วันที่ 25 มิถุนายน 2569

FortiBleed มุ่งเป้าโจมตีไฟร์วอลล์ FortiGate ในปฏิบัติการขโมยข้อมูลรับรองกว่า 110 ล้านรายการ

กลุ่ม Initial Access Broker (IAB) ที่ใช้ภาษารัสเซียและมีแรงจูงใจหลักด้านผลประโยชน์ทางการเงิน ถูกประเมินว่าอยู่เบื้องหลังปฏิบัติการขโมยข้อมูลรับรองขนาดใหญ่ที่มีชื่อว่า FortiBleed ซึ่งมุ่งเป้าโจมตีอุปกรณ์ไฟร์วอลล์ FortiGate มากกว่า 430,000 เครื่องทั่วโลก

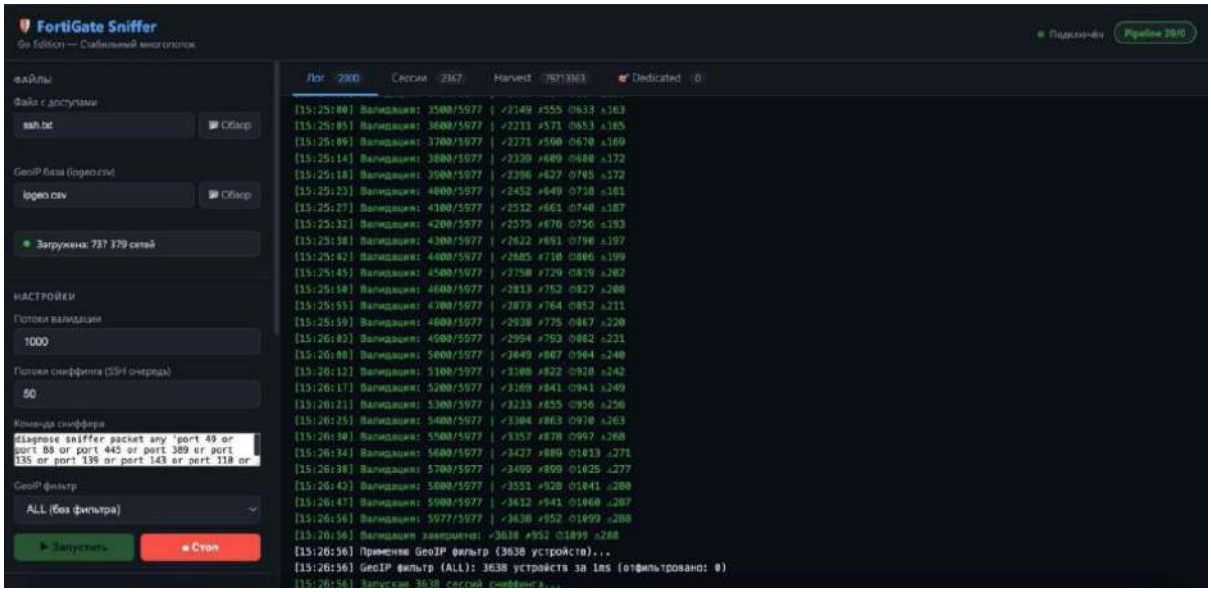
แคมเปญดังกล่าวเริ่มดำเนินการมาตั้งแต่เดือนกุมภาพันธ์ 2026 โดยมีการรวบรวมรายการข้อมูลรับรอง ค้นหาบริการที่เปิดเผยสู่ภายนอก พยายามเดารหัสผ่านเข้าสู่ระบบที่เข้าถึงได้ และติดตั้งโปรแกรมดักจับข้อมูลที่พัฒนาขึ้นเฉพาะบนไฟร์วอลล์ที่ถูกเจาะระบบ

