วันที่ 6 กรกฎาคม 2569

FortiBleed เชื่อมโยงกับกลุ่มเรียกค่าไถ่ INC และ Lynx พบข้อมูลยืนยันว่าขโมยบัญชีผู้ใช้เพื่อนำไปใช้โจมตีองค์กรต่อ

แคมเปญ FortiBleed ที่ถูกเปิดเผยเมื่อไม่นานมานี้ ซึ่งมีเป้าหมายเพื่อแสวงหาผลประโยชน์ทางการเงิน ถูกเชื่อมโยงกับปฏิบัติการของกลุ่มแรนซัมแวร์ INC และ Lynx โดยชี้ให้เห็นว่าข้อมูลบัญชีผู้ใช้ที่ถูกขโมยและผ่านการยืนยันแล้ว มีเป้าหมายเพื่อนำไปใช้เป็นช่องทางสำหรับการโจมตีองค์กรในขั้นตอนถัดไป

บริษัท SOCRadar เปิดเผยในรายงานฉบับใหม่เมื่อวันพุธว่าพบว่าผู้ปฏิบัติการที่เชื่อมโยงกับโครงสร้างพื้นฐานของ FortiBleed กำลังใช้งานระบบเจรจาเรียกค่าไถ่ของทั้งกลุ่ม INC และ Lynx ซึ่งนับเป็นครั้งแรกที่สามารถเชื่อมโยงการขโมยข้อมูลรับรองจากอุปกรณ์ FortiGate ในวงกว้าง เข้ากับการนำไปใช้ในการโจมตีด้วยแรนซัมแวร์ได้โดยตรง โดยบริษัทระบุว่า ได้ตรวจพบการสแกนพอร์ทัล FortiGate ประมาณ 11,250 แห่ง ในกว่า 150 ประเทศ จากนั้นผู้โจมตีสามารถเข้าถึงระบบด้วยสิทธิ์ผู้ดูแลระบบ ได้สำเร็จบน 409 เป้าหมาย และดำเนินกระบวนการโจมตีครบทุกขั้นตอนสำเร็จใน 354 ระบบ จากการเข้าถึงดังกล่าว มีการนำแรนซัมแวร์ไปใช้งานแล้วอย่างน้อย 12 เหตุการณ์ ส่งผลให้อุปกรณ์ปลายทาง (Endpoints) หลายร้อยเครื่องในองค์กรที่ได้รับผลกระทบถูกเข้ารหัสข้อมูล

ปฏิบัติการขโมยข้อมูลรับรองขนาดใหญ่ครั้งนี้ ซึ่งถูกเปิดเผยเมื่อเดือนที่ผ่านมา มีรูปแบบการโจมตีโดยผู้ไม่หวังดีจะสแกนหาอุปกรณ์ Fortinet ที่เปิดให้เข้าถึงจากอินเทอร์เน็ต จากนั้นพยายามเข้าสู่ระบบด้วยชุดชื่อผู้ใช้และรหัสผ่านที่เป็นที่รู้จัก ก่อนติดตั้งโปรแกรมดักจับแพ็กเก็ต (Packet Sniffer) ที่พัฒนาขึ้นเฉพาะ เพื่อดักเก็บข้อมูลบัญชีผู้ใช้และข้อมูลการยืนยันตัวตนอื่นๆ จากทราฟฟิกบนเครือข่าย คาดว่าแคมเปญดังกล่าวมุ่งเป้าไปยังไฟร์วอลล์ FortiGate ทั่วโลกประมาณ 430,000 เครื่อง และสามารถรวบรวมข้อมูลบัญชีผู้ใช้ได้มากกว่า 110 ล้านรายการ

เหตุการณ์นี้ถูกเปิดเผยหลังจากผู้โจมตีเกิดความผิดพลาดด้านความปลอดภัยในการปฏิบัติงาน (Operational Security หรือ OPSEC) ทำให้เซิร์ฟเวอร์ที่ใช้เก็บข้อมูลบัญชีผู้ใช้ซึ่งขโมยมาจากอุปกรณ์ Fortinet หลายพันเครื่อง ถูกเปิดเผยสู่สาธารณะบนอินเทอร์เน็ตโดยไม่ตั้งใจ

SOCRadar ประเมินว่าโปรแกรมดักจับข้อมูลที่พัฒนาด้วยภาษา Golang ถูกติดตั้งบนอุปกรณ์ Fortinet ประมาณ 12,000 เครื่อง ซึ่งเป็นเพียงส่วนหนึ่งของอุปกรณ์เครือข่ายทั้งหมดที่ตกเป็นเป้าหมาย

ผลการวิเคราะห์ล่าสุดของ SOCRadar ยังพบว่า ผู้ปฏิบัติการที่สามารถเข้าถึงโครงสร้างพื้นฐานของ FortiBleed ได้ มีการล็อกอินเข้าสู่ระบบเจรจาเรียกค่าไถ่ของทั้ง INC Ransom และ Lynx อีกทั้งยังพบว่ารายชื่อเหยื่อของ INC มีข้อมูลสอดคล้องกับข้อมูลที่ได้จากแคมเปญ FortiBleed

หลักฐานดังกล่าวมาจากหนึ่งใน 200 เซิร์ฟเวอร์ ที่เพิ่งถูกค้นพบและเกี่ยวข้องกับโครงสร้างพื้นฐานของ FortiBleed ซึ่งเปิดเผยไฟล์ภายใน บันทึกการทำงาน (Logs) และเอกสารที่ใช้ในการปฏิบัติการของกลุ่มผู้โจมตี

Ensar Seker ประธานเจ้าหน้าที่ฝ่ายความมั่นคงปลอดภัยสารสนเทศ (CISO) ของ SOCRadar ให้สัมภาษณ์กับ The Hacker News ผ่านอีเมลว่า เซิร์ฟเวอร์ที่ถูกเปิดเผยดังกล่าวทำหน้าที่เป็นเซิร์ฟเวอร์สำหรับเตรียมการและประสานงานปฏิบัติการ ไม่ได้ถูกใช้สำหรับการส่งอีเมลฟิชชิงหรือการเก็บข้อมูลบัญชีผู้ใช้โดยตรง

เขาอธิบายว่า เซิร์ฟเวอร์ดังกล่าวมีข้อมูลรายการเป้าหมาย ข้อมูลที่รวบรวมมาแล้ว สคริปต์สำหรับระบบอัตโนมัติ ไฟล์กำหนดค่า และหลักฐานการปฏิบัติงาน ซึ่งแสดงให้เห็นว่ามันถูกใช้เพื่อประสานงานการขโมยข้อมูลรับรองจากอุปกรณ์เครือข่ายที่เปิดให้เข้าถึงจากอินเทอร์เน็ตในวงกว้าง กล่าวอีกนัยหนึ่ง เซิร์ฟเวอร์นี้เป็นส่วนหนึ่งของโครงสร้างพื้นฐานเบื้องหลังของผู้โจมตี ไม่ใช่ระบบที่เหยื่อติดต่อหรือใช้งานโดยตรง

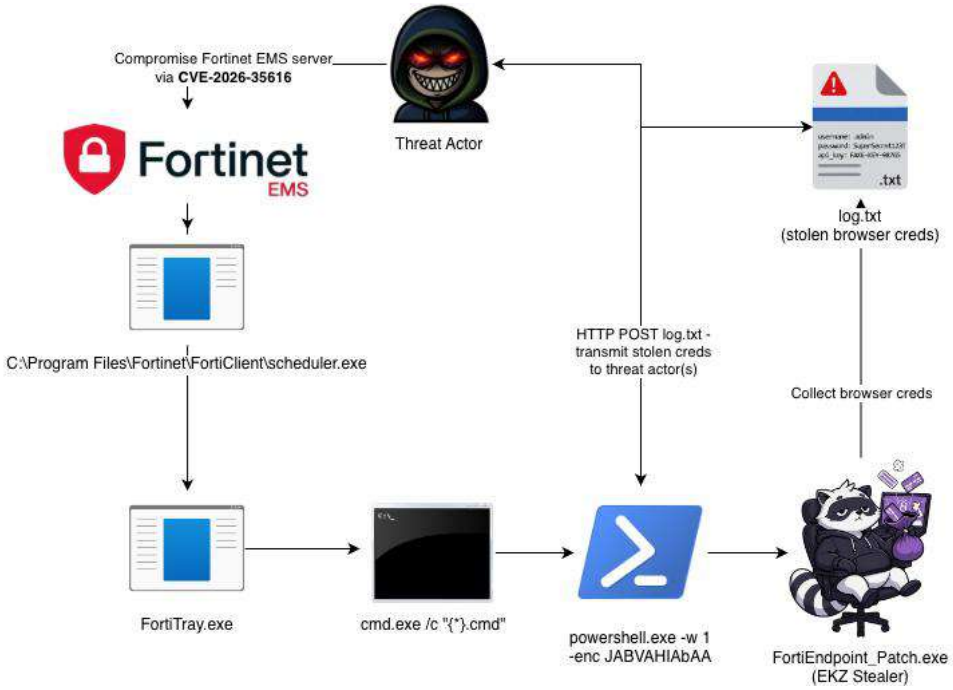
จากการวิเคราะห์เครื่องมือที่ใช้ บันทึกการทำงาน และช่วงเวลาที่มีการปฏิบัติการ SOCRadar ประเมินว่า ผู้ก่อเหตุเป็นกลุ่มที่ใช้ภาษารัสเซีย และมีแนวโน้มทำหน้าที่เป็น Initial Access Broker (IAB) หรือผู้ที่เชี่ยวชาญในการเจาะระบบเพื่อขายสิทธิ์การเข้าถึงให้กับกลุ่มอาชญากรไซเบอร์รายอื่น

