El grupo de cryptojacking conocido como TeamTNT parece estar detrás de una cepa de malware no descubierta antes que se utiliza para extraer la criptomoneda Monero en sistemas comprometidos.

Según Cado Security, que encontró la muestra después de que Sysdig detallara un ataque sofisticado conocido como SCARLETEEL dirigido a entornos en contenedores para, en última instancia, robar datos y software patentados.

Específicamente, la fase inicial de la cadena de ataque involucró el uso de un minero de criptomonedas, que la empresa de seguridad en la nube sospechó que se implementó como señuelo para ocultar la detección de exfiltración de datos.

El artefacto, subido a VirusTotal a fines del mes pasado, *«tiene varias similitudes sintácticas y semánticas con las cargas útiles anteriores de TeamTNT, e incluye una identificación de billetera que se les atribuyó anteriormente»,* reveló un análisis de Cado Security.

Se ha documentado que TeamTNT, activo desde al menos 2019, ataca repetidamente entornos de nube y contenedores para implementar mineros de criptomonedas. También se sabe que libera un gusano de criptominería capaz de robar las credenciales de AWS.

Aunque el atacante cerró voluntariamente sus operaciones en noviembre de 2021, la empresa de seguridad en la nube Aqua reveló en septiembre de 2022 un nuevo conjunto de ataques montados por el grupo dirigidos a instancias de Docker y Redis mal configuradas.

Dicho esto, también existen indicios de que equipos rivales como WatchDog podrían estar imitando las tácticas, técnicas y procedimientos (TTP) de teamTNT para frustrar los esfuerzos de atribución.

Otro grupo de actividades notable es Kiss-a-dog, que también se basa en herramientas e infraestructura de comando y control (C2) previamente asociada con TeamTNT para extraer criptomonedas.

No hay evidencia concreta para vincular el nuevo malware con el ataque SCARLETEEL. Pero Cado Security dijo que la muestra apareció casi al mismo tiempo que se informó este último, lo que plantea la posibilidad de que este podría ser el minero *«señuelo»* que se instaló.

El script de shell, por su parte, toma medidas preparatorias para reconfigurar los límites estrictos de los recursos, evitar el registro del historial de comandos, aceptar todo el tráfico de entrada o salida, enumerar los recursos de hardware e incluso limpiar compromisos anteriores antes de comenzar la actividad.

Al igual que otros ataques vinculados a TeamTNT, la carga útil maliciosa también aprovecha una técnica conocida como secuestro del vinculador dinámico para encubrir el proceso minero por medio de un objeto ejecutable compartido llamado *libprocesshider* que utiliza la variable de entorno LD_PRELOAD.

La persistencia se logra por tres medios distintos, uno de los cuales modifica el archivo *.profile*, para garantizar que el minero siga ejecutándose durante los reinicios del sistema.

Los hallazgos se producen cuando se observó que otro grupo de criptomineros denominado 8220 Gang usa un encriptador llamado ScrubCryp para realizar operaciones ilícitas de criptojacking.

Además, se han encontrado atacantes desconocidos que se dirigen a la infraestructura vulnerable del orquestador de contenedores de Kubernetes con API expuestas para extraer la criptomoneda Dero, lo que marca un cambio de Monero.

La compañía de seguridad cibernética Morphisec, el mes pasado, también arrojó luz sobre una campaña de malware evasivo que aprovecha las vulnerabilidades de ProxyShell en los servidores de Microsoft Exchange para eliminar una cepa de criptominero cuyo nombre en código es ProxyShellMiner.

> *«La minería de criptomonedas en la red de una organización puede provocar la*

> *degradación del rendimiento del sistema, un mayor consumo de energía, el sobrecalentamiento del equipo y puede detener los servicios. Permite el acceso de los actores de amenazas para fines aún más nefastos»,* dijeron los investigadores.