เมื่อถูกติดตั้งแล้ว โปรแกรมดักจับข้อมูลเหล่านี้จะสามารถเก็บทั้งข้อมูลรับรองแบบข้อความธรรมดา (cleartext) และค่าแฮชของรหัสผ่านจากทราฟฟิกที่วิ่งผ่านอุปกรณ์ที่ถูกบุกรุก" SOCRadar ระบุในรายงานฉบับล่าสุด [PDF] "จากนั้นผู้โจมตีจะนำข้อมูลเหล่านี้ไปถอดรหัส ตรวจสอบความถูกต้อง และนำกลับมาใช้กับโดเมน Active Directory รวมถึงบริการอื่นๆ ที่เปิดให้เข้าถึงจากภายนอก

หัวใจสำคัญของปฏิบัติการนี้คือเครื่องมือที่พัฒนาด้วยภาษา Golang ชื่อว่า FortigateSniffer ซึ่งอาศัยคำสั่งวินิจฉัยภายในของ FortiOS อย่าง diagnose sniffer packet เพื่อดักจับทราฟฟิกสำหรับการยืนยันตัวตนแบบเงียบ ๆ จากอุปกรณ์ที่ติดมัลแวร์ เครื่องมือนี้มีทั้งเวอร์ชันสำหรับ Windows และ Unix โดยสามารถตรวจสอบทราฟฟิกได้ถึง 24 โปรโตคอล วิเคราะห์ข้อมูลการยืนยันตัวตน และดึงข้อมูลรับรองออกมาได้

นอกจากนี้ ยังมีความเป็นไปได้ว่าผู้โจมตีอาจใช้ความช่วยเหลือจากแพลตฟอร์มด้าน Offensive Security แบบโอเพนซอร์สที่ขับเคลื่อนด้วย AI ชื่อ CyberStrike เพื่อช่วยใน "บางส่วนของกระบวนการทำงาน" ที่น่าสนใจคือ ก่อนหน้านี้ Amazon Threat Intelligence เคยเปิดเผยว่าเฟรมเวิร์กโอเพนซอร์สอีกตัวหนึ่งชื่อ CyberStrikeAI ถูกนำมาใช้ในแคมเปญสแกนอุปกรณ์ FortiGate แบบอัตโนมัติในวงกว้างเมื่อต้นปีที่ผ่านมา

แคมเปญนี้ให้ความสำคัญกับธุรกิจขนาดเล็กและขนาดกลาง (SMBs) ที่มีพนักงานน้อยกว่า 200 คนเป็นพิเศษ SOCRadar อธิบายว่า ผู้โจมตีมุ่งเป้าหมายไปยังหลายอุตสาหกรรมและหลายภูมิภาค โดยเน้นที่สหรัฐอเมริกาและอินเดียเป็นหลัก กลุ่มธุรกิจด้านบริการไอทีถือเป็นหนึ่งในเป้าหมายสำคัญ เนื่องจากหากสามารถเข้าถึงผู้ให้บริการเหล่านี้ได้ ก็อาจนำไปสู่การเข้าถึงเครือข่ายของลูกค้าได้อีกทอดหนึ่ง



สิ่งที่น่าสนใจมากที่สุดคือ FortiBleed ดูเหมือนจะเป็นส่วนหนึ่งของปฏิบัติการขนาดใหญ่ที่มุ่งโจมตีอุปกรณ์จากหลายผู้ผลิต ไม่ได้จำกัดเฉพาะ Fortinet เท่านั้น แต่ยังรวมถึง Synology NAS, ไฟร์วอลล์ Sophos, พอร์ทัล RDWeb, Citrix SSL-VPN และเซิร์ฟเวอร์ MS-SQL ผ่านการโจมตีแบบเดารหัสผ่านอัตโนมัติมาตั้งแต่วันที่ 28 กุมภาพันธ์ 2026

