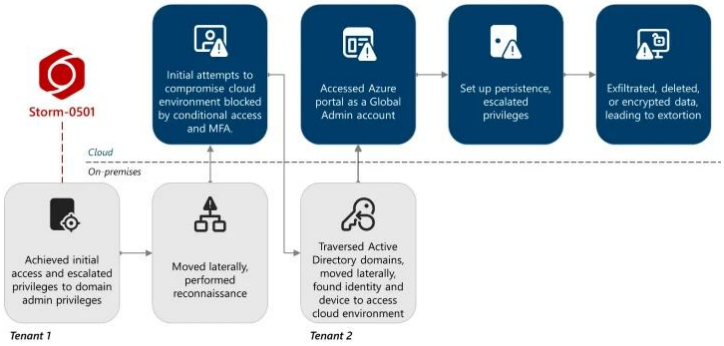
วันที่ 1 กันยายน 2568

Storm-0501 โจมตี Entra ID เพื่อขโมยและลบข้อมูล Azure ในการโจมตีระบบคลาวด์แบบผสม



กลุ่มอาชญากรไซเบอร์ที่มุ่งหวังผลประโยชน์ทางการเงินในชื่อ Storm-0501 ถูกพบว่ากำลังพัฒนากลยุทธ์ใหม่ในการโจมตีเพื่อขโมยข้อมูลและรีดไถเงิน โดยพุ่งเป้าไปที่สภาพแวดล้อมบนคลาวด์โดยเฉพาะ ซึ่งเป็นวิธีการที่แตกต่างจากแรนซัมแวร์แบบดั้งเดิมอย่างสิ้นเชิง

“ไม่เหมือนกับแรนซัมแวร์แบบดั้งเดิมที่ใช้ในระบบภายในองค์กร (on-premises) ซึ่งผู้โจมตีมักจะติดตั้งมัลแวร์เพื่อเข้ารหัสไฟล์สำคัญ แต่แรนซัมแวร์บนคลาวด์กลับเปลี่ยนไปอย่างสิ้นเชิง” ทีม Microsoft Threat Intelligence กล่าวในรายงานที่เผยแพร่กับ The Hacker News

“โดยอาศัยความสามารถของระบบคลาวด์ Storm-0501 สามารถขโมยข้อมูลจำนวนมหาศาลได้อย่างรวดเร็ว ทำลายข้อมูลและระบบสำรอง (backup) ที่อยู่ในสภาพแวดล้อมของเหยื่อ และเรียกค่าไถ่โดยไม่จำเป็นต้องใช้มัลแวร์แบบเดิมเลย”

Storm-0501 ถูกบันทึกครั้งแรกโดย Microsoft เมื่อเกือบหนึ่งปีก่อน โดยมีการโจมตีแรนซัมแวร์ในระบบคลาวด์แบบผสมที่พุ่งเป้าไปยังหน่วยงานรัฐบาล ภาคการผลิต การขนส่ง และหน่วยงานบังคับใช้กฎหมายในสหรัฐฯ โดยผู้โจมตีมักเริ่มจากระบบในองค์กรก่อน แล้วจึงขยายไปสู่ระบบคลาวด์เพื่อขโมยข้อมูล ล้วงรหัสผ่าน และปล่อยแรนซัมแวร์

Microsoft ระบุว่าการโจมตีระลอกล่าสุดเป็นแบบฉวยโอกาส ไม่เจาะจงอุตสาหกรรมใด และมีองค์กรหลายประเภทที่ถูกเล่นงาน ไม่ว่าจะเป็นโรงเรียน, โรงพยาบาล หรือหน่วยงานอื่น ๆ

กลยุทธ์การโจมตีที่ซับซ้อนและเชี่ยวชาญ

กลุ่มนี้ถูกประเมินว่ามีกิจกรรมมาตั้งแต่ปี 2021 และพัฒนาไปเป็นเครือข่าย ransomware-as-a-service (RaaS) ที่ให้บริการแก่พันธมิตร โดยเคยใช้แรนซัมแวร์หลากหลายชนิด เช่น Sabbath, Hive, BlackCat (ALPHV), Hunters International, LockBit และ Embargo

“Storm-0501 แสดงให้เห็นถึงความชำนาญในการเคลื่อนย้ายระหว่างระบบในองค์กรและระบบคลาวด์ ซึ่งสะท้อนให้เห็นว่าผู้โจมตีปรับตัวตามการใช้งานระบบคลาวด์แบบผสมที่เติบโตขึ้น พวกเขามักค้นหาอุปกรณ์ที่ไม่ได้รับการจัดการหรือช่องโหว่ในระบบ เพื่อเลี่ยงการตรวจจับและยกระดับสิทธิ์การเข้าถึงบนคลาวด์ และบางครั้งยังสามารถเจาะทะลุข้ามผู้เช่า (tenant) หลายรายในระบบ multi-tenant ได้ด้วย” Microsoft กล่าว

ลำดับการโจมตีมักเริ่มจากการใช้สิทธิ์เข้าถึงที่ได้มา เพื่อยกระดับไปเป็น domain administrator จากนั้นจึงเคลื่อนย้ายไปทั่วระบบ ทำการสอดส่อง (reconnaissance) แล้วขยายไปยังคลาวด์ เปลี่ยนเป็นการโจมตีหลายขั้นตอน เช่น การฝังตัว (persistence) การยกระดับสิทธิ์ การขโมยข้อมูล การเข้ารหัส และการรีดไถ

การเข้าถึงและเทคนิคที่ใช้

ตามข้อมูลจาก Microsoft การเข้าถึงเริ่มต้น (initial access) มักได้มาจากการแฮกเกอร์รับจ้างขายสิทธิ์ (access broker) เช่น Storm-0249 และ Storm-0900 โดยใช้รหัสผ่านที่ถูกขโมยหรือรั่วไหลเพื่อเข้าสู่ระบบเป้าหมาย หรือไม่ก็ใช้ประโยชน์จากช่องโหว่ remote code execution (RCE) บนเซิร์ฟเวอร์ที่เปิดให้เข้าจากอินเทอร์เน็ตและยังไม่ได้อัปเดตแพตช์

“access broker มักขายหรือมอบสิทธิ์เข้าถึงให้กับองค์กร ซึ่งต่อมาผู้ดำเนินการแรนซัมแวร์จะนำไปใช้เพื่อโจมตี” Sherrod DeGrippo ผู้อำนวยการฝ่ายกลยุทธ์ข่าวกรองภัยคุกคามของ Microsoft กล่าว

“ในอดีต Storm-0501 และพันธมิตรเคยใช้ประโยชน์จากช่องโหว่ RCE ที่ทราบกันแล้วบนเซิร์ฟเวอร์ที่เชื่อมต่ออินเทอร์เน็ต เช่น Zoho ManageEngine, Citrix NetScaler และ Adobe ColdFusion 2016 ซึ่งช่วยให้พวกเขาสามารถเลี่ยงระบบป้องกันรอบนอก (perimeter defenses) และสร้างฐานที่มั่นภายในเครือข่ายเพื่อปูทางไปสู่การโจมตีแรนซัมแวร์ได้”

ในแคมเปญล่าสุดที่พุ่งเป้าไปยังองค์กรขนาดใหญ่ที่มีหลายบริษัทในเครือ Storm-0501 ถูกพบว่าทำการสอดส่องระบบก่อน จากนั้นจึงเคลื่อนย้ายภายในเครือข่ายโดยใช้ Evil-WinRM และยังทำการโจมตีแบบ DCSync Attack เพื่อขโมยรหัสผ่านจาก Active Directory โดยจำลองการทำงานของ domain controller

“จากจุดที่ฝังตัวใน Active Directory ผู้โจมตีได้เคลื่อนย้ายระหว่างโดเมน และในที่สุดก็สามารถเจาะเข้าไปยังเซิร์ฟเวอร์ Entra Connect อีกเครื่องหนึ่งที่เชื่อมกับ Entra ID tenant และ Active Directory domain ที่ต่างออกไป” Microsoft กล่าว

“พวกเขาขโมยบัญชี Directory Synchronization เพื่อนำไปทำกระบวนการสอดส่องซ้ำ คราวนี้เจาะไปที่ตัวตนและทรัพยากรใน tenant ที่สอง”

จาก Global Admin สู่การรีดไถ

ในที่สุดผู้โจมตีก็พบตัวตนที่เป็น non-human ที่ถูกซิงค์ไว้และมีสิทธิ์ Global Admin บน Microsoft Entra ID โดยไม่ได้เปิดใช้การยืนยันตัวตนหลายขั้นตอน (MFA) ซึ่งทำให้สามารถรีเซ็ตรหัสผ่านของผู้ใช้ในระบบ on-premises แล้วทำให้รหัสนั้นถูกซิงค์ขึ้นไปบน Entra ID ผ่าน Entra Connect Sync

เมื่อได้บัญชี Global Admin แล้วผู้โจมตีจะสามารถเข้าสู่ Azure Portal ลงทะเบียน tenant ของตนเองใน Entra ID ให้เป็นโดเมนที่เชื่อถือได้ (trusted federated domain) เพื่อสร้างช่องทางลับ (backdoor) และยกระดับสิทธิ์เข้าสู่ทรัพยากรสำคัญบน Azure ก่อนจะเริ่มกระบวนการขโมยข้อมูลและรีดไถ

“หลังจากเสร็จสิ้นขั้นตอนการขโมยข้อมูล Storm-0501 ได้ทำการลบ Azure resources ที่เก็บข้อมูลของเหยื่อทิ้งทั้งหมด เพื่อป้องกันไม่ให้เหยื่อสามารถกู้คืนหรือแก้ไขได้” Microsoft กล่าว

“เมื่อขโมยและทำลายข้อมูลใน Azure เสร็จแล้ว ผู้โจมตีก็เริ่มขั้นตอนการรีดไถ โดยติดต่อเหยื่อผ่าน Microsoft Teams ด้วยบัญชีที่เคยถูกเจาะ แล้วเรียกค่าไถ่”

คำแนะนำและการป้องกันจาก Microsoft

Microsoft ระบุว่าตอนนี้ได้มีการเปลี่ยนแปลงใน Entra ID เพื่อป้องกันไม่ให้ผู้โจมตีใช้ประโยชน์จากบัญชี Directory Synchronization เพื่อยกระดับสิทธิ์ และยังออกอัปเดต Microsoft Entra Connect เวอร์ชัน 2.5.3.0 เพื่อรองรับ Modern Authentication ที่ช่วยให้ลูกค้าตั้งค่า application-based authentication เพื่อความปลอดภัยที่มากขึ้น

“สิ่งสำคัญอีกอย่างคือควรเปิดใช้ Trusted Platform Module (TPM) บน Entra Connect Sync server เพื่อเก็บรหัสลับและกุญแจเข้ารหัสอย่างปลอดภัย ซึ่งช่วยลดความเสี่ยงจากเทคนิคขโมยรหัสของ Storm-0501 ได้” Microsoft เสริม

ข้อมูลอ้างอิง

Aug 27, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/08/storm-0501-exploits-entra-id-to.html