

วันที่ 7 ตุลาคม 2569

Warlock ใช้ช่องโหว่ SharePoint เพื่อปิดระบบรักษาความปลอดภัยและติดตั้งแรนซัมแวร์



กลุ่มผู้โจมตีที่เชื่อว่าเชื่อมโยงกับจีน ซึ่งรู้จักกันในชื่อ Warlock ยังคงนำช่องโหว่ของ Microsoft SharePoint ทั้ง ช่องโหว่เก่า และ ช่องโหว่ใหม่ มาใช้ในการโจมตีองค์กรในประเทศที่ใช้ภาษาโปรตุเกสและสเปน ทีม Symantec และ Carbon Black Threat Hunter Team ตรวจพบกิจกรรมดังกล่าว โดยพบว่ามีเป้าหมายเป็นองค์กรด้านโครงสร้างพื้นฐานสำคัญ หน่วยงานภาครัฐ และสถาบันการศึกษา

ในช่วงสองเดือนที่ผ่านมา Longlegs ได้โจมตีองค์กรอย่างน้อย 4 แห่ง ซึ่งรวมถึงผู้ให้บริการโครงสร้างพื้นฐานสำคัญ 2 แห่ง ได้แก่ หน่วยงานด้านสาธารณสุขบราซิลและผู้ให้บริการโทรคมนาคม หน่วยงานรัฐบาลระดับภูมิภาค และมหาวิทยาลัย อีก 1 แห่ง หน่วยงานด้านความปลอดภัยทางไซเบอร์ของ Broadcom ระบุว่าเหยื่ออยู่ในประเทศที่ใช้ภาษาโปรตุเกสและสเปน ครอบคลุมพื้นที่ในยุโรป แอฟริกา และลาตินอเมริกา

Warlock ซึ่งมีชื่อเรียกอื่นว่า Gold Salem, Longlegs และ Storm-2603 เริ่มเป็นที่รู้จักอย่างมาก ในช่วงกลางปี 2025 จากการใช้ประโยชน์จากช่องโหว่แบบ Zero-day ของ SharePoint ที่เรียกว่า ToolShell เพื่อกระจายแรนซัมแวร์ไปยังระบบของเป้าหมาย

เมื่อต้นปีที่ผ่านมา กลุ่มดังกล่าว ถูกเชื่อมโยงกับ การเจาะระบบ SmarterTools โดยอาศัย SmarterMail ที่ยังไม่ได้รับการอัปเดตแก้ไขช่องโหว่ นอกจากนี้ยัง มีการใช้ เครื่องมือที่ถูกต้องตามปกติ เช่น Velociraptor เพื่อใช้ในการควบคุมเครื่องที่ถูกโจมตี และใช้เทคนิค Bring Your Own Vulnerable Driver (BYOVD) เพื่อปิดหรือหยุดการทำงานของซอฟต์แวร์รักษาความปลอดภัยบนเครื่องที่ถูกเจาะระบบ จากข้อมูลของ Symantec พบว่า Warlock มีรูปแบบการโจมตีที่คล้ายคลึงกับกลุ่มกิจกรรมที่เคยพบก่อนหน้านี้ ซึ่งรู้จักกันในชื่อ CL-CRI-1040, CamoFei และ ChamelGang

ในการโจมตีครั้งหนึ่งต่อองค์กรด้านโครงสร้างพื้นฐานสำคัญ ผู้โจมตีได้ส่งเครื่องมือที่ออกแบบมาเพื่อปิดซอฟต์แวร์รักษาความปลอดภัยไปยังเครื่องอย่างน้อย 40 เครื่องภายในเวลาประมาณ 2 ชั่วโมง จากนั้นจึงติดตั้ง Warlock ลงบนเครื่องอย่างน้อย 33 เครื่อง โดยนำไฟล์ไปเก็บไว้ในโฟลเดอร์ SYSVOL ของโดเมน ซึ่งระบบจะกระจายไฟล์ไปยังเครื่องต่างๆ ตามกระบวนการทำงานปกติของโดเมน

การโจมตีของ Warlock ใช้ประโยชน์จากช่องโหว่หลายรายการใน Microsoft SharePoint Server ที่ติดตั้งและใช้งานภายในองค์กร เมื่อสามารถเจาะเข้าสู่ระบบได้สำเร็จ ผู้โจมตีจะติดตั้ง Web Shell ซึ่งสามารถทำงานกับ SharePoint ได้หลายเวอร์ชัน เป้าหมายสำคัญของ Web Shell คือการขโมย ASP.NET Machine Keys ของ SharePoint Farm จากนั้นนำคีย์เหล่านี้ไปใช้สร้างข้อมูลที่มีลายเซ็นถูกต้อง เพื่อให้สามารถส่งรันท้าทายที่เป็นอันตรายจากระยะไกลภายใน SharePoint Application Pool ได้ เทคนิคอื่นๆ ที่พบจากการโจมตีมีดังนี้

- ใช้เทคนิค DLL Sideloadng เพื่อโหลดโค้ดที่เป็นอันตรายเข้าไปทำงานในหน่วยความจำ
- ดาวน์โหลดไฟล์หรือโปรแกรมเพิ่มเติมจากบริการแชร์ไฟล์และพื้นที่จัดเก็บข้อมูลบนคลาวด์ที่เป็นบริการถูกต้อง เช่น catbox[.]moe และ wasabisys[.]com เพื่อช่วยหลบเลี่ยงการตรวจจับ
- ใช้ไดรเวอร์ที่เป็นของจริงแต่มีช่องโหว่ K7RKScan.sys (CVE-2025-1055) ในการโจมตีแบบ BYOVD เพื่อปิดซอฟต์แวร์รักษาความปลอดภัย โดยก่อนหน้านี้กลุ่มแรนซัมแวร์ DragonForce ก็เคยนำไดรเวอร์เดียวกันนี้มาใช้ในการโจมตี
- ใช้เครื่องมือที่มีอยู่ในระบบอยู่แล้ว (Living-off-the-Land หรือ LotL) เพื่อสำรวจระบบและสั่งงานบนเครื่องที่ถูกเจาะ ซึ่งรวมถึงการใช้ฟังก์ชัน Tunnel ที่มีอยู่ใน Microsoft Visual Studio Code เพื่อสร้างช่องทางเชื่อมต่อระยะไกลไปยังเครื่องที่ติดมัลแวร์
- นำไฟล์หรือโปรแกรมที่ใช้ในการโจมตีไปเก็บไว้ใน SYSVOL Share ของโดเมนที่ถูกเจาะ เพื่อกระจายแรนซัมแวร์ไปยังเครื่องจำนวนมาก

เมื่อวันที่ 22 กรกฎาคม 2026 ที่ผ่านมา มีรายงานว่ากลุ่มผู้โจมตีใช้ประโยชน์จากช่องโหว่ของ SharePoint Server เพื่อวาง Web Shell สำรวจระบบ ส่งรันท้าทายต่อการภายใน SharePoint Application Pool ติดตั้งไฟล์หรือโปรแกรมเพิ่มเติมเจาะลึกเข้าไปในเครือข่าย สร้าง VS Code Tunnel ปิดการทำงานของซอฟต์แวร์รักษาความปลอดภัย และท้ายที่สุดติดตั้งไฟล์แรนซัมแวร์ลงในระบบ กิจกรรมของ Longlegs ที่ยังคงดำเนินต่อเนื่อง แม้เวลาจะผ่านไปมากกว่าหนึ่งปีหลังจากที่แรนซัมแวร์ Warlock เริ่มเป็นที่รู้จัก แสดงให้เห็นว่าการใช้ประโยชน์จาก ToolShell และช่องโหว่อื่นๆ ที่เกี่ยวข้องกับ SharePoint ยังคงเป็นช่องทางสำคัญที่ผู้โจมตีสามารถใช้เพื่อเข้าสู่ระบบได้ โดยเฉพาะ SharePoint ที่ยังไม่ได้รับการอัปเดตแก้ไขช่องโหว่หรือยังไม่มีมาตรการป้องกันอื่นมาช่วยลดความเสี่ยง Symantec และ Carbon Black ระบุ

การที่ช่วงหลังพบการโจมตีมุ่งเป้าไปยังประเทศที่ใช้ภาษาโปรตุเกสและสเปนมากขึ้น อาจหมายถึงการเลือกเป้าหมายแบบฉวยโอกาส โดยอาศัย SharePoint ที่เปิดให้เข้าถึงจากภายนอกและยังมีช่องโหว่ หรืออาจเป็นการเลือกเป้าหมายตามภารกิจที่กำหนดไว้อย่างชัดเจนมากกว่า

ข้อมูลอ้างอิง

Oct 3, 2026, By Ravi Lakshmanan

- <https://thehackernews.com/2026/10/warlock-exploits-sharepoint-flaws-to.html>