TLP: CLEAR

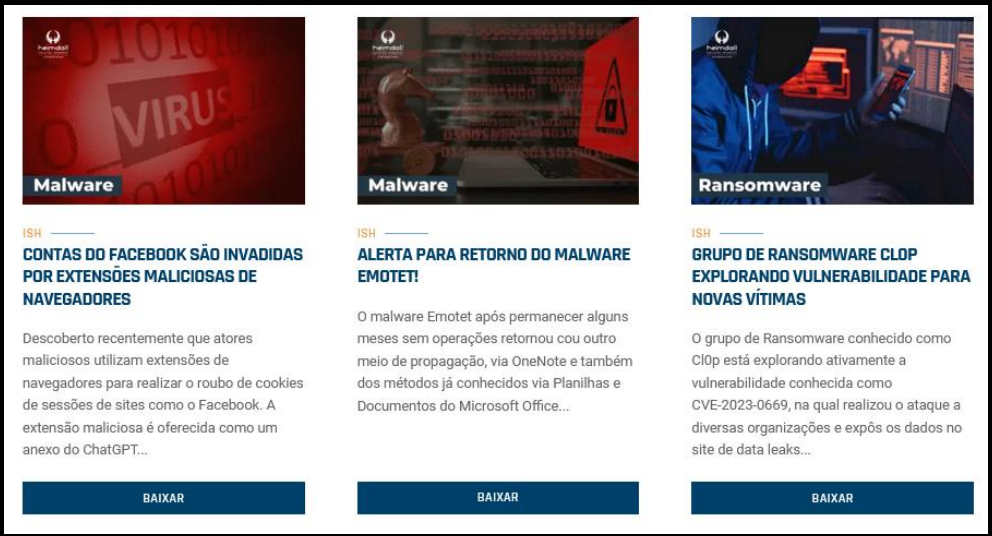
RELATÓRIO DE PESQUISAS

Atualizações da operação do Ransomware MedusaLocker

heimdall
security research
A DIVISION OF ISH

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 MEDUSALOCKER OU BABYLOCKERKZ ?

A Cisco Talos, teria o observado um ataque que teria culminado a implantação de uma variante de ransomware **MedusaLocker**, a qual é conhecida como BabyLockerKZ. As técnicas distinguíveis, incluindo o armazenamento consistente do mesmo conjunto de ferramenta na mesmo local em sistemas comprometidos, a utilização de ferramentas que possuem o caminho PDB com a string “paid_memes” e o uso da ferramenta de movimentação lateral chamada “Checker”, utilizadas no ataque teria chamado a atenção da Talos para entender mais sobre o ator.

O invasor teria utilizado várias ferramentas de ataques conhecidas publicamente e binários de Living-off-the-land (LoLBins), um conjunto de ferramentas criado pelo mesmo desenvolvedor para auxiliar o roubo de credenciais e na movimentação lateral em organizações comprometidas. As ferramentas são, em sua maioria, wrappers em torno de ferramentas disponíveis publicamente que incluem funcionalidades adicionais para agilizar o processo de ataque e fornecer interfaces gráficas ou de linha de comando.

De acordo com o relatório, o mesmo desenvolvedor que teria construído a variante do MedusaLocker e construído as ferramentas mencionadas anteriormente para a prática do ataque. A referida variante utilizou os mesmos URLs de bate-papo e site de vazamento (DLS) e contém algumas diferenças em relação ao ransomware MedusaLocker original, como uma chave de execução automática diferente ou um conjunto extra de chaves públicas e privadas armazenadas no registro. Com base no nome da chave de execução automática, os atores chamam esta variante de BabyLockerKZ.

A Cisco teria analisado que o ator possuí motivação financeira, provavelmente trabalhando com IAB (Corretores de Acessos Iniciais) ou afiliado de um cartel de ransomware, e estaria realizando ataques desde pelo menos 2022. De acordo com as movimentações do grupo, o Brasil teria sido o foco principal do grupo a partir de fevereiro de 2023, indicando que outros países também da América Latina foram alvos do grupo.

