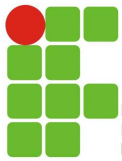
Segurança de Redes

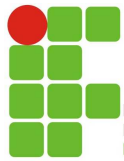
Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 02
Principais Ataques de Segurança da Informação (Parte 01)



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"Problemas são estímulos que a Vida nos apresenta para nos autoconhecer." (Hammed)



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Entender o que são ataques;
- Aprender os principais ataques;
- Conhecer alguns as características de alguns ataques.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Ataques de Segurança da Informação

A Internet se tornou essencial para a sociedade moderna. Mas atrás de toda essa utilidade existe vilões que tentam causar problemas danificando nossos computadore, violando nossa privacidade e tornando inoperantes os serviços da rede dos quais dependemos.

Dadas a frequência e a variedade das ameaças existentes, bem como o perigo de novos e mais destrutivos futuros ataques, a segurança se tornou um assunto principal na área de redes de computadores.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Os principais ataques de segurança da informação são:

- Códigos maliciosos (*Malwares*) para apagar nossos arquivos, monitorar atividades, coleta informações particulares, etc.
- Atacar servidores, serviços e infraestrutura de redes
  - Negação de serviço (DoS e DDoS);
  - Desfiguração de página (*Defacement*);
  - Força bruta (*Brute force*);
- Analisar pacotes e lixo da empresa para obter informações:
  - Varredura em redes (*Scan*);
  - Interceptação de tráfego (*Sniffing*);
  - Dumpsterdiving ou trashing.
- Se passar por alguém de sua confiança ou falsificar informações de rede.
  - Engenharia Social.
  - IP, DNS e e-mail spoofing.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

São programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das formas como eles podem infectar ou comprometer um computador são: pela exploração de vulnerabilidades existentes nos programas, auto-execução de mídias removíveis infectadas (como pen-drives), phishing (e-mail ou mensagem de texto fingindo ser de uma fonte confiável), anexos maliciosos, downloads maliciosos, engenharia social (manipulação psicológica de pessoas) ou acesso a páginas Web maliciosas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Um *malware* pode provocar: perda de desempenho do micro, exclusão de arquivos e alteração de dados, acesso a informações confidenciais por pessoas não autorizadas, perda de desempenho da rede e desconfiguração do Sistema Operacional.

A detecção de qualquer tipo de malware depende, sobretudo, de um software específico: o chamado de "antivírus". Mesmo as opções gratuitas mais simples terão mecanismos de monitoramento em tempo real que são capazes de identificar estes softwares maliciosos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares

Os principais tipos de *malwares* são: Vírus, *Worms*, Bot e *botnet*, *Trojans*, *Spywares*, *Backdoor* e *Ransomware*.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Vírus

É um pedaço de código que se insere em um aplicativo e é executado quando o aplicativo é executado. Ele ficará inativo até que o arquivo ou programa hospedeiro infectado seja ativado. Quando isso acontece, o vírus pode se replicar e se espalhar através de seus sistemas. Os vírus normalmente são usados para roubar dados sensíveis ou lançar outros ataques.

Os vírus são bem específicos, ou seja, um determinado vírus só ataca apenas algumas versões de determinados programas onde ele explora determinada vulnerabilidade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Malwares - Vírus

I Love You tratava-se de um script em Visual Basic disfarçado de uma carta de amor vinda de um conhecido (por e-mail). Foi criado em 2000 nas Filipinas, e danificava a máquina local Windows e mandava uma cópia de si mesmo para todos os contatos do usuário no Outlook. Dentro de dez dias, mais de 50 milhões de computadores foram infectados, e estima-se que o vírus tenha afetado 10% dos dispositivos conectados à rede mundial de computadores, causando um prejuízo da ordem de 8 bilhões de dólares.

Chernobyl é um dos vírus mais nocivos que já existiu. Ele corrompia a BIOS e o MBR (*Master Boot Record*) dos sistemas infectados. Dessa forma, os computadores não inicializavam. Estima-se que 60 milhões de computadores foram infectado pelo vírus, resultando em cerca de US $ 1 bilhão de dólares em prejuízos.

EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Malwares - Worm

Worm (ou verme) é um programa malicioso mais comum. Ele é capaz de se propagar automaticamente sem necessidade de hospedeiros e sem exigir ação de ninguém, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores. Além disso, podem excluir arquivos em um sistema host, criptografar dados para um ataque de ransomware, roubar informações, excluir arquivos e criar botnets.

Malwares - Worm

SQL Slammer era um conhecido worm de computador que gerava endereços IP aleatórios e se enviou para eles, procurando por aqueles que não estavam protegidos por software antivírus. Logo após ter sido atingido em 2003, o resultado foi mais de 75.000 computadores infectados involuntariamente envolvidos em ataques DDoS em vários sites importantes.

MyDoom é um worm que se espalha por e-mail. Estima-se que ele reduziu a velocidade global da internet em 10%. Ele aproveitou vulnerabilidades no Outlook (gerenciador de e-mails da Microsoft) para obter endereços e enviar e-mails. Os computadores foram programados para lançar ataques aos sites da Microsoft e de uma empresas de segurança em informática.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Bot e Botnet

Bot é um programa malicioso que dispõe de mecanismos de comunicação com o invasor e permite que ele seja controlado remotamente. Ele possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente. A comunicação entre o invasor e o computador infectado pode ocorrer via canais de IRC, servidores *Web* e redes do tipo P2P, entre outros meios.

Um computador infectado por um *bot* costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Bot e Botnet

Algumas das ações maliciosas que costumam ser executadas por intermédio de *bot* são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante.

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Bot e Botnet

Geinimi foi desenvolvido para a plataforma móvel Android. O Geinimi é instalado em *smartphones* junto com *games* adulterados, que podem ser encontrados em sites. O *malware* se comunica com um servidor central, que pode, remotamente, enviar comandos para um celular, como baixar ou desinstalar um *software*. Entre os dados enviados estão a localização do dispositivo e detalhes do *hardware* e *software*.

Conficker bloqueia o acesso a *websites* destinados à venda de produtos de sistemas de segurança. Em janeiro de 2009, o número estimado de computadores infectados chegou a 15 milhões. O custo causado pelo Conficker foi estimado em até US $ 9 bilhões.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Spyware

É um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Os três principais tipos de Spywares são:

- *keylogger*: captura e armazena as teclas digitadas pelo usuário.
- *Screenlogger*: capaz de armazenar a posição do cursor e a imagem da tela apresentada no monitor, nos momentos em que o mouse é clicado.
- *Adware*: projetado especificamente para monitorar os usuários e apresentar propagandas sem o consentimento do usuário.
- *Stalkerwares*: são normalmente utilizado para rastrear violência doméstica, traição de cônjuges e suspeitos de crimes. Eles permite, por exemplo, rastrear a localização em tempo real, acessar o registro de chamadas, ler mensagens, ter aceso a câmera e microfone do aparelho, etc.

Malwares - Spyware

CoolWebSearch surgiu em 2003 e utilizava as vulnerabilidades de segurança do Internet Explorer para controlar o browser, alterar as configurações, e enviar os dados de navegação para o seu criador.

Zlob surgiu em 20005 e usava vulnerabilidades no codec ActiveX para se descarregar a si próprio para um computador e gravar históricos de pesquisa e de navegação, bem como as teclas pressionadas pelo utilizador.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Backdoor

São programas maliciosos, também conhecidos por portas dos fundos, que permite o acesso de um invasor a um computador comprometido contornando a autenticação. A partir daí, ele pode ser usado para obter acesso a informações privilegiadas como senhas, excluir dados em discos rígidos, instalar outros *malwares* ou transferir informações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Malwares - Backdoor

WordPress *Backdoor*: eram propagadas em cópias não licenciadas de plug-ins do WordPress. Eles são inseridos como código JavaScript ofuscado e cria uma conta de administrador no banco de dados do site.

Borland Interbase Backdoor, o banco de dados da Borland Interbase versões 4.0 a 6.0 tinha um backdoor, colocado lá pelos desenvolvedores. O servidor continha uma conta, que pode ser acessada através de uma conexão de rede. Este usuário pode assumir o controle total sobre todos os dados do Interbase. A porta dos fundos foi detectada em 2001 e um patch foi lançado.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Trojan

É um programa malicioso, também conhecidos por cavalo de tróia, que além de executar as funções para as quais foi aparentemente projetado (por exemplo, jogos), também executa outras funções sem o conhecimento do usuário. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Por definição, o cavalo de tróia distingue-se de um vírus ou de um *worm* por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Trojan

Emotet banking, surgiu em 2014, ele foi projetada para roubar detalhes de contas bancárias, informações financeiras e carteiras de Bitcoin. Ele se propaga principalmente por meio de e-mails de spam.

Twelve Tricks, surgiu em 1990, tinha como objetivo testar o desempenho dos discos rígidos mas também executava códigos maliciosos. O Trojan altera o registro MBR e, a cada reinicialização, instala um dos doze "truques" que causam problemas de hardware ou de operação do computador. Ele também levava a corromper gradualmente o sistema de arquivos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Malwares - Ransomware

Ransomware é um tipo de *malware* que sequestra os dados do computador e exige um resgate para liberá-las.

WannaCry: Em 2017, um ransomware chamado de WannaCry infectou mais de 10.000 organizações e 200.000 pessoas em mais de 150 países. Os hackers mantém os dados do computador invadido criptografados, de forma que o dono não consiga acessá-los, a menos que eles liberem.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Atividade

1. Descreva cinco casos importantes de ataques de *malwares*, apresentando informações sobre o tipo de ataque, quando surgiu, informações de funcionamento, a quantidade de equipamentos afetados e o impacto financeiro para as organizações, e se conseguiram identificar o responsável pelo ataque.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE