# BOLETIM DE SEGURANÇA

## Nova campanha de exploração tem como alvo organizações que executam o FortiClient EMS da Fortinet

heimdall
security research
A DIVISION OF ISH

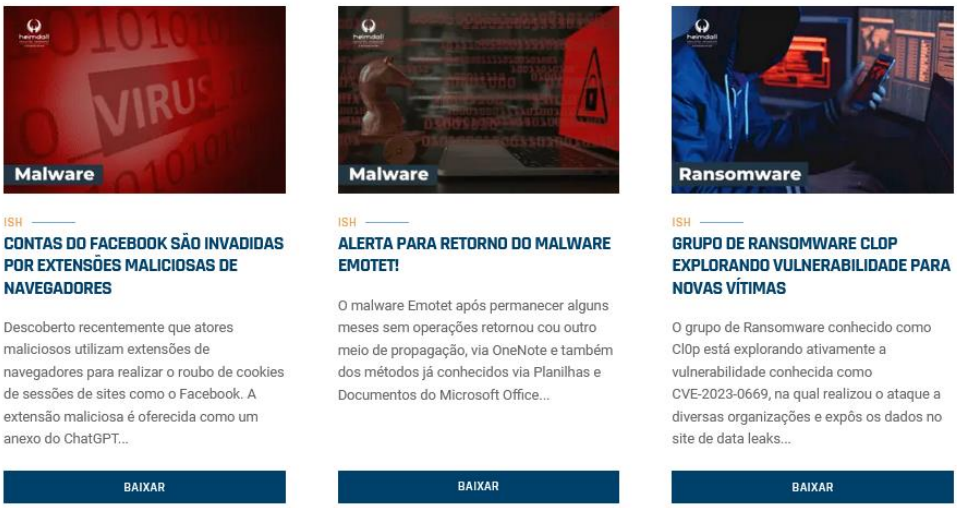
**TLP: CLEAR**

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


1 Sumário Executivo ..... 6
2 Informações sobre a vulnerabilidade ..... 7
3 MITRE ATT&CK - TTPs ..... 10
4 Vulnerabilidade adicionada ao KEV-CISA ..... 11
5 Recomendações ..... 12
6 Indicadores de Compromissos ..... 13
7 Referências ..... 14

# LISTA DE TABELAS

*Tabela 1 – Tabela MITRE ATT&CK.* ..... *10*

*Tabela 2 – Indicadores de Compromissos de Rede.* ..... *13*

## LISTA DE FIGURAS

*Figura 1 – Fluxo de ataque.* ..... 7

*Figura 2 – Vulnerabilidade no catálogo KEV-CISA.* ..... 11

# 1 SUMÁRIO EXECUTIVO

A Forescout Research identificou uma nova campanha maliciosa, denominada Connect:fun, que mira organizações utilizando o FortiClient EMS da Fortinet, suscetível à vulnerabilidade CVE-2023-48788 de nível crítico. A campanha se destaca pelo emprego das ferramentas ScreenConnect e Powerfun para ações após a invasão.

## 2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Em março de 2024, a Fortinet alertou sobre a vulnerabilidade CVE-2023-48788, que permite injeção de SQL no FortiClient EMS. Posteriormente, pesquisadores divulgaram uma exploração PoC dessa falha. Um incidente específico, que afetou uma companhia de mídia explorando a mesma vulnerabilidade, revelou indícios de um agente de ameaça. Este agente parece estar ativo desde 2022, atacando dispositivos Fortinet e operando com infraestrutura vietnamita e alemã.

