เอกสารการแจ้งเตือนกรณีบริษัทรักษาความปลอดภัยเว็บไซต์ Sucuri พบเว็บไซต์มากกว่า 39,000 เว็บ ติดมัลแวร์ Sign1

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ กรณีบริษัทรักษาความปลอดภัยเว็บไซต์ Sucuri พบเว็บไซต์มากกว่า 39,000 เว็บ ติดมัลแวร์ตระกูลใหม่โดยมีชื่อเรียกว่า Sign1[1]

บริษัท Sucuri พบมัลแวร์ใหม่ที่มีชื่อว่า Sign1 ซึ่งมีแคมเปญโจมตีไปที่เว็บไซต์ของ WordPress จำนวน 39,000 เว็บ แคมเปญดังกล่าวถูกนำไปใช้ในการเปลี่ยนเส้นทางเว็บไซต์และโฆษณาที่ไม่พึงประสงค์สำหรับผู้เยี่ยมชมเว็บไซต์โดยแคมเปญของ Sign1 เป็นการผสมผสานการโจมตีแบบ Brute Force และการใช้ประโยชน์จากปลั๊กอินของ WordPress ซึ่งเมื่อผู้โจมตีเข้าถึงจะสามารถทำการฝัง JavaScript ที่เป็นอันตราย ลงในวิดเจ็ต HTML ของ WordPress หรือปลั๊กอิน Simple Custom CSS และ JS WordPress และเมื่อมีผู้เยี่ยมชมจากเว็บไซต์ เช่น Google, Facebook และ Instagram เพื่อหลีกเลี่ยงการตรวจจับ หากพบว่าผู้เยี่ยมชมมาจากเว็บไซต์ที่น่าเชื่อถือได้ มัลแวร์จะดำเนินการสร้างโฆษณาที่ไม่พึงประสงค์หรือเปลี่ยนเส้นทางไปยังเว็บไซต์ที่เป็นอันตราย วัตถุประสงค์ของวิธีการนี้เพื่อหลีกเลี่ยงการตรวจจับของเจ้าของเว็บไซต์[2]

ผู้ดูแลระบบควรปลั๊กอินของ WordPress ผ่านเว็บไซต์ที่น่าเชื่อถือและตรวจสอบว่ามีการสร้างโฆษณาที่ไม่พึงประสงค์หรือเปลี่ยนเส้นทางไปยังเว็บไซต์ที่เป็นอันตรายหรือไม่ หากพบการเปลี่ยนเส้นทางหรือโฆษณาที่ไม่พึงประสงค์ ผู้ใช้หรือผู้ดูแลระบบควรดำเนินการ ดังนี้

- ค้นหาและลบ backdoors ใน webroot และไดเรกทอรี
- ค้นหาและลบ backdoor injectors ในไฟล์ธีม
- ตรวจสอบไฟล์ index.php และไฟล์ WordPress อื่นๆ ว่าถูกแก้ไขหรือไม่ สแกนหา JavaScript และลบเว็บไซต์ที่เป็นอันตราย
- ลบผู้ดูแลระบบหรือผู้ใช้ที่ไม่ได้รับอนุญาตที่อาจถูกสร้างขึ้นโดยผู้โจมตี

ผู้ดูแลระบบอาจต้องติดตามและบล็อกโดเมนที่เป็นอันตรายที่มีความเกี่ยวข้องกับ Sign1 ดังนี้

- js.abc-cdn[.]online
- spf.js-min[.]site
- cdn.jsdevlvr[.]info
- cdn.wt-api[.]top
- load.365analytics[.]xyz
- stat.counter247[.]live
- js.opttracker[.]online
- l.js-assets[.]cloud
- api.localadswidget[.]com
- page.24supportkit[.]com

- streaming.jsonmediapacks[.]com
- js.schema-forms[.]org
- stylesheet.webstaticcdn[.]com
- assets.watchasync[.]com
- tags.stickloader[.]info

สำหรับการป้องกันในเบื้องต้น แนะนำผู้ใช้หรือผู้ดูแลระบบ WordPress กำหนดรหัสผ่านที่คาดเดาได้ยาก ใช้การยืนยันตัวตนแบบ Two Factor Authentication (2FA) จำกัดการเข้าถึงระบบจาก IP ที่ได้รับอนุญาตเท่านั้น ใช้ Completely Automated Public Turing test to tell Computers and Humans Apart(CAPTCHA) เพื่อลดความเสี่ยง จำกัดการเข้าถึงระบบเพื่อลดผลกระทบจากการโจมตีด้วย Brute Force และอัปเดตซอฟต์แวร์ของ WordPress รวมถึงปลั๊กอินและธีมเป็นเวอร์ชันล่าสุด[3]

ทั้งนี้ สามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

<u>อ้างอิง</u>

1. https://securityaffairs.com/160942/hacking/sign1-malware-campaign.html?utm_source=tldrinfosec
2. https://www.bleepingcomputer.com/news/security/evasive-sign1-malware-campaign-infects-39-000-wordpress-sites/
3. https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-031