heimdall

security research

A DIVISION OF ISH

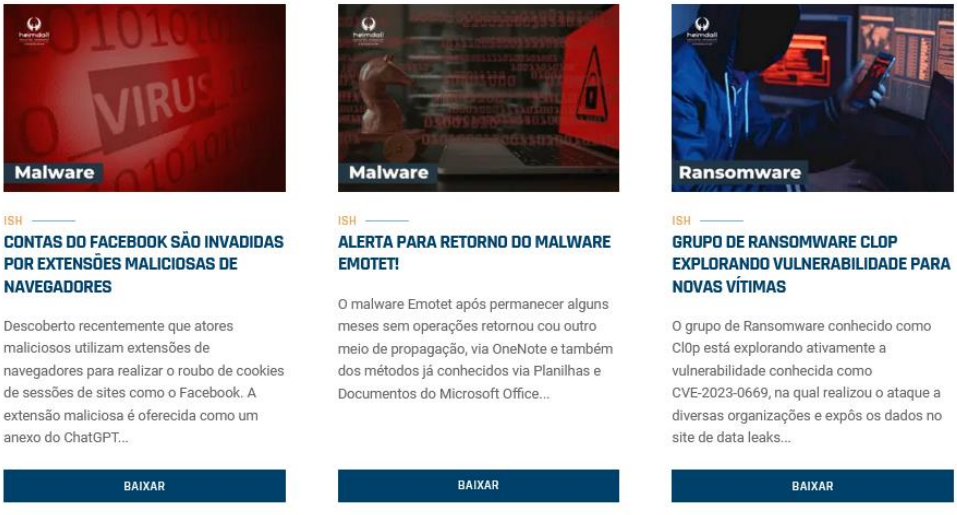
RedDriver realizando o sequestro de navegador

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 Figuras

1 DRIVER MALICIOSO "REDDRIVER"

A empresa de segurança Cisco, publicou uma análise sobre um driver malicioso não documentado chamado "RedDriver", o qual se trata de um sequestrador de navegador baseado em driver que usa a Windows Filtering Platform (WFP) para interceptar o tráfego do navegador. Segundo o relatório, o driver estaria em utilização desde pelo menos 2021.

Houve indícios de que as vítimas pretendidas da ameaça são falantes nativos de chinês, sendo que o driver contém uma lista codificada de nomes de processos de navegador em chinês, que são procurados e sequestrados.

Além disso, o RedDriver continha uma lista de nomes de drivers, muitos dos quais relacionados a vários produtos de software de gerenciamento de cibercafés em chines, bem como houve muitas indicações de que os autores do RedDriver são falantes nativos de chinês.

2 CADEIA DE INFECÇÃO EM VÁRIOS ESTÁGIOS

A cadeia de infecção do RedDriver começa com um único executável empacotado com o Ultimate Packer for eXecutables (UPX), chamado "DnfClientShell32.exe". A seção de recursos do binário contém duas DLLs, uma denominada "DnfClient" e outra "ReflectiveLoader32".

O nome de arquivo "DnfClient" provavelmente é utilizado para se disfarçar como um executável de nome idêntico de um jogo chamado "Dungeon Fight Online", também conhecido como "DNF". (O referido jogo seria muito popular na china).

Após a execução, o DndClientShell32 utiliza o binário ReflectiveLoader32 em sua seção de recursos para injetar o recurso DnfClient em um processo remoto. Após a conclusão do processo de injeção, o DnfClient inicia as comunicações criptografadas com a infraestrutura de comando e controle (C2) para iniciar o download do payload RedDriver.

O DnfClient então abre uma porta de escuta para receber o tráfego redirecionado do navegador do RedDriver.

3 DETALHES DO REDDRIVER

A Cisco afirmou que durante a sua pesquisa contra HooSignTool, observou a implantação de um driver malicioso não documentado que utiliza certificados roubados para forjar carimbos de data e hora de assinatura, ignorando efetivamente as políticas de imposição de assinatura de driver do Windows.

Seu nome se origina da string "RedDriver", a qual está contida no binário eo nome de arquivo em seu caminho (arquivo PDB):

E:\\Project\\PTU\\PTU\\Bin\\x64\\Release\\RedDriver.pdb

```
                    s_r_140009758                          XREF[2,2]:  FUN_140002b54:140002be1(R),
                    s_RedDriver_140009750                              FUN_1400035fc:140003617(R),
                                                                       FUN_140002b54:140002bec(R),
                                                                       FUN_1400035fc:140003623(R)
140009750 52 65 64      ds         "RedDriver"
          44 72 69
          76 65 72...
14000975a cc            ??         CCh
14000975b cc            ??         CCh
14000975c cc            ??         CCh
14000975d cc            ??         CCh
14000975e cc            ??         CCh
14000975f cc            ??         CCh
```

Figura 1 – Nome RedDriver durante a análise no disassembly.

O RedDriver é um componente crítico de uma cadeia de infecção de vários estágios que, por fim, sequestra o tráfego do navegador e redireciona para localhots (127.0.0.1). O navegador de destino é escolhido em uma lista codificada contendo os nomes de processos de muitos navegadores populares em chinês, bem como Google Chrome e Microsoft Edge.

```
local_d8[0] = L"chrome.exe";
browser_list = local_d8;
local_d8[1] = L"360chrome.exe";
local_d8[2] = L"360se.exe";
local_d8[3] = L"qqbrowser.exe";
local_b8 = L"sogouexplorer.exe";
local_b0 = L"firefox.exe";
local_a8 = L"liebao.exe";
local_a0 = L"maxthon.exe";
local_98 = L"xbstarter.exe";
local_90 = L"xbbrowser.exe";
local_88 = L"doreadme.exe";
local_80 = L"fhbrowser.exe";
local_78 = L"dlbrowser.exe";
local_70 = L"ucbrowser.exe";
local_68 = L"tsbrowser.exe";
local_60 = L"fsbrowser.exe";
local_58 = L"qtbrowser.exe";
local_50 = L"tango.exe";
local_48 = L"tango3.exe";
local_40 = L"tangoweb.exe";
local_38 = L"360chromex.exe";
local_30 = L"msedge.exe";
local_28 = L"microsoftedge.exe";
```

Figura 2 – Lista codificada de navegadores.

O RedDriver importa várias funções do “FWPKCLNT.sys”, o qual se trata de um componente de filtragem do Windows.

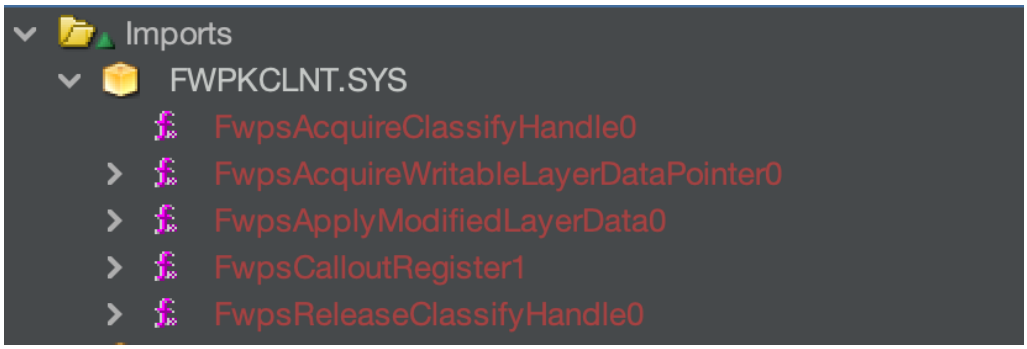


Figura 3 – Funções de importações do RedDriver FWPKCLNT.sys.

Utilizando essas funções importadas, o RedDriver redireciona o tráfego do navegador sequestrado e substitui o endereço IP de destino por 127.0.0.1, redirecionando-o para a porta de escuta que o DnfClient abre. Um certificado também é instalado silenciosamente no sistema de destino sem interação do usuário.

No momento da publicação pela Cisco, não havia significado ou objetivo identificado da ameaça utilizar o redirecionamento de tráfego.

4 EXEMPLOS DE USOS ANTIGOS DO REDDRIVER

Uma versão anterior do RedDriver foi identificada e que estaria ativa desde meados de 2021. Embora haviam claramente diferenças das amostras, foi verificado que a versão anterior do RedDriver continha uma lista de nomes pertencentes a dezenas de drivers, muitos dos quais pertencentes a softwares de origem chinesa.

Abaixo, listamos alguns dos nomes de drivers contidos nas versões do RedDriver anterior:

- atikmdag.sys — Pacote de driver do modo Kernel ATI Radeon
- fastshutdown.sys — iCafe, Sunward Information Technology Co. Ltd
- genfs.sys — Pubwin, Hintsoft (Software de internet de café)
- genvf64.sys — Pubwin, Hintsoft (Software de internet de café)
- genvf.sys — Pubwin, Hintsoft (Software de internet de café)
- Kboot64.sys — Internet Cafe Butler
- nv4_mini.sys — Nvidia, RIVA TNT
- qqprotectx64.sys — Tencent QQ (Mensagens instantâneas)
- devicepnp64.sys — FaceIt (Plataformas de Jogos)
- Tsqbdrv.sys — Driver QQ Browser da empresa de tecnologia Tencent

Além disso, o RedDriver realiza o "contorno" da imposição de assinatura do driver no Windows utilizando o HookSignTool, uma ferramenta de forjamento de carimbo de data/hora de assinatura de código aberto.

Portanto, o RedDriver provavelmente foi desenvolvido por agentes de ameaças altamente qualificados, pois a curva de aprendizado para desenvolver drivers malicioso é íngreme.

Escrever drivers para o Windows requer um conjunto de habilidades específicos e profundos conhecidos do sistema operacional Wndows.

5 IoCs

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 de artefato malicioso/ analisado	
md5:	381c48ba28b806dad43e9d363e639ef6
sha1:	4f74aba2013edf7700dfb54fb7fbcbfabc31c285
sha256:	0201c2999e723d9bbb8b4df8c41030dd25a12ea39671dce2fe4b084b77c4a0d4
File name:	lmPlugin.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	27ff3ec8ae8931c3a500b2a44d3afa45
sha1:	723286e652fd7e63c43d9003cc8d503b1f5a0549
sha256:	fb29ef2e46335719421b747b23096bc6f98df3dc6cd1c0ff9b9174a3827562d5
File name:	FXSCOM.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	e7c1a57c2a8dd073b45974719459c2ee
sha1:	073eae9f93c92643777438e8a3d557ac8fbae8c5
sha256:	f8a1828bc25c8d311e05314ff1da37f9901147a48fbd715e8d1b96c724d71fa0
File name:	lmPluginA.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	adb8e404ae0dcd2d937dbe6f7dbc6d77
sha1:	772b325a53569565866502e4da4225e2a542a85d
sha256:	522b00f45a033c3f7d27a7c0db7dd51dff239fdac56c7a8acf7ff9c542b1e797
File name:	lmPluginC.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	15d9504fec29a115c5bd86c22ce3d096
sha1:	ff1636a5a510992cb3c3c02fde58a47b3e738788
sha256:	ba961c5896b46447cb555dc93f64a78d99da0b2a0a531979545fe7f40279c9c3

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	072ba2309b825ce1dba37d8d924ea8ed
sha1:	89a74d0e9fd03129082c5b868f5ad62558ca34fd
sha256:	24c900024d213549502301c366d18c318887630f04c96bf0a3d6ba74e0df164f
File name:	852448303.sys

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	d209d42e2d604e6018129634fc2a2f38
sha1:	931d1ab97dba24013e97ee6a9247e70b0bf0ef13
sha256:	5a13091832ef2fd837c33acb44b97c37d4f1f412f31f093faf0ce83dcd7c314e

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	1002bd7325b7f739c004400808fb5888
sha1:	e90dc1f706defe530ee8254c9e610128abbad8b1
sha256:	9e59eba805c361820d39273337de070efaf2bf804c6ea88bbafc5f63ce3028b1

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	e026b2666d2ae5583a934b0f9d4b5d03
sha1:	87e4a15228730d10e46e5571d8be576a53858ddf
sha256:	c96320c7b57adf6f73ceaf2ae68f1661c2bfab9d96ffd820e3cfc191fcdf0a9b

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	5aeab9427d85951def146b4c0a44fc63
sha1:	c9e9198d52d94771cb14711a5f6aaf8d82b602a2
sha256:	87565ff08a93a8ff41ea932bf55dec8e0c7e79aba036507ea45df9d81cb36105

URLs de distribuição e endereços IP C2:

poilcy[.]itosha[.]top
newport[.]tofu77[.]top
workpoilcy.zhedwe[.]top
reserve.itosha[.]top
file[.]zhedwe[.]top
red[.]zhedwe[.]top
aireport[.]umpteen[.]top
q5y2qclsk18[.]malaji[.]top
laomao[.]run

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**
- **Cisco – Sequestrador de navegadores baseados em Drivers (RedDriver).**

heimdall
security research

A DIVISION OF ISH