



heimdall  
security research

---

A DIVISION OF ISH



# **Campanha maliciosa para servidores Redis**



Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

### [Heimdall Security Research](#)



Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

### [Boletins de Segurança – Heimdall](#)



**ISH**  
**CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES**

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

[BAIXAR](#)



**ISH**  
**ALERTA PARA RETORNO DO MALWARE EMOTET!**

O malware Emotet após permanecer alguns meses sem operações retomou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

[BAIXAR](#)



**ISH**  
**GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS**

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

[BAIXAR](#)

## Sumário

1	Campana identificada malware “Skidmap”.....	6
2	Referências.....	9

## Lista de Figuras

Figura 1 – Fluxo de ataque relacionado ao malware. ....	6
Figura 2 – Processos ocultos do minerador.....	8

# 1 CAMPANA IDENTIFICADA MALWARE “SKIDMAP”

O malware conhecido como Skidmap, um minerador de criptomoeda detectado pela Trend Micro em setembro de 2019 visando máquinas Linux. O código utilizou rootkits no modo kernel para evitar a detecção, diferindo de mineradores semelhantes devido à maneira como carrega módulos maliciosos do kernel.

Desta vez, os pesquisadores da Trustwave detectaram uma variante Skidmap nova, aprimorada e perigosa, projetada para atingir uma ampla gama de distribuições Linux, incluindo Alibaba, Anolis, openEuler, EulerOS, Steam, CentOS, RedHat e Rock.

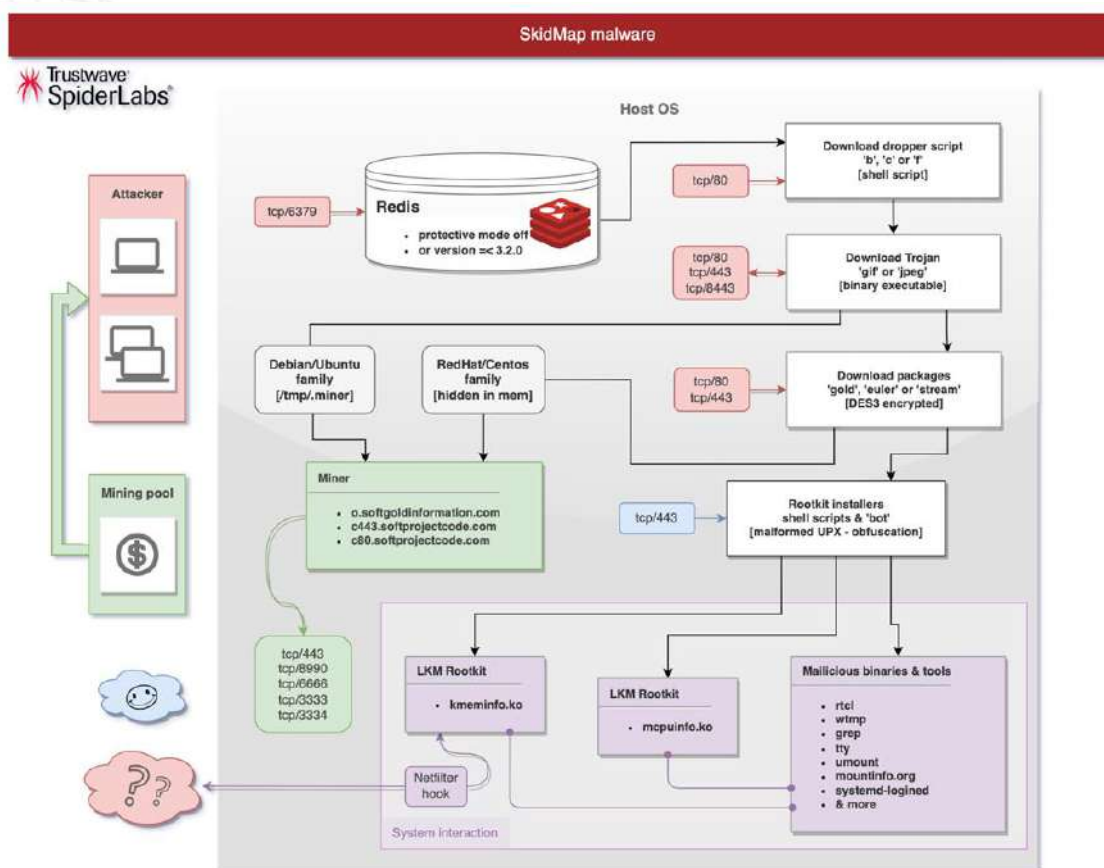


Figura 1 – Fluxo de ataque relacionado ao malware.

A variante analisada pelos pesquisadores foi observada visando apenas instâncias Redis abertas (as chamadas “NO AUTH”). Nenhum ataque de força bruta foi observado pelos pesquisadores.

A cadeia de ataque começa com uma tentativa de fazer login na instância não segura do Redis e configurar variáveis contendo tarefas cron codificadas em base64.

O Cron executa um trabalho a cada 10 minutos alternando entre "curl" e "wget" para baixar e executar o script dropper. A Trustwave observou agentes de ameaças implantando um script shell dropper projetado para distribuir o arquivo binário executável (ELF) que se disfarça como um arquivo de imagem GIF (enquanto uma versão anterior do malware usava "jpeg").

Após o script shell ser implantado, o malware adiciona chaves ssh em locais padrão `"/toor/.ssh/authoried_keys"` e `"/root/.ssh/authoried_keys2"`.

Em seguida, o código malicioso desabilita o SELinux e cria um shell reverso que chamará de volta para o C2 a cada hora via porta TCP/8443. A depender da distribuição específica do Linux e do kernel, o malware baixa um pacote apropriado (chamado gold, stream ou Euler).

O pacote utilizou vários scripts de shell para instalar os módulos do kernel, incluindo um para limpar os logs e lançar um bot que permite aos operadores recuperar cargas adicionais de rootkit. A carga útil "mcpuinfo.ko" é utilizado para ocultar o minerador, enquanto "kmeminfo.ko" permite que o código malicioso inspecione pacotes de rede e os manipule. Algumas variantes observadas pelos especialistas incluíam um minerador embutido.

```
Found HIDDEN PID: 500831
  Cmdline: "/tmp/.miner"
  Executable: "/tmp/.miner"
  Command: ".miner"
  $USER=root
  $PWD=/var/lib

Found HIDDEN PID: 500832
  Cmdline: "/tmp/.miner"
  Executable: "/tmp/.miner"
  Command: ".miner"
  $USER=root
  $PWD=/var/lib

Found HIDDEN PID: 500833
  Cmdline: "/tmp/.miner"
  Executable: "/tmp/.miner"
  Command: ".miner"
  $USER=root
  $PWD=/var/lib

Found HIDDEN PID: 500834
  Cmdline: "/tmp/.miner"
  Executable: "/tmp/.miner"
  Command: ".miner"
  $USER=root
  $PWD=/var/lib

Found HIDDEN PID: 500836
  Cmdline: "/tmp/.miner"
  Executable: "/tmp/.miner"
  Command: ".miner"
  $USER=root
  $PWD=/var/lib

Found HIDDEN PID: 500858
  Cmdline: "/tmp/.miner"
  Executable: "/tmp/.miner"
  Command: ".miner"
  $USER=root
  $PWD=/var/lib

Found HIDDEN PID: 500859
  Cmdline: "/tmp/.miner"
  Executable: "/tmp/.miner"
  Command: ".miner"
  $USER=root
  $PWD=/var/lib
```

Figura 2 – Processos ocultos do minerador.

Por fim, é possível visualizar o avanço do malware de forma bem extensa, sendo ainda identificado em infraestruturas de servidores maiores e que poderá ser difícil.



## 2 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [Pesquisa](#) publicada pela TrustWave, malware Skidmap



**heimdall**  
security research

A DIVISION OF ISH