เป้าหมายหลักของการโจมตีส่วนใหญ่อยู่ในอุตสาหกรรมการผลิต เทคโนโลยี และโลจิสติกส์ โดยเฉพาะในภูมิภาค ลาตินอเมริกา และ เอเชียแปซิฟิก

SOCRadar ยังพบเอกสารภายในที่บ่งชี้ว่า ปฏิบัติการนี้มีการจัดโครงสร้างอย่างเป็นระบบ มีสมาชิกประมาณ 20 คน พร้อมแบ่งหน้าที่รับผิดชอบอย่างชัดเจน บริษัทระบุเพิ่มเติมว่า ผู้ปฏิบัติการหลักเพียงไม่กี่คนเป็นผู้ดำเนินการโจมตีที่สร้างผลกระทบสูง ขณะที่มีผู้เชี่ยวชาญและทีมสนับสนุนคอยช่วยเหลือในส่วนต่างๆ

นอกจากนี้ ยังมีความเป็นไปได้ว่ากลุ่มผู้โจมตีครอบครองช่องโหว่ Zero-Day อย่างน้อยหนึ่งรายการใน Nextcloud โดย SOCRadar ระบุว่ากำลังประสานงานกับผู้พัฒนาซอฟต์แวร์ที่ได้รับผลกระทบแล้ว

บริษัทซึ่งตั้งอยู่ในรัฐเดลาแวร์ของสหรัฐฯ ยังพบหลักฐานที่เกี่ยวข้องกับ Citrix ซึ่งบ่งชี้ว่าผู้โจมตีอาจกำลังขยายเป้าหมายจากอุปกรณ์ Fortinet ไปยังระบบอื่นด้วย โครงสร้างพื้นฐานที่ตรวจพบมีรายการเป้าหมายเฉพาะสำหรับสภาพแวดล้อมของ Citrix ประกอบด้วยที่อยู่ IP ประมาณ 29,000 รายการ และ 37 โดเมน ซึ่งสะท้อนว่ากระบวนการโจมตีแบบอัตโนมัติอาจถูกนำไปประยุกต์ใช้กับเทคโนโลยีการเข้าถึงจากระยะไกลประเภทอื่นในอนาคต



Seker อธิบายว่า ในขณะนี้การพบรายการเป้าหมายดังกล่าวยังไม่สามารถยืนยันได้ว่ามีการขโมยข้อมูลบัญชีผู้ใช้จากอุปกรณ์ Citrix ในวงกว้างแล้ว อย่างไรก็ตาม สิ่งที่พบแสดงให้เห็นอย่างชัดเจนว่าผู้โจมตีกำลังดำเนินการสอดแนมและเตรียมเป้าหมายไว้ล่วงหน้า เขายังเตือนเพิ่มเติมว่า เมื่อพิจารณาจากความซับซ้อนของโครงสร้างพื้นฐาน และความสามารถของผู้โจมตีที่พิสูจน์แล้วว่าสามารถทำระบบอัตโนมัติสำหรับการขโมยข้อมูลบัญชีผู้ใช้จากอุปกรณ์ Fortinet ได้ องค์กรที่มีระบบ Citrix เปิดให้เข้าถึงจากอินเทอร์เน็ตควรถือว่านี่เป็นสัญญาณเตือนล่วงหน้า พร้อมตรวจสอบบันทึกการยืนยันตัวตน เปลี่ยนรหัสผ่านของบัญชีที่อาจได้รับผลกระทบ เปิดใช้งานการยืนยันตัวตนหลายปัจจัย (MFA) และเฝ้าระวังกิจกรรมการเข้าสู่ระบบที่ผิดปกติ

การเปิดเผยข้อมูลครั้งนี้เกิดขึ้นในช่วงเดียวกับที่บริษัท eSentire รายงานว่า พบผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่ CVE-2026-35616 (คะแนนความรุนแรง CVSS 9.1) ใน Fortinet FortiClient EMS เพื่อแพร่กระจายมัลแวร์ขโมยข้อมูล EKZ Stealer ไปยังลูกค้าในกลุ่มธุรกิจพลังงาน สาธารณูปโภค และการจัดการของเสีย

เป้าหมายของการโจมตีคือการขโมยข้อมูลบัญชีผู้ใช้ที่จัดเก็บอยู่ในเว็บเบราว์เซอร์ที่ใช้เอนจิน Chromium และ Firefox ก่อนส่งข้อมูลที่ขโมยได้ออกไปยังผู้โจมตีผ่าน PowerShell

ข้อมูลอ้างอิง

Jul 2, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/fortibleed-credential-theft-linked-to.html