Un actor de amenazas con motivaciones financieras, conocido por sus ataques de cryptojacking, aprovechó una versión revisada de su malware para atacar las infraestructuras de la nube utilizando vulnerabilidades en las tecnologías de servidores web, según una nueva investigación.

Implementado por el grupo de hackers con sede en China, Rocke, el malware de cryptojacking Pro-Ocean ahora cuenta con capacidades mejoradas de rootkit y gusanos, además de albergar nuevas tácticas de evasión para eludir los métodos de detección de las empresas de seguridad cibernética, según informaron los investigadores de la Unidad 42 de Palo Alto Networks.

> *«Pro-Ocean utiliza vulnerabilidades conocidas para apuntar a aplicaciones en la nube. En nuestro análisis, encontramos que Pro-Ocean apunta a Apache ActiveMQ (CVE-2016-3088), Oracle WebLogic (CVE-2017-10271) y Redis (instancias no seguras)»*, dijeron los investigadores.
>
> *«Una vez instalado, el malware mata cualquier proceso que utilice mucha CPU, de forma que pueda usar el 100% de la CPU y extraer Monero de forma eficiente»*, agregaron.

Documentado por primera vez por Cisco Talos en 2018, se descubrió que Rocke distribuye y ejecuta malware de minería criptográfica utilizando un conjunto de herramientas variado que incluye repositorios de Git y diferentes cargas útiles, como scripts de shell, backdoors de JavaScript, además de archivos ejecutables portátiles.

Aunque las variantes anteriores del malware confiaban en la capacidad de apuntar y eliminar productos de seguridad en la nube desarrollados por Tencent Cloud y Alibaba Cloud

mediante la explotación de fallas en Apache Struts 2, Oracle WebLogic y Adobe ColdFusion, Pro-Ocean ha agrandó la amplitud de esos vectores de ataque apuntando a los servidores Apache ActiveMQ, Oracle WebLogic y Redis.

Además de sus características de propagación automática y mejores técnicas de ocultación que le permiten permanecer bajo el radar y propagarse a software sin parches en la red, el malware se propone desinstalar agentes de monitoreo para esquivar la detección y eliminar otros malware y mineros de los sistemas infectados.

Para lograr esto, aprovecha una característica nativa de Linux llamada LD_PRELOAD, con el fin de enmascarar su actividad maliciosa, una biblioteca llamada Libprocesshider, para permanecer oculta y utiliza un script de infección de Python que toma la IP pública de la máquina para infectar todas las máquinas en la misma subred de 16 bits.

Pro-Ocean también trabaja para eliminar la competencia al eliminar otros malware y mineros, incluyendo Luoxk, BillGates, XMRig y Hashfish, que se ejecutan en el host comprometido. Además, cuenta con un módulo de vigilancia escrito en Bash, que asegura la persistencia y se encarga de terminar todos los procesos que utilizan más del 30% de la CPU con el objetivo de minar Monero de forma eficiente.

> *«Este malware es un ejemplo que demuestra que las soluciones de seguridad basadas en agentes de los proveedores de la nube pueden no ser suficientes para prevenir el malware evasivo dirigido a la infraestructura de la nube pública. Esta muestra tiene la capacidad de eliminar los agentes de algunos proveedores de nube y evadir su detección»,* dijo Aviv Sasson, investigador de la Unidad 42.