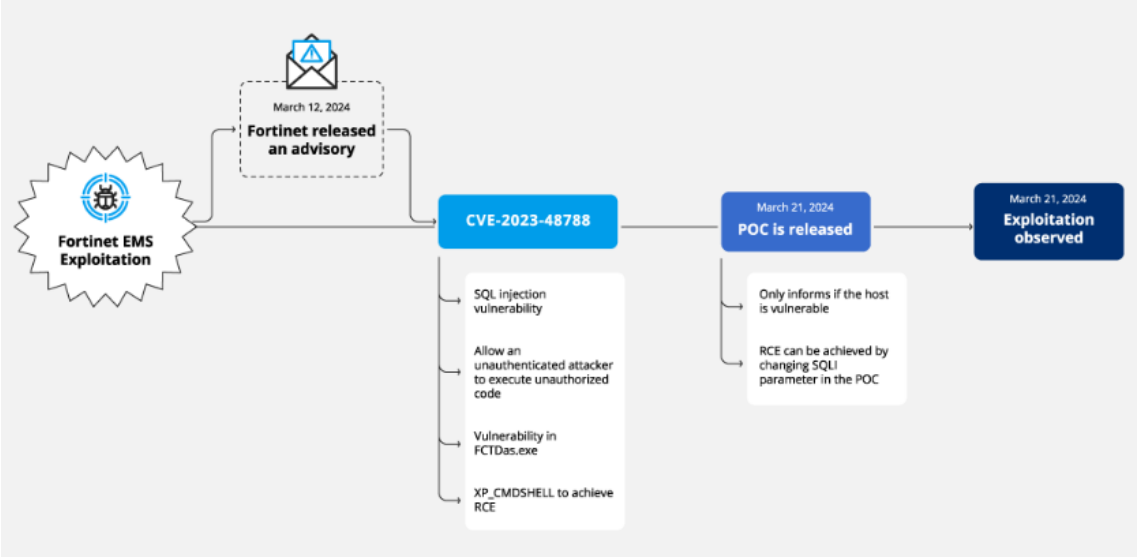



*Figura 1 – Fluxo de ataque.*

Os logs do servidor indicaram que o atacante tentou ativar configurações avançadas e o xp_cmdshell no SQL Server através de uma série de comandos. Em seguida, tentou usar o LOLBAS **finger.exe** para obter um arquivo malicioso do endereço 185[.]56[.]83[.]82, mas falhou devido a erros de sintaxe. Análise dos registros revelou que, o mesmo invasor realizou o comando “FINGER ADMIN@185.56.83.82” e adicionou “WAITFOR DELAY '00:00:10' –” para testar a execução do comando e a persistência da vulnerabilidade. A falha do comando não descarta a possibilidade de o sistema ainda estar exposto a riscos.

Após a confirmação da vulnerabilidade do host, o invasor procedeu com múltiplas injeções de SQL, utilizando comandos camuflados para efetuar o download do ScreenConnect, uma ferramenta de administração remota, e de um script nocivo inspirado no Powerfun de código livre, que possui capacidades para criar shells de conexão direta e reversa, além de permitir a execução de comandos arbitrários para controle remoto. Observou-se também, diversas tentativas de injeção SQL para obter o ScreenConnect através do domínio ursketz[.]com. Os arquivos baixados foram identificados previamente no IP 95[.]179[.]241[.]10.

O invasor utilizou o comando certutil.exe para efetuar o download do ScreenConnect e, em seguida, empregou o msiexec.exe para instalar a ferramenta. O processo de download e instalação ocorreu com êxito, conforme evidenciado pelos registros do firewall que mostraram tráfego direcionado ao domínio de onde o ScreenConnect foi baixado, localizado no endereço 141[.]136[.]43[.]188. As tentativas de conexão do ScreenConnect tinham como destino o IP 144[.]202[.]21[.]16. Entretanto, a recuperação dos logs do ScreenConnect para verificar atividades subsequentes não foi possível.

Este evento não ocorreu de forma isolada. Foi detectado ações de sondagem provenientes do endereço IP 185[.]56[.]83[.]82 direcionadas ao FortiClient EMS em diversas redes de clientes nos dias 21, 22, 25 e 28 de março. Essa sequência de eventos está alinhada com as tentativas de invasão anteriormente mencionadas e foi notada mesmo em clientes que não utilizam o FortiClient EMS, mas operam com outros tipos de dispositivos VPN. Contudo, não foram identificadas tentativas de exploração automatizada e indiscriminada em honeypots, um padrão comum observado anteriormente em outras vulnerabilidades críticas. As ações observadas indicam claramente uma intervenção manual, como demonstrado pelas repetidas tentativas frustradas de download e instalação de ferramentas, além do intervalo considerável entre essas tentativas.

Esses indícios reforçam a ideia de que as atividades detectadas fazem parte de uma campanha direcionada, e não de explorações automatizadas típicas de botnets associados a crimes cibernéticos. As análises sugerem que os responsáveis por essa campanha estão selecionando cuidadosamente os alvos, priorizando ambientes que contam com dispositivos VPN. Empresas do setor de segurança cibernética também reportaram incidentes similares envolvendo a exploração dessa vulnerabilidade para o download de softwares RMM, como ScreenConnect e Atera. Os relatórios analisados apresentam consistência, exibindo endereços IP e infraestruturas que coincidem com as observações, além de características que apontam para uma exploração de natureza manual.

Os endereços IP e domínios mencionados anteriormente têm um histórico de envolvimento em atividades suspeitas:

- O IP 185[.]56[.]83[.]82 foi registrado tentando acessar dispositivos SSLVPN da Fortinet em 14 de março, logo após o anúncio da Fortinet e antes da divulgação pública do PoC para a CVE-2023-48788. A mesma atividade foi notada nos dias 25 e 27 de março. Em 2022, esse IP já havia sido observado tentando acessar dispositivos SSLVPN da Fortinet e empregando métodos similares para baixar e executar payloads mal-intencionados.

- O IP 144[.]202[.]21[.]16, parte do AS20473, tinha as portas 3389 e 5985 abertas e usava o nome de host "vultr-guest" durante o incidente. Esse nome é padrão para endpoints na Vultr, conhecida por hospedar infraestrutura de ameaças, incluindo aquelas que exploraram a vulnerabilidade CVE-2018-13379 do FortiGate em 2022. Outro IP, 45[.]77[.]160[.]195, também hospedado pela Vultr, foi mencionado em um incidente semelhante envolvendo o FortiClient EMS.

- O IP 95[.]179[.]241[.]10 estava associado ao domínio ls[.]vfxtraining[.]shop e hospedado no AS20473 pela Vultr, com o mesmo nome de host "vultr-guest". Este host tinha várias portas abertas, incluindo 22/SSH e 2053/HTTP, exibindo o certificado comum mci11[.]raow[.]fun. A partir desse nome, foi possível identificar IPs adicionais na Alemanha, Emirados Árabes Unidos e Reino Unido. O site continha um diretório aberto com arquivos suspeitos como adduser, delete, kill.php, entre outros.

- O domínio ursketz[.]com foi alvo de um script suspeito do PowerShell chamado jpeg.lnk em 12 de abril de 2021, que tentava baixar arquivos de um repositório GitHub, agora desativado, contendo uma pasta "Projeto Nhap mon an toan thong tin" e vários arquivos suspeitos.

- ursketz[.]com resolvia para os endereços 2a02:4780:a:952:0:1e10:e79b:1 (IPv6) e 141[.]136[.]43[.]188 (IPv4) desde pelo menos 2022. Um instantâneo do site de 21 de julho de 2022 mostrava o título "UrSketz – Digital Assets Investment Company" e conteúdo em alemão, com um endereço de um prédio de escritórios na Alemanha.

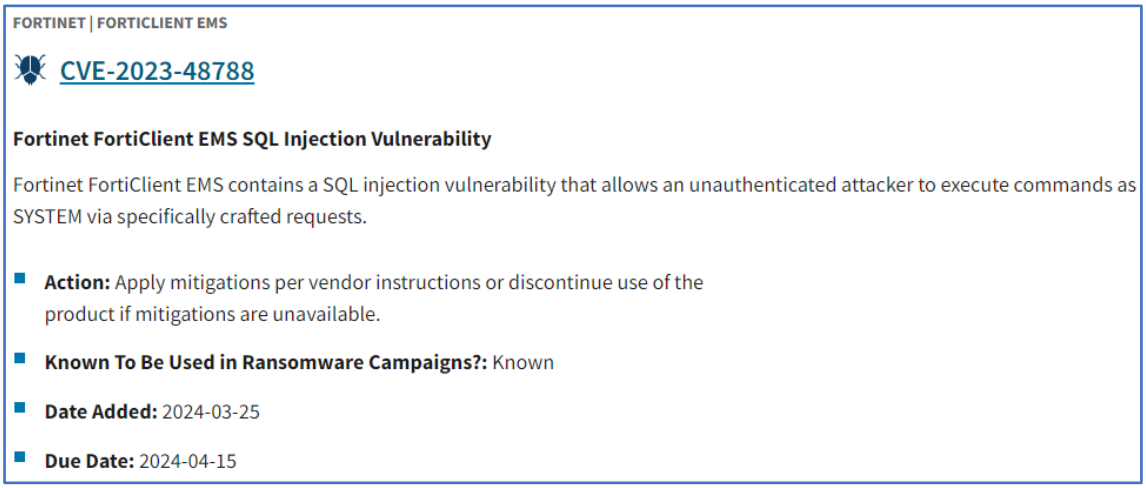
# 3 MITRE ATT&CK - TTPs

| Tática | Técnica | Detalhes |
|---|---|---|
| **Initial Access** | T1190 | Os adversários podem tentar explorar uma fraqueza em um host ou sistema voltado para a Internet para acessar inicialmente uma rede. A fraqueza do sistema pode ser um bug de software, uma falha temporária ou uma configuração incorreta. |
| **Command Control** | T1219 | Um adversário pode usar suporte de desktop legítimo e software de acesso remoto para estabelecer um canal interativo de comando e controle para atingir sistemas dentro de redes. |
| **Execution** | T1059.003 | Os adversários podem abusar do shell de comando do Windows para execução. O shell de comando do Windows ( cmd ) é o prompt de comando principal nos sistemas Windows. |
| **Execution** | T1059.001 | Os adversários podem abusar de comandos e scripts do PowerShell para execução. PowerShell é uma poderosa interface de linha de comando interativa e ambiente de script incluído no sistema operacional Windows. |
| **Defense Evasion** | T1027 | Os adversários podem tentar dificultar a descoberta ou análise de um arquivo executável ou arquivo criptografando, codificando ou ofuscando seu conteúdo no sistema ou em trânsito. |
| **Command Control** | T1105 | Os adversários podem transferir ferramentas ou outros arquivos de um sistema externo para um ambiente comprometido. |
| **Initial Access** | T1133 | Os adversários podem aproveitar serviços remotos externos para acessar inicialmente e/ou persistir em uma rede. |
| **Defense Evasion** | T1218.007 | Os adversários podem abusar do msiexec.exe para executar proxy de cargas maliciosas. Msiexec.exe é o utilitário de linha de comando do Windows Installer e, portanto, é comumente associado à execução de pacotes de instalação (.msi). |

Tabela 1 – Tabela MITRE ATT&CK.

# 4 VULNERABILIDADE ADICIONADA AO KEV-CISA

A agência de segurança cibernética (CISA) adicionou a falha ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), dizendo que tal vulnerabilidade é um "vetor de ataque frequente para atores cibernéticos maliciosos".



FORTINET | FORTICLIENT EMS

CVE-2023-48788

**Fortinet FortiClient EMS SQL Injection Vulnerability**

Fortinet FortiClient EMS contains a SQL injection vulnerability that allows an unauthenticated attacker to execute commands as SYSTEM via specifically crafted requests.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Known
- **Date Added:** 2024-03-25
- **Due Date:** 2024-04-15

*Figura 2 – Vulnerabilidade no catálogo KEV-CISA.*

# 5 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:

Para mitigar a exploração dessa vulnerabilidade é indicado que:

- Aplique o patch fornecido pela Fortinet.
- Certifique-se de que o tráfego que chega ao FortiClient EMS seja constantemente monitorado em busca de sinais de exploração usando sistemas de detecção de intrusão (IDS).
- Considere usar um firewall de aplicativo web (WAF) para bloquear solicitações potencialmente maliciosas.

# 6 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 URL, IPs e Domínios**

| Indicadores de URL, IPs e Domínios | |
|---|---|
| **URL** | hxxp[:]//45.227.255[.]213:20201<br>hxxp[:]//68[.]178.202.116<br>jxqmwbgxygkyftpxykdk8cfkq1hy371pz.oast[.]fun |
| **Domínio** | mci11[.]raow[.]fun |
| **IP** | 141[.]136[.]43[.]188<br>144[.]202[.]21[.]16<br>185[.]56[.]83[.]82<br>95[.]179[.]241[.]10<br>45[.]77[.]160[.]195 |

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.

# 7 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **Forescout**
- **Lolbas**
- **NVD**

heimdall
security research
A DIVISION OF ISH