วันที่ 18 มิถุนายน 2568

มัลแวร์ลบข้อมูลตัวใหม่ PathWiper โจมตีโครงสร้างพื้นฐานสำคัญของยูเครนในปี 2025

ภัยไซเบอร์ยังคงระอุ! องค์กรสำคัญในยูเครนตกเป็นเป้าหมายของมัลแวร์ลบข้อมูลตัวใหม่ “PathWiper” ในขณะเดียวกัน รัสเซียและมอลโดวาก็ยังคงโดนกลุ่ม Silent Werewolf เล่นงาน ส่วนกลุ่มแฮกเกอร์ฝั่งยูเครนก็เดินหน้าโจมตีรัสเซียเช่นกัน

PathWiper: มัลแวร์ลบข้อมูลตัวใหม่ถล่มโครงสร้างพื้นฐานยูเครน

โดยเมื่อเร็วๆ นี้ Cisco Talos ได้ออกมาเปิดเผยถึงมัลแวร์ลบข้อมูลตัวใหม่ที่ไม่เคยปรากฏมาก่อนในชื่อ "PathWiper" ซึ่งมุ่งเป้าโจมตีองค์กรโครงสร้างพื้นฐานสำคัญในยูเครน

เจาะลึกการโจมตี PathWiper:

นักวิเคราะห์จาก Cisco Talos คือ Jacob Finn, Dmytro Korzhevin และ Asheer Malhotra ได้ทำการวิเคราะห์และพบว่ามัลแวร์ PathWiper ถูกเผยแพร่ผ่านเครื่องมือบริหารจัดการลูกข่ายที่เป็นซอฟต์แวร์ถูกลิขสิทธิ์ ซึ่งหมายความว่าผู้โจมตีสามารถเข้าถึงคอนโซลการจัดการได้โดยตรง และใช้สิทธิ์เหล่านั้นเพื่อดำเนินการโจมตีได้อย่างแนบเนียน

ทีม Talos เชื่อว่าการโจมตีครั้งนี้มีความเชื่อมโยงกับกลุ่ม APT (Advanced Persistent Threat) ที่ได้รับการสนับสนุนจากรัฐบาลรัสเซีย ซึ่งมีลักษณะคล้ายกับการโจมตีด้วยมัลแวร์ลบข้อมูลที่เคยเกิดขึ้นในยูเครนก่อนหน้านี้

วิธีการทำงานของ PathWiper:

คำสั่งที่ใช้ในการโจมตีจะมาในรูปแบบไฟล์ .bat ที่รัน VBScript ชื่อ uacinstall.vbs ซึ่งถูกวางไว้ในโฟลเดอร์ TEMP ของ Windows สคริปต์นี้จะทำหน้าที่ติดตั้งและเรียกใช้ไฟล์ไบนารี sha256sum.exe ซึ่งแท้จริงแล้วคือโปรแกรม PathWiper ที่ถูกซ่อนไว้

"ชื่อไฟล์และพฤติกรรมของมัลแวร์ถูกออกแบบมาให้กลมกลืนกับกระบวนการภายในระบบบริหารจัดการ ซึ่งแสดงให้เห็นว่าผู้โจมตีมีความเข้าใจระบบเป้าหมายเป็นอย่างดี" ทีม Talos ระบุ

เมื่อ PathWiper เริ่มทำงาน มันจะรวบรวมข้อมูลของอุปกรณ์จัดเก็บทั้งหมดที่เชื่อมต่ออยู่ ไม่ว่าจะเป็นชื่อไดรฟ์, ชื่อวอลุ่ม, หรือเส้นทางไดรฟ์เน็ตเวิร์ก จากนั้นจะสร้างโปรเซสแยกเพื่อโจมตีแต่ละไดรฟ์โดยเฉพาะ มันจะเขียนข้อมูลสุ่มทับโครงสร้างระบบไฟล์ที่สำคัญ เช่น MBR, $MFT, $MFTMirr, $LogFile, $Boot, $Bitmap, $TxfLog, $Tops และ $AttrDef พร้อมทั้งพยายามลบไฟล์ต่างๆ โดยไม่ให้สามารถกู้คืนได้ และทำการ unmount วอลุ่มทั้งหมด

แม้ PathWiper จะมีลักษณะคล้ายกับ HermeticWiper (หรือที่รู้จักกันในชื่อ FoxBlade, KillDisk, NEARMISS) ที่เคยใช้โจมตียูเครนในช่วงต้นปี 2024 แต่รูปแบบการทำลายข้อมูลนั้นมีความแตกต่างกันอย่างชัดเจน "การที่มีการพัฒนาเทคนิคมัลแวร์ลบข้อมูลอย่างต่อเนื่อง ชี้ให้เห็นว่าโครงสร้างพื้นฐานสำคัญของยูเครนยังคงเป็นเป้าหมายของการโจมตีในระยะยาว" ทีม Talos กล่าว

Silent Werewolf โจมตีรัสเซียและมอลโดวาด้วย XDigo

ในอีกด้านหนึ่ง BI.ZONE บริษัทด้านความปลอดภัยไซเบอร์ของรัสเซีย ได้เปิดเผยว่ากลุ่มแฮกเกอร์ Silent Werewolf ได้เปิดปฏิบัติการโจมตีใหม่สองแคมเปญในเดือนมีนาคมที่ผ่านมา โดยมุ่งเป้าไปยังองค์กรในรัสเซียและมอลโดวา

ผู้โจมตีใช้ตัวโหลดมัลแวร์สองชุด ซึ่งจะทำการโหลดมัลแวร์เพิ่มเติมจากเซิร์ฟเวอร์ควบคุม (C2) ซึ่งคาดการณ์ว่าเป็น XDigo มัลแวร์ที่เคยถูกใช้มาก่อนหน้านี้ในลักษณะเดียวกัน

เป้าหมายในการโจมตีครั้งนี้อยู่ในภาคนิวเคลียร์, อากาศยาน, วิศวกรรมเครื่องกล, และอุตสาหกรรมเครื่องมือวัด โดยเริ่มต้นจากการส่งอีเมลฟิชชิ่งที่แนบไฟล์ ZIP ซับซ้อนมาด้วย ซึ่งประกอบไปด้วย:

- ไฟล์ LNK ที่มุ่งเป้าไปยังโปรแกรม DeviceMetadataWizard.exe
- ไฟล์ DLL อันตราย
- ไฟล์ PDF หลอก
- ไฟล์ ZIP ซ้อน

เมื่อเหยื่อเปิด shortcut ไฟล์ ZIP ที่ซ้อนอยู่จะถูกแตกออกโดยอัตโนมัติ และ DLL อันตรายจะถูก sideload ผ่านไฟล์ DeviceMetadataWizard.exe จากนั้นตัวโหลดซึ่งเขียนด้วยภาษา C# จะดึง payload ระยะที่สองจากเซิร์ฟเวอร์ และแสดงเอกสาร PDF ปลอมเพื่อเบี่ยงเบนความสนใจของเหยื่อ

หากเหยื่อไม่ตรงตามเกณฑ์ที่ผู้โจมตีกำหนด ระบบจะดาวน์โหลดไฟล์โมเดล LLM อย่าง LLaMA 2 (GGUF format) จาก Hugging Face ซึ่งช่วยป้องกันการวิเคราะห์มัลแวร์โดย sandbox "วิธีนี้ทำให้การวิเคราะห์ยากขึ้น และช่วยเลี่ยงการตรวจจับจากระบบอัตโนมัติได้อย่างมีประสิทธิภาพ" BI.ZONE อธิบาย

อีกแคมเปญหนึ่งของ Silent Werewolf ถูกค้นพบในช่วงเวลาเดียวกัน โดยมีเป้าหมายเป็นองค์กรในมอลโดวา และอาจรวมถึงรัสเซีย โดยใช้ตัวโหลดที่แนบมากับอีเมลปลอมที่มีเนื้อหาเกี่ยวกับวันหยุดราชการและคำแนะนำด้านความปลอดภัยจากแรนซัมแวร์ ซึ่ง Silent Werewolf มีประวัติการโจมตีในรัสเซีย, เบลารุส, ยูเครน, มอลโดวา และเซอร์เบียมาตั้งแต่ปี 2011 โดยอาศัยอีเมลปลอมแนบมัลแวร์ในรูปแบบ XDSpy, XDigo และ DSDownloader

BO Team: แฮกเกอร์หนุนยูเครนพุ่งเป้าโจมตีรัสเซีย

ในอีกมุมหนึ่ง กลุ่มแฮกเกอร์ที่รู้จักกันในชื่อ BO Team หรือ Black Owl, Hoody Hyena และ Lifting Zmiy ได้เปิดฉากโจมตีองค์กรภาครัฐของรัสเซียหลายแห่ง รวมถึงในสาขาเทคโนโลยี, โทรคมนาคม, และการผลิต

Kaspersky ระบุว่ากลุ่มนี้มีแรงจูงใจทั้งด้านการเมืองและผลประโยชน์ทางการเงิน โดยปรากฏตัวครั้งแรกในช่วงต้นปี 2024 และใช้เครื่องมือ post-exploitation ขั้นสูง เช่น Mythic, Cobalt Strike รวมถึง Remote Access Tools (RAT) ที่เป็นซอฟต์แวร์ถูกลิขสิทธิ์ การเข้าถึงเหยื่อส่วนใหญ่เกิดจากอีเมลฟิชชิ่งที่แนบไฟล์อันตราย เช่น DarkGate, BrockenDoor, Remcos RAT

หลังจากมัลแวร์เข้าควบคุมระบบสำเร็จ กลุ่มผู้โจมตีจะลบไฟล์สำรอง โดยใช้ SDelete เพื่อทำลายข้อมูลอย่างถาวร และปล่อยแรนซัมแวร์ Babuk เพื่อเรียกค่าไถ่จากองค์กรเป้าหมาย

เทคนิคอื่นๆ ที่ BO Team ใช้ได้แก่:

- ตั้ง Scheduled Tasks เพื่อคงการเข้าถึงระบบอย่างต่อเนื่อง
- ใช้ชื่อไฟล์ที่คล้ายกับไฟล์ของระบบ เพื่อหลบเลี่ยงการตรวจจับ
- ดึงข้อมูลจาก Active Directory ด้วยเครื่องมือ ntdsutil
- สอดแนมข้อมูลบน Telegram, กระบวนการทำงานของระบบ (process), ผู้ใช้งาน, การเชื่อมต่อผ่าน RDP และซอฟต์แวร์ป้องกันไวรัส
- ใช้ RDP และ SSH เพื่อเชื่อมต่อไปยังเครื่องอื่นภายในเครือข่าย
- ติดตั้ง AnyDesk เพื่อควบคุมระบบจากระยะไกล

"BO Team แสดงให้เห็นถึงความสามารถทางเทคนิคขั้นสูง และมีรูปแบบการโจมตีที่แตกต่างจากกลุ่มแฮกเกอร์ยูเครนอื่นๆ โดยไม่ปรากฏความเชื่อมโยงที่ชัดเจนกับกลุ่มอื่นในภูมิภาค" Kaspersky กล่าว

ข้อแนะนำ (Recommendation)

- ตรวจสอบสิทธิ์ผู้ดูแลบน เครื่องมือบริหารจัดการลูกข่าย ทุกระบบ
- จัดเก็บ Backup แยกออกจากเครือข่ายหลัก และตรวจสอบการเข้าถึง Backup Server
- ตรวจสอบและจำกัดการใช้งานเครื่องมือ Remote
- ตรวจสอบนโยบาย Zero Trust สำหรับการเข้าถึงเครือข่ายและแอปพลิเคชันสำคัญ

ข้อมูลอ้างอิง

- https://thehackernews.com/2025/06/new-pathwiper-data-wiper-malware.html