heimdall

security research

A DIVISION OF ISH

Retorno de ataques de malware via dispositivos USB

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 INTRODUÇÃO

Os ataques de malwares via dispositivos USB, também conhecidos como "***USB-based malware attacks***", representam uma ameaça significativa à segurança cibernética e são uma tática popularmente empregada por hackers e cibercriminosos para infiltrar sistemas e redes corporativas, bem como comprometer a privacidade e os dados pessoais de usuários.

Essa técnica de ataque explora a natureza comum e amplamente utilizada dos dispositivos USB, como pen drives, discos rígidos externos e até mesmo cabos de carregamento. Os malwares são inseridos nesses dispositivos de forma oculta ou disfarçada e, quando conectados a um computador ou outro dispositivo, podem ser automaticamente executados sem que o usuário perceba.

Uma das formas mais comuns de ataque via USB é o uso de *autorun* ou arquivos executáveis maliciosos que são automaticamente acionados quando o dispositivo for conectado ao sistema hospedeiro. Outra abordagem é a exploração de vulnerabilidades do sistema operacional relacionadas ao processamento de dados provenientes de dispositivos USB, permitindo a execução do malware.

2 CAMPANHAS MALICIOSAS IDENTIFICADAS

Foi divulgado recentemente que houve um aumento nos ataques cibernéticos usando unidades **USB infectadas** como vetor de acesso inicial em invasões, conforme novas descobertas de pesquisadores de segurança cibernética foram observadas duas campanhas maliciosas em ação, ***SOGU*** e ***SNOWYDRIVE***, visando organizações dos setores público e privado em todo o mundo. ***SOGU malware*** é o ataque de espionagem cibernética baseado em unidades USB mais comum e uma das campanhas de espionagem cibernética mais agressivas voltadas para organizações dos setores público e privado em todo o setor. Ele usa unidades flash USB para carregar o malware SOGU para roubar informações confidenciais de um host infectado.

SNOWYDRIVE, esta campanha usa unidades flash USB para distribuir o malware SNOWYDRIVE. Depois que o SNOWYDRIVE é carregado, ele cria um backdoor no sistema host, dando aos invasores a capacidade de emitir comandos de sistema remotamente. Ele também se espalha para outras unidades flash USB e se propaga por toda a rede.

3 DETALHES DA CAMPANHA SOGU

Pesquisadores informaram que Sogu é atualmente a campanha de ciberespionagem assistida por USB mais agressiva, visando muitos setores em todo o mundo e tentando roubar dados de computadores infectados.

As vítimas do malware Sogu por enquanto estão localizadas nos Estados Unidos, França, Reino Unido, Itália, Polônia, Áustria, Austrália, Suíça, China, Japão, Ucrânia, Cingapura, Indonésia e Filipinas.

A maioria das vítimas pertence aos setores farmacêutico, TI, energia, comunicações, saúde e logística, mas há vítimas em todos os setores.

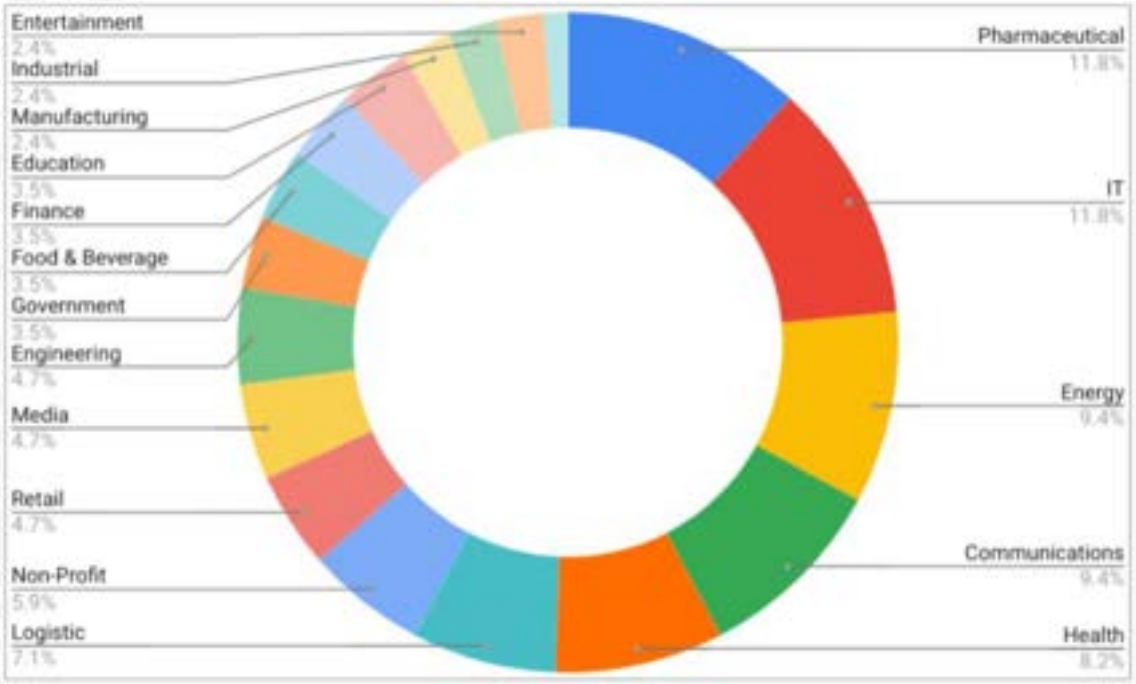

Figura 1 – Setores alvos da campanha SOGU.

4 VETOR DE INFECÇÃO DA CAMPANHA SOGU

Uma unidade flash USB infectada é o vetor de infecção inicial, a unidade flash contém vários softwares mal-intencionados projetados para carregar uma carga maliciosa na memória por meio do sequestro de DLL.

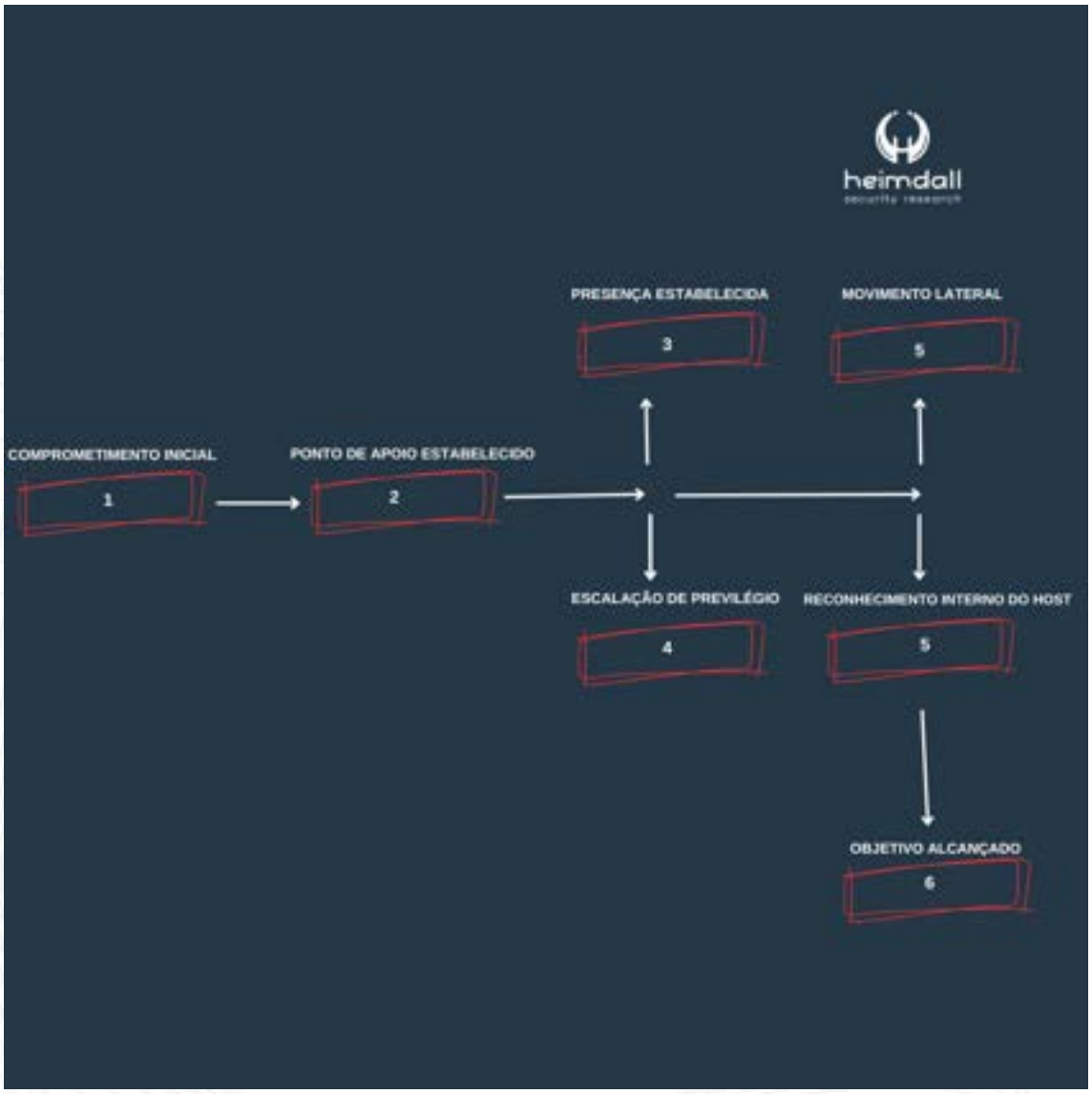

Figura 2 – Cadeia de infecção da campanha Sogu.

1 - Infecção inicial através da unidade flash USB

2 - A vítima é induzida a executar um arquivo legítimo que resulta no carregamento de um arquivo DLL malicioso, que por sua vez injeta e executa um arquivo shellcode na memória

3 - O malware se copia para o host e cria uma chave de execução do registro, usando o agendador de tarefas do Windows para executar o malware de forma programada

4 - O malware se propagará para novas unidades removíveis USB conectadas ao host

5 - O malware realiza o reconhecimento do host e pesquisa documentos, PDFs e arquivos de texto para preparação e exfiltração de dados

6 - É realizada a exfiltração dos dados dos hosts infectados

Quando o executável legítimo é executado, ele carrega de lado um arquivo DLL malicioso, rastreado como **KORPLUG**. O malware **KORPLUG** carregará um shellcode descriptografado, geralmente observado na forma de um arquivo .dat, e o executará na memória. O shellcode é comumente observado como um backdoor que a Mandiant rastreou como **SOGU**, um backdoor escrito em C.

5 VETOR DE INFECÇÃO DA CAMPANHA SNOWYDRIVE

Uma unidade flash USB infectada é o vetor de infecção inicial. A vítima é induzida a clicar em um arquivo malicioso disfarçado de executável legítimo. Ao executar o arquivo malicioso, ele desencadeia uma cadeia de execuções maliciosas, cada uma projetada para realizar sua tarefa específica ao longo do ciclo de vida do invasor.

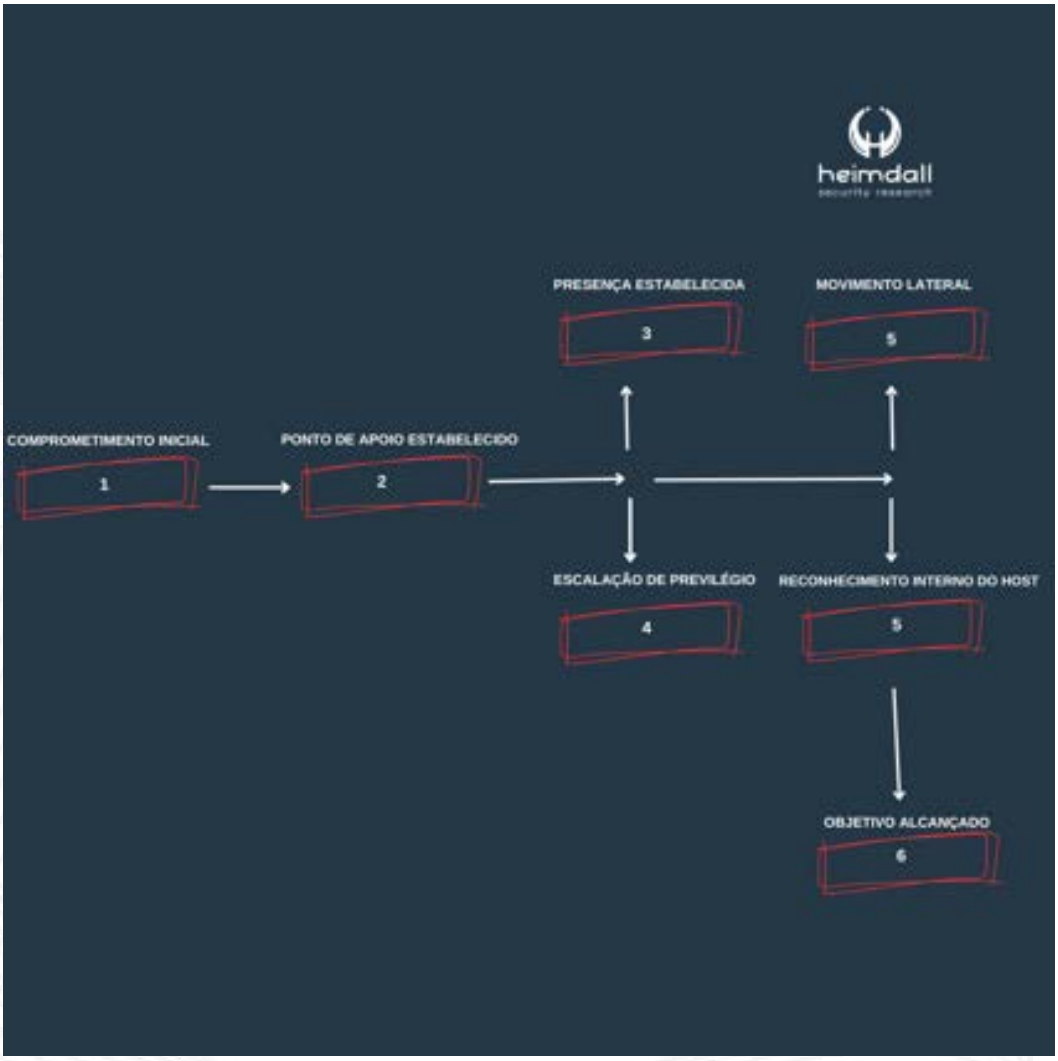

Figura 2 – Cadeia de infecção da campanha SNOWYDRIVE.

1 - Infecção inicial através da unidade flash USB

2 - A vítima é atraída para executar um malware encontrado na pasta raiz do drive USB. Este malware irá extrair e executar vários outros softwares maliciosos criptografados encontrados na pasta da unidade flash USB em "\Kaspersky\USBDriverz3.0"

Cada software malicioso é projetado para executar uma tarefa específica do ciclo de vida do invasor, como manter a propagação de malware de presença e estabelecimento de backdoor

3 - O malware se copia para o host e cria uma chave de execução do registro

4 - O malware se propagará para novas unidades removíveis USB conectadas ao host

5 - Através do backdoor estabelecido, o invasor pode realizar tarefas de manipulação de arquivos remotamente

6 - É realizado os estágios posteriores, como exfiltração de dados

6 Conclusão

As consequências de um ataque bem-sucedido usando malwares via USB podem ser graves. Os malwares podem roubar informações confidenciais, como senhas, dados bancários e informações pessoais, ou serem projetados para espalhar-se pela rede interna, infectando outros sistemas e dispositivos. Além disso, podem ser utilizados para implantar ransomwares, bloqueando o acesso aos dados do usuário ou da organização até que um resgate seja pago aos criminosos.

Os ataques de malwares via dispositivos USB são uma ameaça persistente e de fácil disseminação, por isso é essencial que os usuários e as organizações estejam vigilantes e tomem medidas proativas para mitigar os riscos associados a essa forma de ataque. A prevenção e a educação são fundamentais para proteger-se contra essa ameaça em constante evolução.

7 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:

- **Conscientização dos usuários**, treinamento e conscientização sobre segurança cibernética são essenciais. Os usuários devem ser instruídos a não conectar dispositivos USB desconhecidos ou suspeitos em seus computadores e a relatar quaisquer incidentes incomuns à equipe de segurança.
- **Conscientização de colaboradores para com e-mails**, ligações ou qualquer outro método de ataques utilizados pelos atacantes.
- **Não realizar o *download* de artefatos contidos em e-mails suspeitos**, como não clicar em *links* de e-mails que apresentarem ter comportamento malicioso.
- **Adoção de medidas de antivírus**, visando verificar e varrer constantemente toda a infraestrutura e ativos utilizados.
- **Desabilitar a execução automática**, desativar a execução automática de dispositivos USB no sistema operacional pode reduzir significativamente o risco de infecção acidental.
- **Políticas de segurança**, implementar políticas de segurança que limitem o uso de dispositivos USB não autorizados ou desconhecidos em ambientes corporativos.

8 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:	ebb7749069a9b5bcda98d89f04d889db
sha1:	c4ac1c5f4d3faa00ab846dceca67df3a51ad158b
sha256:	432a07eb49473fa8c71d50ccaf2bc980b692d458ec4aaedd52d739cb377f3428
File name:	AvastAuth.dat

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	ab5d85079e299ac49fcc9f12516243de
sha1:	9c2d957404e4fa80c8275fb75a71aded608e8a86
sha256:	d813af67dd802a33109de79a613dc1fd177a7ef86137eb931aa3173d3aae5f96
File name:	NASHWA.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	fc55344597d540453326d94eb673e750
sha1:	ee4b5f18b4fad719764ac405a56c6dba90d0b554
sha256:	3a53bd36b24bc40bdce289d26f1b6965c0a5e71f26b05d19c7aa73d9e3cfa6ff
File name:	SmadHook32c.dll

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	b061d981d224454ffd8d692cf7ee92b7
sha1:	2c93c30207786343f3de6ca540d14fefc237a9b4
sha256:	14f9278f3515fae71ccb8073cfaf73bdcc00eab3888d8cee6fb43a4f51c9e699
File name:	hex.dll

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	028201d92b2b41cb6164430232192062
sha1:	0ab7ff2dd8a2f241c1e7413087ccf63c11beb8cd
sha256:	9e5b74806a348e723a690d3f4dcd5f2ba6f6c1a03afdcc961c3cacdaf1205a11
File name:	smadavupdate.dat

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	38baabddffb1d732a05ffa2c70331e21
sha1:	39e5b6b33b564e302e8f4a43e96b252bf1b8ccd6
sha256:	f0f2ff31b869fdb9f2ef67bfb0cc7840f098a37b6b21e6eb4983134448e3d208
File name:	adobeupdate.dat

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	722b15bbc15845e4e265a1519c800c34
sha1:	56bac516227d9fddc08ca586dba5c9085d203f99
sha256:	e8f55d0f327fd1d5f26428b890ef7fe878e135d494acda24ef01c695a2e9136d
File name:	wsc.dll

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	848feec343111bc11cceb828b5004aad
sha1:	e489beb7d7543d31d1e88529e043b3d290224a94
sha256:	89558b4190abcdc1a2353eda591901df3bb8856758f366291df85c5345837448
File name:	coreclr.dll

URLs de distribuição e endereços IP C2:

www.beautyporntube[.]com
103.56.53[.]46
45.251.240[.]55
45.142.166[.]112
43.254.217[.]165

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**
- mandiant
- thehackernews
- bleepingcomputer

heimdall
security research

A DIVISION OF ISH