BOLETIM DE SEGURANÇA

Nova campanha é realizada para distribuição de malware

heimdall
security research
A DIVISION OF ISH

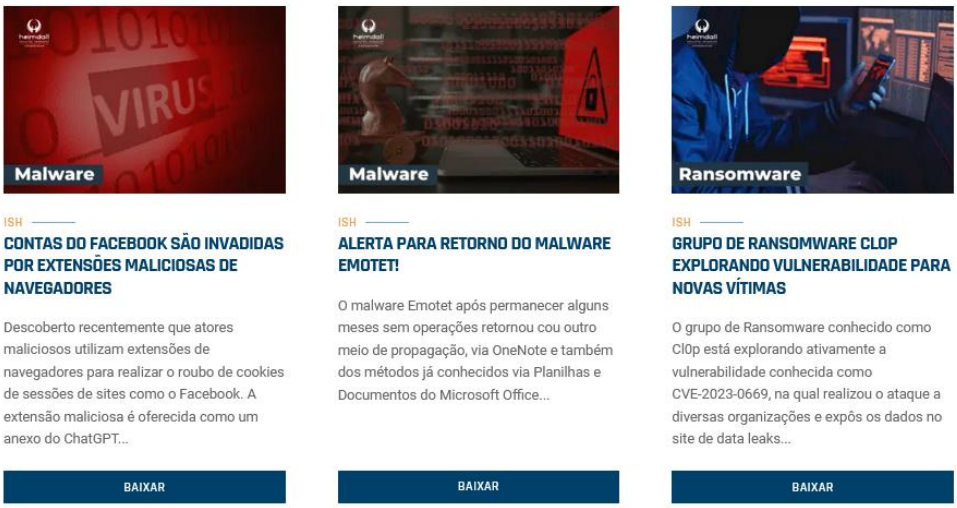
TLP: CLEAR

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

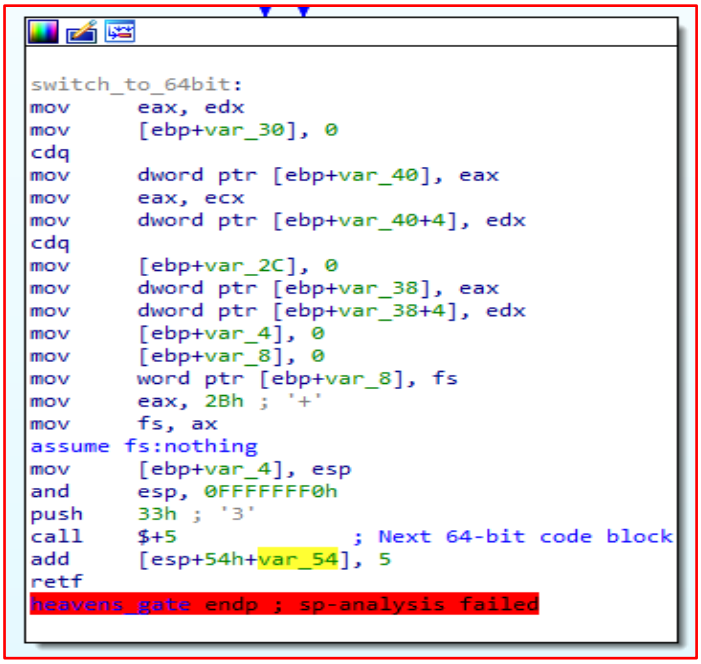
LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A Cisco Talos descobriu uma nova campanha operada por um ator de ameaças que distribui um malware que até então é desconhecido, porém, nomearam de "**TimbreStealer**". Este ator de ameaça foi observado sendo distribuído por meio de uma campanha de spam usando temas relacionados a impostos mexicanos a partir de novembro de 2023. Esse ator de ameaça já usou táticas, técnicas e procedimentos (**TTPs**) semelhantes para distribuir um trojan bancário conhecido como "**Mispadu**". Este malware é um novo *stealer* de informações ofuscado encontrado visando vítimas no México, contendo vários módulos incorporados e é usado para orquestração, descriptografia e proteção do binário do malware.

2 INFORMAÇÕES SOBRE O MALWARE

O malware exibe uma gama de técnicas para contornar a detecção, realizando uma execução furtiva e garantindo sua persistência em sistemas comprometidos, incluindo o aproveitamento de chamadas diretas do sistema para ignorar o monitoramento convencional de API, empregando a técnica *Heaven's Gate* para executar código de 64 bits em um processo de 32 bits e utilizar carregadores personalizados, características essas que indicam um alto nível de sofisticação, sugerindo que os atores de ameaça são altamente qualificados no desenvolvimento desses componentes internamente.



```
switch_to_64bit:
mov     eax, edx
mov     [ebp+var_30], 0
cdq
mov     dword ptr [ebp+var_40], eax
mov     eax, ecx
mov     dword ptr [ebp+var_40+4], edx
cdq
mov     [ebp+var_2C], 0
mov     dword ptr [ebp+var_38], eax
mov     dword ptr [ebp+var_38+4], edx
mov     [ebp+var_4], 0
mov     [ebp+var_8], 0
mov     word ptr [ebp+var_8], fs
mov     eax, 2Bh ; '+'
mov     fs, ax
assume fs:nothing
mov     [ebp+var_4], esp
and     esp, 0FFFFFFF0h
push    33h ; '3'
call    $+5             ; Next 64-bit code block
add     [esp+54h+var_54], 5
retf
heavens_gate endp ; sp-analysis failed
```

Figura 1 – Trecho do código do switch heaven's gate.

Na análise da amostra, foi encontrada na máquina de uma vítima após uma visita a um site comprometido que os usuários clicaram em um link presente em um e-mail de spam.

```
File: catalogo792.exe
Size: 6576640 (6.27mb)
MD5: AA4091290C9C826B614D1A4B9766E5DB
SHA256: 5EFA99B3CB17BEC76FEC2724BCFCC6423D0231BBA9CF9C1AED63005E4C3C2875
Compiled: Fri, Nov 13 2020, 9:45:00 - 32 Bit
```

Figura 2 – Amostra utilizada na análise

Foi identificado vários módulos incorporados na seção ".data" do malware e um processo complexo de descriptografia envolvendo uma DLL de orquestração principal e uma chave de descriptografia global que é usada em todos os diferentes módulos e atualizada em cada estágio.

3 PROCESSO DE DESCRIPTOGRAFIA DO MALWARE

A primeira camada da amostra é compactada, incluindo uma DLL incorporada em sua seção “.data”. Inicialmente o carregador verifica o **Ntdll** em busca de todas as exportações Zw* e construirá uma tabela hash ordenada das funções. Todas as APIs confidenciais a partir deste ponto serão chamadas com chamadas diretas do sistema para o kernel. Para máquinas de 64 bits, isso incluirá uma transição do modo de 32 bits para o modo de 64 bits através do *Heaven's Gate* antes que o **syscall** seja emitido.

