงระบบอย่างต่อเนื่อง และทยอยส่งเพย์โหลดเพิ่มเติมในระยะยาวผ่านเทคนิค Dead Drop Resolver (DDR)" พร้อมระบุว่าเครื่องมือนี้ถูกใช้เพื่อติดตั้ง Dropperที่ออกแบบมาให้เรียกใช้งาน VBScript Loader ซึ่งมีหน้าที่เปิดใช้งานGammaSteel มัลแวร์ขโมยข้อมูลที่มีความสามารถหลากหลาย และสามารถเฝ้าติดตามการเปลี่ยนแปลงของไฟล์ต่าง ๆ ได้แบบเรียลไทม์

**บทสรุปและผลกระทบ**

WinRAR เป็นซอฟต์แวร์ที่ถูกใช้งานอย่างแพร่หลายในงานประจำวันขององค์กรต่างๆ ในยูเครน จึงกลายเป็นเป้าหมายที่น่าสนใจสำหรับการโจมตีผ่านช่องโหว่ Trend Micro กล่าว

การที่ทั้งกลุ่มที่ได้รับการสนับสนุนจากรัฐและกลุ่มที่ถูกติดตามแยกกัน ต่างหันมาใช้ช่องโหว่เดียวกัน สะท้อนให้เห็นถึงขนาดและความรุนแรงของภัยคุกคามทางไซเบอร์ที่ยูเครนกำลังเผชิญอยู่

**ข้อมูลอ้างอิง**

Jun 9, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/winrar-flaw-exploited-by-russia-aligned.html