วันที่ 6 พฤศจิกายน 2568

กลุ่มแฮ็กเกอร์ที่เชื่อมโยงกับจีนถูกเชื่อมโยงกับชุดการโจมตีใหม่ที่ใช้ช่องโหว่ในไฟล์ชอร์ตคัตของวินโดวส์

กลุ่มแฮ็กเกอร์ที่เชื่อมโยงกับจีนและเป็นที่รู้จักภายใต้ชื่อ UNC6384 ถูกเชื่อมโยงกับชุดการโจมตีใหม่ที่น่ากังวล โดยใช้ช่องโหว่ในไฟล์ชอร์ตคัตของวินโดวส์ (.LNK) ที่ยังไม่ได้รับการแพตช์ เพื่อมุ่งเป้าไปที่หน่วยงานทางการทูตและรัฐบาลในยุโรป ระหว่างเดือนกันยายนถึงตุลาคม 2025

กิจกรรมนี้มุ่งเป้าไปยังองค์กรทางการทูตใน ฮังการี, เบลเยียม, อิตาลี, และเนเธอร์แลนด์ รวมถึงหน่วยงานรัฐบาลใน เซอร์เบีย ซึ่งเป็นเป้าหมายที่สอดคล้องกับความต้องการข่าวกรองเชิงกลยุทธ์ของสาธารณรัฐประชาชนจีนเกี่ยวกับความเป็นเอกภาพของพันธมิตรยุโรป โครงการด้านการป้องกันและกลไกการประสานนโยบาย ตามรายงานของบริษัทความปลอดภัย Arctic Wolf

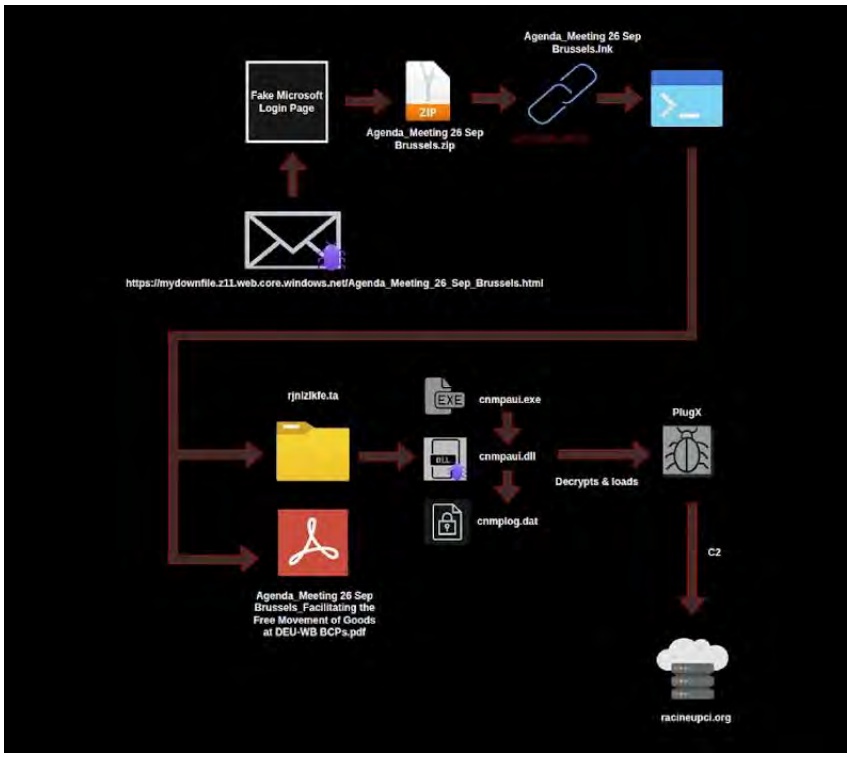
กลยุทธ์การโจมตี: Spear-Phishing & LNK Zero-Day

ห่วงโซ่การโจมตีเริ่มต้นจากอีเมลฟิชชิงแบบเจาะจง (spear-phishing) ที่มี URL ฝังอยู่ ซึ่งเป็นขั้นตอนแรกจากหลายขั้นตอนที่นำไปสู่การส่งไฟล์ LNK ที่เป็นอันตราย โดยมักอ้างอิงหัวข้อที่น่าสนใจเกี่ยวกับความร่วมมือระหว่างประเทศ เช่น การประชุมของคณะกรรมาธิการยุโรป, เวิร์กช็อปที่เกี่ยวกับนาโต้, และกิจกรรมการประสานงานทางการทูตพหุภาคี

การใช้ช่องโหว่ ZDI-CAN-25373

ไฟล์ LNK เหล่านี้ถูกออกแบบมาเพื่อใช้ประโยชน์จากช่องโหว่ ZDI-CAN-25373 (ซึ่งถูกติดตามอย่างเป็นทางการในชื่อ CVE-2025-9491 คะแนน CVSS: 7.0) เพื่อกระตุ้นห่วงโซ่การโจมตีหลายขั้นตอนซึ่งลงท้ายด้วยการติดตั้งมัลแวร์ PlugX โดยใช้วิธี DLL side-loading

- ประวัติช่องโหว่: ช่องโหว่นี้ถูกนำไปใช้โดยกลุ่มผู้โจมตีหลายรายตั้งแต่ปี 2017 ในการสั่งงานที่ซ่อนอยู่บนเครื่องของเหยื่อ การค้นพบแรกเริ่มถูกรายงานโดยนักวิจัย Peter Girnus และ Aliakbar Zahravi ในเดือนมีนาคม 2025 นอกจากนี้ HarfangLab ยังพบว่าช่องโหว่นี้ถูกนำไปใช้โดยกลุ่มสอดแนมไซเบอร์ที่เรียกว่า XDSpy เพื่อแพร่กระจายมัลแวร์ที่เขียนด้วยภาษา Go ชื่อ XDigo ในการโจมตีหน่วยงานรัฐบาลในยุโรปตะวันออกเมื่อเดือนมีนาคม 2025
- การป้องกันเบื้องต้น: ไมโครซอฟท์บอกกับ The Hacker News ว่า Microsoft Defender มีการตรวจจับเพื่อระบุและบล็อกกิจกรรมภัยคุกคามนี้ และ Smart App Control เป็นชั้นป้องกันเพิ่มเติมที่ช่วยบล็อกไฟล์ที่เป็นอันตรายจากอินเทอร์เน็ต



PlugX: RAT โมดูลาร์ที่พัฒนาต่อเนื่อง

PlugX เป็นโทรจันเข้าถึงระยะไกล (RAT) ที่ยังมีชื่อเรียกอื่น ๆ เช่น Destroy RAT, Kaba, Korplug, SOGU และ TIGERPLUG กลุ่ม UNC6384 เคยถูก Google Threat Intelligence Group (GTIG) วิเคราะห์ว่าเป็นกลุ่มที่มีความทับซ้อนด้านยุทธวิธีและ

เครื่องมือกับกลุ่มแฮ็กเกอร์ที่รู้จักกันในชื่อ Mustang Panda โดยกลุ่มนี้ถูกสังเกตว่าเคยส่งตัวแปรของ PlugX แบบอยู่ในหน่วยความจำที่เรียกว่า SOGU.SEC

ห่วงโซ่การติดตั้งมัลแวร์ (DLL Side-loading)

การโจมตีล่าสุดดำเนินการดังนี้:

