

Ameaças Cibernéticas

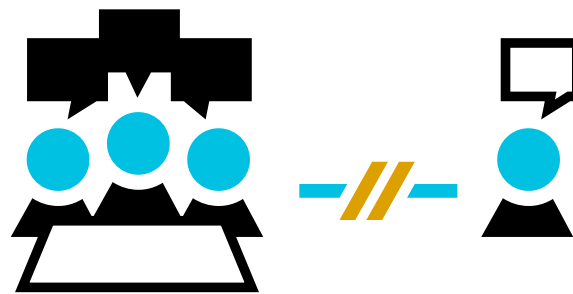


FEBRABAN
/CYBER LAB

Laboratório de Segurança Cibernética - 11/07/2025

TLP:AMBER

Traffic Light Protocol (TLP) Amber: Divulgação limitada aos participantes da organização. Destinatários podem compartilhar essas informações apenas com membros da própria organização que necessitem saber o conteúdo para tomada de ações cabíveis



Magno Logan – Instrutor GoHacking

- Especialista em Segurança da Informação, atuando no Canadá, liderando o programa de Security Champions
- Background em desenvolvimento com +15 anos de XP com AppSec, DevSecOps, Containers e K8s
- Implantou diversas ferramentas de AppSec em pequenas e grandes empresas (SAST, DAST, SCA, Secret Scanning)
- Possui diversas certificações da SANS, CompTIA, EC-Council AWS, Microsoft e EXIN
- Palestrante em diversas conferências internacionais como DEFCON, OWASP AppSec, NorthSec, H2HC, KubeCon, etc.



Magno Logan – Instrutor GoHacking



Agenda

1. Conceitos e definições
2. Origem histórica dos malwares
3. Tipos de software maliciosos (malwares)
 - Vírus, worm, trojan, infostealer, phishing, ransomware, outros

Conceitos e Definições

FEBRABAN
/CYBER LAB



O que é uma ameaça cibernética?


- “Qualquer circunstância ou evento com potencial para impactar negativamente as operações organizacionais, ativos organizacionais ou indivíduos por meio de um sistema de informação por meio de acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço” – NIST
- “Uma ameaça cibernética é uma atividade que visa comprometer a segurança de um sistema de informação, alterando a disponibilidade, integridade ou confidencialidade de um sistema ou das informações que ele contém, ou interromper a vida digital em geral.” – CCCS

Ameaças x Ataques Cibernéticos

- Uma ameaça cibernética é um perigo potencial — representa a possibilidade de uma tentativa maliciosa de danificar ou interromper um sistema, roubar dados ou causar danos.
-
- ✓ Trata-se de possibilidade ou intenção, não de ação
 - ✓ Envolve agentes de ameaças (por exemplo, hackers, Estados-nação, agentes internos)
 - ✓ Inclui coisas como malware, vulnerabilidades e campanhas de phishing — mesmo que nenhum ataque real tenha ocorrido ainda

Ameaças x Ataques Cibernéticos

- Um ataque cibernético é um evento real — ocorre quando uma ameaça se torna realidade e alguém age para comprometer ou danificar um sistema.

 É a execução de uma ameaça

 Resulta em acesso não autorizado, roubo de dados, interrupção de serviços, etc

 Frequentemente rastreado até um agente de ameaça que utiliza ferramentas como malware ou phishing


Ameaças x Ataques Cibernéticos

Funcionalidade	Ameaça Cibernética	Ataque Cibernético
Definição	Potencial ação ou intenção maliciosa	Atividade maliciosa real
Estágio	Pré-incidente / possibilidade	Estágio de execução/incidente
Envolvidos	Atores de ameaças, vulnerabilidades	Exploits, malware, phishing, etc.
Impacto	Nenhum impacto direto ainda	Impacto direto: perda de dados, indisponibilidade do serviço
Exemplo	Descoberta de novo malware	Malware é usado para violar um sistema

Malware

- Malware significa software malicioso. É qualquer software projetado intencionalmente para causar danos a computadores, redes, servidores ou dados — ou para obter acesso não autorizado a eles. Ele pode:
- Roubar informações (senhas, dados de cartão de crédito)
- Destruir ou criptografar arquivos
- Espionar usuários
- Interromper operações comerciais
- Sequestrar dispositivos para ataques posteriores (como em botnets)

Como o malware funciona?

 Pense no malware como um parasita digital: ele entra sorrateiramente, se esconde e causa danos, a menos que seja interrompido

1. Entrega ou Ponto de Entrada
2. Execução
3. Persistência
4. Comunicação

Principais tipos de malware

Tipo	O que faz	Exemplo Real
Virus	Anexa-se a arquivos legítimos e se espalha quando os arquivos são executados	Michelangelo, CIH
Worm	Espalha-se pelas redes sem ação do usuário	ILOVEYOU, WannaCry
Trojan	Finge ser um software legítimo, mas causa danos	Zeus Trojan
Infostealer	Extraí credenciais, histórico do navegador e senhas salvas	RedLine, Vidar
Ransomware	Criptografa arquivos e exige pagamento pela descriptografia	Ryuk, LockBit, REvil
Spyware	Monitora silenciosamente a atividade do usuário	FinFisher, Pegasus
Adware	Exibe anúncios indesejados e pode redirecionar navegadores	Fireball
Rootkit	Esconde malware profundamente no sistema	Necurs
Botnet	Transforma dispositivos em bots para realizar ataques em larga escala	Mirai, Emotet
Fileless Malware	Opera na memória para evitar detecção	Ataques APT usando PowerShell

What Does CIA Stand For?



Tríade CIA

- Confidencialidade - o aspecto da segurança da informação que se preocupa em garantir que os dados sejam acessíveis somente por pessoas autorizadas. É a garantia de que a informação está protegida contra acessos indevidos
- Integridade - é essencialmente sobre manter a exatidão e consistência dos dados ao longo do tempo. Isso significa garantir que as informações não sejam alteradas de forma inadequada ou inapropriada
- Disponibilidade (Availability) - assegura que os sistemas, aplicações e dados estejam disponíveis para os usuários autorizados quando necessários

Origem Histórica dos Malwares

FEBRABAN
/CYBER LAB



Origem dos Malwares – Linha do Tempo por Década

1970s – Conceitos e Protótipos

- **1971 – Creeper** (considerado o primeiro malware)
 - Experimental, infectava sistemas DEC PDP-10 com o SO TENEX
 - Exibia a mensagem: *"I'm the creeper: catch me if you can!"*
 - Não causava dano real; foi neutralizado por outro programa chamado **Reaper**

Origem dos Malwares – Linha do Tempo por Década

1980s – Primeiros Vírus e Disquetes

• 1982 – Elk Cloner

- Um dos primeiros vírus para computadores Apple II
- Espalhava-se por disquetes; exibia poema ao iniciar o sistema

• 1986 – Brain

- Primeiro vírus para PC compatível com MS-DOS
- Criado por dois irmãos no Paquistão para proteger software contra pirataria

• 1988 – Morris Worm

- Criado por Robert Tappan Morris, causou lentidão na ARPANET
- Espalhava-se automaticamente (tipo worm)
- Um dos primeiros casos de malware amplamente disruptivo

Origem dos Malwares – Linha do Tempo por Década

1990s – Explosão e Popularização

- **1995 – Concept**

- Primeiro vírus para documentos do Microsoft Word (macro vírus)

- **1999 – Melissa**

- Espalhava-se via e-mail com anexos do Word
- Infectava contatos do Outlook, causando sobrecarga de servidores

- **1999 – CIH (Chernobyl)**

- Um dos mais destrutivos; corrompia o BIOS, inutilizando o computador

Origem dos Malwares – Linha do Tempo por Década

2000s – Era dos Worms e Criminalização

- **2000 – ILOVEYOU**

- Vírus em forma de carta de amor enviado por e-mail
- Espalhava-se rapidamente, deletava arquivos e comprometia sistemas

- **2003 – Blaster & Slammer Worms**

- Exploração de vulnerabilidades do Windows
- Causavam reinicializações e negação de serviço (DDoS)

- **2004 – Mydoom**

- Considerado um dos worms mais rápidos e danosos da época
- Causava ataques DDoS e abria backdoors

