heimdall

security research

A DIVISION OF ISH

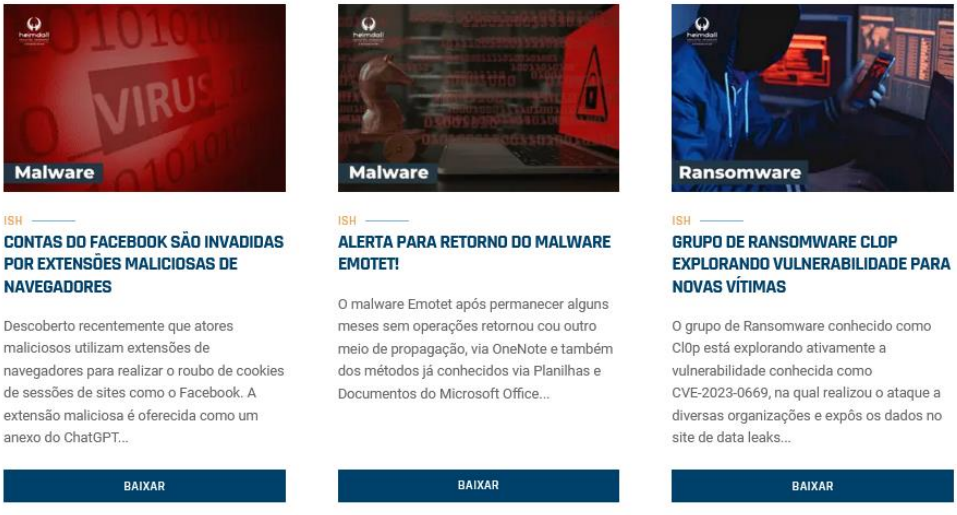
Ransomware Cyclops compartilhando Stealer

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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 RANSOMWARE CYCLOPS

Recentemente é percebido uma grande quantidade de grupos de ransomwares ativos, bem como foi identificada uma nova operação de ransomwares conhecida como **Cyclops Ransomware**.

O grupo de ransomwares Cyclops afirma ter criado um ransomwares para infectar três principais plataformas de sistemas operacionais, como Windows, Linux e macOS, bem como compartilhou um binário utilizado especificamente para roubar dados confidenciais, como um nome de computador e vários processos.

O grupo atua como formato de RaaS (Ransomware-as-a-Service), bem como oferece para o afiliado todo o suporte para o ataque, fato este constatado por meio de compartilhamento e publicações em fóruns da dark web utilizado exclusivamente para promover seu tipo de serviço.

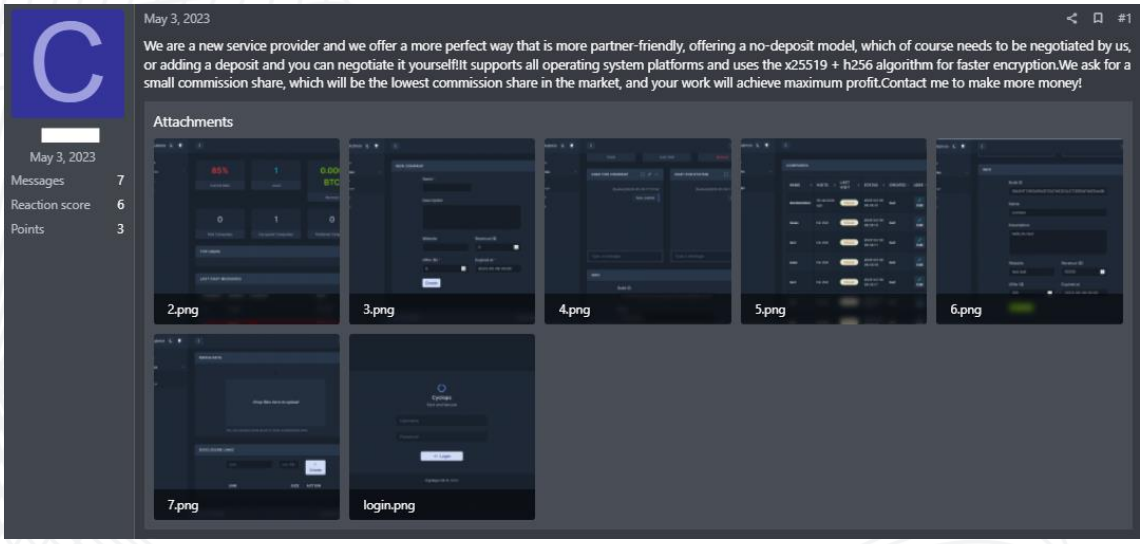


Figura 1 – Postagem do administrador do Cyclops.

O proprietário e desenvolvedor do ransomware forneceu um painel separado para facilitar a distribuição de seu ransomwares para três sistemas operacionais mencionados anteriormente, bem como no painel estão disponíveis binários distintos para o componente do stealer, para as versões Linux e Windows.

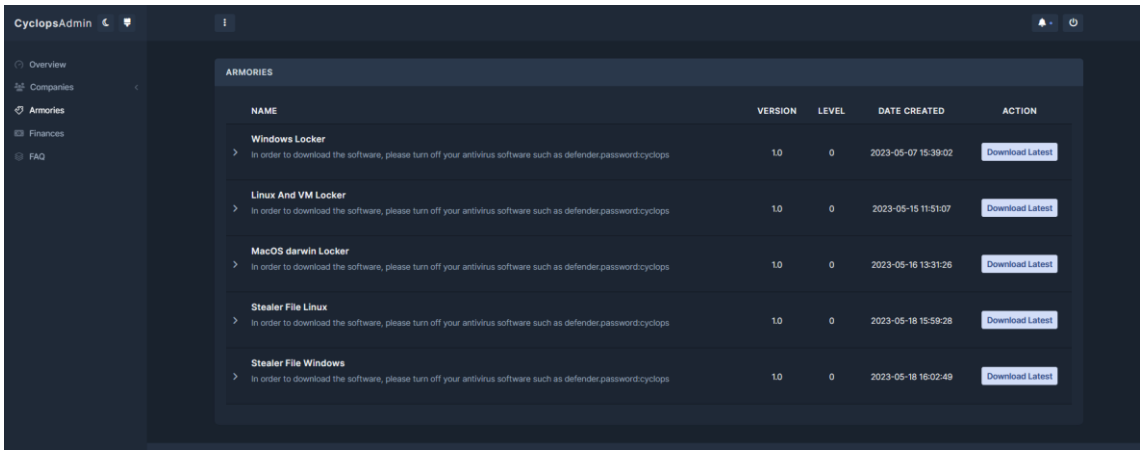


Figura 2 – Painel de administração do Cyclops.

A equipe de pesquisa da Cyclops, afirmou na publicação de seu relatório que o painel financeiro poderá oferecer ao afiliado a capacidade de gerenciar a retirada de valores pagos por determinados ataques, bem como o valor que possui para resgate.

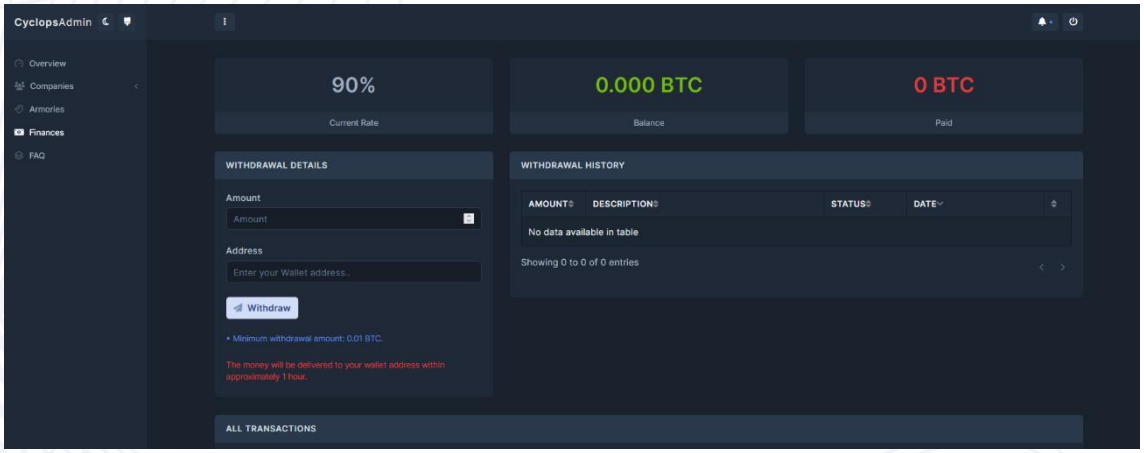


Figura 3 – Painel de pagamento do Cyclops.

Além disso, a equipe forneceu relatório contendo a análise do payload do ransomwares para Windows, Linux e macOS.

2 RANSOMWARE PARA WINDOWS

Após extrair os arquivos baixados do painel, é possível verificar a existência de um "builder.exe" e um arquivo "readme.txt", bem como o ator de ameaça compartilha em particular um ID do builder para criar uma carga de resgate chamada "locker.exe".

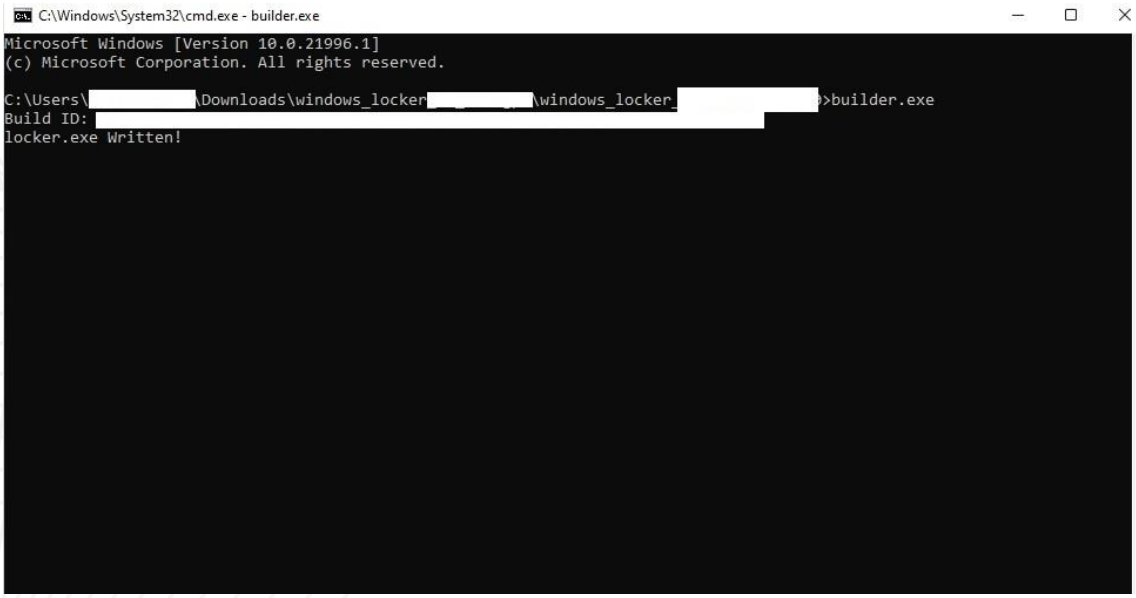


Figura 4 – Gerando payload de resgate.

A carga é projetada especificamente para infectar máquinas locais e em rede, bem como o arquivo de texto que acompanha o builder contém instruções da execução de carga por meio dos argumentos de linha de comando ou sem eles.

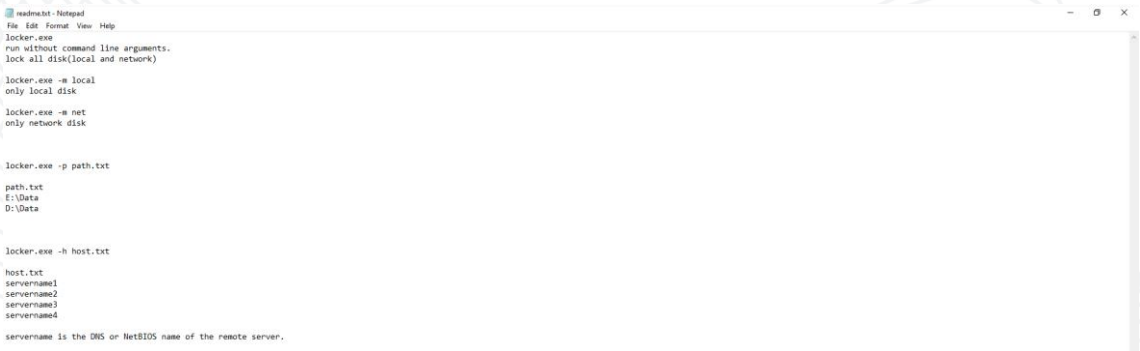


Figura 5 – Linha de comando de execução e carga útil do resgate.

O payload do ransomwares é um binário executável compilado especificamente destinado à arquitetura x64 bits, utilizando o compilador VC++.

Ela realiza a verificação e identificação dos processos que estão em execução nas máquinas das vítimas, encerrando imediatamente qualquer processo que possa impedir a criptografia dos arquivos de destino que pretende manter como reféns.

Abaixo, contém uma tabela de processos que são alvos do Ransomware:

Xfssvccon.exe	Synctime.exe	Ocomm.exe	Excel.exe
Wordpad.exe	Steam.exe	Ocautoupds.exe	Svc.exe
Vision.exe	Sql.exe	Notepad.exe	Dbeng50.exe
Thunderbird.exe	Powerpnt.exe	Mspub.exe	Dbsnmp.exe
Tbirdconfig.exe	Outlook.exe	Msaccess.exe	Agntsvc.exe
Thebat.exe	Onenote.exe	Vmms.exe	TeamViewer.exe
Vmwp.exe	Oracle.exe	Vc.exe	Mydesktopservice.exe
Ig.exe	Ocssd.exe	Firefox.exe	Sqbcoreservice.exe

Tabela 1 – Tabela de processos para finalização.

```
0000000000014FBC1 L"agntsvc.exe"
0000000000014FBA9 L"dbsnmp.exe"
0000000000014FB89 L"dbeng50.exe"
0000000000014FB71 L"encsvc.exe"
0000000000014FB59 L"excel.exe"
0000000000014FB39 L"firefox.exe"
0000000000014FB11 L"isqlplussvc.exe"
0000000000014FAF1 L"msaccess.exe"
0000000000014FAD9 L"mspub.exe"
0000000000014FAB1 L"mydesktopqos.exe"
0000000000014F839 L"mydesktopservice.exe"
0000000000014FA91 L"notepad.exe"
0000000000014FA71 L"ocautoupds.exe"
0000000000014FA59 L"ocomm.exe"
0000000000014FA41 L"ocssd.exe"
0000000000014FA29 L"oracle.exe"
0000000000014FA09 L"onenote.exe"
0000000000014F9E9 L"outlook.exe"
0000000000014F9C9 L"powerpnt.exe"
0000000000014F9A1 L"sqbcoreservice.exe"
0000000000014F989 L"sql.exe"
0000000000014F971 L"steam.exe"
0000000000014F951 L"synctime.exe"
0000000000014F929 L"tbirdconfig.exe"
0000000000014F911 L"thebat.exe"
0000000000014F8E9 L"thunderbird.exe"
0000000000014F8D1 L"visio.exe"
0000000000014F8B1
0000000000014F891 L"wordpad.exe"
0000000000014F871 L"xfssvccon.exe"
```

Figura 6 – Lista de processos de rescisão.

Após obter as letras das unidades de discos, o ransomwares realiza a enumeração das pastas e coloca um arquivo de nota de resgate chamado “How To Restore Your Files.txt” no disco, além disso antes de realizar a criptografia de qualquer arquivo, o payload verifica se a extensão do arquivo corresponde a uma lista predefinida e caso o contrário, o arquivo é criptografado e uma extensão é adicionada “.cyclops”.

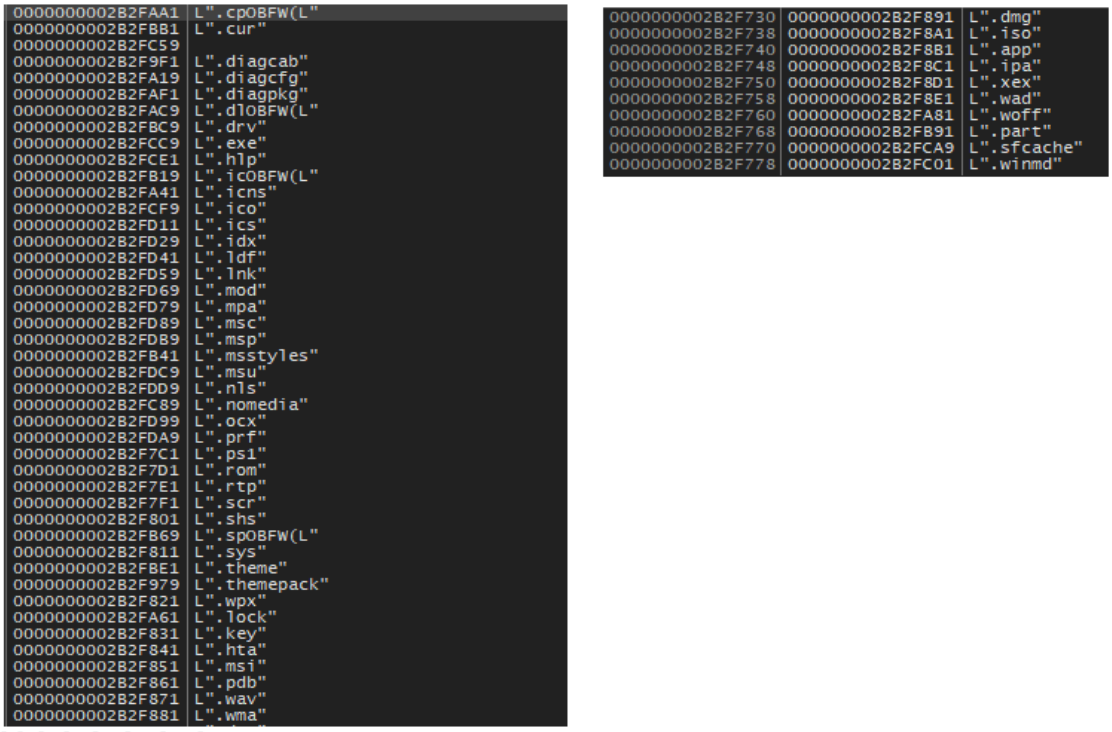


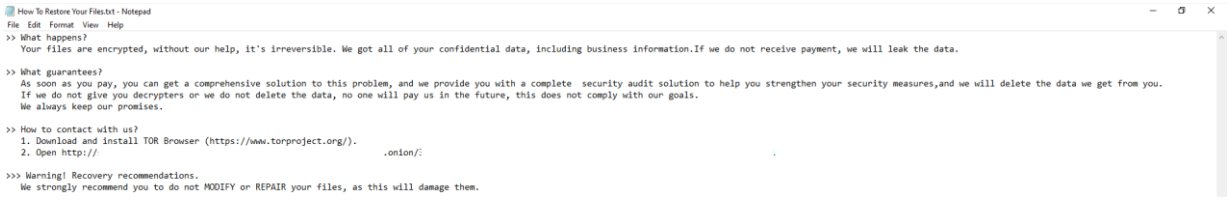
Figura 7 – Arquivos de extensões que são excluídos da criptografia.

O ransomwares para evitar que haja uma fácil recuperação do sistema realiza a exclusão da Shadow Copies por meio do comando:

```
cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadow copy
Where "ID='{<ID>}'" delete
```

Ou seja, ele realiza a consulta a todas as cópias disponíveis, verifica a hora de criação, nome do volume e outros dados, atribuindo na sequência um ID. Este ID é utilizado para exclusão via linha de comando pelo WMIC do Windows.

Após a criptografia, uma nota de resgate é despejada e criada, onde possui orientações para a vítima em realizar o acesso via Rede Tor para iniciar a negociação com os atores maliciosos.


How To Restore Your Files.txt - Notepad

File Edit Format View Help

>> What happens?

Your files are encrypted, without our help, it's irreversible. We got all of your confidential data, including business information.If we do not receive payment, we will leak the data.

>> What guarantees?

As soon as you pay, you can get a comprehensive solution to this problem, and we provide you with a complete security audit solution to help you strengthen your security measures,and we will delete the data we get from you.
If we do not give you decrypters or we do not delete the data, no one will pay us in the future, this does not comply with our goals.
We always keep our promises.

>> How to contact with us?

1. Download and install TOR Browser (https://www.torproject.org/).
2. Open http:// .onion/

>>> Warning! Recovery recommendations.

We strongly recommend you to do not MODIFY or REPAIR your files, as this will damage them.

Figura 8 – Nota de Resgate.

3 RANSOMWARE PARA LINUX

A variante do ransomwares para Linux é compilado na linguagem Golang, sendo baseado em CGO, na qual o código-fonte é escrito em C e construído em Golang, removendo o nome das funções para dificultar a engenharia reversa.

Ao ser executado, o ransomwares fornece opções para criptografar arquivos em um caminho específico, máquinas virtuais ou habilitar a saída detalhada:

```
gambit@Ubuntu:~/Desktop$ ./linux.stub
  -only_vm
        only encrypted virtual machines
  -path string
        path to be encrypted. required
  -verbose
        enable verbose output
```

Figura 9 – Argumentos do ransomware.

Alguns arquivos e pastas de criptografia são excluídos, bem como os arquivos presentes nas pstas /proc e /boot não são criptografados, porém, o ransomwares realiza a criptografia de arquivos com extensões: .vmcx, .vmdk, .vmem, .vmrs, .vmsd, .vmsn, .txt, .csv, .lock, .pdb, .csv e outros.

Após a criptografia, realiza a criação de uma nosta de resgate em cada pasta que criptografa.

```
What happens?
   Your files are encrypted, without our help, it's irreversible. We got all of your confidential data, including business information.If we do not receive payment, we will leak the data.

>> What guarantees?
   As soon as you pay, you can get a comprehensive solution to this problem, and we provide you with a complete  security audit solution to help you strengthen your security measures,and we will delete
 the data we get from you.
   If we do not give you decrypters or we do not delete the data, no one will pay us in the future, this does not comply with our goals.
   We always keep our promises.

>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open http://                                                    .onion/                                                                    )

>>> Warning! Recovery recommendations.
   We strongly recommend you to do not MODIFY or REPAIR your files, as this will damage them.
```

Figura 10 – Nota sobre o Ransomware Linux.

Após criptografar todos os arquivos, ele gera um relatório de estatísticas relacionadas aos arquivos encontrados, arquivos criptografados, arquivos de erros e outros.

4 RANSOMWARE PARA MACOS

O arquivo é compilado por Golang e está a forma de um binário "mach-O".

```
wolverine@wolverines-Mac Documents % file cyclops
cyclops: Mach-O 64-bit executable x86_64
wolverine@wolverines-Mac Documents %
```

Figura 11 – Informações do arquivo mach-O.

Ao executar, o ransomware fornece opções para criptografar arquivos em um caminho específico, máquinas virtuais ou habilitar a saída detalhada.

```
deadpool@Deadpools-Mac Desktop % ./cyclops
  -only_vm
        only encrypted virtual machines
  -path string
        path to be encrypted. required
  -verbose
        enable verbose output
```

Figura 12 – Comando de execução para o Ransomware.

A opção escolhida para a execução de resgate coloca os arquivos criptografados em uma pasta designada, acompanhados a nota de resgate.

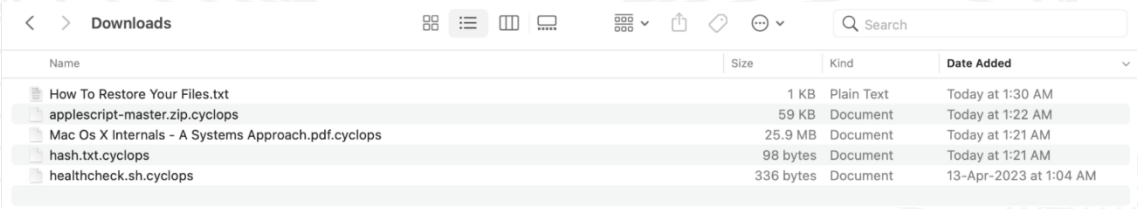


Figura 13 – Finalização do processo de criptografia.

5 STEALER - CYCLOPS

Para o Windows, o Stealer poderá ser baixado diretamente do painel do Cyclops, bem como após o download é obtido o arquivo "stealer.exe" e "config.json".

O binário é um arquivo executável para sistemas x64 que extraí informações dos sistemas das máquinas alvos, como detalhes do SO, nome do computador, Número de Processos e Servidor de Logon.

Em seguida, o stealer faz a leitura do arquivo "config.json" localizado no mesmo diretório de sua execução e contém uma lista de nomes de arquivos anexados com extensões e tamanhos correspondentes.

config.json

```
{
  "filename_list": [
    "finance",
    "passport",
    "statement",
    "insurance",
    "data"
  ],
  "file_extension_list": [
    ".txt",
    ".doc",
    ".pdf",
    "xls",
    "jpeg",
    "jpg",
    "png"
  ],
  "file_maximum_size" : 100,
  "split_size" : 200,
  "name" : "zip file name"
}
```

Figura 14 – Conteúdo do arquivo JSON.

Na sequência, o stealer examina o diretório \system32 em busca da existência de arquivos não identificados (caracterizados por nomes de arquivos excessivamente longos e gerados aleatoriamente).

Após a enumeração dos diretórios, ele verificar a presenta de arquivos de destino e extensões de arquivos específicos e, caso alguma

correspondência for positiva, ele cria um novo arquivo .zip protegido por senha e inclui uma cópia exta do arquivo identificado junto com sua estrutura de arvore de pastas correspondentes, sendo realizada a exfiltração posteriormente.

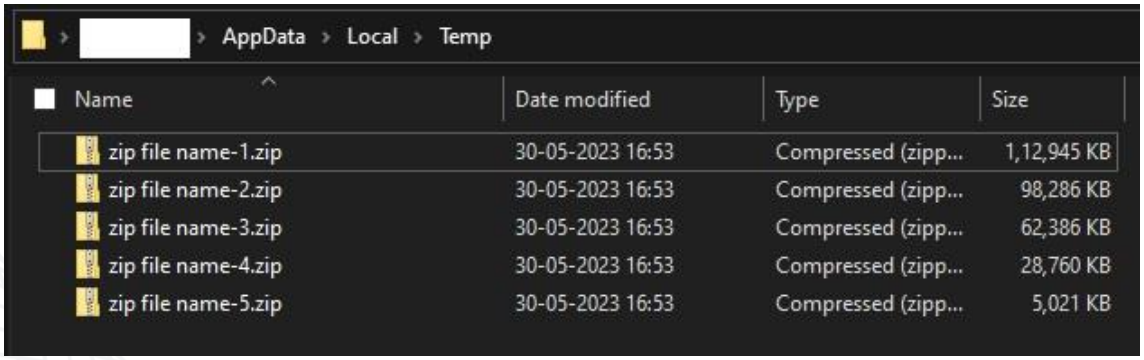


Figura 15 – Arquivos da vítima coletados na pasta temporária.

Para a versão do Linux, a função é semelhante a do Linux, bem como possui uma lista de nomes e tamanhos de arquivos no arquivo .json de configuração.

```
{
  "filename_list": [
    "finance",
    "passport",
    "statement",
    "insurance",
    "data"
  ],
  "file_extension_list": [
    ".txt",
    ".doc",
    ".pdf",
    "xls",
    "jpeg",
    "jpg",
    "png"
  ],
  "file_maximum_size" : 100,
  "split_size" : 200,
  "name" : "zip file name"
}
```

Figura 16 – Conteúdo do arquivo JSON para Linux.

Após a enumeração do arquivo para .zip, o Stealer realiza o carregamento dos arquivos para os domínios:

- **https[:]//api[.]bayfiles[.].com/upload**
- **https[:]//api[.]anonfiles[.].com/upload**

Portanto, podemos perceber a capacidade das operações do Cyclops de oferecer aos afiliados um programa com o Ransomware + Stealer, o qual poderá ser utilizado para prática de ataques cibernéticos.

6 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:

- **Realização de *backups* regulares:** Armazene cópias de segurança de todos os dados importantes em um local seguro e desconectado.
- **Realização de atualizações de *softwares*:** Mantenha todos os *softwares* de ativos atualizados, incluindo sistemas operacionais e aplicativos.
- **Utilização de proteção de rede**, como *firewalls*, antivírus e outras medidas de segurança para proteger sua rede.
- **Realização do trabalho de conscientização** com os colaboradores, ensinando aos mesmos a reconhecer e evitar ameaças, como *phishing* e/ou clicar em *links* maliciosos.
- **Monitoração regular da sua rede e sistemas** para identificar e responder rapidamente a qualquer atividade suspeita.
- **Criação e aplicação de um plano de resposta de incidentes**, sendo que em caso de ataques de *ransomware* poderão ser utilizados e conterão informações como questões relacionadas a *backups* e recuperação de sistema.

7 REGRAS YARA

```
select * from yara where count > 0 and path like
'C:\Users\%\AppData\Local\Temp\%%' and rule = 'rule
Uptycs_Infostealer_Cyclops_windows

{

meta:

     malware_name = "Infostealer"

     description = "Infostealers are malwares that can steal
credentials from browsers, FTP clients, email clients etc from
victim machines."

     author = "Uptycs Inc"

     version = "1"



strings:

     $string_0 = {0F B6 B4 18 EA 01 00 00 40 C0 EE 04 40 0F B6 F6 48
8D 3D ?? ?? ?? 00 0F B6 34 37 0F 1F 00 48 81 FA 0B 02 00 00 0F 83 ??
?? 00 00}

     $string_1 = {44 0F B6 84 18 EA 01 00 00 41 83 E0 0F 41 0F B6 3C
38 48 81 FE 0B 02 00 00 72 95}

     $string_2 = {FF D0 48 81 C4 50 01 00 00 59}

     $string_3 = "GetSystemInfo" ascii wide

     $string_4 = "GetProcessAffinityMask" ascii wide

     $string_5 = "GetEnvironmentStrings" ascii wide

     $string_6 = "GetConsoleMode" ascii wide

     $string_7 = "math.Vr8NUS" ascii wide

     $string_8 = "json:\"status\"" ascii wide



condition:

     all of them

}'
```

```
select * from yara where count > 0 and path like '/tmp' and rule =
'rule                                    Uptycs_Infostealer_Cyclops
{
 meta:
 malware_name                    =                    "Infostealer"
 description = "Infostealers are malwares that can steal credentials
from browsers, FTP clients, email clients etc from victim machines."
 author                =               "Uptycs                Inc"
 version                           =                            "1"


                                  //   All   are   moving   patterns


 strings:
 $Infostealer_Cyclops_0 = {48 81 EC B0 00 00 00 48 89 AC 24 A8 00 00
00 48 8D AC 24 A8 00 00 00 48 BA 2F 70 DC 38 93 99 77 CB 48 89 54 24
6C 48 BA D8 1F 8E E2 21 03 59 E8 48 89 54 24 74 48 BA 21 03 59 E8 CB
81 2D E4 48 89 54 24 78 48 BA E6 FC 0D 2D D9 82 66 1D 48 89 94 24 80
00                               00                                00}
 $Infostealer_Cyclops_1 = {48 BA 46 87 69 74 E3 8F F8 08 48 89 94 24
88 00 00 00 48 BA 73 62 58 40 B0 D3 FC 18 48 89 94 24 90 00 00 00 48
BA 57 FA 61 40 F0 D4 0D 2B 48 89 94 24 98 00 00 00 48 BA 36 0F 3B 23
74   94   3E   B3   48   89   94   24   A0   00   00   00   44   0F   11}
 $Infostealer_Cyclops_2 = {48 BA 64 42 44 53 31 6E 75 39 48 89 54 24
34 48 BA 2D 6F 3E 20 2C 2C 39 72 48 89 54 24 3C 48 BA 2C 2C 39 72 65
00                               37                                46}
 $Infostealer_Cyclops_3 = {48 BA 6D 75 73 71 7A 6F 4C 20 48 89 54 24
1E 48 BA 73 6F 6F 20 72 6F 47 7F 48 89 54 24 26 48 BA 04 01 0F 01 05
08                               05                                03}
 $Infostealer_Cyclops_4 = {49 3B 66 10 0F 86 EC 00 00 00 48 83 EC 50
48 89 6C 24 48 48 8D 6C 24 48 48 BA 73 54 74 75 63 74 75 7F 48 89 54
24 30 48 BA DF 20 6E F2 65 64 01 EB 48 89 54 24 38 48 BA CF 6C FE 49
06 CB F7 3C 48 89 54 24 40 48 BA 08 02 15 17 08 01 0F 01 48}



 condition:
 all                    of                    ($Infostealer_Cyclops*)
}'
```

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Relatório Uptycs referente ao Ransomware Cyclops**

heimdall
security research

A DIVISION OF ISH