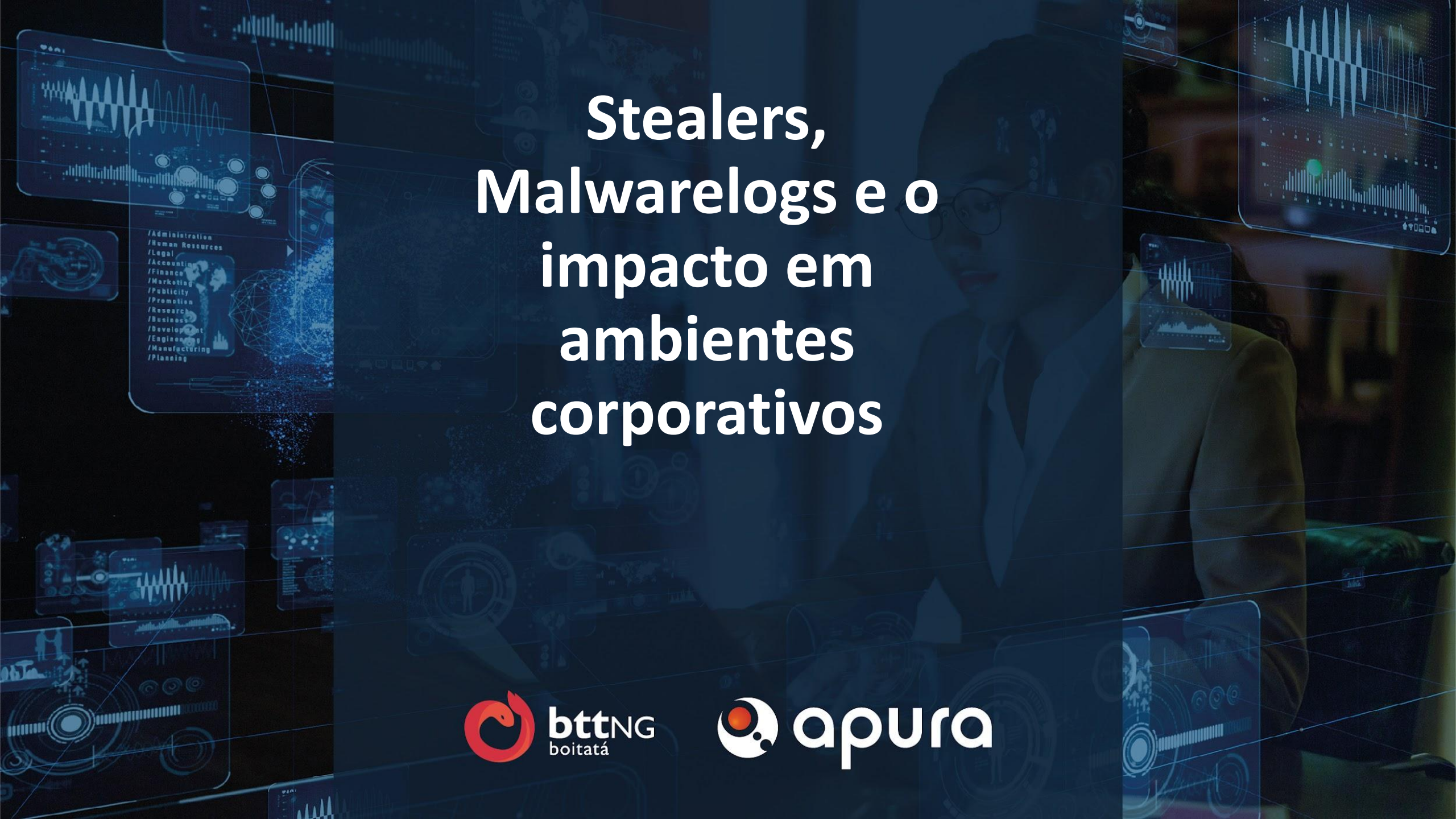
Stealers, Malwarelogs e o impacto em ambientes corporativos



bttNG boitatá

apura

Whoami - Júlio César AKA GreenMind

- Apura CyberSecurity Intelligence
  - Coordenador Time Collection
- Mas já passei pelas seguintes empresas:
- Santander Brasil
  - Threat Intelligence e Purple Team(BRAT)
- Telefonica Tech
  - Threat Intelligence
- Safeway
  - Pentester
- Mandic
  - DevOps
- Idealizador da OSINT Village
  - OSINT em eventos de segurança
- Consultor
  - Investigações para o setor privado
- Professor
  - Atuo como professor realizando treinamentos.

O que são os Malwares ?

Malware é um software malicioso que tem como objetivo Danificar, Injectar, Roubar informações e é instalado sem o consentimento do usuário.

Isso pode acontecer em dispositivos móveis, computadores ou até sistemas de rede, alguns os malwares conhecidos são:

> Spyware(coletar informações sobre atividades)
> Ransomware(Criptografa os dados do usuário e exige resgate em troca das chaves)
> Botnets(uma rede de computadores infectados e controlados remotamente)
> keyloggers(Realiza o registro de todas as teclas digitadas)
> Entre outros ..

O que são os Stealers ?

Antigamente vimos os keyloggers que registrava todas as teclas digitadas da máquina infectada, mas isso gerava muitos falsos positivos e chamava atenção.

Atualmente estão em alta os Malware Stealers, são malwares que tem como objetivo roubar informações salvas dos usuários, essas informações são roubadas das máquinas infectadas e enviadas remotamente para serem vendidas na internet.

Qual o objetivo dos Stealers ?

Os Stealers tem como objetivo roubar informações de usuários, as informações roubadas são:

- Informações de navegadores
- Firefox, Google Chrome, Edge e outros
- Todos os navegadores podem ter as informações roubadas;
- Roubo de informações de aplicativos
- Aplicativos de mensagem
- Telegram, Discord;
- Cripto Wallets
- Exodus, MetaMask, electrum e outras;
- Credenciais de VPN

Qual o objetivo dos Stealers ?

As campanhas funcionam de diversas formas, alguns exemplos conhecidos:

- Campanhas de Phishing
  - Maldocs
  - Engenharia social e redirecionamento para site malicioso
- Pay Per Click
  - Utilizados para direcionar pessoas para sites falsos, seja de software falsos ou softwares piratas
- Pay Per Install
  - Utilizado para infectar usuários, muito utilizado em softwares novos que busca aumentar seu público e assim realiza o pagamento por instalação realizada
- Software Piratas
  - Com certeza o maior risco, muitos usuários querem jogar jogos, utilizar soluções pagas e até serviços. Dessa forma utiliza software piratas comprometendo o computador

Como funcionam os Stealers ?

Informações do usuário

- IP
- Local onde foi executado
- Username
- Timezone
- País
- Sistema operacional
- Linguagem utilizada
- Data e Hora

Como funcionam os Stealers ?

Roubo Web Browsers

- Local onde estão os arquivos
- Fechando navegador
- Listando diretório de perfis
- Cookies
- Autofills
- History
- Passwords
- Cartões

Firefox e derivados

As informações são armazenadas no seguinte diretório:

Linux

- ~/.mozilla/firefox/
- /home/USER/.mozilla/firefox/

Windows

- %APPDATA%\Roaming\Mozilla\Firefox
- C:\Users\<USER>\AppData\Roaming\Mozilla\Firefox

Firefox e derivados

O formato e local dos arquivos serão os mesmos para os sistemas.

Informações importante:

- Banco Sqlite local
- Para ler os arquivos precisa fechar o navegador
- Cada informação está dentro de um diretório de perfil

Firefox e derivados - Cookies, Autofills, History e Cartões

O formato e local dos arquivos serão os mesmos para os sistemas.

Arquivos importantes:

- cookies.sqlite (Cookies)
  - SELECT host, name, value, path, expiry FROM moz_cookies;
- formhistory.sqlite (Autofills)
  - SELECT fieldname, value FROM moz_formhistory;
- places.sqlite (History)
  - SELECT DISTINCT url FROM moz_places
- webappsstore.sqlite (Cartões)
  - SELECT id, name, cardNumber FROM webappsstore2 WHERE scope='creditcard-autofill@mozilla.org'

Firefox e derivados - Password

O formato e local dos arquivos serão os mesmos para os sistemas.

Arquivos importantes:

- signons.sqlite (Senhas)
  - SELECT hostname, encryptedUsername, encryptedPassword, encType FROM moz_logins;
- As informações são criptografadas
- Precisa da biblioteca NSS(Network Security Services)
- Dessa forma consegue obter as informações

Referência:

- https://www.dumpzilla.org/

Chrome e derivados

As informações são armazenadas no seguinte diretório:

Linux

> ~/.config/google-chrome
> /home/USER/.config/google-chrome

Windows

> %APPDATA%\Local\Google\Chrome\User Data
> C:\Users\USER\AppData\Local\Google\Chrome\User Data

Chrome e derivados

O formato e local dos arquivos serão os mesmos para os sistemas.

Informações importante:

- Banco Sqlite local
- Para ler os arquivos precisa fechar o navegador
- Cada informação está dentro de um diretório de perfil

Chrome e derivados - Cookies, Autofills, History e Cartões

O formato e local dos arquivos serão os mesmos para os sistemas.

Arquivos importantes:

- Cookies (Cookies)
  - SELECT host_key, name, value, path, expires_utc FROM cookies;
- Web Data (Autofills)
  - SELECT name,value FROM autofill;
- History (Histórico)
  - SELECT url FROM urls;
- User Data (Cartões)
  - SELECT card_on_name, expiration_mount, expiration_year, card_number_encrypted, billing_address_id FROM credit_cards;

Chrome e derivados - Password

O formato e local dos arquivos serão os mesmos para os sistemas.

Arquivos importantes:

- Login Data
  - SELECT origin_url, username_value, password_value FROM logins;
- As informações são criptografadas
- No linux/mac usa AES-128 CBC com salt
- No Windows usa algoritmo DES triplo e gera senha para cada usuário

Referência:

- https://github.com/priyankchheda/chrome_password_grabber

Como funcionam os Stealers ?

Aplicativos

- Filezilla
- Telegram

Filezilla

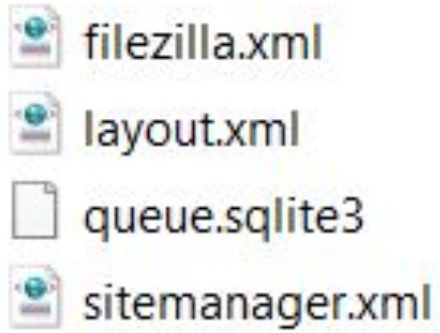
Filezilla é um cliente FTP muito utilizado por desenvolvedores e DevOps.

No Linux:

- ~/.config/filezilla/sitemanager.xml
- /home/USER/.config/filezilla/sitemanager.xml

No Windows:

- %APPDATA%\FileZilla\sitemanager.xml
- C:\Users\<USER>\AppData\FileZilla\sitemanager.xml



Filezilla

Obter as informações salvas

- Por ser um XML basta realizar o parser
- Senha é encodada em Base64
- Filtre por campos necessários
  - Host
  - Port
  - User
  - Password(Base64 decode)
  - Caso esteja usando key .pem
    - Filtre pelo campo <Keyfile> e baixe a key

```
<Server>
        <Host>127.0.0.1</Host>
        <Port>22</Port>
        <Protocol>0</Protocol>
        <Type>0</Type>
        <User>ADMINISTRADOR</User>
        <Pass encoding="base64">U0VOSEE=</Pass>
        <Logontype>1</Logontype>
        <PasvMode>MODE_DEFAULT</PasvMode>
        <EncodingType>Auto</EncodingType>
        <BypassProxy>0</BypassProxy>
        <Name>TESTE</Name>
        <Comments>COMENTARIO</Comments>
        <SyncBrowsing>0</SyncBrowsing>
        <DirectoryComparison>0</DirectoryComparison>
</Server>
```

Telegram

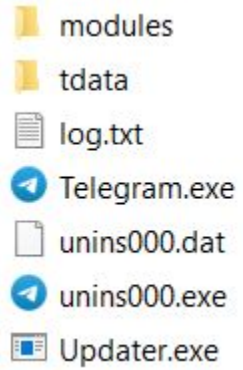
O Telegram é um dos aplicativos roubados pelos Threat Actors.

No Linux:

- ~/.local/share/TelegramDesktop/
- /home/USER/.local/share/TelegramDesktop/

No Windows:

- %APPDATA%\Telegram Desktop
- C:\Users\USER\AppData\Telegram Desktop

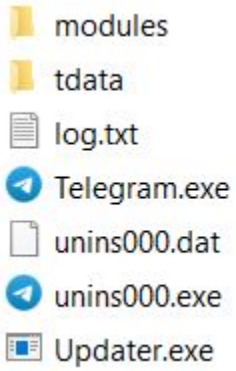


Telegram

O que é enviado para os atacantes é o diretório **tdata.**

Raccoon Stealer

- Ele rouba as informações
- Disponibiliza posteriormente



Como funcionam os Stealers ?

Criptowallets

- Exodus
- Metamask
- Electrum

Exodus

Exodus Wallet é uma carteira de criptomoedas, muito utilizada atualmente e que é uma das queridinhas dos Threat Actors.

No Linux:

> /home/<USUARIO>/.config/Exodus

No Windows:

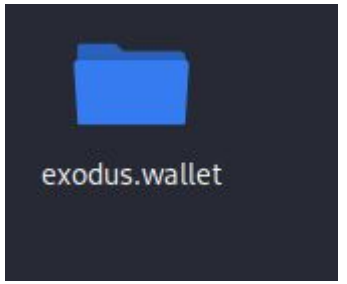
> C:\Users\<USUARIO>\AppData\Roaming\Exodus

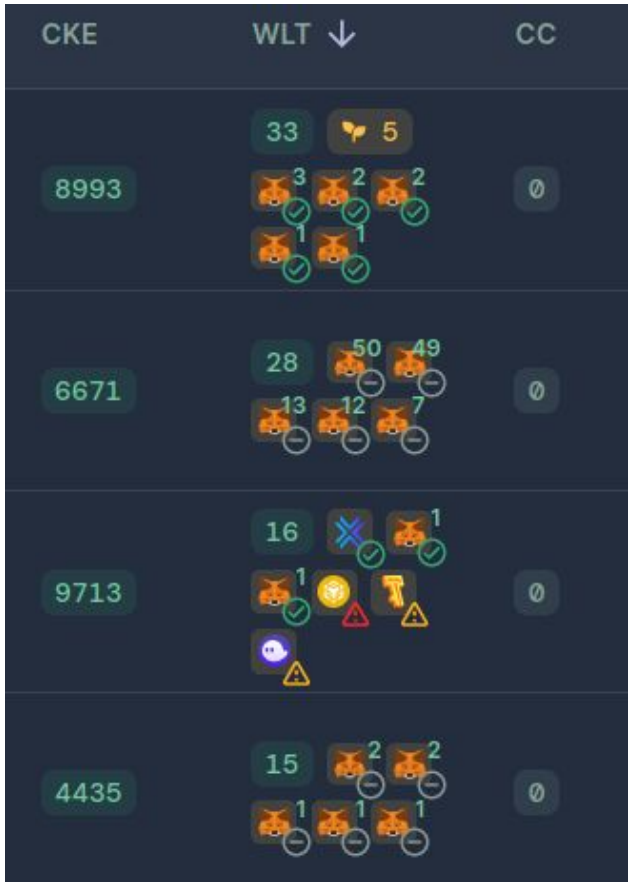
Exodus

Com a máquina infectada é roubado o diretório:

- exodus.wallet
- Depois ele é zipado
- Enviado para uma C2

Imagem abaixo do codigo do **W4SP**






```
PathsToZip = [
    [f"{roaming}/atomic/Local Storage/leveldb", '"Atomic Wallet.exe"', "Wallet"],
    [f"{roaming}/Exodus/exodus.wallet", "Exodus.exe", "Wallet"],
    ["C:\Program Files (x86)\Steam\config", "steam.exe", "Steam"],
    [f"{roaming}/NationsGlory/Local Storage/leveldb", "NationsGlory.exe", "NationsGlory"],
    [f"{local}/Riot Games/Riot Client/Data", "RiotClientServices.exe", "RiotClient"]
]
```

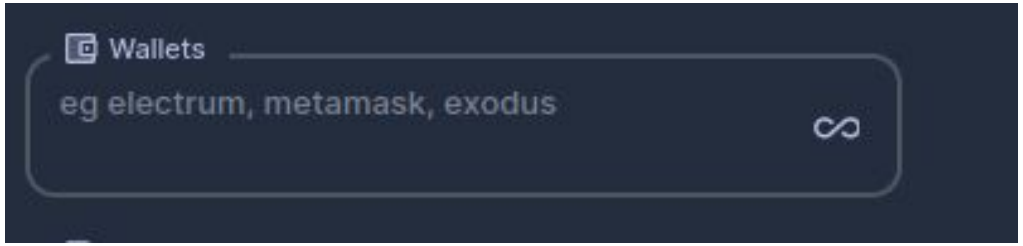
Exodus

Os Drainners:

> De forma automática os Drainners rouba os fundos
> Envia para uma carteira remota

Existem diversas carteiras atingidas:

> Electrum
> Metamask
> Exodus



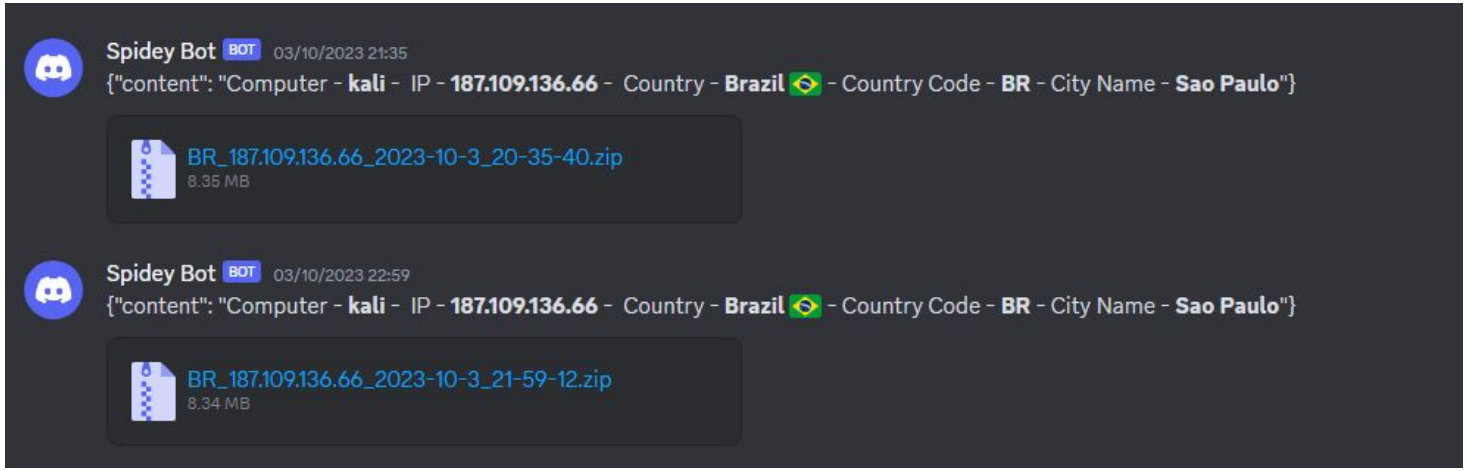
Exfiltração dos dados

Técnicas conhecidas

- Discord
- Telegram
- Gofile
- Anonfile
- C2 - Domain Reflected

Discord

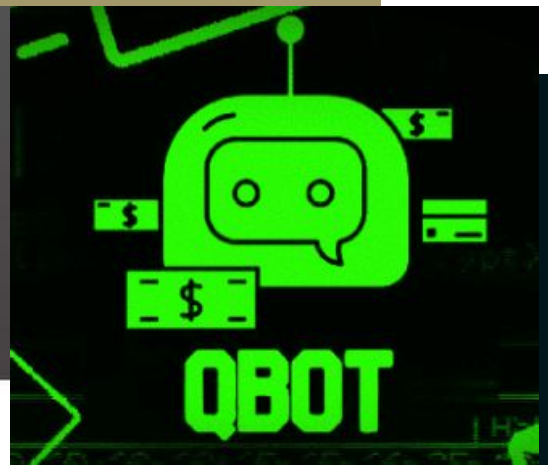
O Discord é muito utilizado pelos Threat Actors, devido a sua facilidade e segurança para armazenar arquivos. Também é muito usado para armazenar arquivos maliciosos.



Grupos conhecidos

Mars Stealer Malware

Arkei Stealer Cracked



Vidar Pro

Algumas famílias de Stealers

Existem diversas formas, seja elas:

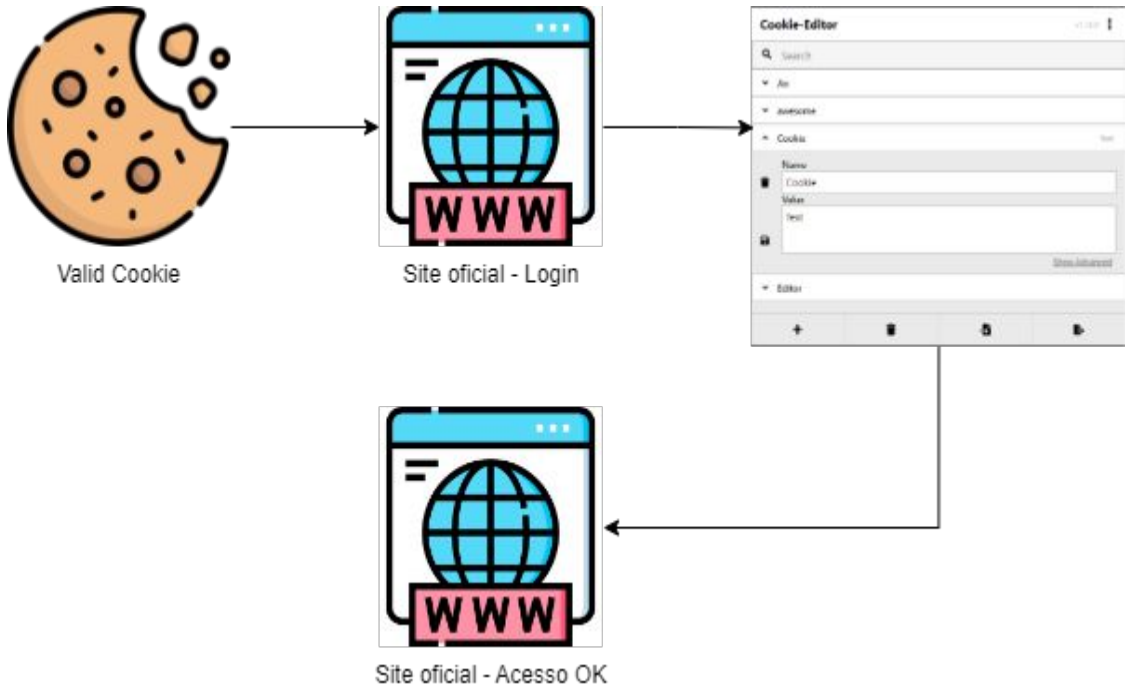
- Malware as Service
  - Raccoon
  - Vidar
  - Redline
  - Mars Stealers
- Seja software crackeados
  - Redline

Existem códigos open source

- Softwares Open Source
  - Stealerium
  - StormKitty
  - Blank-Grabber
- Códigos vazados na internet
  - Arkei Stealer
  - W4SP Stealer
  - Mars Stealer

Bypass autenticação - Cookie Injection

Existem diversas extensões que realizam esse processo de realizar a manipulação de Cookies.



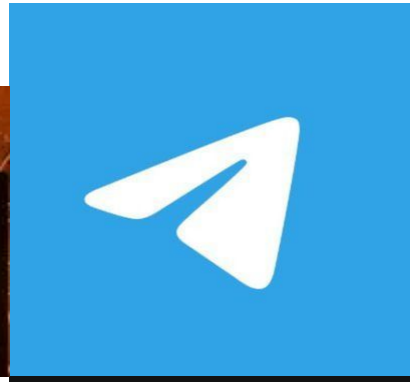
Cookie-Editor
por cgagnier

Como é vendido as informações ?

Existem diversas fontes para obter logs.

Abaixo algumas fontes:

- Telegram
  - Telegram Grupos Públicos
  - Telegram Grupos Privados
- Zelenka Guru Fórum
  - Fórum para troca de informações
  - Marketplace para venda
- Genesis Market
  - Preso em operação internacional
- Russian Market
  - MarketPlace para venda



Ataques realizados

Motivo:

> Versão pirata da estrutura do Microsoft .NET;

Impacto:

> Reputacional;
> Vazamento de mais de 3 mil fornecedores;

Software pirata é a causa provável da violação na Airbus

Violação de dados na gigante da aviação revelada no início da semana teria ocorrido em razão da tentativa de um cliente da companhia aérea Turkish Airlines de baixar uma versão pirata da estrutura do Microsoft .NET

Como se proteger - Usuários

Segurança para usuários:

- Mantenha seu sistema atualizado;
- Utilize antivírus de sua confiança;
- Não utilize softwares crackeados;
- Fique atento com as extensões utilizadas em seu navegador;
- Sempre desconfie;

Segurança para as Senhas:

- Utilize a dupla autenticação
  - Os cookies de sessão pode permitir o acesso
- Não salve informações
  - Cartões
  - Senhas

Como se proteger - Empresas

Segurança para empresas

- Só permita acesso a rede e para trabalho em computadores da empresa
- Force o uso de VPN, antivírus e implemente um endpoint security
- Realize campanhas de conscientização(Phishing, treinamentos)
- Não instale software não homologados pelo time

Segurança para senhas

- Faça o monitoramento pró ativo por possíveis credenciais comprometidas
- Evite o uso pessoal em máquinas corporativas
- Force o uso de aplicativos de dupla autenticação
- Rotina para atualização de senhas

Conclusões

- Essa é uma ameaça que tem aumentando seus alvos nesses últimos anos
- Teve um aumento considerável durante a quarentena
  - As empresas não estarem preparadas para o trabalhar home office
- Medidas de segurança podem ajudar
  - Evite uso de software craqueados
  - Cuidado com softwares falsos
- Dupla autenticação pode ajudar
  - Devido o roubo de cookies de sessão um usuário pode injetar o cookie no navegador e dar bypass no sistema de autenticação
- Monitore seus domínios com o objetivo de se antecipar a possíveis ataques

Muito obrigado

- Dúvidas ?
- Sugestões ?