BOLETIM DE SEGURANÇA

Grupo de Ransomware aproveitando vulnerabilidade no software de Backup Veeam

heimdall
security research
A DIVISION OF ISH

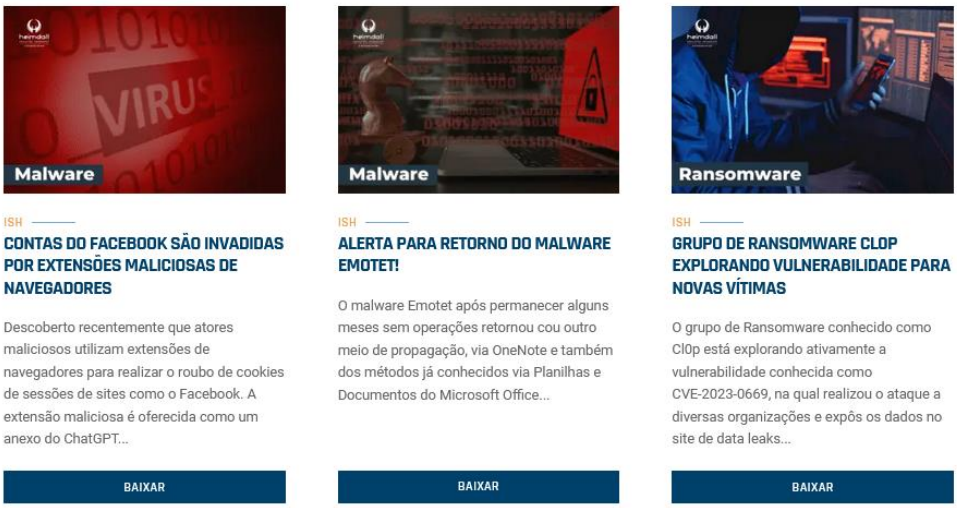
TLP: CLEAR

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

Recentemente o Grupo-IB, identificou um novo grupo de ransomware explorando a vulnerabilidade CVE-2023-27532 no software de backup Veeam. Este grupo malicioso utiliza táticas sofisticadas para atingir sistemas desprotegidos e realizar atividades prejudiciais.

2 INFORMAÇÃO SOBRE A AMEAÇA

Embora a vulnerabilidade CVE-2023-27532 tenha sido divulgada em março de 2023 e posteriormente corrigida pela Veeam nas versões 12/11a e posteriores do software Veeam Backup & Replication, porém foi observado um incidente significativo relacionado a essa vulnerabilidade. Neste blog, exploramos os detalhes desse incidente de ransomware, envolvendo o emergente ator de ameaça chamado EstateRansomware. Esta análise destaca como os agentes da ameaça rapidamente exploraram a vulnerabilidade CVE-2023-27532 para atingir o software Veeam Backup & Replication sem o devido patch. O blog oferece insights sobre as táticas, técnicas e procedimentos (TTPs) utilizados pelos invasores, desde o acesso inicial via FortiGate SSL VPN até o impacto do ransomware.

Em abril de 2024, o agente da ameaça conseguiu, mover-se lateralmente do Firewall FortiGate por meio do serviço SSL VPN para acessar o servidor Failover. Antes do ataque de ransomware, foram observadas tentativas de força bruta de VPN em abril de 2024, usando uma conta inativa identificada como ‘Acc1’. Alguns dias depois, um login VPN bem-sucedido com ‘Acc1’ foi rastreado até o endereço IP remoto 149.28.106[.]252.

Figura 1 – Login bem-sucedido do IP 149.28.106[.]252.

Em abril de 2024, observou-se várias conexões VPN originadas de endereços IP localizados nos Estados Unidos. Essas conexões utilizaram a conta ‘Acc1’ como identificação. Os endereços IP específicos envolvidos foram 149.28.106[.]252, 149.28.99[.]61 e 45.76.232[.]205. Logo após as conexões VPN, houve o estabelecimento de conexões RDP (Remote Desktop Protocol) do Firewall para o servidor de failover. Essa sequência de eventos sugere uma possível exploração maliciosa ou movimentação lateral na rede.

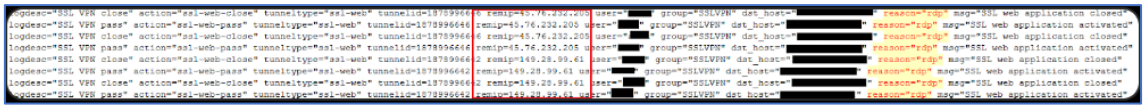


Figura 2 – RDP iniciado após conexões VPN.

Durante a sessão remota, o agente da ameaça executou a instalação de um backdoor persistente chamado “svchost.exe”. Esse backdoor foi projetado para permanecer ativo mesmo após a desconexão do túnel VPN. Além disso, o agente configurou uma tarefa agendada para garantir que o “svchost.exe” fosse executado diariamente. Essa medida visava manter o acesso contínuo e despercebido à rede comprometida. Após a instalação bem-sucedida do backdoor, o agente da ameaça desconectou-se do túnel VPN, evitando detecção adicional. No entanto, quando

necessário, ele utilizou o backdoor para restabelecer uma posição segura e recuperar o acesso à rede comprometida.

Value Name	Value Type	Data	Value Slack
Path	RegSz	\Host	
Hash	RegBinary	5E-98-68-AA-7D-23-2D-25-19-E7-DD-EE-EF-88-...	72-64-73-65
Schema	RegDword	65540	
Date	RegSz	2024-04- T16:07:10.0779887	00-00-7A-04
Author	RegSz		31-30
Triggers	RegBinary	15-00-00-00-00-00-00-00-01-80-A8-4D-F8-7F-0...	00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
Actions	RegBinary	01-00-66-66-00-00-00-00-56-00-00-00-43-00-3...	00-00
DynamicInfo	RegBinary	03-00-00-00-CD-93-78-BE-F9-92-DA-01-00-00-0...	

Figura 3 – Registro de SOFTWARE Tarefa agendada.

Durante a análise das conexões de rede ativas no servidor de failover, foi identificado conexões com o endereço IP 77.238.245[.]11 através de uma porta incomum, a 30001. Essa comunicação suspeita levantou preocupações sobre atividades maliciosas.

Uma investigação mais detalhada do processo ‘svchost.exe’ confirmou que o endereço IP 77.238.245[.]11:30001 funciona como um ponto de comando e controle (C2). Esse backdoor estabelece um túnel reverso usando o protocolo HTTP, permitindo que o agente da ameaça execute comandos remotamente no servidor de failover.

```
 TCP                              192.168.                ESTABLISHED
Can not obtain ownership information
 TCP                              192.168.                ESTABLISHED
[System]
 TCP                              77.238.245.11:30001     SYN_SENT
[Svchost.exe]
 TCP    [::]:88                   [::]:0                  LISTENING
 Kdc
[System]
```

Figura 4 – Conexão ao endereço C2 do servidor de failover.

No dia seguinte, o agente de ameaça transferiu suas atividades do servidor de failover para o servidor de arquivos, utilizando a conexão RDP (Remote Desktop Protocol). Esse movimento sugere uma estratégia deliberada para explorar vulnerabilidades e coletar informações.

Com base nos arquivos acessados pelo agente de ameaça, ficou evidente que seu principal objetivo era coletar credenciais e explorar vulnerabilidades no software Veeam Backup & Replication. Essa abordagem estratégica indica um conhecimento específico sobre os sistemas-alvo.

Alguns dos artefatos encontrados incluem:

- C:\Usuários\[redigido]\Downloads\pasta veeam-creds-main
- C:\Usuários\[redigido]\Downloads\Depuração\Depuração\net6.0\CVE-2023-27532.exe
- C:\Usuários\[redigido]\Downloads\Debug\Debug\Pasta Veeamhax

O agente de ameaça demonstrou intenção ao executar o arquivo 'Veeam-creds-main', e essa ação foi registrada no log de eventos do Windows PowerShell. De acordo com o projeto mantido por sadshade no GitHub, a execução bem-sucedida desse arquivo permitiria ao agente de ameaça obter senhas do gerenciador de credenciais do Veeam Backup and Replication.

Figura 5 – Log de eventos do Windows PowerShell ID do evento 600.

Existe uma forte probabilidade de que os arquivos "CVE-2023-27532.exe" e "VeeamHax" estejam relacionados à Prova de Conceito publicada pelos pesquisadores Horizion3 e sfewer-r7 no GitHub. Essa prova de conceito pode ter sido usada como base para explorar vulnerabilidades no software Veeam Backup & Replication. Tanto o servidor de arquivos quanto o servidor de backup foram identificados como executando versões vulneráveis do Veeam Backup & Replication. O servidor de arquivos estava na versão v9.5.2855, enquanto o servidor de backup estava na versão v9.5.0.1922. A análise do log de eventos do aplicativo do Windows revelou uma tentativa de executar o arquivo "CVE-2023-27532.exe", mas essa ação resultou em uma falha de software.

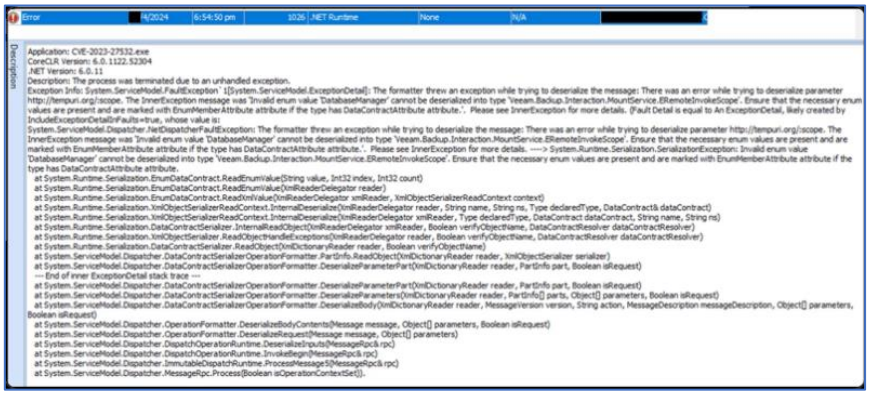
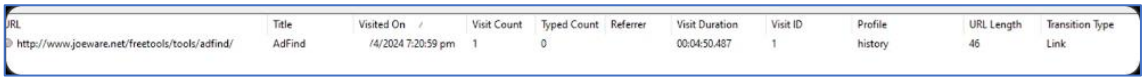


Figura 6 – Software travado.

A partir do servidor de arquivos, o agente da ameaça implantou o SoftPerfect Netscan e várias ferramentas de recuperação de senha da Nirsoft. Essas ferramentas foram utilizadas para escanear a rede, coletando informações sobre hosts ativos, portas abertas, compartilhamentos de arquivos e credenciais.

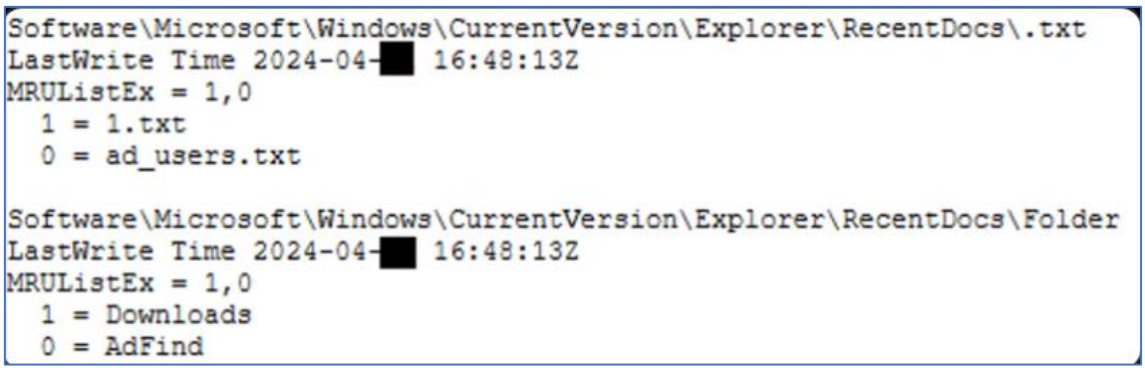
No servidor de backup, o agente da ameaça conduziu a coleta de credenciais adicionais por meio da conta recém-criada 'VeeamBkp'. Com essas informações em mãos, o agente procedeu a pivotar lateralmente para o servidor Active Directory (AD) via RDP, visando uma varredura mais ampla da rede.

No servidor AD, o agente baixou o AdFind, uma ferramenta de consulta de linha de comando que permite coletar informações do Active Directory. Essa ferramenta foi empregada para enumerar os usuários do domínio.



URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit Duration	Visit ID	Profile	URL Length	Transition Type
http://www.joeware.net/freetools/tools/adfind/	AdFind	/4/2024 7:20:59 pm	1	0		00:04:50.487	1	history	46	Link

Figura 7 – AdFind baixado usando o Google Chrome.



```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
LastWrite Time 2024-04-[redacted] 16:48:13Z
MRUListEx = 1,0
  1 = 1.txt
  0 = ad_users.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time 2024-04-[redacted] 16:48:13Z
MRUListEx = 1,0
  1 = Downloads
  0 = AdFind
```

Figura 8 – Pasta AdFind ad_users.txt aberta recentemente.

3 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1078 T1133	Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede.
Execution	T1204.002 T1569.002 T1053.005	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.
Persistence	T1136.001 T1505.001	Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso.
Defense Evasion	T1070.001 T1070.004 T1562.001	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Credential Access	T1555	Consiste em técnicas para roubar credenciais como nomes de contas e senhas. Técnicas usadas para obter credenciais incluem keylogging ou credential dumping.
Discovery	T1018 T1087.002	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Lateral Movement	T1021.001	Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede.
Command & Control	T1571 T1071.001	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.
Impact	T1486	Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade ao manipular processos comerciais e operacionais.

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:

- Monitore e audite contas regularmente. Exclua ou desabilite qualquer conta inativa para evitar acesso não autorizado. Implemente autenticação multifator (MFA) para VPN e outros serviços de acesso remoto.
- Implemente uma política de gerenciamento de patches para garantir que os firmwares e softwares usados sejam atualizados com os patches de segurança mais recentes para proteção contra vulnerabilidades conhecidas.
- Segmente sistemas críticos e imponha regras rígidas de firewall para limitar o movimento lateral dentro da rede. Desabilite o acesso RDP desnecessário e restrinja-o a endereços IP específicos e confiáveis.
- Implemente o controle de aplicativos em hosts para impedir a execução de programas não autorizados. Garanta que apenas aplicativos de segurança aprovados sejam usados e executados em sistemas empresariais.
- Implemento Detecção e resposta de endpoint (EDR)solução para detectar e responder a atividades suspeitas, como implantação de backdoors e uso de ferramentas como o PsExec.

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:	58008524a6473bdf86c1040a9a9e39c3
sha1:	cb704d2e8df80fd3500a5b817966dc262d80ddb8
sha256:	1ef6c1a4dfdc39b63bfe650ca81ab89510de6c0d3d7c608ac5be80033e559326
File name:	dControl.exe

Indicadores de compromisso do artefato	
sha256:	2C56E9BEEA9F0801E0110A7DC5549B4FA0661362
sha256:	5E460A517F0579B831B09EC99EF158AC0DD3D4FA
sha256:	107EC3A7ED7AD908774AD18E3E03D4B999D4690C

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	149.28.106[.]252 149.28.99[.]61 45.76.232[.]205 77.238.245[.]11:30001

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**
- **GroupIB**
- **Thehackernews**
- **NVD**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH