Hackers, InfoStealers e o Mercado de Credenciais

13º Fórum Brasileiro de CSIRTs
Higo Aguiar

TLP:CLEAR

Agenda

- O que são InfoStealers

Definição, objetivos e relevância atual

- Funcionamento

Vetores de infecção, técnicas de coleta e exfiltração

- Stealer Logs

O produto do roubo e seu mercado clandestino

- Mercado Real

Como os Stealer Logs são anunciados, distribuidos e vendidos

- Mitigação

Boas práticas de segurança para indivíduos e organizações

TLP:CLEAR

Apresentação

Higo Aguiar

- Analista Cyber (Kryptus EED).
- MBA CyberSecurity DevSecOps (FIAP).
- Red / Blue / Threat hunter.
- Bug Hunter nas horas vagas.

- Web Application Penetration Tester eXtreme

TLP:CLEAR

Disclaimer

Esta palestra aborda conteúdos sensíveis sobre InfoStealers e o mercado de credenciais. Todos os exemplos de sites e fóruns utilizados estão presentes tanto na Surface Web quanto na Deep Web, e todas as credenciais exemplificadas já foram previamente vazadas e estão disponíveis publicamente. No entanto, as informações sensíveis foram ocultadas em respeito à privacidade dos dados.

As informações aqui abordadas são exclusivamente para fins educacionais e de conscientização em Segurança da Informação. O uso indevido das informações aqui expostas pode ser considerado crime.

TLP:CLEAR

O Que São InfoStealers?

Definição Técnica

Malwares especializados em roubar dados sensíveis: credenciais, informações financeiras, cookies de sessão e dados do sistema.

Objetivo Principal

Coletar dados valiosos para venda ou uso em ataques futuros, operando silenciosamente, sem sinais visíveis de infecção.

TLP:CLEAR

Como os InfoStealers Funcionam?

1

Vetores de Infecção

- Phishing e Spam Elaborado
- Downloads Maliciosos (Software Pirata, Extensões de navegador)
- Redes Wi-Fi Não Confiáveis
- Dispositivos USB Maliciosos
- Exploração de Vulnerabilidades

2

Técnicas de Coleta de Dados

- Keylogging e Form Grabbing
- Browser Session Hijacking
- Credential Dumping
- Screenlogger e Crypto-Wallet Harvesting

