Resumo de Informática

Definição de malware

Códigos maliciosos (Malwares, do inglês Malicious Softwares) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

Formas comuns de infecção de malwares

Pela exploração de vulnerabilidades existentes nos programas instalados ou pela auto-execução de mídias removíveis infectadas, como pen-drives;

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 10.

Pelo acesso a páginas maliciosas, utilizando navegadores vulneráveis ou pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas web ou de outros computadores.

Principais Categorías de Malwares

- VÍRUS
- WORM
- BOT
- TROJAN
- SPYWARE
- BACKDOOR
- ROOTKIT

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 10.

Definição de vírus

Programa ou parte de um programa, normalmente malicioso, que se propaga infectando, inserindo cópias de si mesmo, anexando-se ou hospedando-se em arquivos ou programas existentes na máquina.

Tipos de vírus

- **VÍRUS DE SCRIPT**
    - Escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML.
- **VÍRUS DE MACRO**
    - Tipo específico de vírus de script normalmente recebido ao acessar páginas web ou por e-mail e que tenta infectar arquivos manipulados por aplicativos que utilizam essas linguagens mencionadas anteriormente como os arquivos que compõem o Microsoft Office.

- **VÍRUS DE BOOT**
    - Também conhecido como Vírus de Setor de Carga ou Vírus de Setor de Inicialização, ele é ativado quando o computador é ligado e é carregado na memória antes do sistema operacional.
- **VÍRUS DE ARQUIVO**
    - Também conhecido como Vírus de Programa ou Parasitário, trata-se do vírus mais tradicional e comum. Ele infecta e causa danos ao se conectarem a arquivos executáveis (.exe, .com, .dll, etc), sobrescrevendo o código original e causando danos quase sempre irreparáveis.
- **VÍRUS POLIMÓRFICO**
    - Também conhecido como Vírus Mutante, é capaz de assumir múltiplas formas a cada infecção com o intuito de burlar o software de antivírus.
- **VÍRUS METAMÓRFICO**
    - Trata-se de um vírus que se transforma a cada infecção, mas que – diferentemente do polimórfico – se reescreve completamente a cada infecção, podendo mudar seu tamanho e comportamento, aumentando a dificuldade de detecção.
- **VÍRUS STEALTH**
    - Projetados explicitamente para não serem detectados pelo antivírus e têm a capacidade de se remover da memória temporariamente para evitar que o antivírus o detecte.

- **VÍRUS TIMEBOMB**
    - Conhecido como Vírus Bomba Relógio, trata-se de um vírus que – após infectar a máquina – permanece latente (oculto), apenas se replicando, e seu código malicioso é programado para ser ativado em um determinado momento específico, executando sua carga útil.

Tipos de malwares

- **WORM**
    - Worm (ou Verme) é um programa capaz de se replicar automaticamente, enviando cópias de si mesmo. Diferente dos vírus, ele não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos através da rede, mas – sim – pela exploração automática de vulnerabilidades existentes em programas instalados em computadores ou pela execução direta de suas cópias.
- **BOT**
    - Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do Worm, ou seja, é capaz de

se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

- **BOTNET**
    - Rede formada por centenas ou milhares de computadores zumbis e que permitem potencializar as ações danosas executadas pelos bots.
- **CAVALO DE TROIA**
    - O Trojan é um programa que age utilizando o princípio do Cavalo de Troia, em um arquivo é enviado se fazendo passar por um aplicativo útil, como um "presente de grego", mas que na verdade possui funcionalidades maliciosas escondidas. Muitas vezes, o trojan abre portas de comunicação para que através da Internet a máquina possa ser invadida ou monitorada.
- **RANSOMWARE**
    - Trata-se de um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, e que exige pagamento de um resgate (Ransom, em inglês) para restabelecer o acesso ao usuário – trata-se de uma espécie de extorsão virtual.
- **SPYWARE**
    - Software espião, capaz de violar a privacidade das informações de usuários, coletando dados da máquina ou da rede e disponibilizando-as a terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de

como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.

- **KEYLOGGER**
    - Trata-se de um spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador e enviá-las a um invasor.
- **SCREENLOGGER**
    - Trata-se de um spyware – similar ao keylogger – capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.
- **ADWARE**
    - Trata-se de um spyware projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos quando as propagandas são direcionadas.
- **SNIFFER**
    - Um Sniffer é programa que age monitorando o tráfego na rede, através da captura de pacotes de dados, em busca de informações sensíveis como o endereço dos sites acessados, senhas de acesso, e-mails, etc.

- **BACKDOOR**
    - Um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
- **ROOTKIT**
    - Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
- **BOMBAS LÓGICAS**
    - Trata-se de um software malicioso normalmente instalado por um usuário autorizado, como um administrador da rede, que o mantém no sistema deixando-o programado para causar danos (como excluir arquivos importantes) em um determinado evento, como por exemplo o caso de ficar mais de 30 dias sem efetuar login.
- **EXPLOITS**
    - Trata-se de um software criado por hackers para permitir explorar vulnerabilidades conhecidas de sistemas e assim permitir que iniciantes (Script Kiddies) possam praticar ações de invasões sem conhecimentos avançados.

- **HIJACKER**
    - O Hijacker (sequestro, em inglês) é um software malicioso que modifica o registro do sistema operacional, alterando o funcionamento do navegador, modificando sua página inicial, abrindo páginas automaticamente, inserindo botões inadvertidamente.

Tipos de ataques

- **ENGENHARIA SOCIAL**
    - Trata-se de uma técnica muito utilizada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança.
- **FORÇA BRUTA**
    - Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário. Qualquer computador,

equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta.

- **NEGAÇÃO DE SERVIÇO**
    - Negação de serviço (Denial of Service – DoS) é uma técnica pela qual um atacante busca retirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (Distributed Denial of Service – DDoS).
- **IP SPOOFING**
    - O IP Spoofing (Falsificação/Mascaramento de IP) é uma técnica de invasão comumente empregada quando o mecanismo de autenticação de uma rede é baseado em endereços IP, isto é, quando a identificação de um usuário é realizada baseado em seu número de endereço IP.
- **E-MAIL SPOOFING**
    - Técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Essa técnica é possível devido a características do protocolo SMTP (Simple Mail Transfer Protocol) que permitem que campos do cabeçalho sejam falsificados.

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 10.

- **PHISHING SCAM**
    - Fraude em que o golpista tenta enganar um usuário para obtenção de dados pessoais e financeiros que permitam a aplicação de um golpe, combinando técnicas computacionais e de engenharia social. Um exemplo de phishing é um e-mail que possa induzir o usuário a clicar em um link falso levando-o para uma página clonada ou um arquivo malicioso.
- **PHARMING**
    - Ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original. É um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS. Nesse caso, quando o usuário tenta acessar um site legítimo, o navegador web é redirecionado, de forma transparente, para uma página falsa.
- **HOAX**
    - Trata-se de uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.

- **MAN IN THE MIDDLE**

- Trata-se de um ataque em que os dados trocados entre duas partes são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. Durante o ataque, a comunicação é interceptada pelo atacante e retransmitida. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação.

- **DEFACEMENT**
  - Trata-se de uma técnica que consiste em alterar o conteúdo da página web. Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente os atacantes alteram a página principal do site, porém páginas internas também podem ser alteradas.

Códigos maliciosos

- **FORMAS DE OBTENÇÃO**

	VÍRUS	WORM	BOT	TROJAN	SYPWARE	BLACKDOOR	ROOTKIT
Recebido automaticamente pela rede		X	X				
Recebido por e-mail	X	X	X	X	X		
Baixado de sites na Internet	X	X	X	X	X		
Compartilhamento de arquivos	X	X	X	X	X		
Uso de mídias removíveis infectadas	X	X	X	X	X		
Redes sociais	X	X	X	X	X		
Mensagens instantâneas	X	X	X	X	X		
Inserido por um invasor		X	X	X	X	X	X
Ação de		X	X	X	X	X	X

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 10.

outro código malicioso							

- **FORMA DE INSTALAÇÃO**

	VÍRUS	WORM	BOT	TROJAN	SYPWARE	BLACKDOOR	ROOTKIT
Execução de um arquivo infectado	X						
Execução explícita do código malicioso		X	X	X	X		
Via execução de outro código malicioso						X	X
Exploração de vulnerabilidades		X	X			X	X

- **FORMA DE PROPAGAÇÃO**

	VÍRUS	WORM	BOT	TROJAN	SYPWARE	BLACKDOOR	ROOTKIT

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 10.

Execução de um arquivo infectado	X						
Execução explícita do código malicioso		X	X				
Via execução de outro código malicioso		X	X				
Exploração de vulnerabilidades				X	X	X	X

- **AÇÕES MALICIOSAS MAIS COMUNS**

	VÍRUS	WORM	BOT	TROJAN	SYPWARE	BLACKDOOR	ROOTKIT
Altera e/ou remove arquivos	X			X			X
Consome grande quantidade de recursos		X	X				
Furta informações sensíveis			X	X	X		
Instala outros códigos maliciosos		X	X	X			X

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 10.

Possibilita o retorno do invasor						X	X
Envia spam e phishing			X				
Desfere ataques na Internet		X	X				
Procura se manter escondido	X				X	X	X

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 10.