BOLETIM DE SEGURANÇA

Exploração de túneis Cloudflare por cibercriminosos para disseminação de malware e evasão de defesas

heimdall
security research
A DIVISION OF ISH

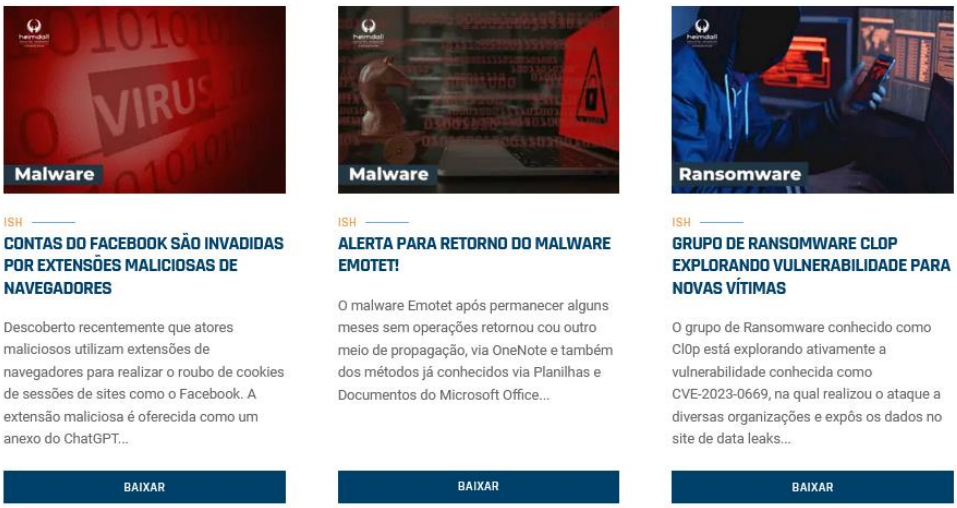
TLP: CLEAR

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 eSentire, em colaboração com a Proofpoint, identificou uma campanha maliciosa que explora o serviço TryCloudflare. Os cibercriminosos utilizam este serviço para estabelecer um túnel de comunicação que permite o tráfego malicioso do servidor do atacante para um dispositivo local, camuflando suas ações através da infraestrutura da Cloudflare.

2 INFORMAÇÕES SOBRE A AMEAÇA

A unidade TRU da eSentire identificou um ataque cibernético em uma entidade governamental, envolvendo malwares como XWorm e VenomRAT, utilizando um servidor WebDAV no TryCloudflare. O WebDAV facilita a gestão de arquivos remotos, sendo útil para a distribuição de malwares. O TryCloudflare, serviço gratuito da Cloudflare, permite criar servidores web temporários. O ataque começou com um e-mail de phishing contendo um arquivo ZIP com um link malicioso que direcionava para um arquivo .lnk no servidor WebDAV. Este arquivo .lnk disparava a execução de arquivos em lote que baixavam e executavam códigos Python mal-intencionados.

O arquivo new.bat (MD5: 0d79c56f9198117a98334ead5d033974) foi ofuscado com bytes específicos para ser interpretado como UTF-16LE.

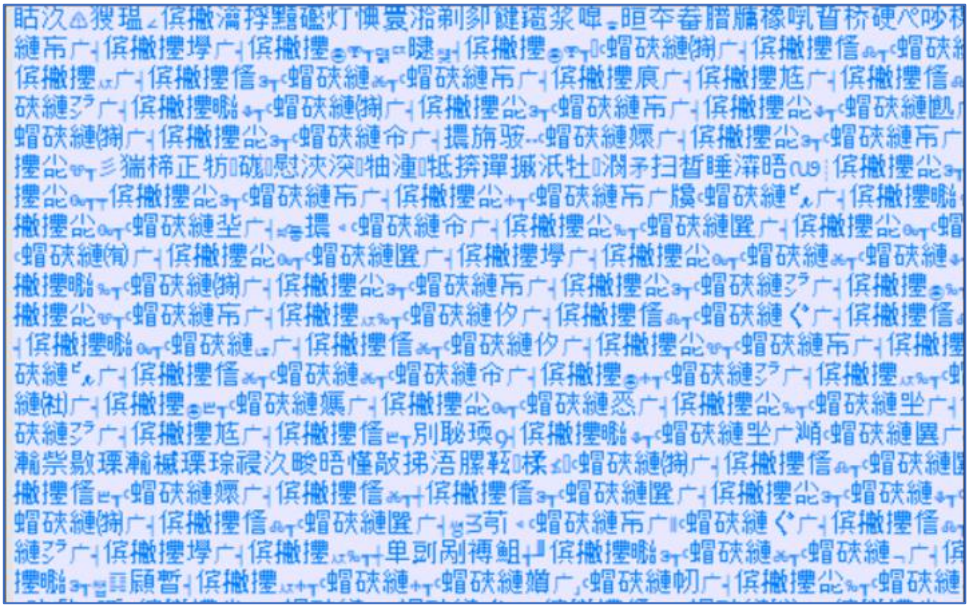


Figura 1 – Conteúdo do arquivo new.bat (UTF-16LE).

A ofuscação utilizava uma cifra de substituição, onde caracteres eram representados por índices em uma string chave. As ações do new.bat incluíam abrir um PDF falso, baixar e extrair arquivos ZIP com PowerShell, ocultar pastas extraídas e baixar o arquivo startupppp.bat (MD5: 1e5fa94c5be0d6f6d57c181c60622b80) para a pasta de inicialização do sistema, além de executar vários scripts Python nocivos.

É importante mencionar que os payloads Python descriptografados nos arquivos DXJS.zip e FTSP.zip eram idênticos, indicando uma estratégia coordenada dos invasores.

Filename	MD5	SHA1
Xwrm3v_6_py.exe	e4093e66d377d1f1552220fb7342385f	e52b1cc79332027b407ac38c3d30ba6d5d1c5...
Xwrm3v_update_py.exe	e4093e66d377d1f1552220fb7342385f	e52b1cc79332027b407ac38c3d30ba6d5d1c5...
AsyncClient_time_py.exe	c9562d033d5e13674af5b5fdc3e5801c	9978d75cf93eee632e32848a9e41d036cc60396f
AsyncClient_2_py.exe	c9562d033d5e13674af5b5fdc3e5801c	9978d75cf93eee632e32848a9e41d036cc60396f
Anarchynostart_kam_py.exe	e618be3fea2925a6637d8fcf05ff5c8a	206a4eca3c98bb5221ba9490fc8e9c2a40f5c4...
Anarchynostart_1_py.exe	e618be3fea2925a6637d8fcf05ff5c8a	206a4eca3c98bb5221ba9490fc8e9c2a40f5c4...
Dghucwmscrj_money_py.exe	1e66092482f2738ff808c2fc076185e6	013b32eaafcb4ad412c190579fd5be43911795...
Dghucwmscrj_4_py.exe	1e66092482f2738ff808c2fc076185e6	013b32eaafcb4ad412c190579fd5be43911795...
ClientVRNM8520_moment_py.exe	58e6b6b4b7f6849749b6374ffbd7fa2e	51179defee9d29718177eb3fd0d0fdd5016165...
ClientVRNM8520_3_py.exe	58e6b6b4b7f6849749b6374ffbd7fa2e	51179defee9d29718177eb3fd0d0fdd5016165...
Xvwrm5v_upload_py.exe	a8bfb9877be0daf890333c91c88c77d8	d382536e8a13310baa477d4dbdcd0fb490f91...
Xvwrm5v_5_py.exe	a8bfb9877be0daf890333c91c88c77d8	d382536e8a13310baa477d4dbdcd0fb490f91...

Figura 2 – Cargas úteis descriptografadas de DXJS.zip e FTSP.zip com os mesmos hashes.