3

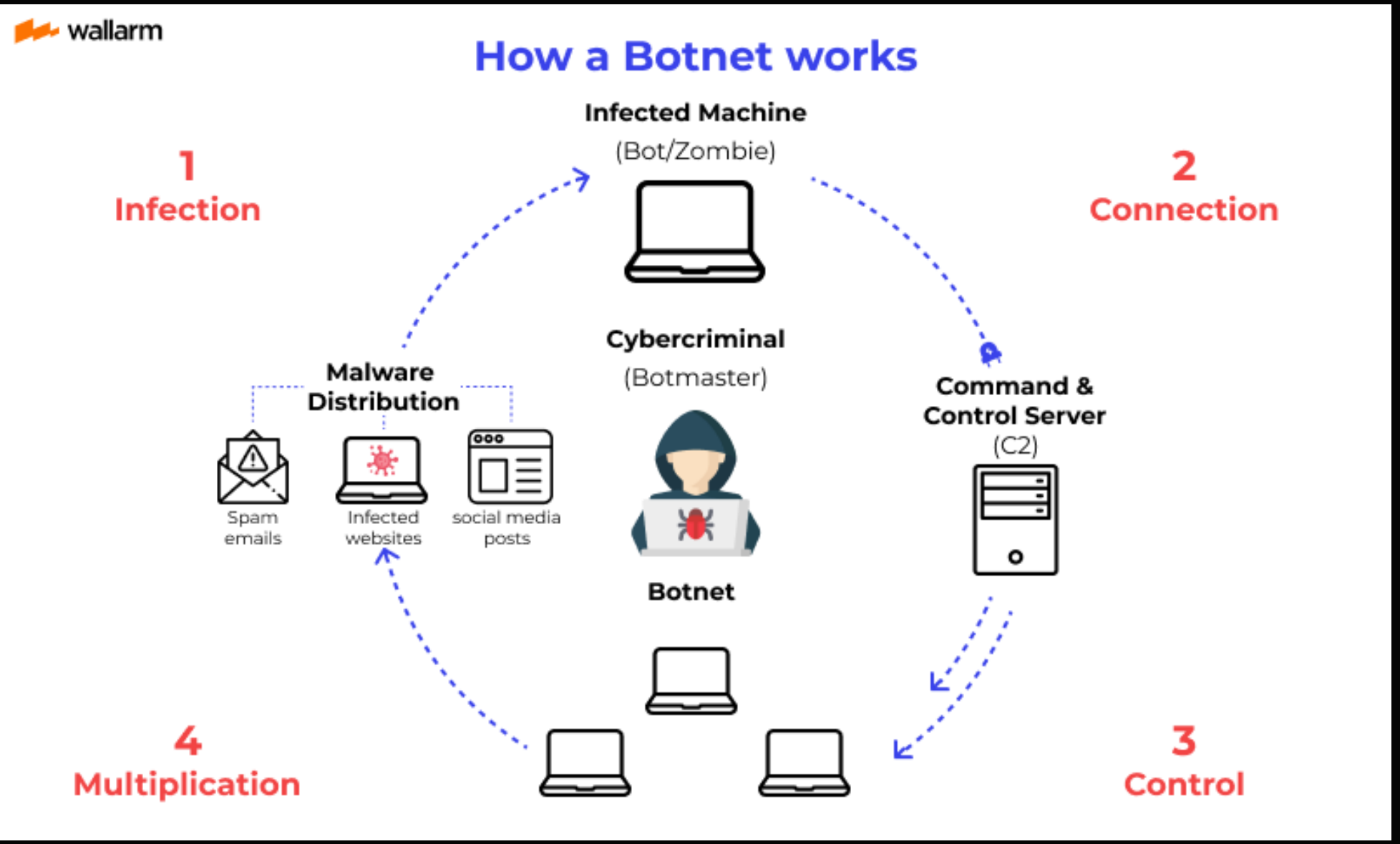
Persistência e Exfiltração

Mantêm-se no sistema, enviando dados para servidores de Comando e Controle (C2), podendo ser via x.com/Telegram/Discord para dificultar detecção.

TLP:CLEAR

BOTNETS?

TLP:CLEAR



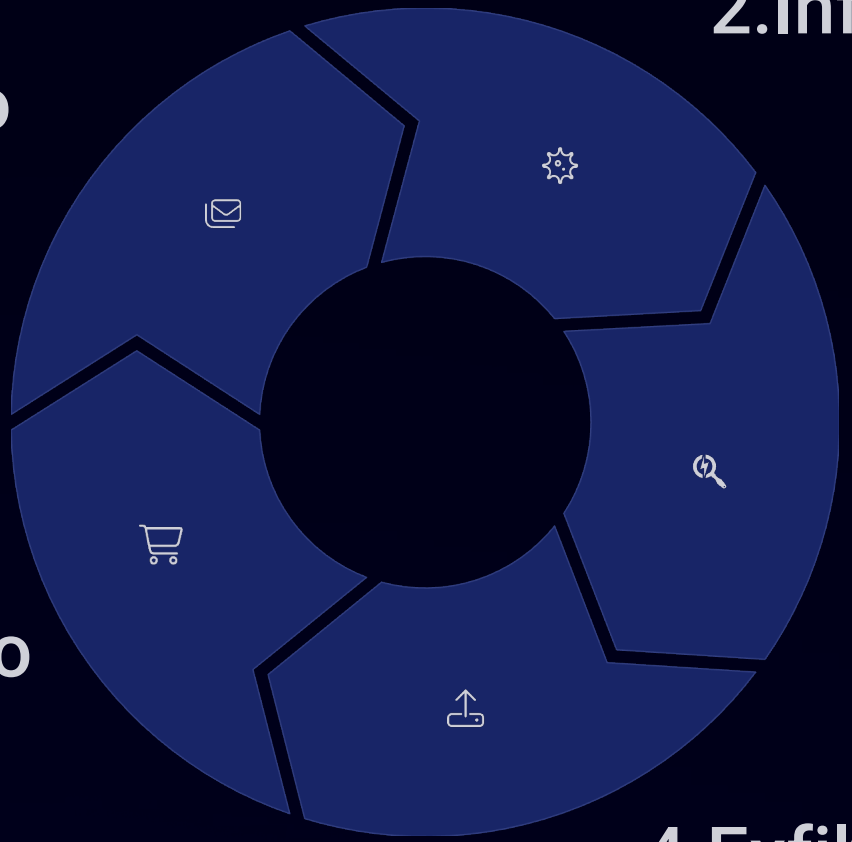
-Distribuição em massa.

-Persistência.

-Comando e Controle.

TLP:CLEAR

Ciclo de Vida do InfoStealer



1.Distribuição

2.Infecção

3.Coleta de dados

4.Exfiltração

5.Monetização

TLP:CLEAR

Stealer Logs: O Produto do Roubo

Dados Coletados Detalhados

- Credenciais de acessos (usuários, e-mails, senhas)
- Cookies de navegador (sessões ativas, histórico)
- Detalhes de carteiras de criptomoedas
- Informações do sistema (IP, localização, SO, softwares, hardware, screenshots)

TLP:CLEAR

Ciclo de vida dos Stealer Logs

1. Quando o atacante infecta a vítima

Somente a vítima e o atacante têm acesso às credenciais salvas

2. Após a venda dos logs

Nesse momento, a vítima, o atacante e os compradores têm acesso às credenciais

3. Distribuição em grupos e fóruns

Nesse estágio, o volume de pessoas que têm acesso às credenciais cresce exponencialmente

4. Redistribuição e indexação por sites

Nesse estágio, os logs ficam disponíveis fora do ambiente Deep e Darkweb disponível nas plataformas CTI.

TLP:CLEAR

Técnicas de Coleta de Dados

Credential Dumping

Extração de senhas armazenadas em navegadores, aplicativos e sistema operacional

Browser Session Hijacking

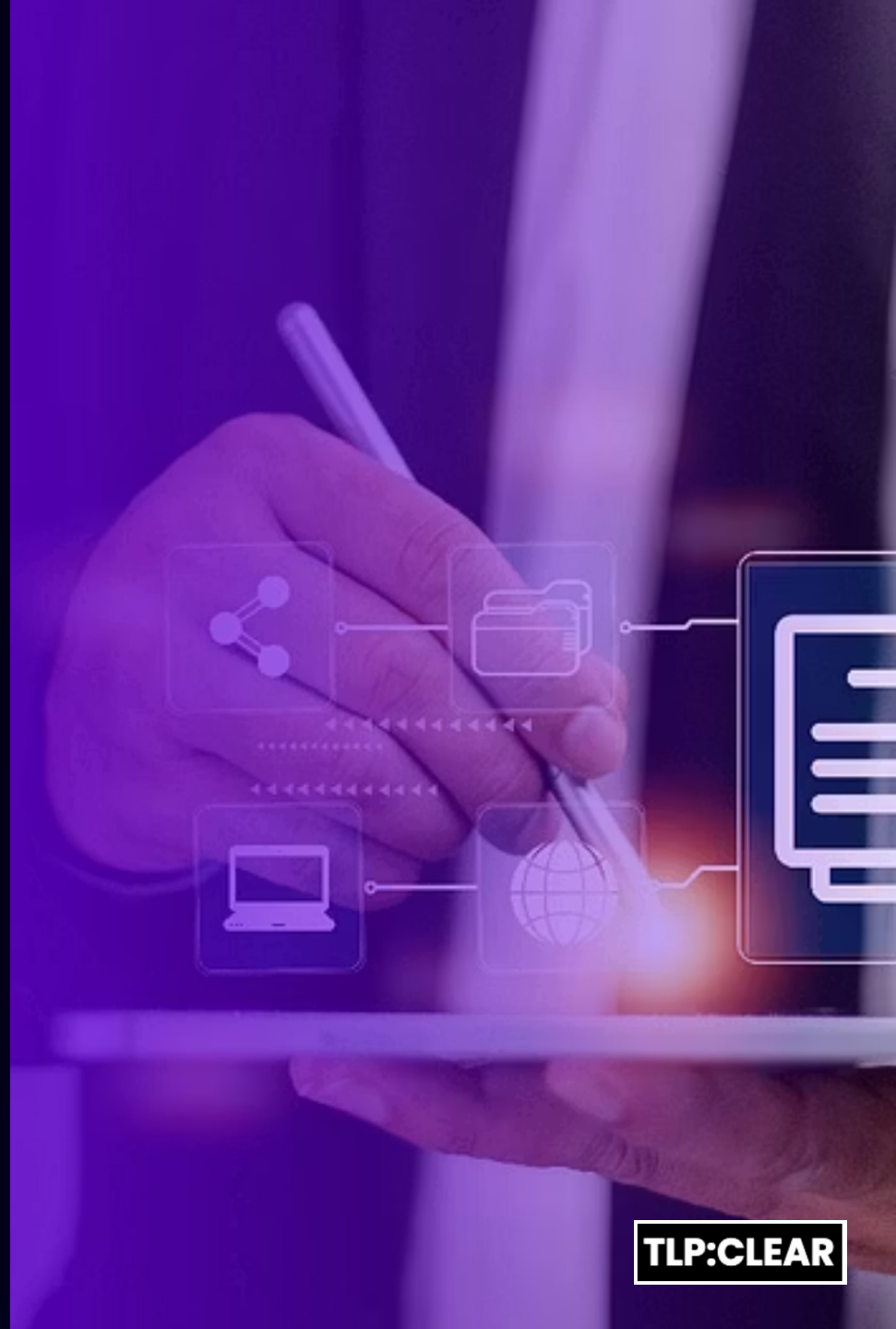
Roubo de cookies de sessão para acessar contas sem necessidade de senha

Form Grabbing

Captura dados inseridos em formulários online antes mesmo da transmissão

Keylogging

Registra todas as teclas digitadas pelo usuário, capturando senhas em tempo real



TLP:CLEAR

ATORES

Nome	Características principais
Lumma Stealer	Rouba credenciais de navegador, dados de carteiras cripto, histórico e informações do sistema. Opera como Malware-as-a-Service, altamente evasivo e atualizado frequentemente.
RedLine Stealer	Foco no roubo de logins salvos, cookies, dados de cartões e carteiras cripto. Pode coletar dados de apps de mensageria/email.
Raccoon Stealer	Malware como serviço, coleta credenciais, cartões, cookies, dados de sistema e carteiras cripto.

TLP:CLEAR

Data types collected by RedLine Stealer

Function name	Description
ScannedBrowser	Browser name, user profile, login credentials and cookies
FtpConnections	Details about FTP connections present on the target machine
GameChatFiles	Files of in-game chats related to any games found
GameLauncherFiles	The list of installed game launchers
InstalledBrowsers	List of installed browsers
MessageClientFiles	Files of messaging clients located on the target machine
City	Detected city
Country	Detected country
File Location	The path where malware .exe file is executed
Hardware	Information about the installed hardware
IPv4	Public IPv4 IP address of the victim PC
Language	OS language
ScannedFiles	Possibly valuable files found in the system
ScreenSize	Screen resolution of the target system

Function name	Description
ScannedWallets	Information about the wallets found in the system
SecurityUtils	List and status of all detected antivirus programs
AvailableLanguages	Languages, supported by the OS version on target PC
MachineName	Name of the target machine
Monitor	The screenshot of the screen at the moment of execution
OSVersion	Information about operating system version
Nord	Credentials for NordVPN
Open	Credentials for OpenVPN
Processes	List of processes running in the system
SeenBefore	Checkup if the report is about a new victim or the one that was attacked earlier
TimeZone	Time zone of the attacked computer
ZipCode	Victim's Zip-code
Softwares	List of the programs installed on the attacked PC
SystemHardwares	Details about PC configuration

TLP:CLEAR

TXTBASE

Não é um malware em si, mas uma compilação gigantesca de logs de infostealers coletados de milhões de dispositivos infectados, vendidos e distribuídos via Telegram. Inclui 1,5TB com 23 bilhões de registros (emails, senhas, sites), oriundos de vários infostealers populares. A maior parte das credenciais foi extraída por malwares que furtam dados de navegadores e sistemas, visando contas online.

TLP:CLEAR

TXTBASE = Megavazamento

tecnoblog

Megavazamento expõe 16 bilhões de senhas na internet; veja como se proteger

Vazamento afeta contas associadas ao Google, Apple, Facebook e outras plataformas. Entenda como funciona e saiba o que fazer para se manter seguro.

Por Gabriel Sérvio
20/06/2025 às 10:33

Buscar

Valor 25 ANOS | 100 ANOS DE GLOBO | PressWorks

Mega vazamento expõe bilhões de senhas: Entenda como proteger seus dados

Por Erik de Lopes Morais, COO da Penso Tecnologia

Por PressWorks
24/06/2025 05h19 · Atualizado há um mês

Segurança Cibernética

O maior megavazamento de senhas da história expõe 16 bilhões de contas

Publicado em 24/06/2025

TLP:CLEAR

Mercado de Credenciais

Como os Stealer Logs são distribuídos e vendidos

O Mercado Clandestino

O roubo e a venda de dados se tornaram um processo "industrializado", com milhões de registros comercializados diariamente.

1

Plataformas

Surface Web, Deep Web, Dark Web ,Telegram e Discord.

2

Modelos de Venda

Lote, individuais (log shops), ofertas privadas e assinaturas.

3

Precificação

Varia por tipo de dado, frescor, perfil da vítima e potencial de exploração.

TLP:CLEAR

Impacto e Consequências dos InfoStealers

1 Bypass de MFA

Cookies de sessão permitem assumir sessões autenticadas sem disparar novos desafios de MFA.

2 Vetor Inicial para ataques

- Atacantes podem executar ataques secundários (Ramsomware).

- Não precisa realizar Brute-force.

3 Violações Corporativas

- 88% das violações envolvem credenciais roubadas;
- E-mails corporativos em 40% dos incidentes de ransomware.

Fonte: DBIR 2025 (Data Breach Investigations Report)

TLP:CLEAR

Boas Práticas para Indivíduos

Autenticação Multifator (MFA)
Habilitar sempre que disponível, mas estar ciente do risco de bypass por cookies.

Gerenciadores de Senha
Usar um cofre de senha para criptografar credenciais. **NUNCA** salvar senhas diretamente no navegador.

Higiene Digital
Trocar senhas periodicamente, limpar cookies, evitar softwares crackeados e links suspeitos.

Segmentação
Usar dispositivos separados para trabalho/atividades sensíveis e uso pessoal.

TLP:CLEAR

Boas Práticas para Organizações

1

Gestão Centralizada de Credenciais

Implementar solução unificada e centralizada de gerenciamento de identidades e acessos corporativos

2

Segurança de Endpoint

Adotar ferramentas de EDR/XDR com detecção específica para InfoStealers e monitoramento de comportamentos suspeitos

3

Monitoramento Contínuo

Implementar monitoramento de credenciais corporativas comprometidas, acessos indevidos e da Dark Web

4

Políticas Internas

Proibir instalação de softwares não autorizados e extensões de navegador não homologadas

TLP:CLEAR

Resposta a Incidentes

Ordem Crítica de Ações

É fundamental sanitizar a máquina infectada ANTES de trocar as senhas, pois o InfoStealer pode roubar as novas credenciais imediatamente.

⊗ Nunca efetue a troca de senhas no dispositivo comprometido sem antes realizar uma formatação completa ou substituição do equipamento.

Passos de Mitigação

1. Isolar o dispositivo comprometido da rede
2. Sanitizar completamente
3. (formatar ou substituir)
3. Trocar **todas** as credenciais
4. potencialmente expostas
4. Verificar persistências (regras de encaminhamento de e-mail)
5. Investigar o vetor inicial de ataque

TLP:CLEAR

Conclusão:
Não Existe Bala de Prata

InfoStealers são a força motriz por trás de muitos ataques sofisticados baseados em credenciais, incluindo ransomware. A defesa efetiva requer uma abordagem em camadas.

- **Vigilância Constante**
  Tanto tecnológica quanto comportamental é essencial para proteção contínua
- **Conscientização**
  Representa a primeira e mais importante linha de defesa contra InfoStealers
- **Defesa em Profundidade**
  Combine múltiplas camadas de proteção, pois nenhuma solução isolada é suficiente

TLP:CLEAR

Dúvidas?

Obrigado!!

Linkedin: Higo Aguiar

TLP:CLEAR