วันที่ 20 สิงหาคม 2569

## StopAndProtect ใช้เว็บไซต์ WordPress ที่ถูกแฮ็กเกือบ 2,000 แห่งเพื่อแพร่มัลแวร์และขโมยข้อมูล


นักวิจัยด้านความปลอดภัยทางไซเบอร์ได้เปิดเผยปฏิบัติการอาชญากรรมไซเบอร์ระดับโลกที่ใช้เว็บไซต์ WordPress หลายพันแห่งซึ่งถูกแฮ็กเป็นโครงสร้างพื้นฐานสำหรับแพร่กระจายมัลแวร์ ควบคุมเครื่องที่ติดมัลแวร์ รวมถึงจัดเก็บเอกสารที่ถูกขโมย ภาพหน้าจอ และบันทึกกิจกรรมที่ใช้ติดตามสถานะของการดำเนินงาน ปฏิบัติการนี้ไม่ได้พึ่งพามัลแวร์เพียงตัวเดียว แต่เป็นชุดเครื่องมืออาชญากรรมไซเบอร์ทั้งหมดที่ทำงานร่วมกัน โดยบางส่วนใช้เข้ารหัสไฟล์ บางส่วนแอบขโมยเอกสารหรือล็อกหน้าจอ และอีกส่วนทำหน้าที่เป็นแชทสดระหว่างผู้โจมตีและเหยื่อ

Check Point บริษัทด้านความปลอดภัยทางไซเบอร์ได้ติดตามแคมเปญขนาดใหญ่ดังกล่าวภายใต้ชื่อ StopAndProtect หลังจากค้นพบตระกูลแรนซัมแวร์ที่ใช้ชื่อเดียวกันในช่วงกลางเดือนพฤษภาคม 2026 โดยกระบวนการติดเชื้อเริ่มต้นจากการโจมตีแบบ Social Engineering ที่เรียกว่า ClickFix ซึ่งทำให้มีการรันคำสั่ง PowerShell และนำไปสู่การติดตั้งตัวดาวน์โหลดและตัวโหลด .NET เพิ่มเติม

จากนั้นจึงนำไปสู่การทำงานของส่วนประกอบหลักต่างๆ ได้แก่ Ransomware, SMB/USB worm, LockScreen, VBS spreader, เครื่องมือแชท และโปรแกรมขโมยข้อมูลรับรอง อย่างไรก็ตาม ควรสังเกตว่าปฏิบัติการนี้ไม่ได้ลงแรนซัมแวร์ในทุกครั้ง ในกรณีส่วนใหญ่พบว่ากลุ่มผู้โจมตีแอบขโมยรายชื่อไฟล์ และจากนั้นจึงเลือกขโมยไฟล์บางรายการจากระบบ

ปฏิบัติการนี้ได้รับการสนับสนุนจากกลุ่มเว็บไซต์ WordPress ที่ถูกแฮ็ก ซึ่งทำหน้าที่หลายอย่าง ได้แก่

- ใช้โฮสต์ไฟล์มัลแวร์ในแต่ละขั้นตอน
- ทำหน้าที่เป็นเซิร์ฟเวอร์ Command-and-Control (C2) เพื่อส่งคำสั่ง
- ใช้จัดเก็บบันทึกข้อมูลที่ถูกขโมยออกมาจากเครื่องของเหยื่อ

Check Point ยังระบุว่าสามารถค้นพบข้อมูลเพิ่มเติมเกี่ยวกับแคมเปญนี้ได้จากความผิดพลาดด้านการรักษาความปลอดภัยของผู้โจมตีเอง ซึ่งทำให้พบทั้งบันทึกการติดเชื้อโดยละเอียด ภาพหน้าจอจากเครื่องของเหยื่อ รวมถึงเครื่องมือที่ใช้จัดการเว็บไซต์ที่ถูกแฮ็กจำนวนมาก โดยคาดว่ามีเว็บไซต์ WordPress เกือบ 2,000 แห่งถูกแฮ็กเป็นส่วนหนึ่งของแคมเปญนี้

เว็บไซต์ส่วนใหญ่ที่พบไม่เพียงใช้ WordPress เวอร์ชันเก่า แต่ยังมีการติดตั้งปลั๊กอินที่ล้าสมัยอีกด้วย ตัวอย่างเช่น หนึ่งในเว็บไซต์ที่ถูกแฮ็กใช้ WordPress เวอร์ชันจากปี 2021 ทำให้เว็บไซต์ดังกล่าวมีช่องโหว่ที่อาจถูกโจมตีได้ประมาณ 40 รายการ

เว็บไซต์เหล่านี้ถูกแก้ไขเนื้อหาเพื่อแสดงหน้า CAPTCHA ปลอมในลักษณะเดียวกับ ClickFix ให้กับผู้เข้าชม ซึ่งทำให้ผู้เข้าชมติดมัลแวร์ได้ในที่สุด คำสั่ง PowerShell ที่ถูกเรียกใช้ด้วยวิธีนี้จะทำหน้าที่เป็นจุดเริ่มต้นของกระบวนการหลายขั้นตอน ได้แก่

- ตัวดาวน์โหลด .NET ระยะที่ 1 ซึ่งส่งผลกลับไปยังเซิร์ฟเวอร์ C2 และโหลดขั้นตอนถัดไป
- ตัวดาวน์โหลดและตัวโหลด .NET ระยะที่ 2 ซึ่งมีการตรวจสอบสภาพแวดล้อมแบบ Sandbox รวมถึงระบบบันทึกข้อมูลเพิ่มเติม และทำการเรียกใช้ส่วนประกอบหลัก
- ระยะที่ 3 ซึ่งประกอบด้วยส่วนประกอบ 6 รายการ
    - **SilentEncryptor** ซึ่งเข้ารหัสคอมพิวเตอร์ที่ติดมัลแวร์ทั้งหมด หรือเลือกเข้ารหัสเฉพาะคอมพิวเตอร์ที่มีชื่อ Host name ที่กำหนด
    - **NetworkShareScanner** ซึ่งทำหน้าที่คล้าย SMB/USB worm เพื่อแพร่กระจายไปยังอุปกรณ์อื่น
    - **VBS spreader** ซึ่งแพร่กระจายมัลแวร์ไปยังฮาร์ดดิสก์และอุปกรณ์จัดเก็บข้อมูลแบบถอดออกได้ สแกนเครือข่าย และเคลื่อนที่ไปยังระบบอื่นผ่าน WMI
    - **LockScreen** ซึ่งบล็อกการใช้งานของผู้ใช้และแสดงข้อความเรียกค่าไถ่พร้อม QR Code สำหรับชำระเงิน
    - **SimpleChatProxy** ซึ่งเป็นแอปพลิเคชันแชทที่สร้างขึ้นโดยเฉพาะสำหรับใช้สื่อสารระหว่างเหยื่อกับผู้โจมตี
    - **SilentDataCollector** ซึ่งสร้างรายชื่อไดรฟ์ทั้งหมด เข้ารหัสข้อมูลดังกล่าว และส่งรายชื่อกลับไปยังเซิร์ฟเวอร์ C2 โดยผู้โจมตีสามารถอัปโหลดไฟล์คำสั่งไปยังเซิร์ฟเวอร์ เพื่อให้โปรแกรมขโมยข้อมูลอ่านและนำไปใช้ขโมยไฟล์ที่ต้องการได้

มัลแวร์ขโมยข้อมูลในเวอร์ชันใหม่ๆ ยังมีความสามารถเพิ่มเติม เช่น การบันทึกการกดแป้นพิมพ์ (Keylogger) พร้อมตรวจจับที่อยู่อีเมลที่ใช้งานได้ การขโมยข้อมูลจาก WhatsApp การเชื่อมต่อและยกเลิกการเชื่อมต่อ Network Share รวมถึงการจับภาพหน้าจอการใช้งานของผู้ใช้ทุกๆ 30 วินาที ผู้โจมตีสามารถกำหนดคำค้นหาใน WhatsApp ได้ โดยรองรับทั้งเวอร์ชันบนเว็บและเวอร์ชันเดสก์ท็อป

Check Point ระบุว่าโปรแกรมขโมยข้อมูลจะรอจนกว่าเหยื่อจะไม่ได้ใช้งานเครื่อง จากนั้นจึงใช้ระบบอัตโนมัติของ WhatsApp เพื่อเลือกช่องค้นหา กรอกคำค้นหาที่กำหนด เช่น ชื่อผู้ติดต่อ เปิดข้อมูลของผู้ติดต่อนั้น และจับภาพหน้าจอ

การตรวจสอบเพิ่มเติมพบว่าผู้โจมตีใช้ไฟล์ ZIP ที่มีไฟล์ PHP ชื่อ uploader-installer.php เพื่อทำการติดตั้งปลั๊กอิน WordPress ที่สร้างขึ้นโดยเฉพาะ ซึ่งปลั๊กอินดังกล่าวถูกใช้เพื่อสร้างไฟล์ must-use (MU) plugin ในไดเรกทอรี wp-content/mu-plugins

ปลั๊กอินนี้เปิดให้ผู้ที่มีข้อมูลรับรองที่ถูกต้องสามารถอัปโหลดไฟล์ใดๆ รวมถึงไฟล์ PHP ไปยังเว็บไซต์ WordPress ได้เกือบทุกตำแหน่งภายใต้ไดเรกทอรีหลักของ WordPress การอัปโหลดไฟล์ PHP ในลักษณะนี้สามารถนำไปสู่การรันโค้ดจากระยะไกลได้ หลังจากเว็บไซต์ถูกเจาะแล้ว ปลั๊กอินจะปิดการทำงานและลบตัวเองเพื่อหลีกเลี่ยงการถูกตรวจพบ

ไฟล์ที่ถูกอัปโหลดประกอบด้วยข้อมูลที่ขโมยมาจากเครื่องของเหยื่อ โดยพบไฟล์ Archive มากกว่า 700 ไฟล์ตั้งแต่ช่วงกลางเดือนพฤษภาคมจนถึงสิ้นเดือนกรกฎาคม 2026 ในบรรดาไฟล์เหล่านี้ยังพบไฟล์และเครื่องมือสำหรับการพัฒนาภายในซึ่งดูเหมือนว่าจะเป็นกรณีที่ผู้โจมตีเผลอทำให้ระบบของตัวเองติดมัลแวร์ด้วย หนึ่งในนั้นคือเครื่องมือระบบอัตโนมัติที่สร้างขึ้นโดยเฉพาะชื่อ fMain.frm ซึ่งใช้สำหรับจัดการเว็บไซต์ WordPress ที่ถูกแฮ็ก

เครื่องมือระบบอัตโนมัตินี้ช่วยให้ผู้ควบคุม Botnet สามารถจัดการหน้า WordPress ที่ถูกแฮ็กจำนวนมากได้พร้อมกัน Check Point ระบุว่าเครื่องมือนี้ใช้สคริปต์ PHP สำหรับอัปโหลดและลบไฟล์อย่างปลอดภัยบนเว็บไซต์ที่ถูกแฮ็ก เพื่ออัปโหลดหรือลบไฟล์เพิ่มเติม เปิดหรือปิดการทำงานของ ClickFix CAPTCHA ปลอม เปิดหรือปิดระบบแคช และอื่นๆ

เว็บไซต์ที่ถูกแฮ็กยังมีปลั๊กอินอันตรายชื่อ verify ซึ่งจะแสดง CAPTCHA ปลอมทับเนื้อหาจริงของเว็บไซต์สำหรับผู้เข้าชมที่ไม่ได้ใช้ Windows ปลั๊กอินนี้จะถูกเปิดใช้งานหลังจากผู้โจมตีอัปโหลดไฟล์ชื่อ activator.php จากนั้นไฟล์ดังกล่าวจะลบตัวเองออก

ณ วันที่ 24 กรกฎาคม 2026 แคมเปญนี้ได้โจมตีและทำให้ที่อยู่ IP ที่ไม่ซ้ำกันมากกว่า 6,000 รายการ ถูกบุกรุก โดยส่วนใหญ่อยู่ในสหรัฐฯ จำนวน 1,852 รายการ รัสเซีย 630 รายการ และอินเดีย 630 รายการ

StopAndProtect แสดงให้เห็นว่าผู้โจมตีสามารถเปลี่ยนเว็บไซต์ WordPress หลายพันแห่งที่ไม่ได้รับการดูแลอย่างเหมาะสมให้กลายเป็นโครงสร้างพื้นฐานอาชญากรรมแบบกระจายศูนย์ สำหรับใช้แพร่กระจายมัลแวร์ เฝ้าติดตาม ขโมยข้อมูล และเรียกค่าไถ่ Eli Smadja จาก Check Point กล่าว

แนะนำให้องค์กรระมัดระวัง CAPTCHA ที่ปรากฏขึ้นโดยไม่คาดคิด โดยเฉพาะกรณีที่ CAPTCHA ขอให้ผู้ใช้คัดลอก วาง หรือรันคำสั่ง ควรอัปเดตอุปกรณ์และซอฟต์แวร์รักษาความปลอดภัยให้เป็นเวอร์ชันล่าสุดอยู่เสมอ และออกจากเว็บไซต์ทันทีหากเว็บไซต์ขอให้ดำเนินการที่ผิดปกตินอกเหนือจากการใช้งานผ่านเบราว์เซอร์

**ข้อมูลอ้างอิง**

Aug 19, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/stopandprotect-uses-nearly-2000-hacked.html