โดยรวมแล้ว คาดว่าผู้โจมตีได้ดำเนินกระบวนการเก็บข้อมูลรับรองอย่างน้อย 659 ชุด ระหว่างวันที่ 31 พฤษภาคม ถึง 15 มิถุนายน 2026 ส่งผลให้สามารถระบุข้อมูลรับรองได้มากกว่า 110 ล้านรายการ ซึ่งประกอบด้วย

- ข้อมูลรับรอง RADIUS (Remote Authentication Dial-In User Service) จำนวน 14.8 ล้านรายการ
- ค่าแฮช NTLM จำนวน 924,000 รายการ
- ค่าแฮช Kerberos จำนวน 130,000 รายการ
- โทเคนยืนยันตัวตน MySQL จำนวน 89 ล้านรายการ

แคมเปญ FortiBleed ประกอบด้วย 5 ขั้นตอนหลัก ดังนี้

- ดำเนินการสำรวจเป้าหมายในวงกว้างโดยใช้เครื่องมืออย่าง Masscan และ Shodan เพื่อค้นหาไฟร์วอลล์ FortiGate ที่เปิดให้เข้าถึงจากอินเทอร์เน็ต จากนั้นใช้เครื่องมือเฉพาะชื่อ FortiProbe-fast และ GeoSplit เพื่อคัดกรองอุปกรณ์ FortiGate และจัดกลุ่มตามประเทศ

- เจาะระบบอุปกรณ์ด้วยเครื่องมือตรวจสอบข้อมูลรับรองชื่อ "forticheck" ซึ่งออกแบบมาเพื่อโจมตีหน้าแอดมินและ SSL-VPN ของ FortiGate รวมถึงใช้เทคนิค Credential Stuffing และ Dictionary Attack เพื่อพยายามเข้าสู่ระบบ SSH ในระดับผู้ดูแลระบบ
- หลังจากเข้าถึง SSH ได้สำเร็จ จะติดตั้ง FortigateSniffer เพื่อดักจับทราฟฟิกการยืนยันตัวตนแบบเงียบ ๆ บน 24 โปรโตคอล เช่น TACACS+, Kerberos, RPC, SMB, LDAP, SMTP, FTP, Telnet, RDP, WinRM, MS-SQL, MySQL, PostgreSQL และ RADIUS โดยใช้คำสั่งวินิจฉัยภายในของ FortiOS ทำให้สามารถเก็บข้อมูลรับรองและค่าแฮชรหัสผ่านได้
- ค่าแฮชที่ได้จะถูกถอดรหัสด้วย Hashcat และ Hashtopolis โดยมี Telegram Bot ชื่อ HASHBOT คอยควบคุมกระบวนการ จากนั้นนำข้อมูลที่ถอดรหัสแล้วไปใช้สำหรับการเคลื่อนที่ภายในเครือข่าย (Lateral Movement) การสำรวจ Active Directory การตรวจสอบ Kerberos และการยืนยันตัวตนผ่าน SMB
- ข้อมูลสำคัญจาก Network Share จะถูกดึงออกจากระบบ ขณะที่คุกกี้เซสชันที่ถูกขโมยจะถูกใช้เพื่อรักษาสิทธิ์การเข้าถึงแบบต่อเนื่อง

กลุ่มนี้ไม่ได้ปฏิบัติต่อเป้าหมายทุกแห่งเหมือนกัน" SOCRadar กล่าว "แต่จะจัดอันดับเป้าหมายตามมูลค่าทางเศรษฐกิจก่อนตัดสินใจว่าจะทุ่มทรัพยากรโจมตีมากน้อยเพียงใด

นอกจากนี้ กลไกการดักจับข้อมูลยังมีระบบ Geofencing ที่จำกัดการทำงานเฉพาะช่วง IP ที่กำหนด และจำกัดเวลาในการปฏิบัติการไว้ระหว่าง 07:00 น. ถึง 18:00 น. ตามเวลามอสโกว์ ตามไทม์ไลน์ที่ SpyCloud เปิดเผย วงจรการดักจับข้อมูลจาก FortiGate เริ่มต้นเมื่อวันที่ 19 พฤษภาคม 2026 ขณะที่โครงสร้างพื้นฐานสำหรับการถอดรหัสค่าแฮชถูกจัดเตรียมในช่วงปลายเดือนเดียวกัน