O script Python 2.py (MD5: a84994e9e9de4fd82f721dbf2c8d9c58) contém um shellcode criptografado com RC4 e codificado em base64. Após a descriptografia, o shellcode é executado diretamente na memória. Isso é feito alocando um buffer para o shellcode descriptografado e alterando a proteção de memória para permitir a execução de código.

Figura 3 – Conteúdo do script Python 2.py incluindo o algoritmo de descriptografia RC4.

O payload descriptografado no shellcode realiza a descriptografia de outro payload de shellcode usando AES. Isso envolve a criação de um conjunto de chaves redondas a partir da chave de criptografia principal. Durante a descriptografia, os dados são manipulados em blocos e passam por várias transformações.

Cada byte do bloco é substituído de acordo com uma tabela predefinida, revertendo o embaralhamento da criptografia. As posições dos bytes são reorganizadas para sua ordem original e os dados do bloco são misturados com as chaves redondas usando operações XOR. Uma função personalizada realiza transformações adicionais nos dados. Finalmente, uma operação XOR é aplicada a cada byte do bloco de dados, concluindo o processo de descriptografia.

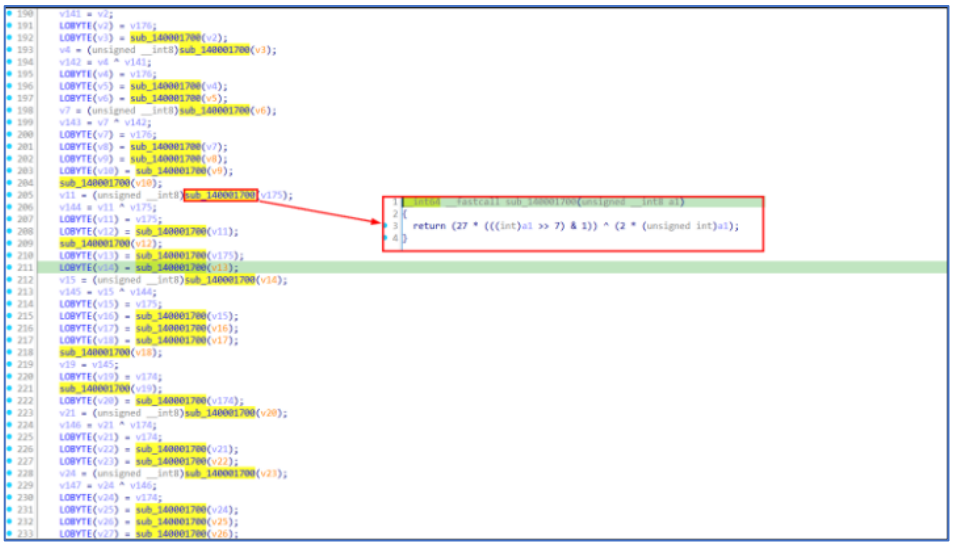


Figura 4 – A função executa transformações personalizadas adicionais nos blocos de dados.

A carga útil do injetor emprega syscalls diretas para acionar funções de API nativas como NtClose, NtResumeThread, entre outras. Essa abordagem é adotada para driblar sistemas de detecção e resposta de endpoint (EDR) e outras ferramentas de segurança. O injetor tem a função de inserir o shellcode descriptografado, que contém a carga final criptografada, no processo notepad.exe. Isso é feito através da injeção de código de fila APC Early Bird, utilizando APIs nativas. O shellcode descriptografado, que contém o payload final criptografado, é semelhante ao shellcode descriptografado inicial (Donut Loader) que examinamos. A descriptografia do payload final depende também da implementação da cifra Chaskey no Donut Loader.

```
.text:0000000140008600    sub     rsp, 58h
.text:0000000140008604    mov     [rsp+58h+var_50], rdx
.text:0000000140008609    mov     [rsp+58h+var_58], rcx
.text:000000014000860D    mov     rax, [rsp+58h+var_58]
.text:0000000140008611    mov     rcx, [rsp+58h+var_50]
.text:0000000140008616    mov     eax, [rax]
.text:0000000140008618    mov     [rsp+58h+var_8], rcx
.text:000000014000861D    mov     [rsp+58h+var_C], eax
.text:0000000140008621    mov     rax, [rsp+58h+var_8]
.text:0000000140008626    mov     [rsp+58h+var_18], rax
.text:000000014000862B    mov     eax, [rsp+58h+var_C]
.text:000000014000862F    mov     r10, [rsp+58h+var_18]
.text:0000000140008634    syscall                 ; Low latency system call
.text:0000000140008636    mov     [rsp+58h+var_44], eax
.text:000000014000863A    mov     [rsp+58h+var_18], r10
.text:000000014000863F    mov     [rsp+58h+var_20], rdx
.text:0000000140008644    mov     [rsp+58h+var_28], r8
.text:0000000140008649    mov     [rsp+58h+var_30], r9
.text:000000014000864E    mov     [rsp+58h+var_38], rcx
.text:0000000140008653    mov     [rsp+58h+var_40], r11
.text:0000000140008658    mov     eax, [rsp+58h+var_44]
.text:000000014000865C    add     rsp, 58h
.text:0000000140008660    retn
```

Figura 5 – Trecho do código usando uma chamada de sistema direta.

Nisto, foi possível extrair a configuração para os payloads finais - XWorm, VenomRAT e AsyncRAT. Eles estão disponíveis aqui, juntamente com indicadores de comprometimento. Em suma, essa campanha de malware envolvendo XWorm, VenomRAT, PureLogs Stealer e AsyncRAT foi desencadeada por um e-mail de phishing. Os agentes de ameaças implantaram arquivos Python criptografados e

em lote ofuscados de um servidor WebDAV para distribuir vários RATs mencionados.

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:

Autenticação multifator

- Além da senha, é necessária outra forma de confirmação, como o envio de uma mensagem de texto para o seu celular.

Senhas fortes

- Uma senha forte terá pelo menos 12 caracteres e incluirá uma mistura de letras maiúsculas e minúsculas, números e símbolos.

Instalar um antivírus

- Proteção contra malware é essencial para a sua proteção.

Monitoramento de ameaças

- Implementação de soluções de monitoramento de ameaças, como o Kaspersky Security Cloud.

Conexão VPN segura

- Use uma conexão VPN segura para criptografar seus dados de navegação privados e protegê-los de possíveis ameaças.

Backup

- Fazer um backup dos dados mais importantes do usuário, como fotos e documentos principais.

Encerrar a sessão de dispositivos

- É importante encerrar a sessão de qualquer programa, site ou aplicativo ao terminar de usá-lo.

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:	0d79c56f9198117a98334ead5d033974
sha1:	bdbaf479a206a83d830298105c80194be00d53ce
sha256:	2dd731fa64db167b90ea6e16896c61f66fa3cde7c6d1b4ed69367c83e68b9f1c
File name:	new.bat

Indicadores de compromisso do artefato	
md5:	1e5fa94c5be0d6f6d57c181c60622b80
sha1:	ee6154fe3c490d7a175cde106cfb38fbf17d7b32
sha256:	d400cf9a804c654667dba326757df90f3d41e7fcea7e11bcf6a7bd3604fef5ea
File name:	startupppppp.bat

Indicadores de compromisso do artefato	
md5:	58e6b6b4b7f6849749b6374ffbd7fa2e
sha1:	51179defee9d29718177eb3fd0d0fdd5016165fc
sha256:	c2278039f0acee06931c3e5f137605c175dab3174c327d9b87842975bf8ca36e
File name:	Client.exe

Indicadores de compromisso do artefato	
md5:	9320932e570d27bd88ee600b3961eecc
sha1:	9bb9817bc4acccca2efbc8763e929dd664831533
sha256:	e2efa139497e3b4aa2eb471f32699bcc9df8ba93d8cc2b4949c2397338d06cfb
File name:	1.py

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **eSentire**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH