VOLTAR

# Segurança de Sistemas Operacionais

Abordar a importância da segurança no Sistema Operacional (SO).

NESTE TÓPICO



Marcar tópico

## Introdução

Desde os primeiros computadores a preocupação com a segurança teve grande peso na área de informática pelo simples fato de que informações que não são íntegras não são confiáveis, logo, não faz sentido armazenar e/ou utilizar informações não confiáveis.

O Sistema Operacional (SO) é o software que gerencia todo o hardware e os outros softwares, além de cuidar das informações nos computadores.

O SO é o principal envolvido na garantia da segurança dos computadores e tem como funções principais:

- Criar uma camada de controle entre o hardware e as aplicações;
- Gerenciá-las de forma segura, rápida e inteligente.

O avanço computacional fez com que surgissem novos SO, com novas funcionalidades e novos aplicativos, um grande exemplo foi a criação da rede de computadores (década de 80) que interliga um computador a outro e

também a grande rede mundial, a Internet (“www”: World Wide Web), mas toda essa evolução teve um preço: a segurança das informações foi e continua cada vez mais violada.

Windows, Linux e Mac são três exemplos de Sistemas Operacionais mais presentes nos computadores, ou seja, são os chamados de terceira geração. Cada um deles possui um conceito próprio de segurança, rotulado pelo mercado:

### Windows

Desenvolvido pela empresa Microsoft, tem a preferência mundial, tanto para utilização doméstica (uso em cada, particular) como corporativa (nas empresas). Está instalado na grande maioria dos computadores de todo o mundo. Porém se tratando de segurança, muitos profissionais de TI descartam o Windows por ter uma ampla quantidade de usuários, ou seja, quanto mais popular, mais aplicativos e ferramentas estarão à disposição dos usuários, tendo como referência uma maior manifestação de malicias dos hackers.

### Mac OS X

O MacOS desenvolvido pela empresa Apple, tem sua seleção de uuários em função do seu elevado custo: é o sistema operacional mais caro do mercado. É um SO bem detalhado e funcional, e também possui belos temas. No quesito segurança, o Mac é bem instável devido a pouca popularidade. Por não ser comercializado em sistemas computacionais que utilizam Linux e Windows (PCs), o Mac não é atingido por vírus desses sistemas. Apesar de possuir um sistema pouco diferente e não ter brechas de seguranças parecidas com Windows e Linux, nenhum sistema possuí 100% de segurança e está sempre vulnerável.

### Linux

O Linux, por sua vez é um sistema totalmente funcional, principalmente para servidores de web, e também preferido por desenvolvedores de sistemas e aplicativos por possuir código aberto e ser totalmente editável. Devido o Linux ser pouco popular por usuários comuns, isso pode representar uma segurança mais aprimorada neste caso, mais quando o assunto está relacionado aos servidores isso pode mudar.

### Vírus em Sistemas Operacionais

Vírus são um dos problemas mais abrangentes que podemos enfrentar em segurança de sistemas operacionais, vírus causam enormes problemas e chegam causar milhões em prejuízos financeiros em todo o mundo. Um Vírus é um programa projetado para infectar outros programas e causar algum

dano. Ele se aproveita de falhas na segurança, brechas deixadas por programadores em seus sistemas para se instalar e infectar em outras maquinas que estejam conectadas na mesma rede.

Os SO de computadores Mainframes não são suscetíveis a ataques de virus, em contra partida, os Mainframes são utilizados somente por empresas que possuem grandes volumes de dados para processamento e estejam dispostas a arcar também com altos custos.

Geralmente, os vírus agem de maneira simples:

- Primeiro tentam se esconder da melhor maneira possível;
- Depois ele tenta se replica: infectar outros programas ou computadores que estejam na mesma rede;
- Após infectar cumprem seu papel para o qual foi escrito: roubar dados, espionar ou até mesmo danificar o equipamento.

Os Vírus podem ser categorizados em diversos segmentos, abaixo citamos alguns:

### Vírus de programa executáveis

Um vírus de programa executável é complex: suas ações consistem em sobrepor o arquivo executável de um programa com seu próprio código binário e quando o usuário invocar esse programa o vírus é executado. Essa técnica chama se vírus sobreposição. Outra tática desse tipo de vírus é de alterar o atalho do programa executável para que execute primeiramente o vírus e depois execute o programa invocado pelo atalho sem que o usuário perceba. Esse tipo de vírus é geralmente disseminado junto com programas pagos que são crakeados e levam junto com seu executável o código malicioso ou infectam o equipamento invadindo e se multiplicando anexando seu próprio código a outros programas.

### Vírus de memória

Um vírus de memória ao contrário de um vírus de programa executável ele fica residente na memória por um longo período alocado na parte superior da memória ou nas inferiores onde é raramente utilizado pelo sistema. Alguns vírus têm até mesmo a capacidade de disfarçar esse espaço de memória onde estão alocados como espaço em uso para evitar que seu código se sobrescrito pelo sistema. Esses tipos de vírus podem fazer alterações no controle de chamadas ao sistema.

### Vírus de setor de boot

O computador quando é ligado faz uma leitura de um pequeno programa gravado em sua placa mãe que chamamos de BIOS, esse pequeno espaço de memória é lido e executado, nele o computador encontra informações sobre o funcionamento da placa mãe e a localização do setor de boot. Na maioria dos computadores modernos esses programas da BIOS podem ser reescritos, o que permite o fabricante lançar atualizações e correções do programa, mas também abre uma brecha na segurança. Um vírus que consegue reescrever a BIOS pode danificar o setor de boot impedido que o sistema operacional carregue, ou até mesmo que carregue o vírus juntamente com o S.O.

### Vírus de drivers de dispositivo

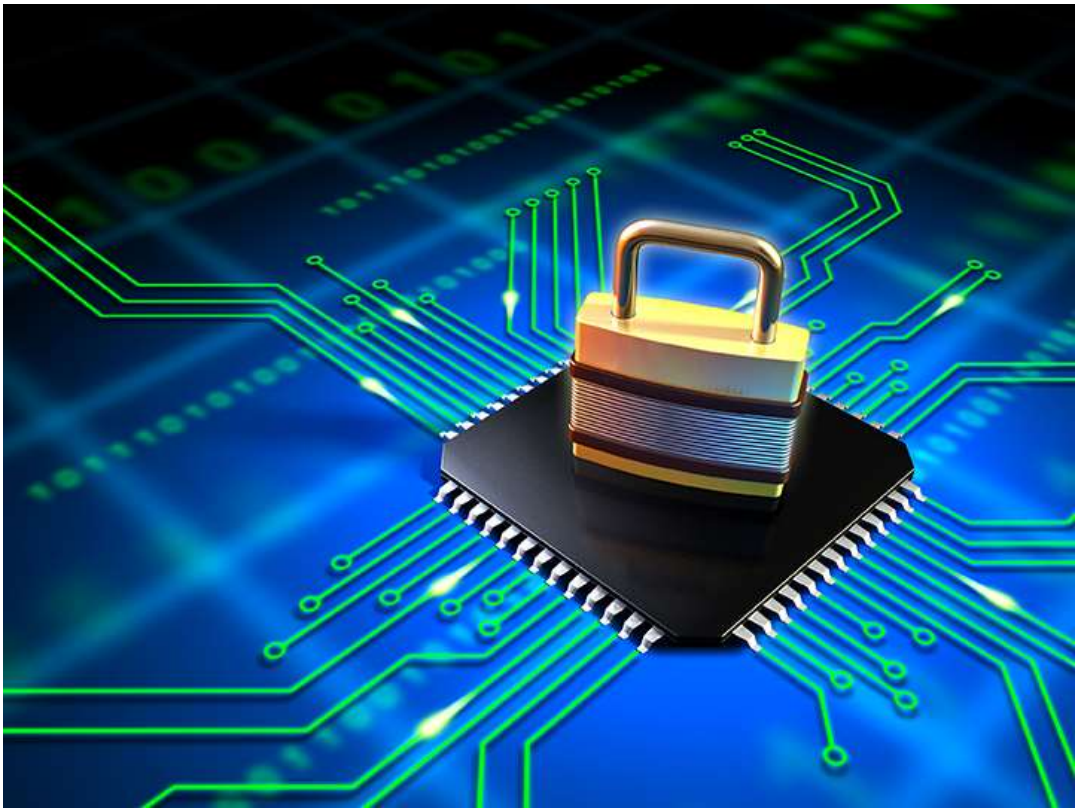
É um vírus parasita que consegue infectar um driver de dispositivo e, com isso, terá a oportunidade de ser carregado diretamente no sistema durante o processo de boot sem muita dificuldade e com uma grave consequência, os drivers são carregados em modo Kernel (Núcleo: instruções privilegiadas)) o que permite ao vírus capturar o controle das Chamadas ao Sistema. (System Calls).

### Vírus de macro

Programas como o Word, Excel e Power Point da Microsoft permitem a criação de macros usando linguagem Visual Basic que é uma linguagem de programação completa. As macros existem para permitir que o usuário carregue uma sequência de comandos gravados. Porém isso também permite que vírus possam ser codificados usando Visual Basic. Um vírus de macro pode apagar arquivos, modificar propriedades e causar grandes transtornos. Importante lembrar que sempre que um arquivo com macro for aberto o programa informa que existem macros no arquivo e pergunta se deseja executar, se executar e a macro for um código malicioso é problema na certa.

### Vírus de código fonte

Um vírus de código fonte consiste em um programa que buscam, por exemplo, arquivos de códigos em C e faz a alteração de arquivo incluindo seu próprio código no contexto do código original de maneira que quando o arquivo for copilado o vírus também é copilado e executado junto ao programa aparentemente seguro. É possível que o programador desconfie da alteração do seu próprio código, mas na maioria das vezes os códigos mal organizados facilitam essa pratica de manipulação de arquivo.



Segurança: sempre é uma grande preocupação!

## IMPORTANTE:

Atualmente, é comum lermos ou ouvirmos nas mídias “Hackers invadiram...” ou “Hackers roubaram as informações da...” ou ainda “Hackers derrubaram o site...”.

Há muito tempo, o comproimetimento da segurança dos computadores vem sendo equivocadamente divulgado pelas mídias.

**Hackers** não praticam atos ilícitos digitais, não sao criminosos digitais, antes são exímios profissionais, especialistas altamente técnicos e responsáveis. Foram Hackers que ajudaram grandemente nas estratégias de segurança dos computadores, desenvolvimento e aprimoração de SO e programas antivirus.

Os responsáveis pelos crimes digitais são os **Crackers**, o nome vem de “quebra”. História: no final da década de 80 e início de 90, tendo ciência de seu conhecimento técnico e das vulnerabilidades dos computadores, alguns Hackers resolveram praticar atos ilícitos: fazer o mal e causar prejuízos. Os outros Hackers os nomearam de Crackers para que sua imagem não fosse afetada.

Cracker

A escolha de um SO pode ser dada por muitos motivos, desde a lista de aplicativos compatíveis a ele, quanto aos próprios recursos oferecidos pelo SO.

A segurança da execução do SO aplica-se a requisitos que vão além dos softwares antivírus ou outros específicos para segurança.

Os três SO citados tem seus pontos negativos com falhas de segurança, porém é importante citar que todos são atualizados constantemente com correções. Ainda, a vulnerabilidades dos sistemas estão ligadas ao grau de comportamento de cada usuário, salientando que a atuação comercial do SO é também muito significativa para que um Cracker se empenhe ou não em fabricar um programa malicioso para quais fins este desejar.

Este tópico finaliza aqui, esperamos que você tenha entendido a importância da segurança nos sistemas operacionais.

Bom estudo!

## Quiz

Exercício

Segurança de Sistemas Operacionais

INICIAR

Quiz

Exercício Final

Segurança de Sistemas Operacionais

INICIAR

# Referências

DEITEL, H. M.; DEITEL, P. J.; CHOFFNES, D. R. Sistemas operacionais. 3. ed. São Paulo: Pearson Prentice Hall, 2005.

TANENBAUM. Andrew. Sistemas operacionais modernos, New Jersey; Prentice Hall; 2a; 2008.

Site Security Report: Windows e Linux. The Register. Disponível em: <**theregister.co.uk (http://www.theregister.co.uk/2004/10/22/security_report_windows_vs_linux/)**>. Acesso em 03/05/2016.

Site Portal SIS – Sistemas de Informação. Disponível em: <**portalsis.wordpress.com (https://portalsis.wordpress.com/2011/06/15/seguranca-em-sistemas-operacionais/)**>. Acesso em 03/05/2016.

Avalie este tópico

ANTERIOR
Gerenciamento de Entrada e Saída

Índice

Biblioteca (https://www.uninove.br/conheca-a-uninove/biblioteca/sobre-a-biblioteca/apresentacao/)
Portal Uninove (http://www.uninove.br)
Mapa do Site



Ajuda? (https://ava.unidCurso=)