วันที่ 5 กันยายน 2568

APT28 ของรัสเซียใช้ช่องโหว่ "NotDoor" Outlook เพื่อโจมตีบริษัทต่างๆ ในประเทศสมาชิก NATO

นักวิจัยด้านความปลอดภัยได้ออกมาเปิดเผยว่า กลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐบาลรัสเซียซึ่งถูกติดตามในชื่อ APT28 ถูกเชื่อมโยงกับแบ็กดอร์ใหม่บน Microsoft Outlook ที่ชื่อว่า NotDoor ซึ่งใช้ในการโจมตีบริษัทหลายแห่งในประเทศสมาชิก NATO

NotDoor “เป็นมาโคร VBA สำหรับ Outlook ที่ถูกออกแบบมาให้คอยตรวจสอบอีเมลขาเข้าและหาคำสั่งกระตุ้นที่ถูกตั้งไว้” ทีมข่าวกรองภัยคุกคาม LAB52 ของบริษัท S2 Grupo กล่าว “เมื่อพบอีเมลที่มีคำดังกล่าว ผู้โจมตีจะสามารถดึงข้อมูลออกไป อัปโหลดไฟล์ หรือรันคำสั่งบนคอมพิวเตอร์ของเหยื่อได้”

มัลแวร์ตัวนี้ได้ชื่อมาจากการใช้คำว่า “Nothing” ที่อยู่ในซอร์สโค้ด เหตุการณ์นี้สะท้อนถึงการนำ Outlook มาใช้เป็นช่องทางที่แนบเนียนในการสื่อสาร, การขโมยข้อมูล และการส่งต่อมัลแวร์ วิธีการเข้าถึงในช่วงแรกที่ใช้ติดตั้งมัลแวร์นี้ยังไม่ถูกเปิดเผย แต่จากการวิเคราะห์พบว่า มันถูกปล่อยผ่านไฟล์ปฏิบัติการของ Microsoft OneDrive (“onedrive.exe”) โดยใช้เทคนิคที่เรียกว่า DLL side-loading

ซึ่งจะนำไปสู่การรัน DLL อันตราย (“SSPICLI.dll”) ที่จะติดตั้ง VBA backdoor และปิดการป้องกันความปลอดภัยของมาโคร โดยเฉพาะ มันจะรันคำสั่ง PowerShell ที่ถูกเข้ารหัสด้วย Base64 เพื่อทำหลายอย่าง เช่น ติดต่อกับ webhook[.]site ที่ผู้โจมตีควบคุม, ตั้งค่าการคงอยู่ผ่านการแก้ไข Registry, เปิดใช้งานการรันมาโคร และปิดหน้าต่างข้อความต่างๆ ของ Outlook เพื่อหลีกเลี่ยงการถูกตรวจจับ

กลไกการทำงานของ NotDoor

NotDoor ถูกสร้างขึ้นในรูปแบบโปรเจกต์ Visual Basic for Applications (VBA) ที่ถูกทำให้อ่านยาก โดยใช้ event อย่าง Application.MAPILogonComplete และ Application.NewMailEx เพื่อรันเพย์โหลดทุกครั้งที่ Outlook ถูกเปิดหรือมีอีเมลใหม่เข้ามา

จากนั้นมันจะสร้างโฟลเดอร์ที่ %TEMP%\Temp หากยังไม่มีอยู่ และใช้โฟลเดอร์นี้เก็บไฟล์ TXT ที่ถูกสร้างขึ้นระหว่างการทำงาน เพื่อส่งออกไปยังอีเมล Proton Mail รวมถึงยังตรวจสอบอีเมลที่เข้ามาหาคำสั่งพิเศษ เช่น “Daily Report” เพื่อดึงคำสั่งที่ซ่อนอยู่มารันต่อ

มัลแวร์นี้รองรับคำสั่ง 4 แบบ คือ:

- cmd: รันคำสั่งและส่งผลลัพธ์กลับมาเป็นไฟล์แนบอีเมล
- cmdno: รันคำสั่งโดยไม่ส่งผลลัพธ์กลับ
- dwn: ขโมยไฟล์จากเครื่องเหยื่อแล้วส่งออกมาเป็นไฟล์แนบอีเมล
- upl: วางไฟล์ลงในเครื่องเหยื่อ

“ไฟล์ที่ถูกขโมยจะถูกเก็บไว้ในโฟลเดอร์ดังกล่าว เนื้อหาของไฟล์จะถูกเข้ารหัสด้วยวิธีพิเศษของมัลแวร์ ส่งออกไปทางอีเมล แล้วจึงถูกลบออกจากระบบ” LAB52 กล่าว

การโจมตีที่ใช้ Telegram และ Microsoft Dev Tunnels

การเปิดเผยนี้เกิดขึ้นพร้อมกับรายงานจากศูนย์ข่าวกรองภัยคุกคาม 360 ในจีน ที่พบว่า กลุ่ม Gamaredon (หรือ APT-C-53) ได้ปรับเปลี่ยนวิธีการโจมตี โดยใช้ Telegraph ซึ่งเป็นแพลตฟอร์มของ Telegram เป็นตัวกลางชี้ไปยังโครงสร้าง C2 (Command-and-Control)

การโจมตีเหล่านี้ยังมีความน่าสนใจตรงที่มีการใช้ Microsoft Dev Tunnels (devtunnels.ms) ซึ่งเป็นบริการที่ช่วยให้นักพัฒนาสามารถเปิดเว็บเซอร์วิสในเครื่องออกสู่อินเทอร์เน็ตเพื่อทดสอบและดีบัก มาเป็นโดเมน C2 เพื่อเพิ่มความแนบเนียน

“เทคนิคนี้ให้ข้อได้เปรียบสองด้าน อย่างแรก IP ของเซิร์ฟเวอร์ C2 จริงจะถูกซ่อนด้วยโหนดรีเลย์ของ Microsoft ทำให้การสืบย้อนกลับทำได้ยาก” บริษัทไซเบอร์ฯ กล่าว “อย่างที่สอง การใช้ความสามารถของบริการที่เปลี่ยนชื่อโดเมนได้ทุกนาที ทำให้ผู้โจมตีหมุนเวียนโครงสร้างพื้นฐานได้รวดเร็ว และยังอาศัยความน่าเชื่อถือและปริมาณการใช้งานมหาศาลของคลาวด์หลักเพื่อดำเนินการต่อเนื่องโดยแทบไม่ถูกเปิดเผย”

ห่วงโซ่การโจมตียังรวมถึงการใช้โดเมนปลอมของ Cloudflare Workers เพื่อกระจายสคริปต์ Visual Basic ที่ชื่อ PteroLNK ซึ่งสามารถแพร่ไปยังเครื่องอื่นผ่านการคัดลอกตัวเองลงใน USB drive ที่เชื่อมต่อ รวมถึงดาวน์โหลดเพย์โหลดเพิ่มเติม

“ห่วงโซ่การโจมตีนี้แสดงถึงการออกแบบที่ซับซ้อน ใช้เทคนิคปกปิดถึงสี่ชั้น (การคงอยู่ใน Registry, การคอมไพล์แบบไดนามิก , การปลอมเส้นทาง, การใช้บริการคลาวด์) เพื่อทำให้การโจมตีตั้งแต่เริ่มจนถึงการขโมยข้อมูลเป็นไปอย่างแนบเนียน” ศูนย์ข่าวกรองภัยคุกคาม 360 กล่าว

ข้อมูลอ้างอิง

Sep 4, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/russian-apt28-deploys-notdoor-outlook.html