Los servidores Linux están siendo el blanco de una campaña activa que distribuye un malware furtivo llamado perfctl, cuyo objetivo principal es ejecutar un software de minería de criptomonedas y proxyjacking.

«Perfctl es especialmente difícil de detectar y persistente, utilizando varias técnicas avanzadas», explicaron los investigadores de seguridad de Aqua, Assaf Morag e Idan Revivo, en un informe.

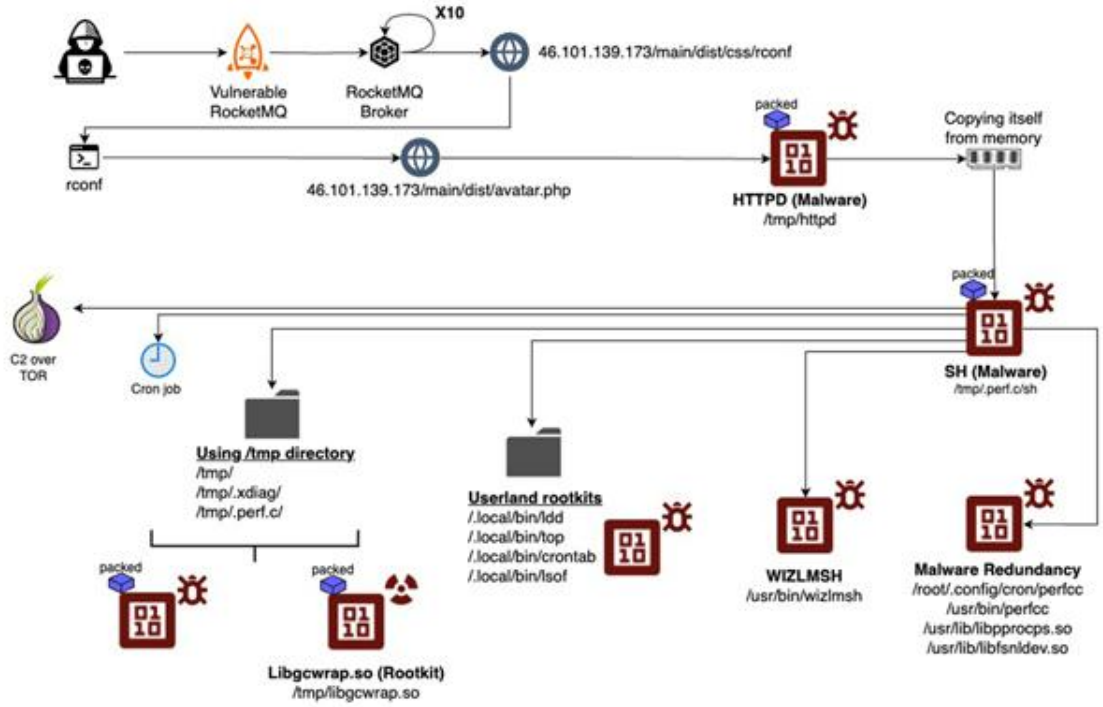
> *«Cuando un nuevo usuario accede al servidor, detiene de inmediato todas las actividades 'ruidosas', quedando inactivo hasta que el servidor vuelve a estar desocupado. Tras su ejecución, borra su archivo binario y continúa funcionando de forma silenciosa en segundo plano como un servicio».*

Cabe destacar que algunos elementos de esta campaña fueron revelados el mes pasado por Cado Security, que describió un ataque dirigido a instancias de Selenium Grid expuestas a internet, utilizando software tanto para minería de criptomonedas como proxyjacking.

El malware perfctl explota una vulnerabilidad de Polkit (CVE-2021-4043, también conocida como PwnKit) para elevar sus privilegios a nivel root y desplegar un minero llamado perfcc.

El nombre «perfctl» parece ser un intento deliberado de evitar la detección y pasar desapercibido entre los procesos del sistema, ya que «perf» hace referencia a una herramienta de monitoreo de rendimiento en Linux, y «ctl» indica control en diversas herramientas de línea de comandos como systemctl, timedatectl y rabbitmqctl.

La cadena de ataque, observada por la empresa de seguridad en la nube en sus servidores honeypot, implica la explotación de una instancia vulnerable de Apache RocketMQ en servidores Linux para entregar un archivo malicioso llamado «httpd».



Una vez ejecutado, se copia en una nueva ubicación en el directorio «/tmp», ejecuta el nuevo binario, finaliza el proceso original y elimina el binario inicial, todo con el objetivo de ocultar su presencia.

Además de replicarse en otros directorios con nombres aparentemente inofensivos, el malware está diseñado para desplegar un rootkit que le permite evadir mecanismos de defensa, así como la carga útil del minero. En algunos casos, también descarga y ejecuta software de proxyjacking desde un servidor remoto.

Para reducir el riesgo que presenta perfctl, se recomienda mantener los sistemas y software actualizados, restringir la ejecución de archivos, desactivar servicios no utilizados, segmentar la red y utilizar Control de Acceso Basado en Roles (RBAC) para limitar el acceso a archivos sensibles.

> *«Para detectar el malware perfctl, se deben observar picos inusuales en el uso del*

> *CPU o una disminución en el rendimiento del sistema si se ha instalado un rootkit. Esto puede ser indicativo de actividades de minería de criptomonedas, especialmente durante los momentos en que el sistema está inactivo»*, señalaron los investigadores.