Criando o meu primeiro malware

Cassiano Peres

Sobre Mim

- Tecnólogo em Análise e Desenvolvimento de Sistemas (UTFPR)
- Pós-graduado em Defesa Cibernética (UNICIV)
- AWS Certified Architect Solution Associate (2022-2025)
- Apaixonado por criptomoedas e blockchain
- Entusiasta em Cibersegurança
- Futuro Hacker - Pentester

Introdução

- Hoje vamos trocar uma ideia sobre malwares, o que são, o que fazem, o que comem e como ferram com a vida da gente.
- Vamos ver na prática como criar um exemplo de keylogger.

Malwares

Malware (software malicioso) é qualquer software projetado para causar danos a um computador, servidor ou rede.

Tipos

- Vírus: se replica e se espalha ao infectar outros arquivos ou sistemas.
- Worm: se replica automaticamente para outros computadores em uma rede sem a necessidade de hospedeiro.
- Trojan: Disfarçado como software legítimo, para realizar ações maliciosas.
- Ransomware: Sequestra os dados do sistema, criptografando-os e exigindo pagamento (resgate) para liberá-los.

Tipos

- Spyware: captura informações do usuário, como dados pessoais e atividades online.
- Adware: Exibe anúncios indesejados, muitas vezes abrindo portas para outras ameaças.
- Rootkit: Se esconde profundamente no sistema, permitindo controle remoto ou ocultação de outros malwares.
- Keylogger: Captura tudo o que o usuário digita, muitas vezes usado para roubar credenciais de login e dados sensíveis.

Tipos

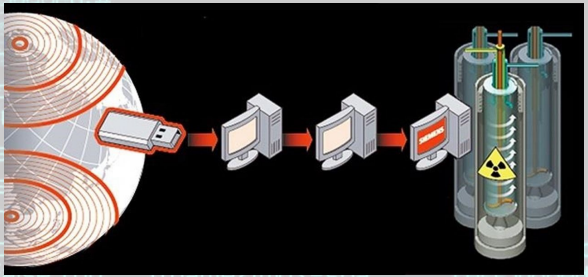
- Botnet: Rede de computadores infectados controlados remotamente - DDoS.
- Backdoor: Cria uma “porta dos fundos” no sistema, permitindo que hackers entrem no sistema sem serem detectados.
- Fileless Malware: Opera na memória do computador, sem deixar rastros em arquivos, dificultando sua detecção.
- Scareware: Induz o usuário ao medo, levando-o a tomar ações que facilitem o ataque.

História

- Anos 80: Surgimento dos primeiros vírus como "Brain" e "Morris Worm".
- Anos 90: Surgimento de trojans e worms mais complexos.
- Anos 2000: Aumento de ataques e sofisticação, ransomwares.
- Anos 2010: Malwares para dispositivos móveis; ataques mais direcionados e complexos.
- Anos 2020: Guerra cibernética, ciberspy.

Casos notáveis

- ILoveYou
- Stuxnet
- WannaCry
- Zeus



Motivações

- Financeiras: Roubo de dados bancários, ransomware, adware.
- Espionagem: Coleta de informações governamentais ou corporativas.
- Hacktivismo: Promoção de causas políticas ou sociais.
- Competição: Sabotagem entre empresas.
- Curiosidade/Desafio: Interesse técnico.

Estrutura

- Dropper/Loader: Componente responsável por instalar o malware no sistema.
- Exploit: Código que aproveita vulnerabilidades em softwares ou sistemas para permitir a execução do malware.
- Payload (Carga útil): Parte do malware que executa a ação maliciosa.

Técnicas

- Obfuscação: Esconde o código malicioso para evitar detecção por antivírus e análises.
- Criptografia de comunicação: Protege os dados enviados entre o malware e o servidor de controle (C&C).
- Evasão de sandbox: Detecta ambientes de análise virtualizados para evitar ser executado neles.
- Escalação de privilégios: Ganha permissões elevadas para controlar o sistema ou modificar configurações críticas.
- Injeção de código: Insere código malicioso em processos legítimos para ocultar sua execução.

Técnicas

- Persistência: Garante que o malware continue ativo após reinicializações ou logouts do usuário.
- Movimentação lateral: Se espalha dentro da rede para infectar outros dispositivos.
- Keylogging: Captura teclas digitadas.
- Desativação de segurança: Desabilita ou remove software de segurança para evitar detecção.
- Exfiltração de dados: Roubo de dados.

Técnicas

- Botnet control: Permite controlar múltiplos dispositivos infectados remotamente para ataques coordenados.
- Anti-forense: Apaga ou modifica registros de log para dificultar a análise de incidentes.
- Phishing: Engana usuários para que executem ou permitam a instalação do malware.
- Ransomware encryption: Criptografa arquivos do usuário para extorquir pagamento em troca da chave de descriptografia.

Ferramentas

- Ambientes de Desenvolvimento: Visual Studio, GCC, etc.
- Linguagens de Programação: C, C++, Python, Assembly.
- Frameworks e Bibliotecas: Metasploit, Veil, SET (Social Engineering Toolkit).
- Ferramentas de Obfuscação: Themida, VMProtect.
- Análise e Debug: OllyDbg, IDA Pro, Wireshark.

Análise

Análise Estática: Estudo do código do malware sem executá-lo.

- Ferramentas: IDA Pro, Ghidra.

Análise Dinâmica: Execução do malware em um ambiente controlado.

- Ferramentas: Sandboxie, Cuckoo Sandbox.

Análise de Memória: Inspeção da memória do sistema para identificar comportamentos maliciosos.

- Ferramentas: Volatility, Rekall.

Proteção

- Manter software atualizado
- Senhas Fortes e 2FA
- Educação e conscientização
- Backup regular
- Monitoramento contínuo
- Políticas de segurança

O futuro dos malwares com a IA

- Malwares adaptativos: Ajustar o comportamento em tempo real para evitar detecção com base nas defesas encontradas.
- Autonomia total: Operar e se espalhar sem a necessidade de controle humano, tomando decisões próprias.
- Ataques personalizados: Criar ataques sob medida para cada alvo, aumentando a eficiência de phishing e ransomware.
- Evasão avançada: Identificar e evitar ambientes de análise ou detecção, tornando-se mais furtivos.
- Uso de deepfakes: Enganar usuários e sistemas de autenticação, facilitando fraudes e invasões.

Links úteis

- Malware bazaar: https://bazaar.abuse.ch/
- MalAPI: https://malapi.io/
- VirusTotal: https://www.virustotal.com/

Exemplo

Vamos ver como funciona um keylogger que envia em tempo real para o servidor as teclas acionadas pelo usuário.

GitHub: https://github.com/devs-cassiano/udc-xi-seicom

Perguntas?

GitHub: devs-cassiano

LinkedIn: peres-cassiano