ปฏิบัติการนี้ทำงานเป็นรอบๆ ละ 300 นาที (5 ชั่วโมง) และรายงานสถานะทุกหนึ่งนาที Zenox ระบุ ในแต่ละรอบ ระบบจะโหลดรายการเป้าหมายตามภูมิภาคและตรวจสอบพร้อมกันด้วย 1,000 เธรด โดยแสดงจำนวนการเชื่อมต่อสำเร็จ ล้มเหลว หมดเวลา และคำเตือนต่างๆ ในช่วงแรกๆ อัตราความสำเร็จในการตรวจสอบอยู่ใกล้ระดับ 90%

บริษัทด้านความมั่นคงปลอดภัยไซเบอร์จากบราซิลยังระบุอีกว่า พบชื่อผู้ใช้และรหัสผ่านบางชุดถูกใช้งานซ้ำบน IP หลายพันรายการ ซึ่งอาจเป็นไปได้ว่าผู้โจมตีได้สร้างบัญชีเหล่านี้ไว้เป็นช่องทางลับสำหรับเข้าถึงระบบในภายหลัง

สถิติดังกล่าวได้มาจากการรวบรวมคอลัมน์ username:password จากไฟล์ all_valid.txt ของผู้โจมตี ซึ่งเป็นรายการข้อมูลรับรองที่ตรวจสอบแล้วในรูปแบบ IP:PORT:USERNAME:PASSWORD โดยมีทั้งหมด 21,976 รายการ" Acassio Silva ผู้ร่วมก่อตั้งและหัวหน้าฝ่าย Threat Intelligence ของ ZenoX

ข้อมูลชุดเดียวกันยังปรากฏในไฟล์ EU.txt ซึ่งเป็นรายการเป้าหมายที่โปรแกรม Go ของผู้โจมตีโหลดกลับมาตรวจสอบซ้ำทุกครั้ง รวมถึงไฟล์ต่อยอดอื่นๆ เช่น valid_*.txt, matched_targets*, corps.txt, targets_300M_plus.txt และไฟล์ JSON ที่

เก็บข้อมูลที่ขโมยมา ในไฟล์ all_valid.txt พบว่าบัญชี adminin:ITAdmin@888 ปรากฏอยู่บนอุปกรณ์ถึง 3,947 เครื่อง ส่วนในกลุ่มเป้าหมายยุโรปเพียงอย่างเดียว พบข้อมูลชุดนี้บนอุปกรณ์ 1,562 เครื่อง

ข้อสันนิษฐานว่าบัญชีเหล่านี้อาจถูกสร้างขึ้นโดยผู้โจมตีเอง แทนที่จะเป็นบัญชีจริงขององค์กร มาจาก 3 ปัจจัย ได้แก่ การใช้ข้อมูลชุดเดียวกันในองค์กรที่ไม่เกี่ยวข้องกันหลายพันแห่ง การไม่พบรหัสผ่านดังกล่าวในแหล่งข้อมูลบางชุด และชื่อผู้ใช้ที่ถูกตั้งให้คล้ายกับบริการของ Fortinet หรือ FortiCloud เพื่อให้ดูกลมกลืนกับสภาพแวดล้อมจริง

เหตุการณ์นี้เกิดขึ้นในช่วงเดียวกับที่บัญชีผู้ใช้ภาษารัสเซียชื่อ "SantaAd" นำการเข้าถึงอุปกรณ์ Fortinet หลายพันเครื่องออกประกาศขาย โดยตั้งราคาเริ่มต้นที่ 30,000 ดอลลาร์ ก่อนจะเพิ่มเป็น 60,000 ดอลลาร์ในอีกไม่กี่ชั่วโมงต่อมา อย่างไรก็ตาม ยังไม่มีหลักฐานยืนยันว่ามีความเกี่ยวข้องกับ FortiBleed หรือไม่

กลุ่มผู้โจมตีที่อยู่เบื้องหลัง FortiBleed ไม่ได้มุ่งเป้าเฉพาะ VPN ของ FortiGate SpyCloud พวกเขายังโจมตีอุปกรณ์ที่เปิดให้เข้าถึงจากอินเทอร์เน็ตหลากหลายประเภท โดยใช้แนวทางแบบหว่านแห ซึ่งอาศัยการสแกนจำนวนมากและการเดารหัสผ่านเป็นหลัก

FortiBleed กับการใช้ CyberStrike Harvester v1.5

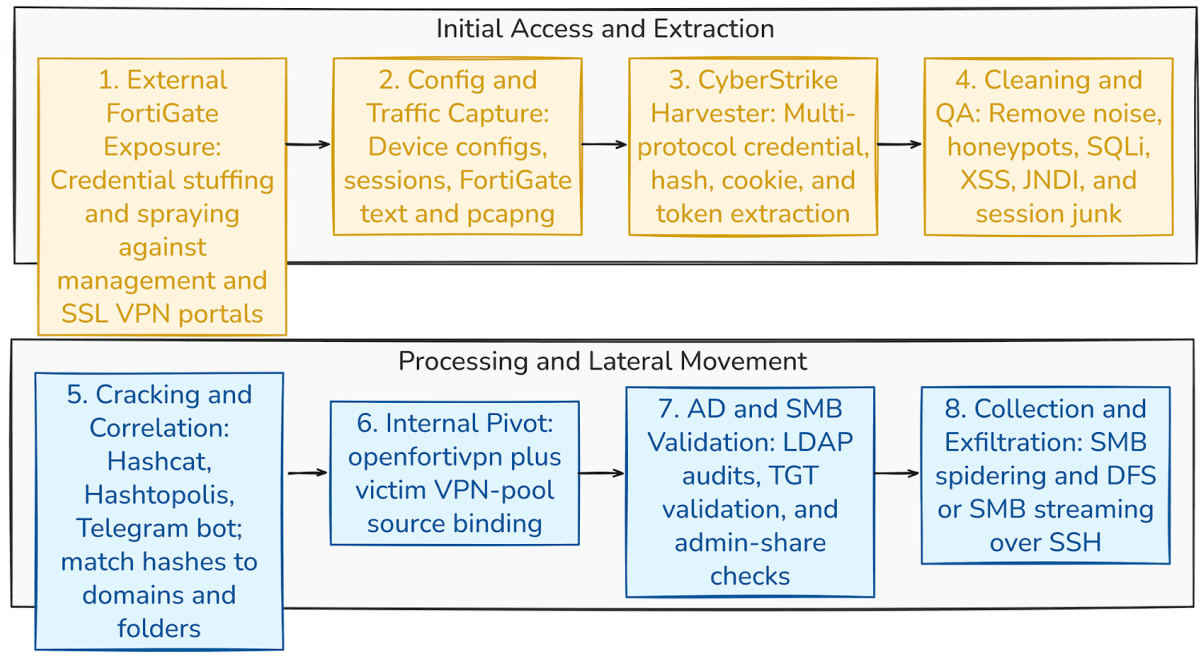
ในรายงานติดตามผล Arctic Wolf อธิบายว่า FortiBleed เป็นแคมเปญที่ใช้ "กระบวนการจัดการข้อมูลรับรองแบบครบวงจร ซึ่งประกอบด้วย Credential Stuffing, Password Spraying, การดึงค่าคอนฟิก การถอดรหัสแบบออฟไลน์ และการประมวลผลข้อมูลที่ได้หลังการยืนยันตัวตน" โดยเมื่อสามารถเข้าถึง FortiGate ได้แล้ว จะขยายผลไปสู่การดึงข้อมูลรับรองหลายโปรโตคอล การถอดรหัสค่าแฮช การเข้าถึง AD/SMB ผ่าน VPN และการดึงข้อมูลจาก File Share

ลักษณะสำคัญของการโจมตีครั้งนี้คือ ไม่มีการใช้ช่องโหว่ Zero-Day ใหม่แต่อย่างใด โดย Fortinet ระบุว่าผู้โจมตีน่าจะนำข้อมูลรับรองจากเหตุการณ์ก่อนหน้ามาใช้ซ้ำ รวมถึงพยายามเดารหัสผ่านบนอุปกรณ์ที่ใช้รหัสผ่านอ่อนแอและไม่ได้เปิดใช้งานการยืนยันตัวตนหลายปัจจัย (MFA)

"จุดเด่นของปฏิบัติการนี้คือวงจรย้อนกลับของข้อมูลรับรอง" Arctic Wolf กล่าว "เมื่อสามารถเข้าถึงระบบภายนอกได้สำเร็จ ก็จะได้คอนฟิกหรือทราฟฟิกที่นำไปสู่ข้อมูลรับรองและค่าแฮชเพิ่มเติม จากนั้นข้อมูลที่ถอดรหัสได้จะถูกนำไปใช้กับ VPN, Kerberos, SMB และการเข้าถึง Share ต่างๆ และการเข้าถึงที่ยืนยันแล้วก็จะนำไปสู่การเก็บข้อมูลเพิ่มเติมต่อไป"

กิจกรรมดังกล่าวยังรวมถึงการส่งออกไฟล์คอนฟิกจากอุปกรณ์ FortiGate ที่เปิดสู่ภายนอก และนำค่าแฮชที่จัดเก็บอยู่ภายในมาถอดรหัส พร้อมใช้ชุดเครื่องมือดึงข้อมูลแบบกำหนดเองชื่อ "harvest_orig" เพื่อเปลี่ยนข้อมูลที่ดักจับได้ให้กลายเป็น "ข้อมูลรับรองที่นำไปใช้งานได้จริง ค่าแฮชที่สามารถถอดรหัสได้ เซสชันเว็บ ข้อมูลด้านตัวตน และข้อมูลสำหรับการโจมตีในขั้นตอนถัดไป"

ไฟล์ ELF ที่พัฒนาด้วยภาษา Go ซึ่งระบุตัวเองว่า CyberStrike Harvester v1.5 มีฟังก์ชันสำหรับอ่านไฟล์ pcap, pcapng และข้อมูลจาก FortiGate รวมถึงฟังก์ชันสำหรับแยกและจัดรูปแบบคุกกี้ เซสชัน และโทเคนของโปรโตคอลต่างๆ กว่าสองโหล



ชั้นการถอดรหัสค่าแฮชถูกออกแบบอย่างเป็นระบบ ไม่ใช่การประกอบเครื่องมือแบบชั่วคราว รายงานระบุ Telegram Bot จะรับค่าแฮช ตรวจสอบสิทธิ์ผู้ใช้ตามชื่อบัญชี Telegram ตรวจจับประเภทของแฮช ขอข้อมูลประกอบ จัดคิวงาน จัดสรร GPU เริ่มกระบวนการ Hashcat หลายขั้นตอน ติดตามเวลาและความคืบหน้า ก่อนส่งผลลัพธ์กลับ

โหมดการถอดรหัสที่รองรับ ได้แก่ NetNTLMv2, FortiGate256, RAKP, MS-SQL และ Kerberos หลายรูปแบบ ขณะที่ Hashtopolis และ HashPanel แบบกำหนดเองถูกใช้สำหรับบริหารจัดการการถอดรหัสแบบกระจายศูนย์ รวมถึงมีสคริปต์สำหรับเตรียมเครื่อง GPU และลงทะเบียนเอเจนต์อัตโนมัติ

ในกรณีที่ข้อมูลรับรองที่กู้คืนมาใช้งานได้จริง ผู้โจมตีจะใช้ SSL-VPN ที่ผ่านการยืนยันตัวตนแล้ว ร่วมกับเครื่องมือ Impacket เพื่อสำรวจ Active Directory ตรวจสอบ Kerberos ยืนยันตัวตนผ่าน SMB ตรวจสอบ Administrative Share ค้นหาไฟล์ใน SMB Share และเก็บข้อมูลจาก DFS/SMB

องค์กรที่ได้รับผลกระทบควรดำเนินการเปลี่ยนรหัสผ่านทั้งหมด ยกเลิกเซสชันที่ยังคงใช้งานอยู่ ตรวจสอบการส่งออกไฟล์คอนฟิก ทบทวนบันทึกการเข้าใช้งาน SSL-VPN ตรวจสอบกิจกรรม AD และ SMB ที่มาจากกลุ่ม IP ของ VPN สแกนหาร่องรอยการส่งข้อมูลผ่าน SSH ออกนอกเครือข่าย และตรวจสอบบันทึกการเข้าถึง SMB Share ที่มีการอ่านข้อมูลจำนวนมากแบบต่อเนื่อง

FortiBleed แสดงให้เห็นว่าข้อมูลรับรองที่รั่วไหลบนระบบภายนอก สามารถนำไปสู่การเปิดเผยเครือข่ายภายในได้อย่างสมบูรณ์" บริษัทกล่าวเพิ่มเติม "สิ่งที่สำคัญที่สุดคือความเป็นระบบของกระบวนการทั้งหมด ตั้งแต่ห้องปฏิบัติการของผู้โจมตี แผงควบคุม Sniffer เครื่องมือ CyberStrike Harvester สคริปต์ทำความสะอาดข้อมูล โครงสร้างพื้นฐาน Hashcat/Hashtopolis เครื่องมือตรวจสอบ Kerberos ระบบจัดอันดับโดเมนและรายได้ ตลอดจนเครื่องมือ SMB/DFS ซึ่งทั้งหมดถูกออกแบบให้เป็นกระบวนการที่สามารถนำกลับมาใช้ซ้ำได้

CloudSEK เรียกกิจกรรมนี้ว่าเป็น "การกวาดค้นหาเป้าหมายทั่วอินเทอร์เน็ตแบบไม่เลือกหน้า" พร้อมระบุว่าชุดเครื่องมือของผู้โจมตีถูกใช้เพื่อสร้างฐานข้อมูลเป้าหมายการเข้าถึงระยะไกลที่ถูกจัดเรียงตามมูลค่าทางธุรกิจ ซึ่งอาจถูกนำไปขายต่อในตลาดใต้ดิน

ภายในไดเรกทอรียังพบไฟล์คอนฟิก SSL VPN ที่ยังใช้งานได้จริงอย่างน้อยหนึ่งไฟล์ ซึ่งเชื่อมต่อเข้าสู่เครือข่ายของเหยื่อโดยตรง ยืนยันว่าผู้ปฏิบัติการเหล่านี้ไม่ได้มีเพียงรายการรหัสผ่านที่ถอดรหัสได้เท่านั้น แต่ยังมีสิทธิ์เข้าถึงระบบที่ใช้งานได้จริงอยู่ด้วย" บริษัทระบุ

(บทความนี้ได้รับการอัปเดตหลังเผยแพร่เมื่อวันที่ 24 มิถุนายน 2026 โดยเพิ่มข้อมูลเชิงลึกจาก Arctic Wolf, CloudSEK และ Zenox)

ข้อมูลอ้างอิง

Jun 23, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/06/fortibleed-targeted-fortigate-firewalls.html