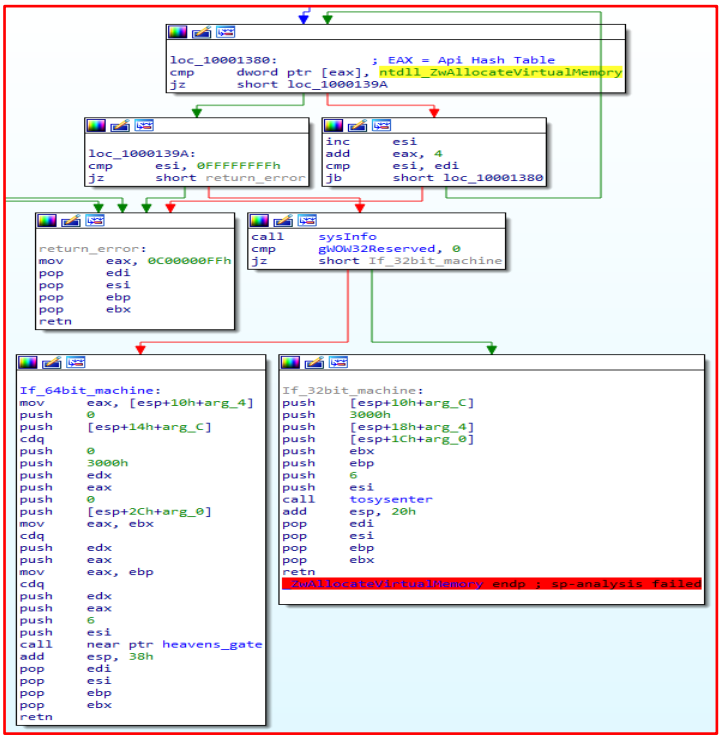


Figura 3 – Métodos diferentes usados pelo TimbreStealer.

Quando estiver concluída, ele irá descriptografar a carga útil do próximo estágio da seção ".data”. A DLL descriptografada tem seu cabeçalho MZ e assinatura PE apagados. O carregador PE personalizado inicia a DLL passando a tabela hash Zw* como argumento para sua função exportada. A descriptografia de todos os submódulos utiliza uma chave global. À medida que a execução do malware avança, esta chave é criptografada continuamente. Se a execução não seguir todas as etapas do caminho esperado, a chave de descriptografia ficará fora de sincronia e todas as descriptografias subsequentes falharão. Todos os estágios deste malware usam o mesmo estilo e técnicas de codificação. Portanto, foi realizada uma avaliação com alta confiança que todas as camadas de ofuscação e carga útil final foram desenvolvidas pelos mesmos autores.

Uma vez extraída a camada inicial, o malware verificará se o sistema é de interesse e se está ou não sendo executado em uma sandbox. Ele também extrairá os vários submódulos incorporados na carga útil. Foi identificado pelo menos três camadas diferentes após a extração da carga principal, com vários módulos em cada camada usados para funções diferentes.

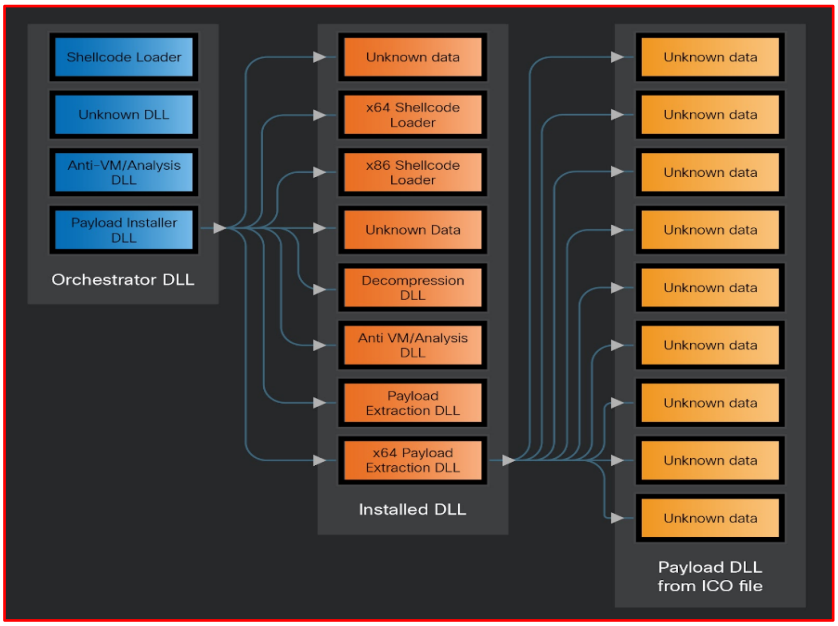


Figura 4 – Diagrama de módulos do TimbreStealer

O malware também fará uma verificação **mutex**, procurará arquivos e chaves de registro que possam ser indicativos de infecção anterior e verificará os navegadores do sistema em busca de sinais de uso natural.

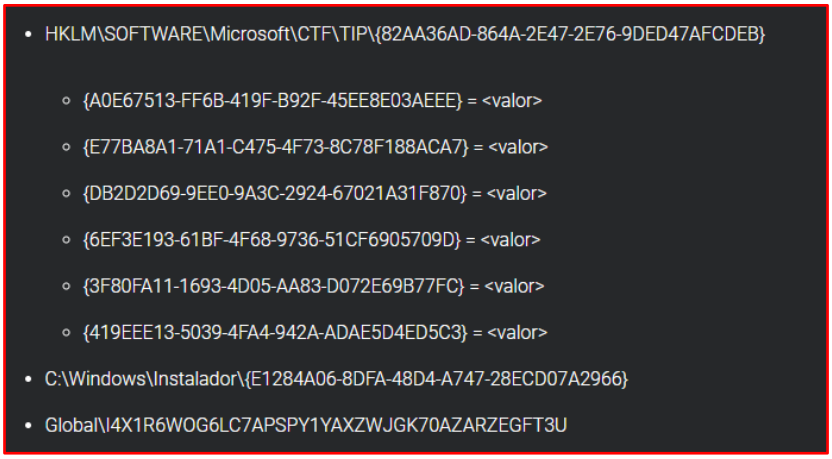


Figura 5 – Chave de registro

A presença dessas chaves junto com outras verificações impedirá a execução dos estágios restantes do malware.

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:

Atualize Regularmente o Software

- Mantenha seu sistema operacional, navegador e todos os softwares, especialmente os de segurança, atualizados.

Antivírus

- Instale e mantenha um software antivírus atualizado.

Firewall

- Use o firewall do seu sistema operacional ou um firewall de terceiros para monitorar e controlar o tráfego de entrada e saída do seu computador.

Pratique a Navegação Segura

- Evite clicar em links desconhecidos ou suspeitos. Não faça downloads de fontes não confiáveis. Verifique sempre os URLs para garantir que você está visitando sites legítimos.

Restrinja Privilégios

- Limite as permissões de acesso dos usuários e aplicativos. Isso reduz a superfície de ataque.

Monitoramento Contínuo

- Implemente sistemas de detecção de intrusão e monitore regularmente a atividade da rede.

Treinamento de Funcionários

- Eduque sua equipe sobre os riscos de malwares e phishing. Eles devem estar cientes das práticas seguras.

Backup Regular

- Faça backups frequentes dos dados importantes e armazene-os em locais seguros.

Segurança de Senhas

- Use senhas fortes e altere-as regularmente. Considere o uso de autenticação de dois fatores.

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 URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps://hamster69[.]senac2021[.]org/~armadillo492370/ hxxps://snapdragon50[.]crimsondragonemperor[.]com/~aster963249/ hxxps://69[.]64[.]35[.] 1/~rota649289/
Domínio	trilivok[.]com, chidoriland[.]com, manderlyx[.]com, bailandolambada[.]com auditório38[.]meinastrohoroskop[.]com, auditório42[.]altavista100[.]com auditoria67[.]mariageorgina[.]com, auditório7[.]miramantolama[.]com auditório82[.]taoshome4sale[.]com, auditório84[.]meinastrohoroskop[.]com
IP	24[.]199[.]98[.]128, 159[.]89[.]50[.]225, 104[.]131[.]169[.]252, 104[.]131[.]67[.]109, 137[.]184[.]108[.]25, 137[.]184[.]115[.]230 138[.]197[.]34[.]162, 142[.]93[.]50[.]216, 143[.]244[.]144[.]166 143[.]244[.]160[.]115, 146[.]190[.]208[.]30, 157[.]230[.]238[.]116 157[.]245[.]8[.]79, 159[.]223[.]96[.]160, 159[.]89[.]226[.]127 159[.]89[.]90[.]109, 162[.]243[.]171[.]207, 167[.]71[.]24[.]13 167[.]71[.]245[.]175, 167[.]71[.]246[.]120, 192[.]241[.]141[.]137 24[.]144[.]96[.]15, 45[.]55[.]65[.]159, 64[.]225[.]29[.]249

Tabela 1 – 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**
- **CiscoTalos**

heimdall
security research
A DIVISION OF ISH