heimdall

security research

A DIVISION OF ISH

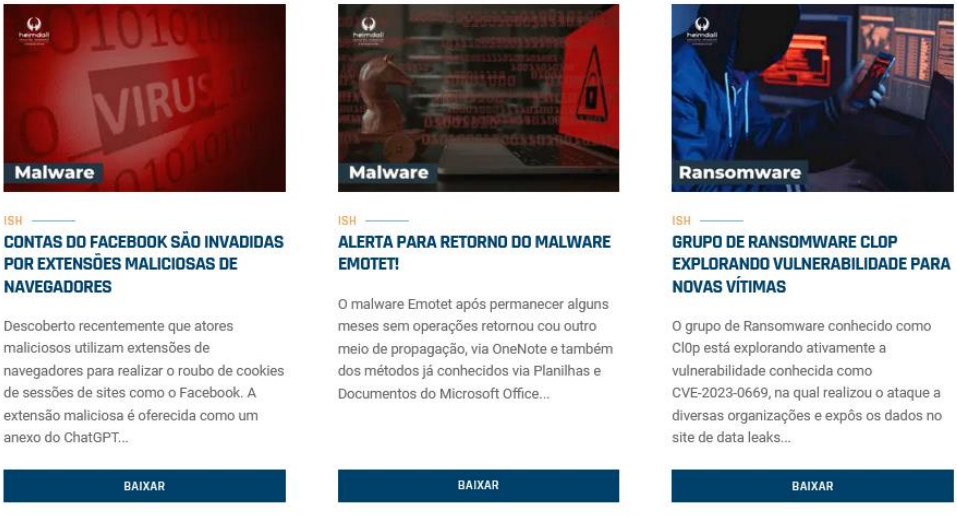
TTPs comuns contra Organizações Industriais

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

1 Introdução 7
2 Implantes de primeira fase 8
3 Implantes de Segunda Fase 12
4 Implantes de Terceira Fase 17
5 TTPs – MITRE ATT&CK 19
6 IoCs 21
7 Referências 23

Lista de Tabelas

Tabela 1 – Tabela MITRE ATT&CK. 20
Tabela 2 – Indicador de Compromisso – MD5. 21
Tabela 3 – Indicadores de Compromissos – Domínio e IPs C2. 22

Lista de Figuras

Figura 1 – Código FouteenHi x64 para analisar uma resposta C2. 8
Figura 2 – Serviço criado pelo implante MeatBall. 10
Figura 3 – Log contendo o resultado da execução do comando usado cmd. 11
Figura 4 – Diagrama simplificado da interação do implante com uma mídia removível. 13
Figura 5 – Esquema simplificado de infectar um computador em um segmento de rede isolado através de uma mídia removível infectada. 14
Figura 6 – Esquema simplificado para coletar dados roubados de um computador em um segmento de rede isolado por meio de uma mídia removível infectada. 15

1 INTRODUÇÃO

A equipe de inteligência da ISH, Heimdall através das informações publicadas pela Kaspersky sobre os TTPs comuns de ataques contra organizações industriais.

Vale salientar que o relatório foi produzido com base no ano de 2022, na qual segundo a Kaspersky foi elaborado com base em investigações de diversos ataques contra organizações industriais na Europa Oriental.

Nas campanhas identificadas, fora identificada uso de variantes FourteenHi, TTPs específicos e o escopo do ataque, tendo apresentado que o ator de ameaça chamado APT31, também conhecido como "Judgment Panda e Zircônio", está por trás das atividades descritas no estudo.

Para realizar a exfiltração de dados e entregar o malware de próximo estágio, o ator de ameaça abusa um serviço de armazenamento de dados baseados em nuvem, por exemplo, DropBox ou Yandex Disk, bem como um serviço utilizado para compartilhamento temporário de arquivos. Os agentes também utilizaram um C2 implantado em servidores privados virtuais regulares (VPS) e, implantam uma pilha de implantes que coletam dados de redes sem fio por meio de unidades removíveis infectadas.

Para a maioria dos implantes, os agentes de ameaças usam implementações semelhantes de sequestro de DLL (malware Shadowpad) e técnicas de injeção de memória, juntamente com o uso de criptografia RC4 para ocultar a carga útil e evitar a detecção.

De acordo com a Kaspersky, foi identificado três categorias de pilhas, bem como identificando 15 implantes e suas variantes implantadas pelo agente de ameaça, como:

- Implantes de primeiro estágio para acesso remoto persistente;
- Implantes de segundo estágio para coleta de dados e arquivos;
- Implantes de terceiro estágio e ferramentas usadas para enviar dados para C2;

2 IMPLANTES DE PRIMEIRA FASE

Variantes de FourteenHi

FourteenHi é uma família de malware descoberta em 2021 em uma campanha batizada de ExCone, ativa desde meados de março de 2021 e direcionada a entidades governamentais. Em 2022, foi descoberto novas variantes utilizadas em ataques à infraestrutura de organizações industriais.

Vários exemplos de FourteenHi (ambos x64 e x86) são significativamente diferentes uns dos outros em termos de estrutura de códigos, implementação de seus loaders e tipos de C2. Os principais recursos distintivos, como protocolo de comunicação C2 e a lista de comandos, são praticamente os mesmos, sendo esta a diferença mais significativa entre as variantes x64 e x86.

As amostras para x64 têm recursos de persistência e um protocolo de comunicação C2 de 2 etapas, aceitando os comandos:

- Realizar um upload de arquivos arbitrários
- Baixar arquivos arbitrários
- Executar comandos arbitrários
- Definir um atraso de comunicação
- Iniciar um shell reverso
- Encerrar o processo e remover a persistência

Para proteger a comunicação com C2, eles utilizam a API da biblioteca OpenSSL vinculado estaticamente. Além disso, eles utilizam RC4 para criptografar/descriptografar os dados que enviam/recebem do C2.

```
if ( command == 0x253AB )
{
  if ( v7 == 4 )
  {
    handle = kernel32_CreateRemoteThreat_902(0i64, 0i64, C2_command_ReadWrite_file, *buffer);
    kernelbase_CloseHandle_425(handle);
  }
}
else if ( command == 0xB8C2D )
{
  exception = check_alloc_exception(24i64);
  qword_1BAAAC251D8 = exception;
  *exception = 0i64;
  exception[1] = -1i64;
  exception[2] = -1i64;
  CreateRemoteThreat_C2_command_CMD_exec(exception, cmd_command, buffer, SHIDWORD(command));
}
```

Figura 1 – Código FouteenHi x64 para analisar uma resposta C2.

As amostras para x86 não tem recursos de persistência, não estando vinculadas ao OpenSSL, mas ainda usam criptografia RC4. O malware utiliza um protocolo de comunicação de 1 etapa, mas a lista de comandos é quase a mesma, exceto pela remoção de mecanismo de persistência.

A rotina de loader é praticamente o mesmo para todas as variantes e consiste em três componentes principais usados pelo agente de ameaça para implantar na máquina da vítima:

1. Um aplicativo legítimo que é vulnerável ao sequestro de DLL.
2. DLL maliciosa é carregada por sequestro de DLL e é usada para ler e descriptografar a carga útil FourteenHi de um arquivo de dados binários e injetá-la em algum processo do sistema, como "svchost.exe ou msiexec.exe".
3. Um arquivo de dados binários contendo o código binário FourteenHi criprotrafado com RC4.

Vale salientar que todas as ariantes conhecidas do FourteenHi têm dados de configurações incorporados em seu código e criptografados com RC4. A configuração define o ID a campanha, o endereço C2 e a porta. A configuração do FourteenHi x64 também define o nome a descrição do serviço do Windows que ele cria para persistência quando executado sem parâmetros.

MeatBall BACKDOOR

O backdoor MeatBall é um novo implante que a Kaspersky descobriu no processo de pesquisa de ataques. O malware possui vastos recursos de acesso remoto, incluindo listas de processos em execução, dispositivos e disco conectados, execução de operações de arquivos, captura de tela, uso de shell remoto e atualizações automática. O implante existe para variantes x86 e x64.

O malware também utiliza um esquema de carregamento baseado na técnica de sequesrtro de DLL, mas ao contrário de outros malwares, o payload é armazenado no próprio loader de DLL malicioso, não em um arquivo separado.

Quando o aplicativo host é vulnerável é executado sem parâmetros, o implante chama lsNTAdmin e, se tiver privilégios suficientes, cria um

serviço chamado "esetcss" e, caso contrário, ele simplesmente se adiciona à chave de registro "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\esetcss" para ser executado automaticamente na inicialização do sistema operacional.

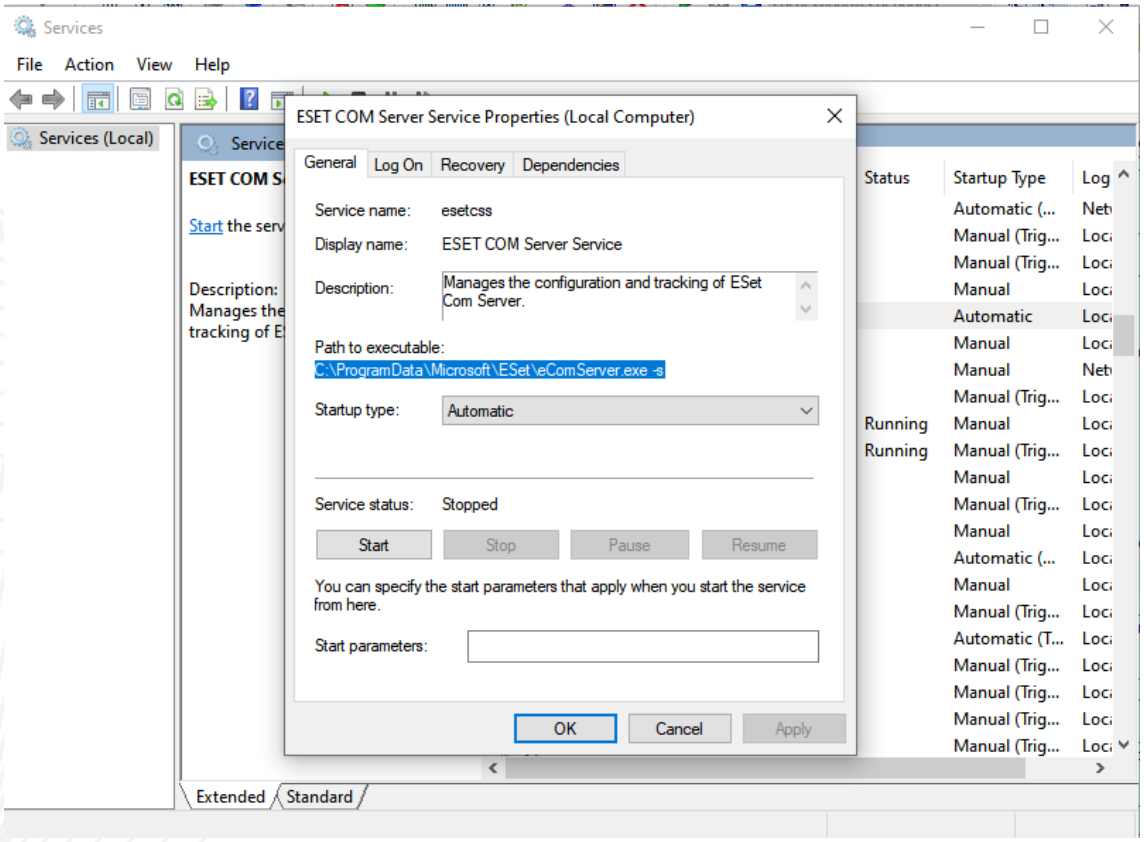


Figura 2 – Serviço criado pelo implante MeatBall.

Em ambos os casos, os implantes são configurados para serem executados com o parâmetro "-S", que diz ao malware para ler o payload de seu próprio arquivo de módulo (dll), descriptografar a carga usando uma chave XOR de um byte, iniciar "svchost.exe" e injetar a carga útil descriptografada nele. Em seguida, ele inicia o loop de comunicação C2 principal chamado ResumeThread para "svchost.exe".

O malware é vinculado estaticamente ao libssl.dll, que é usado para criptografia SLL da comunicação C2.

Yandex Cloud como C2

Outro implante localizado foi um que utiliza o armazenado de dados Yandex Cloud como um C2 (https[:]//cloud-api.yandex[.]net) de forma semelhante ao malware descrito em outro relatório. O implante utiliza um esquema de carregamento baseado em sequestro de DLL, no qual a DLL maliciosa descriptografa o corpo do implante armazenado em um arquivo separado e o injeta na memória de um processo legítimo.

O implante utiliza libcurl.dll vinculado estaticamente para comunicação criptografada por SSL.

Ele realiza a coleta dos dados:

- Nome do computador
- Nome de usuário
- Endereço de IP
- Endereço do MC
- Versão do SO
- Caminho para o %system%

Para fazer upload dos dados coletados para C2, o implante utiliza uma solicitação usando um token de API incorporado para criar um diretório com nome exclusivo do host da vítima.

```
C:\Windows\system32>sc query WinCoreSvc

SERVICE_NAME: WinCoreSvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Windows\system32>
```

Figura 3 – Log contendo o resultado da execução do comando usado cmd.

3 IMPLANTES DE SEGUNDA FASE

Os implantes de segunda fase possuem o foco realizar a coleta de dados e arquivos, tratados por subtítulos:

Implante dedicado para reunir arquivos locais

Em maio de 2022, foi descoberto um implante dedicado para coletar arquivos locais, onde este utiliza um esquema de carregamento baseado na técnica de sequestro de DLL, onde o loader de DLL malicioso garante e persiste criando um serviço chamado "WinSystemHost", descriptografando e injetando a carga armazenada como dados binários em arquivos separados na máquina de um processo legítimo.

O impkante inicia o "msiexec.exe", depois lê e descriptografa o payload de um arquivo separado e o injeta na memória do "msiexec.exe".

Uma vez que o payload começa a ser executado na memória de "msiexec.exe", ele entra em um loop infinito que consiste em 6 etapas simples:

- Crie pastas para armazenamento de arquivos (se não existirem) e encontre o caminho para "WinRar.exe".
- Descriptografar strings
- Leia a comunicação e comece a procurar arquivos em tdos os discos
- Copie arquivos e grave logs
- Arquivar arquivos copiados e limpar
- Durma por 10 minutos

Para realizar a exfiltração dos dados, o agente de ameaça utiliza uma pilha de implantes para carregar os arquivos no Dropbox.

Implante usado para exfiltrar dados de redes sem fio por meio de unidades removíveis

Em abril de 2022, foi descoberto um malware projetado para exfiltrar dados de sistemas isolados infectando unidades removíveis.

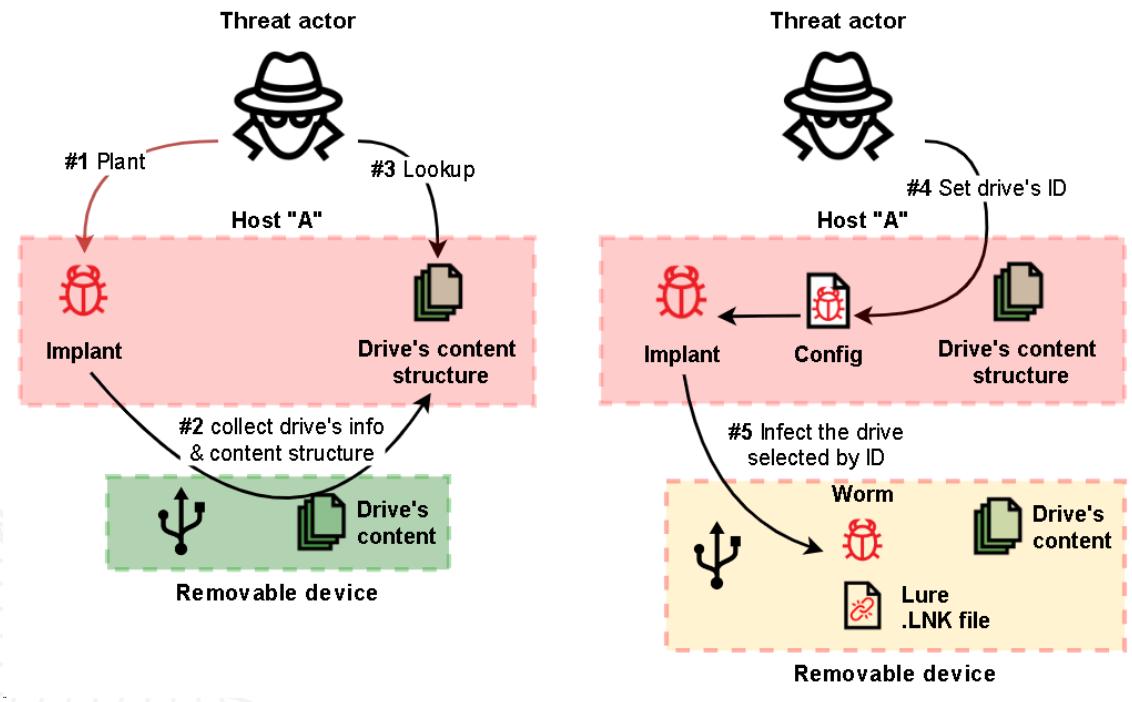


Figura 4 – Diagrama simplificado da interação do implante com uma mídia removível.

O primeiro modulo (principal) é responsável por lidar com unidades removíveis, incluindo:

- Coleta de informações sobre uma unidade
- Clonar a estrutura do sistema de arquivos de cada unidade para uma pasta temporária local e manter a estrutura atualizada.
- Coleta arquivos roubados de uma unidade e implantar malware de segunda etapa em unidades recém-conectadas.
- Captura de telas e títulos máquina Windows infectada.

O módulo principal cria uma pasta em "%TEMP%", onde armazenará os logs, informações de drivers conectados e conteúdos dos drivers.

O implante também verifica nessas pastas os seguintes arquivos que são usados para infectar uma unidade removível cujo número de série corresponde ao número da pasta:

- "mscods.exe" que é um executável legítimo da McAfee vulnerável ao sequestro de DLL.
- "MsVsoCfg.dll" que é o payload da segunda etapa.
- Arquivos DOC, PDF ou DIR, que definem o arquivo de link de isca a ser utilizado.

A presença dos arquivos mencionados acima na pasta atribuída a uma unidade removível específica indica que os invasores primeiro analisam o conteúdo das unidades removíveis por algum tempo e só depois copiam os arquivos usados para infectar uma unidade removível específica para a pasta especificada.

Para infectar uma unidade removível, o módulo principal simplesmente copia dois arquivos, "mcods.exe" e um **malware de** segunda etapa **"McVsoCfg.dll"**, para o diretório raiz da unidade e define o atributo "Oculto" para ambos os arquivos.

Além disso, caso exista um malware de quarta etapa, ele também será copiado para a unidade removível junto com o implante de segunda etapa.

Após gerar um arquivo lnk, após a sua abertura, o sistema operacional carrega o "mcods.exe", que carrega McVsoCfg.dll e chama a sua função.

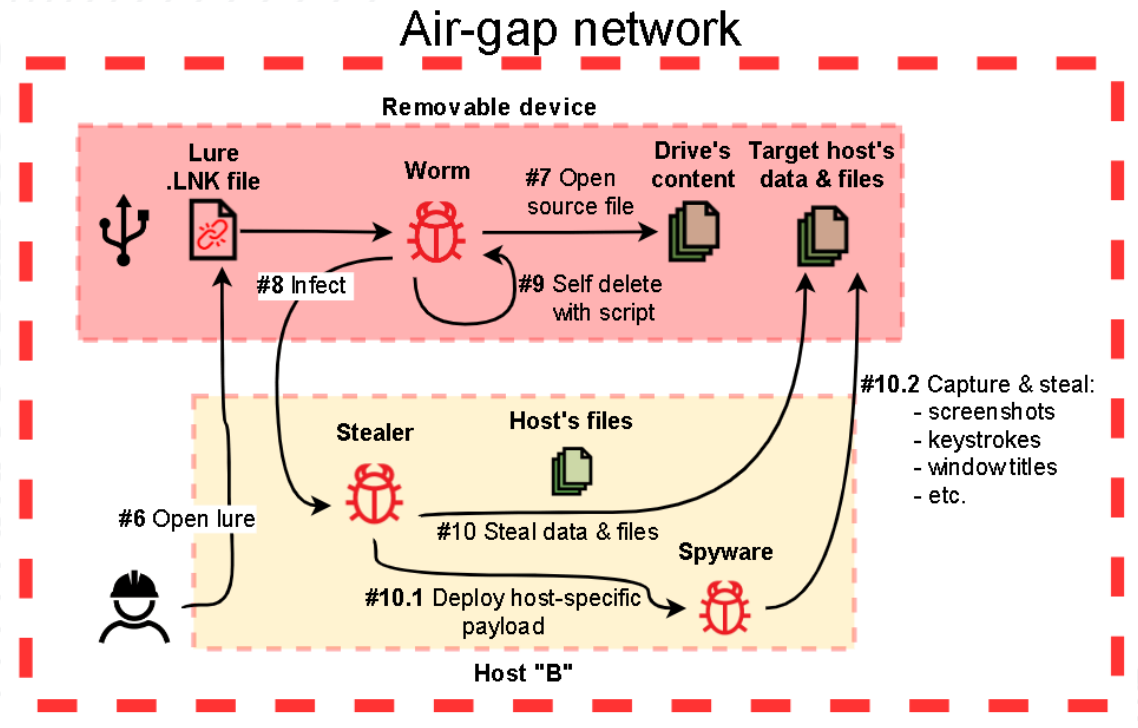


Figura 5 – Esquema simplificado de infectar um computador em um segmento de rede isolado através de uma mídia removível infectada.

Depois disso, o malware implanta o executável de terceira etapa, extraindo-o de seu próprio arquivo e salvando-o em **"%APPDATA%"** com o nome "msgui.exe" no host que está sendo atacado.

O malware de quarta etapa é procurado em dois arquivos:

- Um dropper simples de payload
- O payload útil, que é, na verdade uma versão modificada do módulo de primeira etapa e é projetada para coletar informações sobre uma unidade, coletar arquivos, captura de tela e pressionamento de tecla.

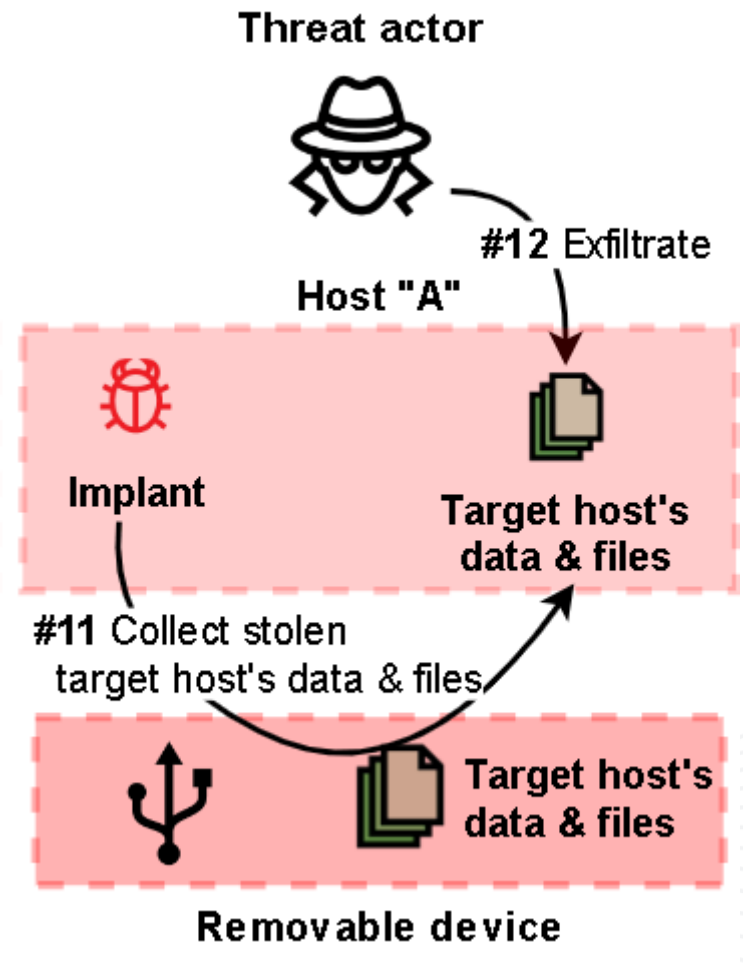


Figura 6 – Esquema simplificado para coletar dados roubados de um computador em um segmento de rede isolado por meio de uma mídia removível infectada.

Para coletar todos os dados roubados, o ator de ameaça utiliza um shell remoto para executar os payloads e malwares projetados para carregar os dados.

4 IMPLANTES DE TERCEIRA FASE

Implantes de terceiro estágio e ferramentas usadas para enviar dados ao C2

Os implantes de terceiro estágio foram implantados pelo ator de ameaça por meio do primeiro estágio, bem como os de segundos.

Os implantes de terceiro estágio têm muito m comum com os implantes de primeiro estágio, incluindo o uso de armazenamento de dados baseados em nuvem, ofuscação de código e implementação de técnicas de sequestros de DLL.

Pilha utilizada para carregar arquivos no Dropbox

Uma pilha de implantes para upload de arquivos para o Dropbox foi projetada para funcionar em conjunto com um implante de coleta de arquivos de segundo estágio. O endereço de IP C2 em uma das variantes da terceira etapa chamou a atenção dos pesquisadores porque era um endereço IP local, significando que o ator de ameaça implantou um C2 dentro do perímetro corporativo e aparentemente o usou como proxy para extrair dados de hosts que não tinham acesso direto à internet.

Para fazer o upload de arquivos locais, o implante de segunda etapa chama um implante de terceira etapa, que já deve estar implantado na máquina no caminho definido estaticamente **"C:\Users\public\"** ou no mesmo caminho do segundo.

Todas as variantes da terceira etapa são projetadas para carregar os arquivos ".rar" coletados no Dropbox de **"C:\ProgramData\NetWorks\ZZ"** na máquina local.

Ferramentas para exfiltração manual de arquivos roubados

Duas ferramentas foram utilizadas para realizar a exfiltração de dados, uma chamada **"AuditSvc.exe"** e a segunda seria a **"Transfer.exe"**, ambas projetadas para realizar o upload e download de ferramentas e arquivos.

Implante utilizado para fazer upload de arquivos por meio de serviços de e-mail Yandex

O implanta projetado para enviar arquivos pelo serviço de e-mail Yandex foi baixado do Yandex Disk, sendo vinculado estaticamente com **“libcurl.dll”.**

O implante foi projeto para exfiltrar um único arquivo localizado no caminho estático **“C:\Users\Public\Downloads\111.log”**, sendo enviado como anexo de e-mail.

Após uma única tentativa de enviar um e-mail, o implante é encerrado.

5 TTPs – MITRE ATT&CK

Tática	Técnica	Detalhes
Initial Access	Phishing: Spearphishing Attachment T1566.001	Atores de ameaças usaram documentos de atração para implantar spywares disponíveis no mercado.
Execution	User Execution: Malicious File T1204.002	Um sistema é infectado quando o usuário executa o malware acreditando ser um documento legítimo.
	Command and Scripting Interpreter: Windows Command Shell T1059.003	Usa cmd.exe para executar váriso comandos.
	Native API T1106	Usa a função CreateProcessW para executar comandos no interpretador de linha de comando do Windows.
	Scheduled Task/Job Scheduled Task T1053.005	O malware é executado com uma tarefa do Windows criada pelo agente de ameaça.
Persistence	Registry Run Keys/ Startup Folder T1547.001	O malware consegue persistência adicionando-se ao Registro ccomo um programa de inicialização.
	Create or Modify System Process: Windows Service T1543.003	Instala-se como um serviço para obter a persistência.
	Sceduled Task/Job: Sceduled Task T1053.005	O malware é executado como uma tarefa do Windows criado pelo ator de ameaça
Defense Evasion	Deobfuscate/Decode Files or Information T1140	Usa a chave RC4 para descriptografar a configuração do malware, bem como para proteger a comunicação.
	Process Injection: Portable Executable Injection T1055.002	O malware se injeata em vários processos legítimos durante a execução (msiexex.exe e svchost.exe).
	System Checks T1497.001	Emprega várias verificações de sistema para detectar e evitar ambientes de virtualização e análise.
	Time Based Evasion T1497.003	Emprega vários métodos baseados em tempo para detectar e evitar ambientes de virtualização e análise.
	Hijack Execution Flow: DLL Side-Loading T1574.002	Os agntes de ameaças abusam de um binário de aplicativo legítimo para carregar uma DLL maliciosa.

Discovery	File and Directory Discovery T1083	O malware tenta descobrir arquivos de vários tipos (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .rtf e .eml).
	System Network Configuration Discovery T1016	Os agentes de ameaças usam os utilitários netstat e ipconfig para obter a configuração da interface de rede local e enumerar as portas abertas.
	System Owner/ User Discovery T1033	Atores de ameaças usam systeminfo, whoami e utilitários de tede para obter informações sobre o usuário e o sistema infectado.
	Process Discovery T1057	Atores de ameaças usam lista de tarefas para enumerar processos em execução.
Command and Control	Application Layer Protocol: Web Protocols T1071.001	O malware usa HTTPS e TCP bruto para comunicação com C2.
	Encrypted Channel: Symmetric Cryptography T1573.001	O malware usa RC4 e SSL TLS v3 (usando libssl.dll) para criptografar a comunicação.
Credential Access	OS Credential Dumping: Cached Domain Credentials T1003.004	Atores de ameaças usam Mimikatz e Reg para extrair credenciais em cache.
Collection	Data from Local System T1005	Malware projetado para coletar e exfiltrar dados arbitrários, incluindo sistemas air-gapped, abusando de dispositivos removíveis.
	Data from Removable Media T1052.001	O malware foi projetado para armazenar todos os dados coletados em uma unidade UBS infectada específica, a fim de extraí-los de uma rede sem fio.
Exfiltration	Exfiltration Over C2 Channel T1041	Atores de ameaças exfiltram dados usando Dropbox, Yandex Disk, Yandex e-mail e serviços de compartilhamento de arquivos temporários como um canal C2.

Tabela 1 – Tabela MITRE ATT&CK.

6 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:	4c1adc1778ce07cd655db129af1da7e0
md5:	71d919105627c67ab9fb9a7152015cf6
md5:	3e22e7f5a6ee0a7d3d9a5cbfa7939c98
md5:	2db858c4ca836120d3124eb5490195ea
md5:	d2d7fd5c7372cd81d6bc4199f211a42c
md5:	4d5963b7d931a02265ea5231961935e9
md5:	3a532b8481f22b78abc718ac5cdb3f06
md5:	36a029cb62bfcb86394b49e5acf36bef
md5:	1dbc1defc2ac6578d83d5c45d9836482
md5:	9f402f0b2c84ed577e9ee76dcf640b70
md5:	0e69850a0f67165d4e3d06987d14b2e6
md5:	c929dcc69cf6546d56c2a68d31d7728d
md5:	8ba9ee9fd6bd4b9304f7fb868ce975d8
md5:	971b0687c8281778b28721239801084e
md5:	fff248db8066ae3d30274996baeddab6
md5:	7332710d10b26a5970c5a1ddf7c83fba
md5:	2a1cfa6d17627eaaa7a63f73038a93da
md5:	bb02a5d3e8807d7b13be46ad478f7fbb
md5:	22e66e0be712f2843d8db22060088751
md5:	d75c7bd965c168d693ce8294138136ae

Tabela 2 – Indicador de Compromisso – MD5.

URLs de distribuição e endereços IP C2:

img[.]onl/api/upload.php
litterbox.catbox[.]moe/resources/internals/api.php
imgbb[.]com
transfer[.]sh
share.schollz[.]com
0x0[.]st/
tinyimg[.]io/upload
gifyu[.]com/
imgshare[.]io
imgpile[.]com/
zippyimage[.]com
extraimage[.]info

upload.picpaste[.]me
imgurupload[.]org
sm[.]ms/api/v2/upload
easycaptures[.]com/upload_file_new.php
freetranslatecenter[.]com
help.freetranslatecenter[.]com
onlinenewscentral[.]com
onlinemapservices[.]com
search.onlinemapservices[.]com
help.onlinemapservices[.]com
apps.onlinemapservices[.]com
edit.onlinemapservices[.]com
booking-onlines[.]com
81.28.13[.]74
92.38.160[.]142
92.38.188[.]135
92.38.190[.]55
103.221.222[.]133
193.109.78[.]243
193.124.112[.]206
sfb.odk-saturn[.]com/dialin/login
87.121.52[.]86
194.87.95[.]125

Tabela 3 – Indicadores de Compromissos – Domínio e IPs C2.

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.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **TTPs comuns contra organizações industriais - Kaspersky**
  - **Primeira etapa**
  - **Segunda etapa**
  - **Terceira etapa**

heimdall
security research

A DIVISION OF ISH