BOLETIM DE SEGURANÇA

Fickle Stealer distribuído por meio de múltiplas cadeias de ataque

heimdall
security research
A DIVISION OF ISH

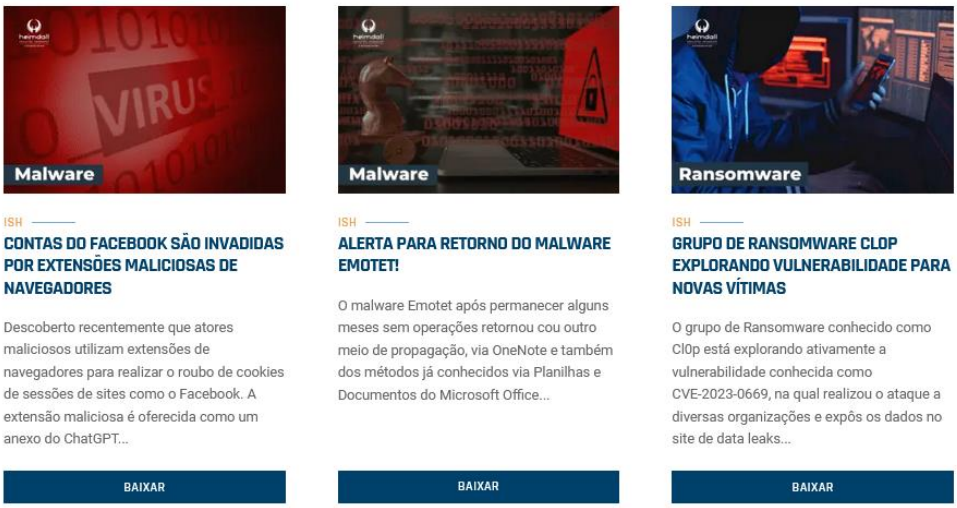
TLP: CLEAR

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

Em maio de 2024, pesquisadores do FortiGuard Labs identificaram um novo stealer de dados, denominado **Fickle Stealer**. Este stealer, programado na linguagem de programação Rust, se destaca por seu código complexo e pela maneira como é distribuído, a qual é descrita neste relatório de segurança.

2 INFORMAÇÕES SOBRE A AMEAÇA

Utilizando uma variedade de estratégias, o Fickle Stealer demonstra uma capacidade notável de adaptabilidade na escolha de seus alvos. A natureza ambígua e flexível deste stealer de dados reforça a necessidade de vigilância constante e medidas de segurança robustas.

A campanha em questão foi estruturada em torno de uma sequência de três fases distintas: a fase de Entrega, a fase de Trabalho Preparatório e, finalmente, a fase que envolve a Carga Útil do Empacotador e do stealer. Cada estágio desempenha um papel crucial na execução bem-sucedida da campanha, demonstrando a complexidade e o planejamento envolvidos neste processo. A análise detalhada dessas etapas fornece uma visão valiosa sobre a operação da campanha e as estratégias empregadas pelos atacantes.

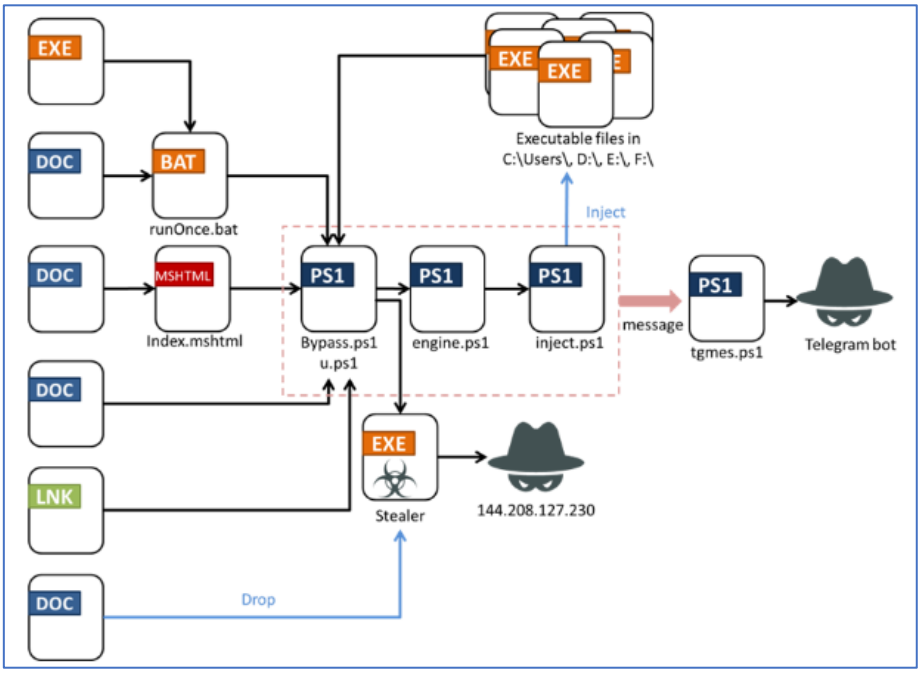


Figura 1 – Cadeia de ataque.

O Fickle Stealer é entregue por meio de quatro métodos distintos: VBA dropper, VBA downloader, link downloader e executável downloader. Em geral, esses métodos baixam um script do PowerShell para realizar tarefas preparatórias. O arquivo baixado é geralmente chamado de u.ps1 ou bypass.ps1, ambos se referem ao mesmo arquivo. Em certas cadeias de ataque, um arquivo adicional é inserido entre o downloader e o u.ps1.

A cadeia de ataque se inicia com um documento do Word. A macro VBA do documento carrega um arquivo XML que está armazenado na legenda de um objeto UserForm. Em seguida, um script codificado com o Windows Script Encoder é executado a partir deste arquivo XML.

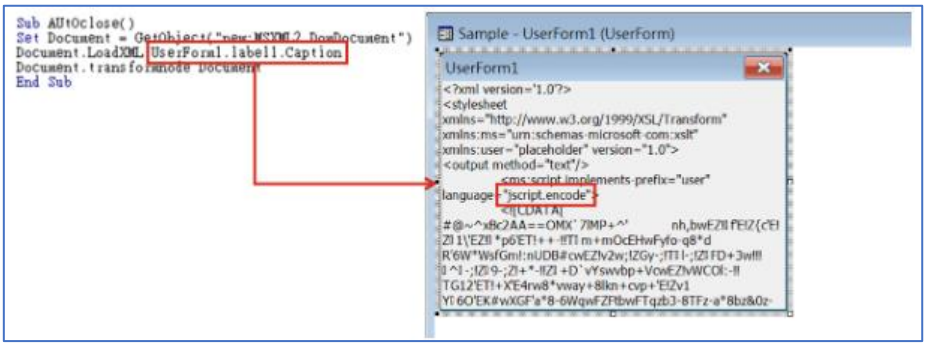


Figura 2 – Código VBA que executa o script codificado.

O script contido no arquivo XML tem a função de posicionar o Fickle Stealer na pasta Temp e, em seguida, iniciar sua execução.

Figura 3 – Script decodificado.

Existem três variantes de downloaders VBA, todos sendo documentos do Word. O primeiro deles realiza o download direto do arquivo u.ps1. O terceiro downloader, por outro lado, emprega um método indireto para entregar o downloader VBA. Ele incorpora um controle de navegador da web em um quadro no documento, que acessa um arquivo MSHTML no servidor. Quando o conteúdo ativo e a macro são habilitados pela vítima, o arquivo MSHTML é lido e o comando é extraído. Geralmente, o método WebBrowser.Navigate é usado para carregar um URL especificado. No entanto, o Word armazena o último URL carregado no arquivo do documento e esse URL será usado se um novo não for fornecido. Isso significa que, uma vez que a URL é carregada, ela pode ser carregada novamente na próxima execução, mesmo na ausência de qualquer macro relacionada. Uma variante adicional utiliza essa técnica para esconder o URL (8d3ccfafc39830ee2325170e60a44eca4a24c9c4dd682a84fa60c961a0712316).

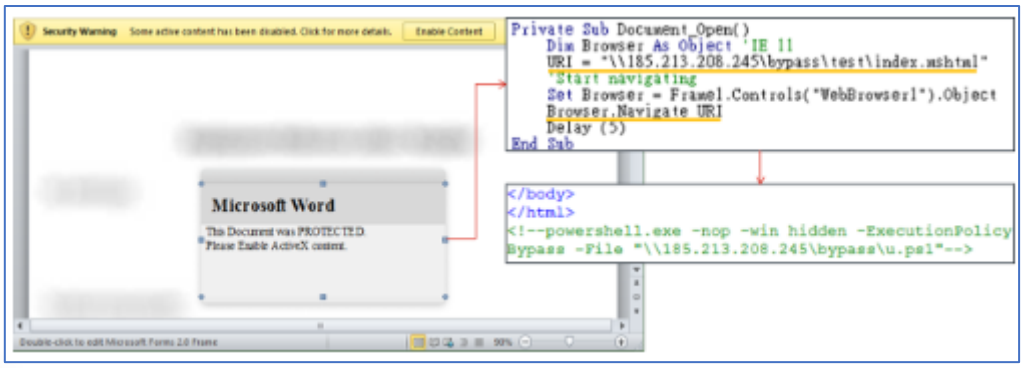


Figura 4 – Código sublinhado pode ser removido após o carregamento do URL.

Este script tem como principal objetivo contornar o Controle de Conta de Usuário (UAC) para executar o Fickle Stealer. Ele também configura uma nova tarefa para executar engine.ps1 após um intervalo de 15 minutos. Para burlar o UAC, o u.ps1 descarta uma cópia do WmiMgmt.msc e um WmiMgmt.msc falso nos caminhos especificados.

- Normal: C:\Windows \System32
- Fake: C:\Windows \System32\en-US

O arquivo MSC, que é hospedado no Microsoft Management Console (MMC), é responsável pelo gerenciamento de hardware, software e componentes de rede e necessita de direitos de administrador. Os snap-ins fornecem a interface para a tarefa de gerenciamento e acesso aos programas e dados necessários. O WmiMgmt.msc falso explora um objeto Shockwave Flash do controle ActiveX, que por padrão abre um navegador da web. A URL do navegador da web é definida como localhost e o u.ps1 cria um HttpListener, que exibe uma página da web quando o WmiMgmt.msc é executado. Esta página da web contém um script que configura exclusões para o Fickle Stealer e, em seguida, faz o download para execução.

O caminho do arquivo emprega uma técnica conhecida como Método de diretórios confiáveis simulados. Durante um processo de solicitação de avaliação, um espaço à direita após “Windows” é removido ao converter uma string. Como resultado, o WmiMgmt.msc será tratado como se estivesse sendo executado a partir de um caminho confiável. Além disso, o MMC procura os idiomas locais no arquivo MSC. Se não for encontrado, ele tenta encontrar um para en-US. Assim, quando o Fickle Stealer executa a cópia do WmiMgmt.msc, o WmiMgmt.msc falso é executado, com autenticação elevada e sem nenhum prompt do UAC.

O engine.ps1 lista arquivos exe em C:\Users, D:, E:, F:. Quando um arquivo é encontrado, ele executa o inject.ps1 para injetar código shell, que simplesmente executa o u.ps1 da Internet. Os caminhos dos arquivos injetados são codificados em base64 e gravados em C:\Users\Public\prepares.dat. Antes da injeção, o engine.ps1 verifica a lista para evitar injeção dupla.

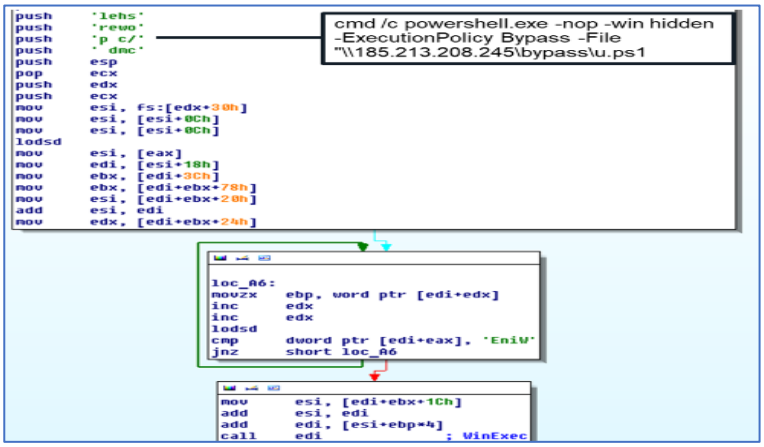


Figura 5 – Código shell injetado.

Os scripts u.ps1, engine.ps1 e inject.ps1 comunicam-se regularmente com o bot do invasor no Telegram para atualizar seu status. Para transmitir uma mensagem, eles baixam o tgmes.ps1 na pasta Temp com um nome de arquivo gerado aleatoriamente e o executam com a mensagem como argumento. O tgmes.ps1 é imediatamente excluído após cada envio de mensagem. Além da mensagem, o tgmes.ps1 também envia informações detalhadas da vítima, incluindo país, cidade, endereço IP, versão do sistema operacional, nome do computador e nome de usuário para o bot do Telegram.

O Fickle Stealer é protegido por um empacotador que se disfarça de um executável legítimo. O invasor parece ter criado o empacotador substituindo parte do código de um executável legítimo pelo código do empacotador e modificando uma função chamada na rotina de inicialização para a função do empacotador. Isso pode dificultar a análise estática. A imitação de vários aplicativos torna mais difícil a detecção do malware usando regras de detecção específicas.

Por exemplo, existe uma variante (a641d10798be5224c8c32dfaab0dd353cd7bb06a2d57d9630e13fb1975d03a53) onde a função __cinit na rotina de inicialização é alterada para a função do empacotador.

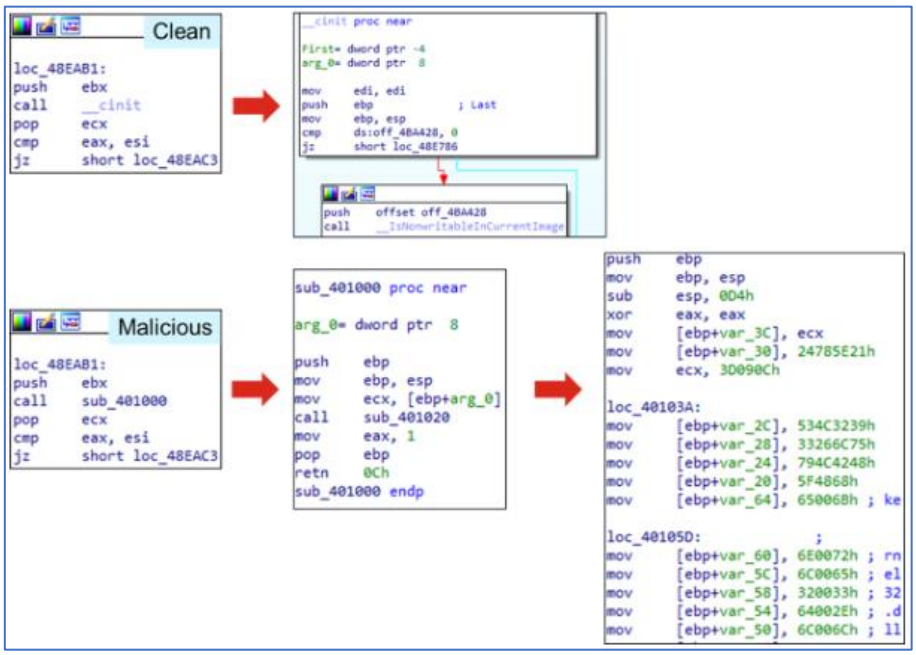


Figura 6 – Comparação entre o programa e o empacotador do Fickle Stealer.

Neste cenário, o código mal-intencionado é ativado antes da função WinMain, que é comumente o ponto de entrada definido pelo usuário para um aplicativo GUI C/C++. Isso pode levar à omissão do código malicioso por aqueles que seguem as regras padrão de análise. O empacotador simplesmente aloca memória para registrar os dados de carga útil decifrados e, em seguida, executa-os na memória.

As técnicas de anti-análise utilizadas são as seguintes:

- **Sinalizador BeingDebugged**

O Fickle Stealer analisa a estrutura PEB (Process Environment Block) para verificar o sinalizador BeingDebugged no deslocamento 0x2. Se o sinalizador estiver definido, indicando que está sendo depurado, o Fickle Stealer encerra o processo sem exibir uma mensagem falsa.

- **Processos em execução no momento**

O Fickle Stealer compara os nomes dos processos com os nomes das ferramentas de análise e algumas palavras-chave que podem ser usadas em um ambiente de análise.

- **Módulo carregado**

Quando um arquivo é executado em uma sandbox, os arquivos DLL correspondentes são carregados para auxiliar na análise. O Fickle Stealer chama a função GetModuleHandleW para verificar se algum deles está carregado na memória.

- **Máquina virtual**

Os resultados da consulta dos seguintes objetos WMI são nulos em algumas máquinas virtuais.

- **ID de hardware**

O Fickle Stealer compara o ID de hardware com IDs que podem ter sido usados em ambientes de análise.

- **Nome de usuário**

O Fickle Stealer chama a função GetEnvironmentVariableW e compara o resultado com nomes que podem ter sido usados em ambientes de análise.

Finalmente, o Fickle Stealer cria uma nova pasta na pasta Temp com um nome aleatório, coloca sua cópia na nova pasta e executa a cópia. O stealer em execução será encerrado e a cópia concluirá o trabalho restante para se comunicar com o servidor e enviar os dados roubados ao servidor.

Figura 7 – Comunicação entre o servidor e o Fickle Stealer.

3 CONCLUSÃO

O Fickle Stealer, além de visar aplicativos comuns, busca por arquivos sensíveis nos diretórios raiz dos locais de instalação padrão, garantindo assim uma coleta de dados extensa. Sua flexibilidade é evidenciada pela capacidade de receber uma lista de alvos do servidor. Há variantes que são atualizadas com novas listas de alvos. A frequente atualização da sequência de ataques indica que o Fickle Stealer ainda está em fase de desenvolvimento.

4 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:

Atualizações de software

- Mantenha todos os seus softwares, incluindo o sistema operacional, atualizados. Muitas vezes, os malwares exploram vulnerabilidades em softwares desatualizados.

Antivírus

- Use um software antivírus confiável e mantenha-o atualizado. Além disso, realize varreduras regulares em seu sistema.

Downloads seguros

- Evite baixar arquivos ou clicar em links de fontes desconhecidas ou não confiáveis.

Anexos de e-mail

- Tenha cuidado com anexos de e-mail desconhecidos ou suspeitos. Eles são uma maneira comum de distribuir malwares.

Senhas fortes

- Use senhas fortes e únicas para todas as suas contas. Considere o uso de um gerenciador de senhas.

Autenticação de dois fatores

- Sempre que possível, ative a autenticação de dois fatores em suas contas online.

Backup de dados

- Faça backup regular de seus dados importantes. Em caso de infecção por malware, isso pode ajudar a minimizar a perda de dados.

5 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:	d77bea7c331aae01debc4b29a3f2d535
sha1:	d30d428d31a85ac1c70f42eb42ca69a1a3fc022d
sha256:	1b48ee91e58f319a27f29d4f3bb62e62cac34779ddc3b95a0127e67f2e141e59
File name:	RB.doc

Indicadores de compromisso do artefato	
md5:	390838a85591302af29356b7307d39f9
sha1:	bbb25d2dadcbe9747c0d751bf8646764caa56553
sha256:	ad57cc0508d3550caa65fcb9ee349c4578610970c57a26b7a07a8be4c8b9bed9
File name:	Document_signed_test.doc

Indicadores de compromisso do artefato	
md5:	67a83a0cc016579f1a11f177e888729d
sha1:	8a2350510a6c16458639c8e210834d3e6c84fb15
sha256:	c6c6304fea3fd6f906e45544b2e5119c24cda295142ed9fafd2ec320f5ff41cc
File name:	Glue.lnk

Indicadores de compromisso do artefato	
md5:	8e7d32179baafa63e24465a0640c1cfb
sha1:	a1366e748719291a2dd7c8631d00ae62fcfa6d03
sha256:	f878a88b7dda1155fe939abe0500e32d5fba34569ca933bccb5603d9e0e96cc0
File name:	app.pln

Indicadores de compromisso do artefato	
md5:	019f3bdbec3910e02de1888a4aff8409
sha1:	b37d1d3a2d5211d61f244f94d60d209707ab10bb
sha256:	a641d10798be5224c8c32dfaab0dd353cd7bb06a2d57d9630e13fb1975d03a53
File name:	QHFileSmasher.exe

Indicadores de compromisso do artefato	
md5:	b563008bdef8ce3d8598e97b2669170c
sha1:	97699577bdb2c980b39f42abd2aa3791bb35f760
sha256:	48e2b9a7b8027bd03ceb611bbfe48a8a09ec6657dd5f2385fc7a75849bb14db1
File name:	BLAST.doc

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps: // github[.]com/SkorikJR
IP	144[.]208[.]127[.]230 185[.]213[.]208[.]245 138[.]124[.]184[.]210

Tabela 2 – Indicadores de Compromissos de Rede.

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**
- **Fortinet**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH