วันที่ 18 มิถุนายน 2568

แกะกลยุทธ์ใหม่ของกลุ่ม Fog Ransomware: ผสมผสานเครื่องมือทั่วไปเข้ากับโปรแกรมสอดแนมพนักงาน

กลุ่มแฮกเกอร์ Fog ransomware กำลังใช้เทคนิครูปแบบใหม่ที่น่าจับตา โดยผสมผสานเครื่องมือไอทีทั่วไปเข้ากับโปรแกรมโอเพนซอร์สสำหรับตรวจสอบพนักงานที่ชื่อ Syteca กลยุทธ์นี้ทำให้การโจมตีซับซ้อนยิ่งขึ้นและยากต่อการตรวจจับ

การโจมตีของ Fog ransomware ถูกพบครั้งแรกเมื่อเดือนพฤษภาคมปีที่แล้ว โดยเริ่มต้นจากการใช้ข้อมูลล็อกอิน VPN ที่ถูกขโมยมาเพื่อเข้าถึงเครือข่ายของเหยื่อ เมื่อเข้าไปได้แล้ว แฮกเกอร์จะใช้การโจมตีแบบ “pass-the-hash” เพื่อยกระดับสิทธิ์เป็นผู้ดูแลระบบ จากนั้นจะทำการปิดการใช้งาน Windows Defender และเข้ารหัสไฟล์ทั้งหมด รวมถึงพื้นที่เก็บข้อมูลของเครื่องเสมือน นอกจากนี้ กลุ่มผู้คุกคามนี้ยังถูกพบว่าใช้ช่องโหว่ N-day ที่ส่งผลกระทบต่อเซิร์ฟเวอร์ Veeam Backup & Replication (VBR) รวมถึง SonicWall SSL VPN endpoints

ชุดเครื่องมือโจมตีใหม่ที่ซับซ้อนขึ้น

นักวิจัยจาก Symantec และทีม Carbon Black Threat Hunter ได้ค้นพบชุดเครื่องมือโจมตีนี้ระหว่างการทำ Incident Response (IR) เมื่อเดือนที่แล้วที่สถาบันการเงินแห่งหนึ่งในเอเชีย แม้ว่า Symantec จะไม่สามารถระบุต้นตอของการติดเชื้อในครั้งแรกได้ แต่ก็ได้บันทึกการใช้เครื่องมือใหม่หลายตัวที่ไม่เคยพบเห็นในการโจมตีลักษณะนี้มาก่อน

เครื่องมือที่แปลกใหม่และน่าสนใจที่สุดคือ Syteca (เดิมชื่อ Ekran) ซึ่งเป็นซอฟต์แวร์ที่ถูกกฎหมายสำหรับตรวจสอบพนักงานที่บันทึกกิจกรรมบนหน้าจอและการกดแป้นพิมพ์ ผู้โจมตีอาจใช้เครื่องมือนี้เพื่อรวบรวมข้อมูล เช่น ข้อมูลบัญชีที่พนักงานพิมพ์โดยไม่รู้ตัวว่ากำลังถูกตรวจสอบจากระยะไกล

Syteca ถูกส่งไปยังระบบอย่างลับๆ โดย Stowaway ซึ่งเป็นเครื่องมือพร็อกซีแบบโอเพนซอร์สสำหรับการสื่อสารและการถ่ายโอนไฟล์แบบปกปิด และถูกสั่งให้ทำงานโดย SMBExec ซึ่งเป็นเครื่องมือที่เทียบเท่า PsExec ในเฟรมเวิร์กโอเพนซอร์ส Impacket ที่ใช้สำหรับการเคลื่อนไหวภายในเครือข่าย

การโจมตีนี้ยังเกี่ยวข้องกับ GC2 ซึ่งเป็น backdoor แบบโอเพนซอร์สหลังการโจมตีที่ใช้ Google Sheets หรือ Microsoft SharePoint สำหรับการควบคุมและสั่งการ (C2) และการขโมยข้อมูล ที่น่าสนใจคือ GC2 ไม่ค่อยพบเห็นในการโจมตี ransomware และเคยถูกใช้ในการโจมตีที่เชื่อว่าเป็นฝีมือของกลุ่มภัยคุกคามจีน APT41

นอกจากเครื่องมือเหล่านี้ Symantec ยังระบุเครื่องมืออื่นๆ ที่เป็นส่วนหนึ่งของ Fog ransomware ที่ใช้ในการโจมตี ได้แก่:

- **Adapt2x C2** – โอเพนซอร์สของ Cobalt Strike ที่รองรับการดำเนินการหลังการโจมตี
- **Process Watchdog** – โปรแกรมตรวจสอบระบบที่สามารถรีสตาร์ทกระบวนการสำคัญได้
- **PsExec** – เครื่องมือ Microsoft Sysinternals สำหรับการสั่งงานจากระยะไกลบนเครื่องในเครือข่าย
- **Impacket SMB** – ไลบรารี Python ที่เข้าถึง SMB ได้ในระดับต่ำ ซึ่งน่าจะใช้สำหรับการติดตั้ง payload ของ ransomware บนเครื่องของเหยื่อ

เพื่อเตรียมข้อมูลสำหรับการขโมยและส่งไปยังโครงสร้างพื้นฐานของตนเอง Fog ransomware ยังใช้โปรแกรม **7-Zip, MegaSync** และ **FreeFileSync**

“ชุดเครื่องมือที่ผู้โจมตีนำมาใช้นั้นค่อนข้างผิดปกติสำหรับการโจมตี ransomware” Symantec ให้ความเห็นในรายงาน "ไคลเอนต์ Syteca และเครื่องมือ GC2 ไม่ใช่เครื่องมือที่เราเคยเห็นถูกนำมาใช้ในการโจมตี ransomware มาก่อน ในขณะที่เครื่องมือพร็อกซี Stowaway และ Adap2x C2 Agent Beacon ก็เป็นเครื่องมือที่ไม่ค่อยถูกพบเห็นในการโจมตี ransomware” นักวิจัยกล่าว

ชุดเครื่องมือที่ไม่ธรรมดา เช่นเดียวกับที่ Symantec ตรวจพบในการโจมตี Fog ransomware ล่าสุด สามารถช่วยให้ผู้ก่อภัยคุกคามหลีกเลี่ยงการตรวจจับได้ ดังนั้นรายงานของนักวิจัยยังให้ข้อมูล **indicators of compromise (IoC)** ที่สามารถช่วยให้องค์กรต่างๆ ป้องกันตัวเองจากเหตุการณ์ดังกล่าวได้

สรุป: Fog ransomware ยกระดับการโจมตีด้วยกลยุทธ์ที่ซับซ้อนยิ่งขึ้น

การโจมตีล่าสุดของ Fog ransomware แสดงให้เห็นถึงการปรับเปลี่ยนกลยุทธ์ของผู้ไม่หวังดี ที่หันมาใช้เครื่องมือที่ถูกกฎหมายและโอเพนซอร์สผสมผสานกับการโจมตี ทำให้การตรวจจับยากขึ้นและสร้างความเสียหายได้มากขึ้น การทำความเข้าใจชุดเครื่องมือที่ Fog ransomware ใช้และการนำ IoC ไปปรับใช้จึงเป็นสิ่งสำคัญสำหรับองค์กรในการป้องกันตนเองจากภัยคุกคามที่กำลังพัฒนาอย่างต่อเนื่องนี้

ข้อแนะนำ (Recommendation)

- ตรวจสอบและอัปเดตอุปกรณ์รักษาความปลอดภัยให้เป็นเป็นเวอร์ชั่นล่าสุด
- ตรวจสอบและควบคุมการใช้งานเครื่องมือต่างๆ ภายในองค์กร ว่าใครใช้ ใช้ทำอะไร ใช้เมื่อไร
- จัดเก็บ Backup แยกออกจากเครือข่ายหลัก และตรวจสอบการเข้าถึง Backup Server อย่างเข้มงวด

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/fog-ransomware-attack-uses-unusual-mix-of-legitimate-and-open-source-tools/