2 ATUALIZAÇÕES DE TTPS

O afiliado que teria utilizado a variante do **BabyLockerKZ**, teria utilizado várias ferramentas de ataques conhecidas publicamente e outras que podem ser exclusivas do referido ator.

O grupo utiliza frequentemente pastas de usuários de Músicas, Imagens ou Documentos de sistemas comprometidos para armazenar ferramentas de ataques, conforme o exemplo dos caminhos a seguir:

```
c:\users\<user>\music\advanced_port_scanner_2.5.3869.exe
c:\users\<user>\music\hrsword\hrsword install.bat
c:\users\<user>\music\killav\build.004\disabler.exe
c:/users/<user>/music/checker/checker(222).exe
c:/users/<user>/music/checker/invoke-thehash.ps1
c:/users/<user>/music/checker/checker (222).exe
c:/users/<user>/music/checker/invoke-smbexec.ps1
c:/users/<user>/music/checker/invoke-wmiexec.ps1
c:/users/<user>/appdata/roaming/ntsystem/ntlhost.exe.exe
c:/users/<user>/appdata/local/temp/advanced port scanner 2/advanced_port_scanner.exe
c:/users/<user>/appdata/local/temp/is-juad3.tmp/advanced_port_scanner_2.5.3869.tmp
```

Tabela 1 – Caminhos das ferramentas sendo executadas.

Estas ferramentas são semelhantes a um ataque que teria levado a um ransomware MedusaLocker, documentado pela **ASEC** em fevereiro de 2023. Além disso, algumas das ferramentas publicamente conhecidas utilizadas pelo invasor são:

- **HRSword_v5.0.1.1.rar:** Ferramenta utilizada para desativar software AV e EDR.
- **Avanced_Port_Scanner_2.5.3869.exe:** Uma ferramenta utilizada para verificação de rede com vários recursos adicionais para mapear redes e dispositivos internos.
- **Netscan.exe (SoftPerfect Network Scanner):** uma ferramenta semelhante ao Advanced Port Scanner.
- **Processhacker.exe:** Software de monitoramento e administração de processos. Permite que um Ator de Ameaça enumere e controle processos em execução no endpoint infectado.
- **PCHunter64.exe:** Uma ferramenta semelhante ao Process Hacker.
- **Mimikatz:** Uma ferramenta para extrair credenciais de usuário do Windows da memória.

De acordo com a Cisco, embora a maioria das ferramentas que os atores utilizaram estão disponíveis publicamente, acabam também utilizando ferramentas que não são amplamente distribuídas e que agilizam o processo de ataque, automatizando a interação entre ferramentas de ataque populares.

Uma das ferramentas é a conhecida como “Checker”, utilizada em um ataque que implantou o BabyLockerKZ. A referida ferramenta também utilizava o mesmo caminho de PDB, contendo a string “paid_memes” **(E:\ paid_memes \wmi_smb_rdp_checker\Release\checker.pdb)**. Esta ferramenta fornece uma tela gráfica para o usuário e apresenta outras ferramentas como: Mimikatz, PSEXEC e Remote Desktop Plus. Além disso, utiliza um conjunto de scripts baseados na ferramenta **“Invoke-TheHash”.**

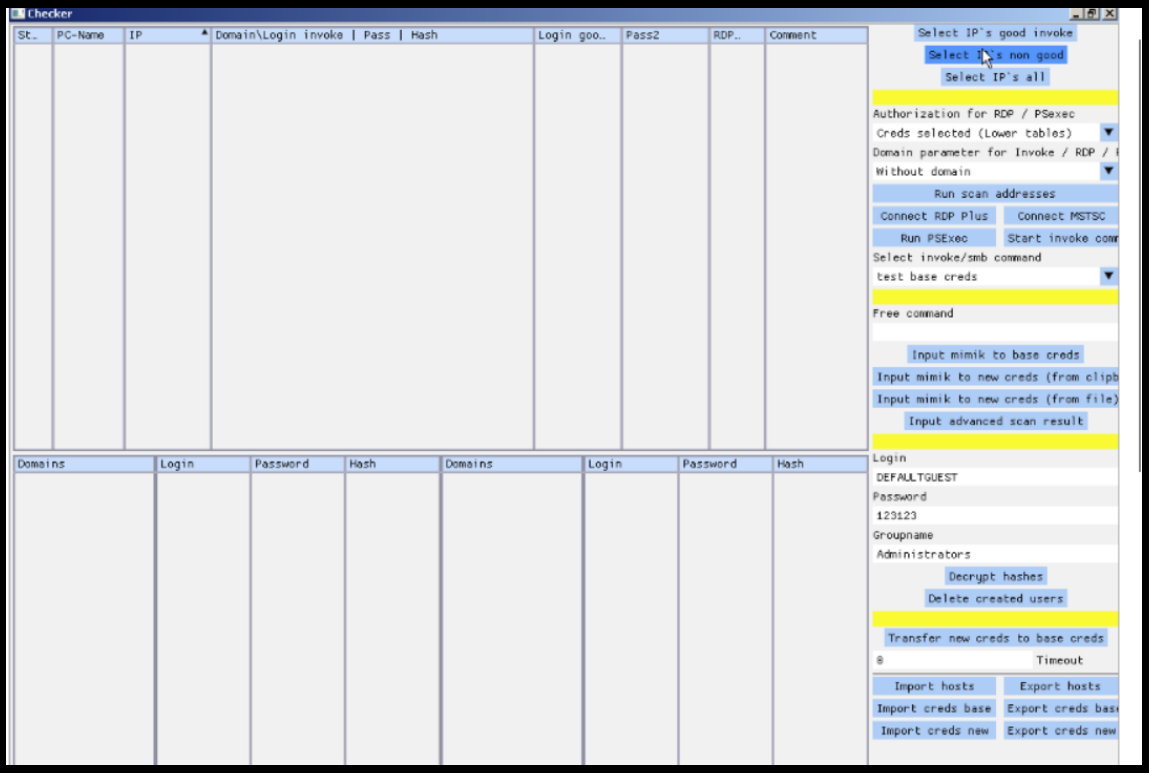


Figura 1 – Interface Gráfica da ferramenta “Checker”.

De acordo com a imagem fornecida pela Talos, a ferramenta poderia ser utilizada para escâner IPs em busca de credenciais válidas utilizando diversos protocolos/técnica se estaria preparada para importar dados de lista de hosts e algumas das ferramentas do ator de ameaça.

Outra ferramenta conhecida é a PTH Project, a qual também possui o caminho de PDB **(D:\Projects\paid_memes\PTH\Release\PTH.pdb),** a qual é utilizada para fins da técnica **“pass-the-hash”** em NTLM, visando se autenticar remotamente sem precisar quebrar a senha. Alguns dos scripts são:

- **Invoke-SMBClient.ps1**
- **Invoke-SMBEnum.ps1**
- **Invoke-SMBExec.ps1**
- **Invoke-TheHash.ps1**

- **Invoke-WMIExec.ps1**

A ferramenta MIMIK também foi utilizada pelos atores e utiliza do mesmo caminho de PDB das anteriores **(D:\Projects\paid_memes\PTH\Release\PTH.pdb)**, a qual seria um wrapper em torno de Mimikatz e Rclone, que pode ser utilizado para roubar credenciais e carregá-las automaticamente em um servidor controlado pelo invasor.

Os comandos abaixo são exemplos de comandos utilizados por meio do uso das ferramentas:

```
64.exe privilege::debug sekurlsa::logonPasswords token::elevate lsadump::sam full exit
C:\Users\user\Desktop\64.exe 64.exe "privilege::debug" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam full" exit
64.exe "privilege::debug" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam full" exit
C:\Users\user\Desktop\rclone.exe rclone rcd --rc-no-auth --bwlimit=30M
C:\Users\user\Desktop\rclone.exe rclone rc operations/stat
```

Tabela 2 – Comandos relacionados a ferramentas.

Por fim, a Cisco abordou a variante do Ransomware conhecida como BabyLockerKZ, a qual estava sendo utilizada desde o final de 2023. Em outro momento, a empresa Cynet teria anunciado que o malware teria utilizado **"Hazard"** como uma variante do Ransomware MedusaLocker e mencionou a existência da chave de registro BabyLockerKZ.

Além disso, a Whitehat, mancionou a existência de chaves de registro PAIDMEMES PUBLIC e PRIVATE em uma amostra do MedusaLocker.

A referida variante não recebeu muita atenção além destes relatórios, possivelmente porque seria muito semelhante ao MedusaLocker. Mas dentre as diferenças, estão:

- Não há o mutex: {8761ABBD-7F85-42EE-B272-A76179687C63}.
- Nenhuma chave de registro MDSLK.
- As chaves públicas e privadas PAIDMEMES.
- A chave de execução necessária do BabyLockerKZ.

De acordo com a Cisco, a utilização de chaves públicas e privadas PAIDMEMES não seria claro.

Diante disto, a Cisco disponibilizou ainda os Indicadores de Comprometimento relacionado aos malwares e ferramentas mencionados neste boletim.

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:

- Implemente um plano de recuperação para manter e reter múltiplas cópias de dados sensíveis ou proprietários e servidores em um local fisicamente separado, segmentado e seguro (por exemplo, disco rígido, dispositivo de armazenamento, na nuvem).
- Exija que todas as contas com login de senha (por exemplo, contas de serviço, contas de administrador e contas de administrador de domínio) cumpram os padrões do NIST. Em particular, exija que os funcionários usem senhas longas e considere não exigir alterações de senha recorrentes, pois isso pode enfraquecer a segurança.
- Exija autenticação multifator para todos os serviços na medida do possível, principalmente para correio da web, redes privadas virtuais e contas que acessam sistemas críticos.
- Mantenha todos os sistemas operacionais, software e firmware atualizados. A atualização oportuna é uma das medidas mais eficientes e econômicas que uma organização pode tomar para minimizar sua exposição a ameaças de segurança cibernética.
- Segmente redes para evitar a propagação de ransomware. A segmentação de rede pode ajudar a evitar a propagação de ransomware controlando os fluxos de tráfego entre e o acesso a várias sub-redes e restringindo o movimento lateral do adversário.
- Identifique, detecte e investigue atividades anormais e potenciais travessias do ransomware indicado com uma ferramenta de monitoramento de rede.
- Filtre o tráfego de rede impedindo que origens desconhecidas ou não confiáveis acessem serviços remotos em sistemas internos.
- Instale, atualize regularmente e ative a detecção em tempo real para software antivírus em todos os hosts.
- Revise controladores de domínio, servidores, estações de trabalho e diretórios ativos para contas novas e/ou não reconhecidas.
- Audite contas de usuário com privilégios administrativos e configure controles de acesso de acordo com o princípio do menor privilégio.
- Desative portas não utilizadas.
- Considere adicionar um banner de e-mail para e-mails recebidos de fora da sua organização.
- Desative hiperlinks em e-mails recebidos.
- Implemente acesso baseado em tempo para contas definidas no nível de administrador e superior.
- Desative atividades e permissões de linha de comando e script.

- Mantenha backups offline de dados e realize regularmente backup e restauração.
- Assegure-se de que todos os dados de backup sejam criptografados, imutáveis e cubram toda a infraestrutura de dados da organização.

4 INDICADORES DE COMPROMETIMENTO

A ISH Tecnologia realiza o tratamento de diversos indicadores de Comprometimento 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 Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	56b6d9b9fbcb471d5447fdfd362f0a71
sha1:	28c1fefc10b890cef70a3f0fc40ba121ee44c475
sha256:	33a8024395c56fab4564b9baef1645e505e00b0b36bff6fad3aedb666022599a
File name:	pomochit01.exe

Indicadores de compromisso do artefato	
md5:	27e341c1f696245b81537fd9e3b93a94
sha1:	d18351335232ae4fdd0b693945acd00a79c2e81b
sha256:	b8c994e3ed7dcc9080916119ddc315533c129479f508676d7544b82b2e24745f
File name:	lock6n.exe

Indicadores de compromisso do artefato	
md5:	022a903fe51bf05830c679503233d7b6
sha1:	ca42b7fa4f292fb2fbe29f30bb1c84fb8d357a3c
sha256:	63eb3d2886d9cb880c9b0d54b94f3e149b3b5b6215a33a0ef63588a09dcd4499
File name:	iN-mamai.exe

Indicadores de compromisso do artefato	
md5:	c22d9e6d04b8396793c41e96388e92ab
sha1:	4c90556604df03ac74466da6cd15fd1c239418c1
sha256:	270c3354b3ee2940b499e365eaba143fba9d458f434dc38e663dc0f08e96121e
File name:	readtext24.exe

Indicadores de compromisso do artefato	
md5:	2aed9553069de3ea13ceb7bfb8d62302
sha1:	474dbdecdcb966747360ada83ed83b391ef3eb53
sha256:	759b96f44806578cc0836a3a2bf11c8bc553effac72f8d28b94aec78b66be906
File name:	iN.exe

Indicadores de compromisso do artefato	
md5:	8cbcb7dc9d6d5847bb8391cb1e0d4986
sha1:	e834573675941729abacdf4b7e1abe1eaf3b94e2
sha256:	9f066975f1e02b29c7c635280f405c59704ce4f4e06b04e9ac8a7eac22acd3c7
File name:	PTH.exe

Indicadores de compromisso do artefato	
md5:	689ce296ec723cb01f885c0466eb9e0c
sha1:	d9da5eaff17f6c72fd29f9032e9c0f0ef33171af
sha256:	8bc455e5de35290f8a94376357947bd72aaf6f4d452c25a8ef444e037ef76b9f

File name:	PTH.exe

Indicadores de compromisso do artefato	
md5:	f2465e305c6ffe9853928c9127f53485
sha1:	fdb01ab55c0ec4da517bb6374b0e99174d3f95cc
sha256:	d00f7cf6af68ba832b9d364f28411346cfe66fd3b1f5bcac318766add29ff7f0
File name:	checker (222).exe

Indicadores de compromisso do artefato	
md5:	32239cf8ee32f98a3c0a9e3349dd634e
sha1:	9a76d6a82b1aa47b33713bcde6d41abe3f29dbf2
sha256:	1f2df15442593b159e45d16a27e4d43d3a9062da212a588ba4c048f214a0b7be
File name:	checker (225).exe

Indicadores de compromisso do artefato	
md5:	a98675c091691c273694578843d4a780
sha1:	9079acbbd2466fd79488b8405bb8f770a7b2ae52
sha256:	1e9246e6a35731143368eaa0ade4f3cf576d6b22e6090152f6e94f1fa3070651

Indicadores de compromisso do artefato	
md5:	e635aba475e892d35b6326f90e861a43
sha1:	27d425d4046bfe9e6e61f6bc771f025e4aa6fb22
sha256:	6ae3a58a78be9c606009c657de4e390538b21ad951e62b6f4d31138e1a75732c
File name:	checker (112) stable.exe

Indicadores de compromisso do artefato	
md5:	f32af20bbe82c33dffa9ac6a50ecb278
sha1:	52a08d0fb6cc37c2d4804198c1db6c2e7e8c6fc6
sha256:	2eddfe711c32ef1668e14a10d00452c83c29e394e17c41f491550a1583c1bcac
File name:	dropped.bin

Indicadores de compromisso do artefato	
md5:	51afb877c52cc888f55819996fffbcc2
sha1:	e2030f46b171a6fbd1d9509f3189b921b6e80425
sha256:	dc4840a0992b218cbedd5a7ac5c711cb98f1f9e78a8ffdea37c694061dfd34c6
File name:	S.exe

Indicadores de compromisso do artefato	
md5:	afddf1db7b4dd2928105e34d2e3e7054
sha1:	bba5a0c24a06abc2edc79bd1432b74f217a9da25
sha256:	48046fb0e566f5a2d184f84b76d6cadc458762556daed0ae4a3a1200afbefb54

Indicadores de compromisso do artefato	
md5:	2dc0dad1939edfdf997525bac94cdc21
sha1:	e3e398a3eed8ffc0266dbe37c396909eee150cf4
sha256:	c0c726a23111c220d022fcd01a85f9788249e42baece03f83b6059170453b801
File name:	64New_bull4.exe

Indicadores de compromisso do artefato	
md5:	d398931b11050272def14cc8b1838ed5
sha1:	1fa9ea8fee507630d905f6ff04c8044765687cc3
sha256:	012657c4548d9c98223caa4cc7aa52fc083d6983d42fde16ca3271412e7fe3fe
File name:	software.exe

Indicadores de compromisso do artefato	
md5:	db82819a9a7d3951c9ed989093b97b62
sha1:	b9d5d4e74d3a8560728479ed1011a2df70a06e03
sha256:	8edbb1944d94ff91ee917c31590b6d1d5690a52fc153e44355ee9749aa0f4625
File name:	LN3.exe

Indicadores de compromisso do artefato	
md5:	73fc61bbec7230ef268be95246dbfa67
sha1:	d700c6548240a75fc8a0b72ac4ad2cca1b6d4fe5
sha256:	364f1b7466d8e4c9f55294ecf1f874c763bcf980c59b0250c613ac366def6aca

Indicadores de compromisso do artefato	
md5:	aa0dec3adef08a4dbd655183de9d2843
sha1:	30e74bcafb2edee17e10f765dbc3724ae2b467f1
sha256:	5d5d639fdfbf632bb7d9f1bb28731217d09d36078ab5e594baf2a5a41267a5d2
File name:	decrypter.exe

Tabela 3 – Indicadores de Comprometimento de artefatos.

```
d:/projects/paid_memes/virus/release/stub.pdb
e:/locker/bin/stub_win_x64_encrypter.pdb
i:/locker/bin/stub_win_x64_encrypter.pdb
d:/education/locker/bin/stub_win_x64_encrypter.pdb
d:/education/locker/bin/stub_win_x86_encrypter.pdb
d:/projects/paid_memes/wmi_smb_rdp_checker/release/checker.pdb
d:/projects/paid_memes/mimik/release/stub_mimik.pdb
i:/locker/x64/release/phantom.pdb
d:/projects/paid_memes/pth/release/pth.pdb
```

Tabela 4 – Indicadores de PDB de caminhos de arquivos.

```
Registry keys:
HKEY_USERS\%SID%\SOFTWARE\PAIDMEMES\PRIVATE
HKEY_USERS\%SID%\SOFTWARE\PAIDMEMES\PUBLIC
HKEY_CURRENT_USER\SOFTWARE\PAIDMEMES\PUBLIC
HKEY_CURRENT_USER\SOFTWARE\PAIDMEMES\PRIVATE
HKCU\SOFTWARE\PAIDMEMES\PUBLIC
HKCU\SOFTWARE\PAIDMEMES\PRIVATE
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ
HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ
```

Tabela 5 – Chaves de Registro Modificadas.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Threat Actor believed to be spreading new MedusaLocker variant since 2022 – Cisco Talos**
- **Globeimposter Ransomware Being Distributed with MedusaLocker via RDP – ASEC**
- **Dynamic Analysis: Hazard Ransomware – Cynet**
- **MedusaLocker Ransomware - Parte 2 – White Hat**

6 AUTORES

- **Caique Barqueta**

heimdall
security research
A DIVISION OF ISH