Origem dos Malwares – Linha do Tempo por Década

2010s – Profissionalização e Extorsão

• 2010 – Stuxnet

- Malware altamente sofisticado, sabotava centrífugas nucleares no Irã
- Desenvolvido provavelmente por governos (EUA e Israel)
- Inaugura a era da guerra cibernética

• 2013 – CryptoLocker

- Populariza o conceito moderno de ransomware com pagamento em Bitcoin

Origem dos Malwares – Linha do Tempo por Década

- **2014 – Emotet**

- Começa como trojan bancário, evolui para plataforma modular de infecção em massa

- **2016 – Mirai Botnet**

- Compromete dispositivos IoT para ataques DDoS massivos
- Causa indisponibilidade em serviços como Twitter, Netflix, etc.

- **2017 – WannaCry**

- Ransomware global, explora falha EternalBlue (NSA)
- Infecta hospitais, empresas e governos em mais de 150 países

Origem dos Malwares – Linha do Tempo por Década

2020s – Malware como Serviço e Ameaças Avançadas

- **2020 – SolarWinds**

- Ameaça à cadeia de suprimentos de software
- Implantação de backdoor (SUNBURST) em atualizações de software legítimo

- **2021 – Colonial Pipeline Attack (Ransomware DarkSide)**

- Ataque a infraestrutura crítica nos EUA
- Provoca escassez de combustível temporária

Origem dos Malwares – Linha do Tempo por Década

2020s – Malware como Serviço e Ameaças Avançadas

- **2022 – HermeticWiper (Guerra Cibernética Rússia-Ucrânia)**

- Malware destrutivo usado antes da invasão da Ucrânia
- Apaga dados de sistemas visados

- **2023 – Ransomware Clon (MoveIT breach)**

- Ataca milhares de empresas ao explorar vulnerabilidade em solução de transferência de arquivos
- Enorme vazamento de dados e extorsão em massa

Tendências Atuais e Futuras

- Malware impulsionado por IA (automação de spear phishing e evasão)
- Ataques a supply chain mais frequentes
- Crescimento de malware-as-a-service (MaaS) e afiliados de ransomware
- Foco em dispositivos IoT e sistemas industriais (ICS/SCADA)
- Aumento de infostealers e cryptojackers silenciosos

Tipos de Malware

FEBRABAN
/CYBER LAB



Vírus

- Tipo de malware que se anexa a arquivos ou programas legítimos, replicando-se quando o arquivo infectado é executado. Ele precisa da interação do usuário para ser ativado!
- **Características:**
 - Requer execução manual para se propagar
 - Pode corromper ou apagar dados
 - Geralmente se espalha via arquivos, pendrives, e-mails infectados
 - Depende de um hospedeiro (arquivo ou sistema)
- **Origem:**
 - Primeiros vírus surgiram nos anos 80, como experimentos acadêmicos
 - "Brain" (1986) foi o primeiro vírus para PC amplamente disseminado

Worm

- Malware autônomo, que se propaga automaticamente pela rede, sem depender da ação do usuário ou de arquivos hospedeiros
- **Características:**
 - Explora falhas em redes ou sistemas
 - Pode causar congestionamento de rede e sobrecarga de sistemas
 - Frequentemente usado para espalhar payloads adicionais, como backdoors
- **Origem:**
 - Termo surgiu da ficção científica (livro “The Shockwave Rider”, 1975)
 - Um dos primeiros worms foi o Morris Worm (1988), criado como experimento acadêmico, mas causou danos significativos

Trojans

- Malware que se disfarça como um software legítimo ou útil, mas esconde uma função maliciosa. Não se replica por si só!
- **Características:**
 - Engana o usuário para ser instalado (engenharia social)
 - Pode abrir backdoors, roubar dados, espionar o sistema
 - Costuma ser parte de campanhas de phishing ou downloads suspeitos
- **Origem:**
 - Nome inspirado na história do Cavalo de Troia, da mitologia grega
 - Primeiros trojans apareceram como jogos ou utilitários falsos

Infostealers

- Malwares projetados para roubar informações sensíveis, como credenciais, dados de cartão de crédito, cookies, carteiras de criptomoedas e histórico do navegador.
- **Características:**
 - Roubo silencioso e rápido de dados
 - Foco em navegadores, clientes de e-mail, carteiras cripto e arquivos locais
 - Muitas vezes vendidos como malware-as-a-service (MaaS)
 - Podem ser entregues via phishing, exploit kits ou sites falsos
- **Origem:**
 - Surgiram com o aumento do uso da internet para operações bancárias
 - A popularização se deu com o surgimento de fóruns clandestinos e dark web

Ransomware

- Malware que **criptografa arquivos da vítima** e exige um **resgate (ransom)** em troca da chave de descriptografia.
- **Características:**
 - Pode afetar arquivos locais e compartilhamentos em rede
 - Cria pressão psicológica com ameaças de vazamento ou destruição de dados
 - Evoluiu para ataques duplos: criptografia + extorsão de dados
 - Distribuído via phishing, RDP exposto ou falhas de segurança
- **Origem:**
 - Primeiro caso: **AIDS Trojan** (1989), em disquetes
 - Explosão de casos após 2013, com o surgimento de criptomoedas (ex: Bitcoin)

Adware e Spyware

Adware exibe anúncios indesejados; **Spyware** monitora secretamente a atividade do usuário, coletando dados sem consentimento

Características Adware:

- Redirecionamento de navegador
- Pop-ups excessivos
- Coleta de preferências de navegação

Características Spyware:

- Captura de tela, keylogging, escuta de microfone
- Monitoramento de e-mails e bate-papos
- Pode se esconder como software legítimo

Origem:

- Com o crescimento da publicidade online e monetização de dados
- Muito comum em *freeware* ou aplicativos de terceiros

Rootkits e Botnets

Rootkits são malwares que se **instalam em camadas profundas do sistema**, como kernel ou firmware, para esconder a presença de outras ameaças.

Características:

- Altíssimo nível de privilégio (nível de sistema operacional)
- Difíceis de detectar e remover
- Usados para manter persistência e ocultar atividades maliciosas

Botnets são redes de dispositivos infectados (bots), controlados remotamente por um atacante, geralmente para fins como DDoS, spam ou mineração.

Características:

- Controladas via **C&C (Command and Control)**
- Usadas em ataques massivos e coordenados
- Podem envolver milhões de dispositivos IoT

Cryptominers

São malwares que exploram recursos computacionais (CPU/GPU) da vítima para **minerar criptomoedas**, gerando lucros para os atacantes.

Características:

- Roubam energia e processamento, tornando o sistema lento
- Podem ser instalados via sites comprometidos (*drive-by mining*) ou arquivos maliciosos
- Foco em moedas que permitem mineração anônima, como Monero

Origem:

- Cresceram com o boom das criptomoedas a partir de 2017
- Começaram como scripts JavaScript embutidos em sites (ex: Coinhive)

Como se proteger?

FEBRABAN
/CYBER LAB



Como se proteger contra malwares?

Boas Práticas Gerais

- Mantenha o sistema operacional e softwares sempre atualizados
(corrige vulnerabilidades exploradas por worms, ransomware, rootkits)
- Use soluções de segurança confiáveis (antivírus, EDR, firewall)
(detecta vírus, trojans, spyware, infostealers)
- Evite clicar em links suspeitos ou baixar anexos de e-mails não solicitados
(proteção contra trojans, infostealers e ransomware via phishing)
- Baixe softwares apenas de fontes oficiais e verificadas
(evita adware, spyware, cryptominers embutidos)

Como se proteger contra malwares?

Higiene Digital do Usuário

- Desconfie de ofertas "boas demais para ser verdade"
- Use senhas fortes e únicas com autenticação de dois fatores (2FA)
- Desabilite macros em documentos por padrão

Para Ambientes Corporativos

- Segmentação de rede e controle de acesso (Zero Trust)
- Backup regular e offline dos dados críticos (essencial contra ransomware)
- Monitoramento de comportamento anômalo e logs de eventos (detecção proativa de botnets, rootkits e acesso não autorizado)
- Educação contínua de colaboradores em segurança da informação