แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนเพื่อเฝ้าระวัง มัลแวร์ที่มีแคมเปญมุ่งโจมตีเว็บไซต์ที่พัฒนาด้วย WordPress

วันที่แจ้งเตือน 10 เมษายน 2567

ThaiCERT สกมช. ได้เผยแพร่รายงาน กรณีที่ Sucuri บริษัทผู้ให้บริการแพลตฟอร์มการรักษาความมั่นคงปลอดภัยเว็บไซต์ พบเว็บไซต์มากกว่า 39,000 รายการ ที่พัฒนาด้วย WordPress ถูกติดตั้งมัลแวร์ “Sign1” โดยมีวัตถุประสงค์เพื่อเปลี่ยนเส้นทางผู้เข้าชมไปยังเว็บไซต์ของผู้ไม่หวังดี และรับชมโฆษณาที่ไม่พึงประสงค์ได้

โดยผู้ไม่หวังดีใช้วิธีสุ่มรหัสผ่าน (Brute Force) และใช้ประโยชน์จากช่องโหว่บนปลั๊กอินของ WordPress เพื่อให้มีสิทธิเข้าถึงเว็บไซต์เป้าหมาย และทำการฝังโค้ดที่เป็นอันตรายลงใน HTML widgets ของ WordPress หรือปลั๊กอินของ WordPress โดยสามารถหลีกเลี่ยงการตรวจจับของเจ้าของเว็บไซต์ได้ และใช้โค้ดอันตรายดังกล่าวตรวจสอบที่มาของผู้เข้าชมเว็บไซต์หากพบว่ามาจากเว็บไซต์ที่มีชื่อเสียง เช่น Google, Facebook และ Instagram เป็นต้น มัลแวร์จะดำเนินการสร้างโฆษณาที่ไม่พึงประสงค์หรือเปลี่ยนเส้นทางไปยังเว็บไซต์ที่เป็นอันตราย

ThaiCERT แนะนำให้ ผู้ดูแลระบบควรติดตั้งปลั๊กอินของ WordPress ผ่านเว็บไซต์ที่น่าเชื่อถือและตรวจสอบว่ามีการสร้างโฆษณาที่ไม่พึงประสงค์หรือเปลี่ยนเส้นทางไปยังเว็บไซต์ที่เป็นอันตรายหรือไม่ หากพบการเปลี่ยนเส้นทางหรือโฆษณาที่ไม่พึงประสงค์ ผู้ใช้หรือผู้ดูแลระบบควรดำเนินการ ดังนี้ (1) ค้นหาและลบ backdoors ใน *“webroot และ upload directories”* (2) ค้นหาและลบ backdoor injectors ในไฟล์ *“Theme”* (3) ตรวจสอบการแก้ไขไฟล์ *“index.php”* และไฟล์หลักของ WordPress อื่น ๆ และสแกนหาโค้ดอันตรายและทำการลบทิ้ง และ (4) ลบบัญชีของผู้ดูแลระบบหรือผู้ใช้งานที่ไม่ได้รับอนุญาตที่อาจถูกสร้างขึ้นโดยผู้ไม่หวังดี

นอกจากนี้ ผู้ดูแลระบบควรติดตามและปิดกั้นโดเมนอันตรายที่มีความเกี่ยวข้องกับมัลแวร์ Sign1 โดยมีรายละเอียดตาม**อ้างอิง 2)**

ทั้งนี้ มีคำแนะนำในการป้องกันเบื้องต้น สำหรับผู้ใช้งานหรือผู้ดูแลระบบ WordPress ดังนี้

(1) กำหนดรหัสผ่าน หรือ passphrase ที่คาดเดาได้ยาก
(2) เปิดการใช้งานการยืนยันตัวตนแบบหลายปัจจัย Two Factor Authentication (2FA)
(3) จำกัดการเข้าถึงระบบจาก IP ที่ได้รับอนุญาตเท่านั้น
(4) เปิดใช้งาน CAPTCHA เพื่อลดความเสี่ยงในการพยายามเข้าถึงเว็บไซต์จาก automated bots
(5) จำกัดจำนวนครั้งในการพยายามเข้าถึงระบบ (login attempt) เพื่อลดผลกระทบจากการโจมตีด้วย Brute Force
(6) หมั่นอัปเดตซอฟต์แวร์ของ WordPress รวมถึงปลั๊กอินและธีมเป็นเวอร์ชันล่าสุดอยู่เสมอ

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 9 เม.ย. 2567
2) https://blog.sucuri.net/2024/03/sign1-malware-analysis-campaign-history-indicators-of-compromise.html#malware-analysis
3) https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-031
4) https://www.bleepingcomputer.com/news/security/evasive-sign1-malware-campaign-infects-39-000-wordpress-sites/