1. จดหมายฟิชชิงชักจูงให้ผู้รับคลิกเปิดไฟล์แนบปลอมที่ออกแบบมาเพื่อใช้ประโยชน์จาก CVE-2025-9491
2. ไฟล์ .LNK ถูกออกแบบให้เรียกคำสั่ง PowerShell เพื่อถอดรหัสและแตกไฟล์จากอาร์ไคฟ์ TAR และในขณะเดียวกันจะแสดงเอกสาร PDF หลอกให้ผู้ใช้เห็น
3. อาร์ไคฟ์นั้นประกอบด้วยไฟล์สามไฟล์:
    - โปรแกรมช่วยของเครื่องพิมพ์ Canon ที่ถูกต้องตามกฎหมาย (ตัวจริง)
    - DLL ที่เป็นอันตราย ชื่อ CanonStager ซึ่งถูก sideload ผ่านไบนารี Canon ตัวนั้น
    - ปลายทาง PlugX ที่เข้ารหัสไว้ ("cnmplog.dat") ซึ่ง DLL จะเป็นผู้เรียกใช้งาน

ความสามารถและการวิวัฒนาการทางเทคนิค

- ความสามารถของ PlugX: “มัลแวร์ให้ความสามารถเข้าถึงระยะไกลอย่างครบถ้วน รวมถึงการรันคำสั่ง, การบันทึกแป้นพิมพ์, การอัปโหลดและดาวน์โหลดไฟล์, การตั้งค่าความคงทน, และฟังก์ชันสำรวจระบบอย่างละเอียด” Arctic Wolf กล่าว “สถาปัตยกรรมแบบโมดูลาร์ของมันช่วยให้ผู้ปฏิบัติการสามารถขยายความสามารถผ่านปลั๊กอินที่ออกแบบเฉพาะตามความต้องการปฏิบัติการได้”
- การหลบเลี่ยง: PlugX ยังมีเทคนิคต่อต้านการวิเคราะห์และการตรวจจับหลายอย่างเพื่อยากต่อการถอดรหัสภายในและทำให้ไม่ถูกตรวจจับ โดยมันตั้งความคงทนไว้โดยการแก้ไข Registry ของวินโดวส์
- การปรับปรุงกลไกส่งมอบ: เพื่อปรับปรุงกลไกการส่งมอบมัลแวร์ UNC6384 ยังถูกพบว่าใช้ ไฟล์ HTML Application (HTA) ในต้นเดือนกันยายน เพื่อโหลด JavaScript ภายนอก ซึ่งต่อมาจะดึงเพย์โหลดที่เป็นอันตรายจากซับโดเมนของ cloudfront[.]net
- วิวัฒนาการขนาดเล็ก: Arctic Wolf ระบุว่า เศษซากของ CanonStager ที่พบในต้นเดือนกันยายน และ ตุลาคม 2025 มีขนาดลดลงอย่างต่อเนื่องจากประมาณ 700 KB เหลือเพียง 4 KB ซึ่งบ่งชี้ถึงการพัฒนาอย่างต่อเนื่องและวิวัฒนาการให้เป็นเครื่องมือขนาดเล็กที่สามารถบรรลุเป้าหมายโดยไม่ทิ้งร่องรอยทางนิติวิทยาศาสตร์มากนัก

นอกจากนี้ เพื่อปรับปรุงกลไกการส่งมอบมัลแวร์ UNC6384 ยังถูกพบว่าใช้ไฟล์ HTML Application (HTA) ในต้นเดือนกันยายน เพื่อโหลด JavaScript ภายนอก ซึ่งต่อมาจะดึงเพย์โหลดที่เป็นอันตรายจากซับโดเมนของ cloudfront[.]net

“แคมเปญนี้มุ่งเป้าไปยังหน่วยงานทางการทูตของยุโรปที่เกี่ยวข้องกับความร่วมมือด้านการป้องกัน การประสานนโยบายข้ามพรมแดน และกรอบการทูตพหุภาคี ซึ่งสอดคล้องกับความต้องการข่าวกรองเชิงกลยุทธ์ของสาธารณรัฐประชาชนจีนเกี่ยวกับความเป็นเอกภาพของพันธมิตรยุโรป โครงการด้านการป้องกัน และกลไกการประสานนโยบาย” Arctic Wolf สรุป

ข้อมูลอ้างอิง

Oct 31, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/10/china-linked-hackers-exploit-windows.html