Los investigadores en ciberseguridad están alertando sobre un incremento de ataques automatizados dirigidos a servidores PHP, dispositivos IoT y pasarelas en la nube, ejecutados por distintos botnets como *Mirai*, *Gafgyt* y *Mozi*.

"Estas campañas automatizadas aprovechan vulnerabilidades CVE conocidas y errores de configuración en la nube para tomar el control de sistemas expuestos y expandir las redes de botnets," señaló la *Qualys Threat Research Unit (TRU)* en un informe.

La empresa de ciberseguridad explicó que los servidores PHP se han convertido en los principales objetivos de estos ataques debido al uso masivo de sistemas de gestión de contenido como *WordPress* y *Craft CMS*. Esto, a su vez, amplía significativamente la superficie de ataque, ya que muchas implementaciones de PHP pueden presentar configuraciones incorrectas, complementos o temas obsoletos, y almacenamiento de archivos inseguro.

Algunas de las vulnerabilidades más relevantes explotadas por los atacantes en frameworks PHP incluyen:

- CVE-2017-9841 – Vulnerabilidad de ejecución remota de código en *PHPUnit*.
- CVE-2021-3129 – Vulnerabilidad de ejecución remota de código en *Laravel*.
- CVE-2022-47945 – Vulnerabilidad de ejecución remota de código en *ThinkPHP Framework*.

Qualys también señaló haber detectado intentos de explotación que implican el uso del parámetro *"/?XDEBUG_SESSION_START=phpstorm"* en solicitudes HTTP GET, con el propósito de iniciar una sesión de depuración Xdebug desde un entorno de desarrollo integrado (IDE) como *PhpStorm*.

"Si Xdebug permanece activado accidentalmente en entornos de producción, los atacantes podrían aprovechar estas sesiones para obtener información sobre el comportamiento de la aplicación o extraer datos confidenciales," advirtió la compañía.

De forma paralela, los actores maliciosos continúan buscando credenciales, claves API y tokens de acceso en servidores expuestos a internet para tomar el control de sistemas vulnerables, además de explotar fallos de seguridad conocidos en dispositivos IoT para integrarlos en redes de botnets. Entre ellos destacan:

- CVE-2022-22947 – Vulnerabilidad de ejecución remota de código en *Spring Cloud Gateway*.
- CVE-2024-3721 – Vulnerabilidad de inyección de comandos en *TBK DVR-4104* y *DVR-4216*.
- Configuración incorrecta en MVPower TV-7104HE DVR, que permite a usuarios no autenticados ejecutar comandos arbitrarios mediante una solicitud HTTP GET.

Según *Qualys*, la actividad de escaneo a menudo se origina desde infraestructuras en la nube como *Amazon Web Services (AWS)*, *Google Cloud*, *Microsoft Azure*, *Digital Ocean* y *Akamai Cloud*, lo que demuestra cómo los atacantes están aprovechando servicios legítimos para ocultar su verdadera ubicación.

"Los atacantes actuales no necesitan ser altamente sofisticados para ser efectivos," señaló la compañía. *"Con kits de explotación, frameworks de botnets y herramientas de escaneo fácilmente disponibles, incluso los atacantes principiantes pueden causar daños significativos."*

Para mitigar estos riesgos, se recomienda mantener los dispositivos actualizados, eliminar herramientas de desarrollo y depuración en entornos de producción, proteger credenciales con *AWS Secrets Manager* o *HashiCorp Vault*, y restringir el acceso público a las infraestructuras en la nube.

"Aunque tradicionalmente las botnets se asociaban con ataques DDoS a gran escala o campañas de criptominería, en la era de las amenazas a la identidad, observamos que están asumiendo un nuevo papel dentro del ecosistema de amenazas," explicó *James Maude*, CTO de campo en *BeyondTrust*.

"Contar con una extensa red de routers y direcciones IP permite a los atacantes realizar ataques de relleno de credenciales y pulverización de contraseñas a gran escala. Además, las botnets pueden evadir los controles de geolocalización robando credenciales o secuestrando sesiones del navegador, utilizando un nodo del botnet cercano a la ubicación real de la víctima —e incluso el mismo proveedor de servicios de internet— para evitar detecciones o bloqueos de acceso inusuales."

La revelación coincide con el informe de *NETSCOUT*, que clasificó al botnet de alquiler para ataques DDoS conocido como *AISURU* como una nueva clase de malware denominada *TurboMirai*, capaz de ejecutar ataques DDoS que superan los 20 terabits por segundo (Tbps). Este botnet está conformado principalmente por routers domésticos, sistemas de videovigilancia en línea y otros equipos de acceso residencial (*CPE*).

"Estos botnets incorporan capacidades dedicadas de ataque DDoS y funciones multiuso, permitiendo tanto ataques de denegación de servicio como otras actividades ilícitas, entre ellas el relleno de credenciales, scraping web impulsado por inteligencia artificial (IA), envío masivo de spam y campañas de phishing," explicó la empresa.

"AISURU incluye un servicio de proxy residencial integrado que se utiliza para reflejar ataques DDoS a nivel de aplicación HTTPS generados por herramientas externas."

Transformar dispositivos comprometidos en proxies residenciales permite a los clientes que pagan enrutar su tráfico a través de los nodos del botnet, lo que les brinda anonimato y la capacidad de mezclarse con el tráfico legítimo de la red. Según el periodista independiente de seguridad *Brian Krebs*, todos los principales servicios de proxy han experimentado un crecimiento exponencial durante los últimos seis meses, basándose en datos de *spur.us*.