วันที่ 14 พฤษภาคม 2568

แฮกเกอร์โจมตีเว็บเซิร์ฟเวอร์ Windows IIS ด้วยมัลแวร์ Native Module

Executive Summary

ตรวจพบรายงานการโจมตีที่พุ่งเป้าไปยัง Windows IIS Web Server โดยใช้มัลแวร์ชนิด Native Module ซึ่งพบครั้งแรกในเดือนกุมภาพันธ์ 2025 การโจมตีนี้เริ่มจากผู้ไม่หวังดีได้สิทธิ์เข้าถึงเซิร์ฟเวอร์ที่ไม่ได้รับการดูแลอย่างเหมาะสม ส่งผลให้สามารถใช้เซิร์ฟเวอร์ดังกล่าวเป็นช่องทางในการโจมตีได้อย่างต่อเนื่อง โดยผู้โจมตีสามารถใช้ WebShell ที่พัฒนาด้วย .NET เป็นตัวโหลดเริ่มต้น ก่อนจะติดตั้งโมดูลอันตรายของ IIS ผ่านเครื่องมือ AppCmd.exe โดยฝังไฟล์มัลแวร์ caches.dll ที่จะปรากฏในระบบ IIS ในชื่อ IsapiCachesModule หลังการติดตั้งโมดูลนี้จะเชื่อมต่อกับขั้นตอนสำคัญของ HTTP request ได้แก่ OnGlobalPreBeginRequest, OnBeginRequest, และ OnSendResponse เพื่อดักจับและเข้าถึงข้อมูลที่รับส่งผ่านเว็บเซิร์ฟเวอร์

โมดูลอันตรายประกอบด้วย 5 คลาสหลัก ได้แก่

1. WebdllServer - ทำหน้าที่รันไฟล์ ASP อัตโนมัติเมื่อ URL มีคำว่า web.dll
2. RedirectServer - ทำหน้าที่เปลี่ยนเส้นทางของผู้ใช้งานไปยังเว็บไซต์ของผู้โจมตี
3. AffLinkServer - ทำหน้าที่แอบแทรกลิงก์แบบ Affiliate ใน HTTP response
4. HiJackServer - ใช้สำหรับจัดการและควบคุมการตั้งค่าภายในเซิร์ฟเวอร์
5. UploadServer – รองรับการอัปโหลดไฟล์ขึ้นสู่เซิร์ฟเวอร์

ผู้โจมตีใช้ rootkit ที่ชื่อว่า HijackDriverManager เพื่อหลีกเลี่ยงการถูกตรวจจับโดยโปรแกรมรักษาการปลอดภัย นอกจากนี้ยังพบการติดตั้ง Gh0stRAT ซึ่งเป็น backdoor ที่นิยมใช้โดยกลุ่มผู้โจมตีในประเทศจีน

คำแนะนำ (Recommendation)

- ดำเนินการอัปเดตระบบปฏิบัติการของ Server ให้เป็นเวอร์ชั่นปัจจุบัน
- ดำเนินการเปิดใช้งานระบบรักษาความปลอดภัยคอมพิวเตอร์ เช่น แอนติไวรัส หรือ IDS/IPS
- ตรวจสอบการติดตั้งหรือการเปลี่ยนแปลงของ IIS module
- ตรวจสอบการตั้งค่าเว็บเซิร์ฟเวอร์อย่างสม่ำเสมอ

ข้อมูลอ้างอิง

- https://cybersecuritynews.com/windows-iis-web-server-attacked/