# BOLETIM DE SEGURANÇA

## Nova campanha de malware tem como alvo Estados Unidos e União Europeia

heimdall
security research
A DIVISION OF ISH

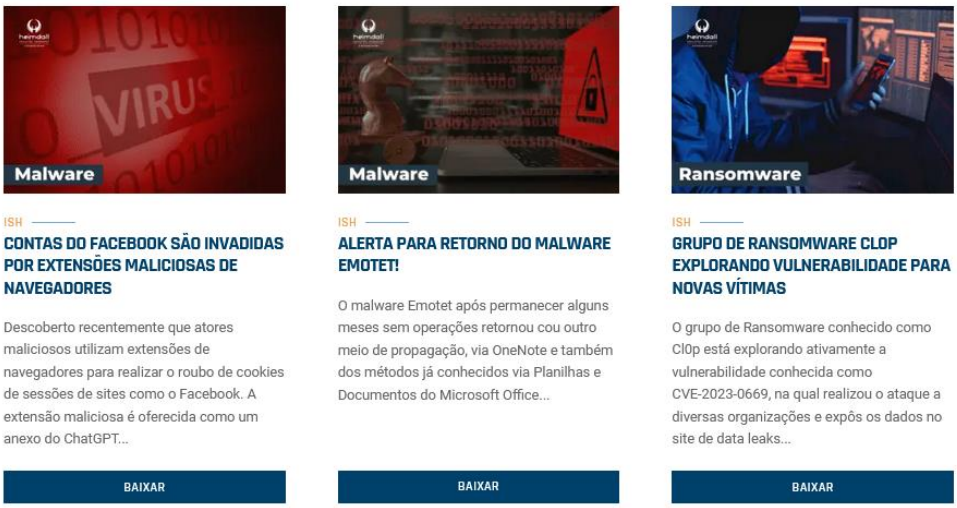
TLP: CLEAR

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

Recentemente a equipe da Unit42 informaram sobre uma ameaça chamada StrelaStealer, que se trata de um malware que tem como alvo as credenciais de e-mail dos usuários, enviando-as para o servidor C2 do invasor. Uma vez que um ataque é bem-sucedido, o agente da ameaça ganha acesso às informações de login do e-mail da vítima, permitindo a realização de ataques subsequentes. Desde sua aparição em 2022, o agente por trás do StrelaStealer tem conduzido várias campanhas de e-mail de grande escala, sem sinais de desaceleração. Detectando-se também uma série de campanhas em grande escala, afetando mais de 100 organizações na UE e nos EUA. Essas campanhas são caracterizadas por e-mails de spam contendo anexos que, quando abertos, liberam a carga útil de DLL do StrelaStealer.

# 2 INFORMAÇÕES SOBRE O MALWARE

O StrelaStealer, é um malware que rouba credenciais de e-mail, foi relatado pela primeira vez por *DCSO_CyTec* em 8 de novembro de 2022. O ator da ameaça responsável pelo StrelaStealer tem conduzido várias campanhas de e-mail de grande escala desde a sua aparição, principalmente na UE e nos EUA. Por exemplo, uma campanha de grande escala foi lançada em novembro de 2023 e notou-se uma nova campanha que começou no final de janeiro de 2024, visando diversos setores na UE e nos EUA. O propósito principal deste malware permaneceu relativamente inalterado, e a DLL de carga útil ainda pode ser identificada pela string strela. No entanto, foi observado que o ator de ameaça fez atualizações no malware para tentar evitar a detecção. Esta nova versão agora é distribuída através de um JScript compactado e utiliza uma técnica de ofuscação atualizada na carga útil da DLL.

O StrelaStealer, desde a sua origem, tem sido associado a várias campanhas de grande magnitude. A equipe de pesquisa do WildFire notou que a campanha mais recente ocorreu em novembro de 2023, com foco em entidades nos EUA e na UE.

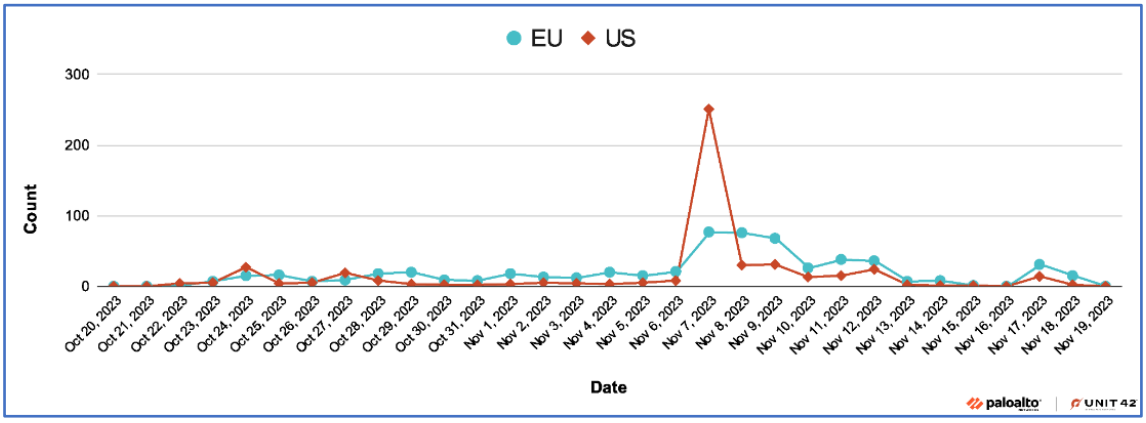



*Figura 1 – Campanha de novembro de 2023.*

Em fevereiro de 2024, os responsáveis pelo StrelaStealer iniciaram mais uma campanha de grande porte, com foco novamente nas mesmas áreas geográficas e o cronograma da recente campanha, que teve seu ápice no dia 29 de janeiro de 2024.

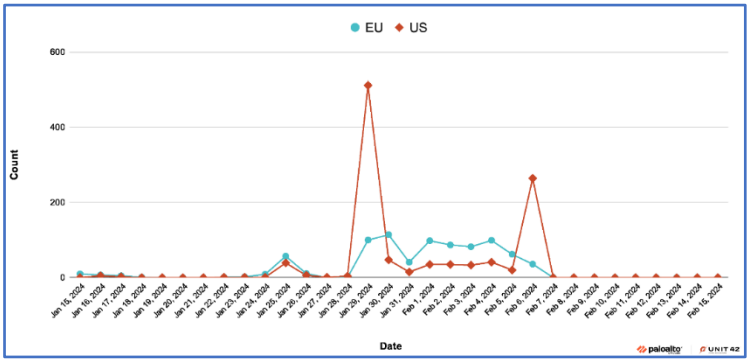



*Figura 2 – Campanha de janeiro de 2024.*

A versão mais recente do malware propaga-se através de e-mails de spear phishing que incluem um anexo .ZIP. Quando o usuário faz o download e abre o anexo, um arquivo JScript é instalado no sistema. Este arquivo JScript descarrega um arquivo criptografado em Base64 e um arquivo batch. O arquivo Base64 é decodificado utilizando o comando "*certutil -f decode*", resultando na geração de um arquivo DLL portátil executável (PE). Dependendo dos privilégios do usuário, o arquivo é armazenado em *%appdata%\temp* ou *c:\temp* no disco rígido local. O arquivo DLL é então executado através da função exportada hello usando **rundll32.exe**.

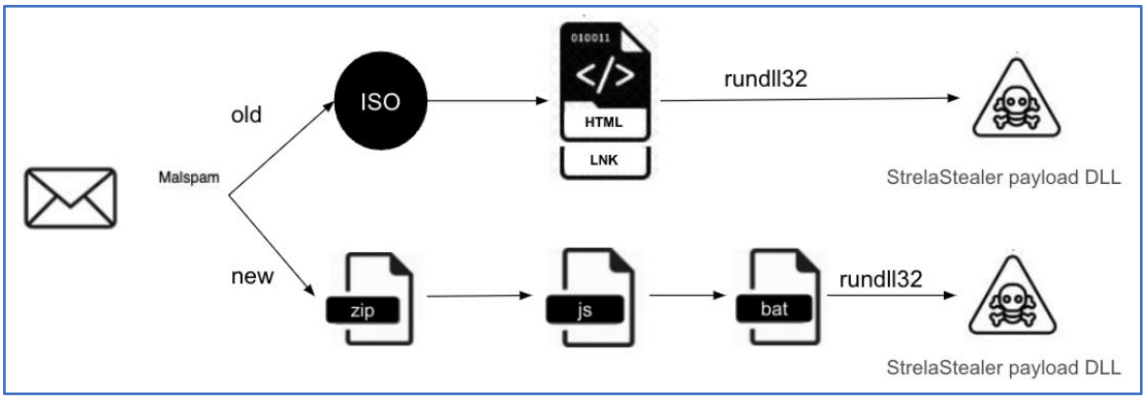



*Figura 3 – Cadeia de infecção.*

Nesta versão do StrelaStealer, observada na campanha de janeiro de 2024, apresenta uma evolução no packer, que agora utiliza uma técnica de ofuscação de fluxo de controle para tornar a análise mais desafiadora. A função inicial, exemplifica a técnica de ofuscação de fluxo de controle com blocos de código extremamente longos, compostos por inúmeras instruções aritméticas. Esta é uma estratégia anti-análise, que pode resultar em pausas durante a execução de amostras em um ambiente de sandbox.

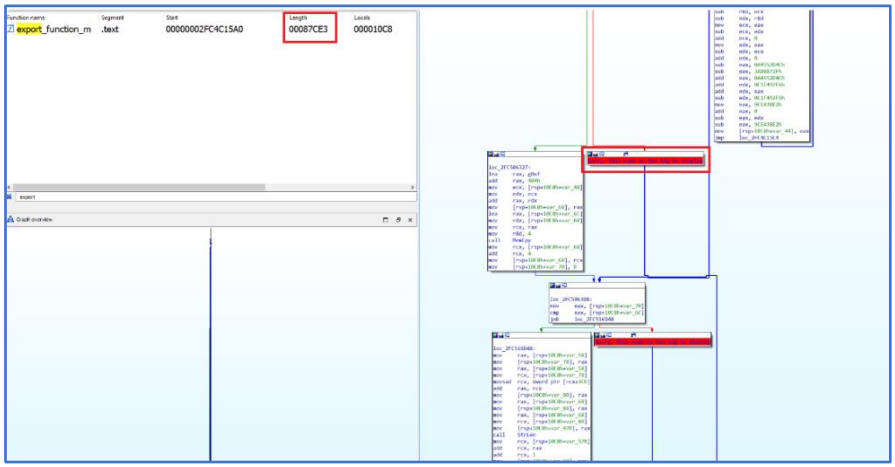


*Figura 4 – Técnica de Ofuscação*

Em ambas as cargas úteis, a original e a nova, são arquivos DLL que possuem uma função de exportação maliciosa acionada para dar início ao ataque. Na figura abaixo apresenta a função de exportação maliciosa da DLL de carga útil em uma comparação lado a lado. É possível observar que a versão mais antiga do StrelaStealer não estava adequadamente ofuscada, uma vez que esses blocos funcionais são claros e de fácil leitura quando desmontados. Por outro lado, a versão mais recente, indica que os operadores da ameaça utilizaram a ofuscação do fluxo de controle para dificultar a análise e a detecção.

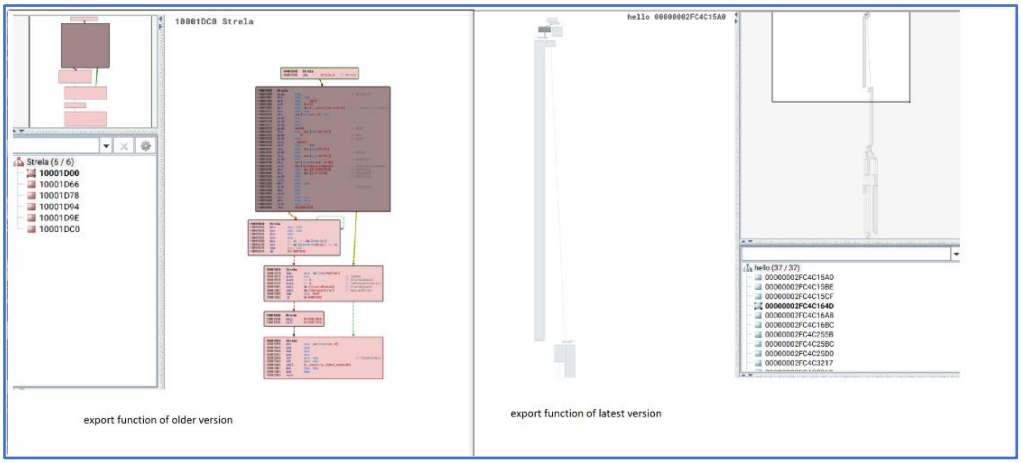



*Figura 5 – Funções de exportação das versões antiga e nova*

A existência de strings como strela, server.php, key4.db e login.json na carga útil descriptografada fornce uma ligação com o StrelaStealer. A principal finalidade é extrair informações de login de e-mail de clientes de e-mail populares e transmiti-las de volta ao servidor C2 especificado na configuração do malware.

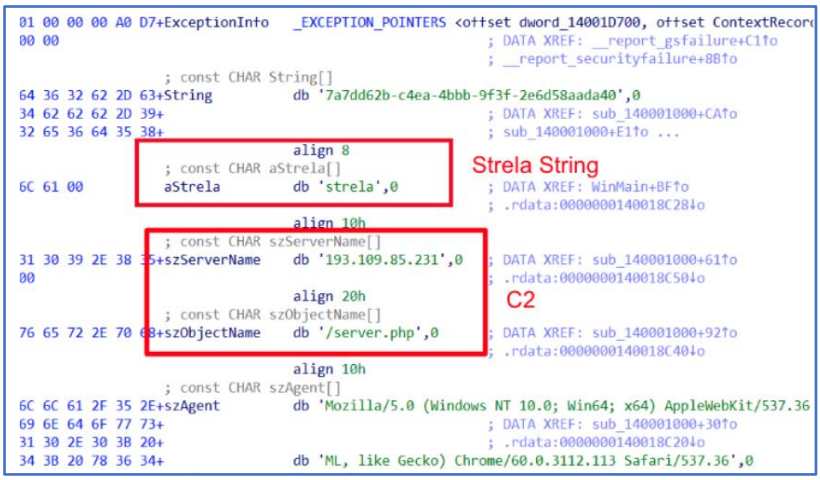



*Figura 6 – String como nome do servidor C2.*

O StrelaStealer, implementou diversas alterações significativas, possivelmente com o intuito de evitar detecção. Um exemplo disso são as strings PDB que estavam presentes em versões anteriores, e que não são mais encontradas nas amostras da campanha mais recente. Isso torna menos evidente que se trata de um binário e pode tornar certas assinaturas estáticas simplistas ineficazes, caso dependam da presença desta string.

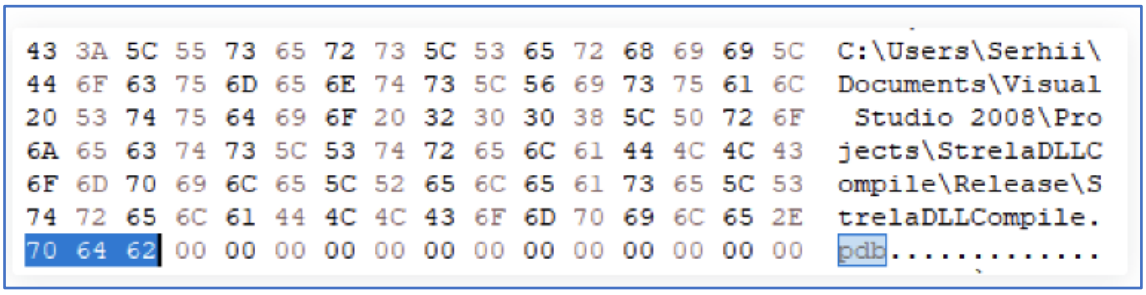



*Figura 7 – String PDB de uma amostra antiga do malware*

A função de exportação foi alterada de StrelaStealer para hello.

| Ordinal | Function RVA | Name Ordinal | Name RVA | Name |
|---|---|---|---|---|
| | | | | |
| (nFunctions) | Dword | Word | Dword | szAnsi |
| 00000001 | 00001DC0 | 0000 | 0000AF87 | Strela |

earlier version of strela

| Ordinal | Function RVA | Name Ordinal | Name RVA | Name |
|---|---|---|---|---|
| | | | | |
| (nFunctions) | Dword | Word | Dword | szAnsi |
| 00000001 | 000015A0 | 0000 | 0002903A | hello |

*Figura 8 – String PDB de uma amostra*

# 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:

**Atualizações de segurança**

- Manter o software atualizado é uma das melhores maneiras de se proteger contra muitos tipos de malware. As atualizações de software muitas vezes incluem patches de segurança que corrigem vulnerabilidades que poderiam ser exploradas por malwares.

**Uso de senhas fortes e únicas**

- Usar uma senha forte e única para cada conta pode ajudar a prevenir o acesso não autorizado. Se uma senha for comprometida, as outras contas permanecerão seguras.

**Implementação de MFA**

- A autenticação multifator adiciona uma camada extra de segurança, exigindo mais de uma forma de verificação para acessar uma conta.

**Conscientização de segurança**

- Estar ciente das táticas comuns de phishing pode ajudar a evitar ser vítima desses ataques. Isso inclui ser cauteloso com e-mails não solicitados, links suspeitos e solicitações de informações pessoais.

# 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:** | 830fc4d3eb1a57d969e2db2007a3f779 |
| **sha1:** | f9d4e1db530e27817d4c61b7a057567f6543df5f |
| **sha256:** | f95c6817086dc49b6485093bfd370c5e3fc3056a5378d519fd1f5619b30f3a2e |
| ***File name:*** | 63b44fa009fcb849c3af83bcf704d1edde6ed8fc6dec8c9f74f21dfb7a46368b.eml |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | 1096f27f41868601b382018c3daf895c |
| **sha1:** | e5ac5b229f0525c407e8d8eeec5abeda5af8ff25 |
| **sha256:** | aea9989e70ffa6b1d9ce50dd3af5b7a6a57b97b7401e9eb2404435a8777be054 |
| ***File name:*** | Rechnung298158492.eml |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | ebb7cf1ce051a233b763f25ff52f5d56 |
| **sha1:** | 1d1d47e11c57cdc599649f07c2f026ee54a6f2f5 |
| **sha256:** | b8e65479f8e790ba627d0deb29a3631d1b043160281fe362f111b0e080558680 |
| ***File name:*** | Rechnung2030879317.eml |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | 9499f14143b34ea7703c73b5f9b37013 |
| **sha1:** | ceff6b19826c9a4e9b9e8cbcc512d5241a27825e |
| **sha256:** | e6991b12e86629b38e178fef129dfda1d454391ffbb236703f8c026d6d55b9a1 |
| ***File name:*** | returnready.dll |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | e2936de211b980bb9bc042c04348978e |
| **sha1:** | f16890fb143741ec118befd22f6903a18f8f1315 |
| **sha256:** | 3189efaf2330177d2817cfb69a8bfa3b846c24ec534aa3e6b66c8a28f3b18d4b |
| ***File name:*** | falkenhahn.zip |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | 301503edfb1ea723b231b416c2a81f0f |
| **sha1:** | dd41fda85637d2593ef4aad407371ec830fe171d |
| **sha256:** | 544887bc3f0dccb610dd7ba35b498a03ea32fca047e133a0639d5bca61cc6f45 |
| ***File name:*** | 18262829011200.js |

Tabela 1 – Indicadores de Compromissos de artefatos

## Indicadores de URL, IPs e Domínios

| Indicadores de URL, IPs e Domínios | |
|---|---|
| **IP** | 193[.]109[.]85[.]231 |

Tabela 2 – 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.

# 5 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **Unit42**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH