CST0201-Ameaças, vulnerabilidades e ataques a Segurança Cibernética: Parte 1 - Tipos de malwares e defesa contra malwares

Data do Post	@June 10, 2022 9:00 AM (GMT)
Status	Done
Palavras-chave	Ameaças vulnerabilidades e ataques a Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

Post- Linkedin

Depois de algum tempo parado e sem postar conteúdos característicos da área em que me dedico como autodidata e profissional, retorno a rotina com mais uma série de cinco (5) artigos com um assunto relevante e interessante, não apenas para os profissionais de tecnologia, mas também para todos os usuários - Ameaças, vulnerabilidades e ataques a Segurança Cibernética.

No processo de utilização da tecnologia, dos usuários mais experientes até aos rookies, todos já ouviram falar pelo menos de um vírus. Nessa série de dois artigos sobre ameaças e vulnerabilidades, estabeleço a diferença entre vírus e outros malwares que, de certa forma, são denominados de forma genérica como vírus. Também falarei sobre a forma que pode mos nos proteger contra essas ameaças e vulnerabilidades.

Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.

Guarde para rever noutro momento.

Compartilha o conteúdo com os amigos e não só

Comente o que acha do conteúdo e da iniciativa e deixe sugestões.

#cybersecurity #technology #linux #programming #hacking #vulnerabilities #maliciouscode #malwares #protection

Introdução

Malwares, do “Malicious Software”, são ameaças virtuais que têm como objectivo executar atividades maliciosas em computadores e smartphones sem o conhecimento ou permissão do usuário Cada um tem o seu próprio comportamento de acordo a intenção da pessoa que o desenvolve O malware pode ser óbvio e simples de identificar ou pode ser muito discretos e quase impossível de detetar.

Existem inúmeros códigos maliciosos, mas, nesse artigo, apresento alguns mais comuns e que com alguma frequência tem feito vítimas.

Tipos de Malwares

Vírus

Um vírus é um código malicioso executável que está anexado a outro arquivo executável, como um programa legítimo. A maioria dos vírus necessita que o usuário final inicie e podem ser ativados a uma hora ou data específica. Os vírus de

computador geralmente são transmitidos através de uma das três formas: de dispositivos removíveis; de downloads na Internet; e de anexos de e-mail.

O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção. Eles podem infectar vários tipos de dispositivos tais como: computadores desktops, computadores portáteis, telemóveis entre outros.

Normalmente o vírus tem controle total sobre o computador, podendo fazer de tudo, desde mostrar uma mensagem de “feliz aniversário”, até alterar ou destruir programas e arquivos do disco.

Para que um computador seja infectado por um vírus, é preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

- Abrir arquivos anexados aos e-mails;
- Abrir arquivos do Word, Excel, etc;
- Abrir arquivos armazenados em outros computadores
- Através do partilha de recursos;
- Instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes, pen drives, CDs, DVDs, etc;
- Ter alguns dispositivos removível (infectado) conectado ou inserido no computador, quando ele é ligado.

Existem vírus que procuram permanecer ocultos, infectando arquivos do disco e executando uma série de actividades sem o conhecimento do usuário. Ainda existem outros tipos que permanecem inativos durante longos períodos, e entram em atividade em datas específicas.

Worms

Worms são programas capazes de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Eles consumem muitos recursos da rede, tornando as redes mais lentas, podendo ocupar espaço no disco duro dos computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar.

Enquanto um vírus requer um programa do host para execução, os worms podem ser executados de modo autônomo. Excepto pela infecção inicial, os worms não necessitam mais da participação do usuário. Após afetar o host, um worm é pode ser transmitido muito rapidamente pela rede. Worms compartilham padrões similares. Todos eles habilitam uma vulnerabilidade, uma maneira de se propagar, e todos eles contêm uma carga.

Os worms são responsáveis por alguns dos ataques mais devastadores na Internet. Por exemplo, em 2001, o worm Code Red infectou 658 servidores. Em 19 horas, o worm infectou mais de 300.000 servidores.

Cavalo de troia

Cavalo de tróia (trojan horse) consiste em um programa, normalmente recebido como um "presente" (um cartão virtual, um álbum de fotos, um protetor de tela ou um jogo), que além de executar funções para as quais foi aparentemente projetado, executa outras normalmente maliciosas e sem o conhecimento do usuário.

Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:

- Roubo de senhas e outras informações sensíveis, como números de cartões de crédito/débito digitadas pelo usuário;
- Inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador;
- Alteração ou destruição de arquivos.
- Acesso e copia de arquivos;

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.

Normalmente um cavalo de tróia consiste em um único arquivo que necessita ser explicitamente executado. Podem existir casos onde um cavalo de tróia contém um vírus ou worm, mas mesmo nestes casos é possível distinguir as ações realizadas como conseqüência da execução do cavalo de tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou worm.

Enquanto estão sendo executados, estes programas podem ao mesmo tempo enviar dados confidenciais para outro computador, instalar backdoors, alterar informações, apagar arquivos ou formatar o disco rígido ou apenas exibirem uma mensagem de erro.

Bombas lógicas

Uma bomba lógica é um código malicioso que utiliza um gatilho para ativar o código malicioso. Por exemplo, os acionadores podem ser datas, horas, outros programas em execução ou a exclusão de uma conta de usuário.

A bomba lógica permanece inativa até que o evento acionador aconteça. Assim que ativada, a bomba lógica implementa um código malicioso que danifica um computador.

Uma bomba lógica pode sabotar os registros de banco de dados, apagar arquivos e atacar sistemas operacionais ou aplicativos. Recentemente, foram descobertas bombas lógicas que atacam e destroem os componentes de hardware em uma estação de trabalho ou servidor, incluindo as ventoinhas, CPU, memória, discos rígidos e fontes de alimentação. A bomba lógica sobrecarrega esses dispositivos até o superaquecimento ou falha.

Ransonware

O ransomware aprisiona um sistema de computador ou os dados nele encontrados até que a vítima faça um pagamento. O ransomware normalmente criptografa os dados no computador com uma chave desconhecida ao usuário. O usuário deve pagar um resgate aos criminosos para remover a restrição.

Outras versões do ransomware utilizar as vulnerabilidades de sistemas específicos para bloquear o sistema. O ransomware se propaga como um cavalo de Troia e resulta de um arquivo baixado ou de um ponto fraco no software.

A meta do criminoso é sempre o pagamento através de um sistema de pagamento indetectável. Hoje em dia o bitcoin e outras criptomoedas têm sido o principal meio de pagamento. Depois que a vítima efetua o pagamento, o criminoso fornece um programa que descriptografa os arquivos ou envia um código de desbloqueio.

Backdoors

Um backdoor refere-se ao programa ou código desenvolvido e enviado por um criminoso que comprometeu um sistema. O backdoor ignora a autenticação normal usada para acessar o sistema. Alguns permitem o acesso remoto a usuários do sistema não autorizados.

A finalidade do backdoor é conceder aos criminosos virtuais o acesso futuro ao sistema, mesmo se a empresa corrigir a vulnerabilidade original usada para atacar o sistema. Em geral, os criminosos fazem com que usuários autorizados executem inconscientemente um programa Cavalo de Troia na máquina, para instalar um backdoor.

A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou substituição por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet).

A existência de um backdoor não depende necessariamente de uma invasão. Alguns dos casos onde não há associação com uma invasão são:

- Instalação através de um cavalo de tróia;
- Inclusão como conseqüência da instalação e má configuração de um programa de administração remota;

Alguns fabricantes incluem/incluíam backdoors nos seus produtos (softwares, sistemas operacionais), alegando necessidades administrativas. Estes casos constituem uma séria ameaça à segurança de um computador que contenha um destes produtos instalados, mesmo que os backdoors tenham sido incluídos por fabricantes conhecidos.

Rootkits

Um rootkit é um conjunto de programas que fornece mecanismos para que um invasor possa esconder e assegurar a sua presença no computador comprometido. Ou seja, ele modifica o sistema operacional para criar um backdoor. Os invasores usam o backdoor para acessar o computador remotamente. A maioria dos rootkits utiliza as vulnerabilidades do software para escalonar privilégios e modificar arquivos de sistema.

O nome rootkit não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (root ou Administrator) a um computador, mas sim para mantê-lo.

O invasor, após instalar o rootkit, terá acesso privilegiado sem precisar recorrer novamente aos métodos utilizados na invasão, e as suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Um rootkit pode fornecer ferramentas com as mais diversas funcionalidades, podendo ser citados:

- Programas utilizados para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os rootkits), tais como arquivos, diretórios, processos, conexões de rede, etc;
- Backdoors, para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos rootkits);
- Programas para remoção de evidências em arquivos de logs;
- Sniffers, para capturar informações na rede onde o onde o computador está localizado como, por exemplo, senhas que estejam trafegando em claro, sem qualquer proteção de criptografia;

Bots

Bot é um programa capaz se propagar automaticamente (modo similar ao worm), explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.

Adicionalmente ao worm, dispõe mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente.

Normalmente, o bot se conecta a um servidor de IRC (Internet Relay Chat) e entra em um canal determinado, onde aguarda instruções do invasor monitorando, paralelamente, as mensagens que estão sendo enviadas para este canal.

O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por sequências especiais de caracteres, que são interpretadas pelo bot. Estas sequências correspondem a instruções que devem ser executadas pelo bot.

Um invasor, ao se comunicar com um bot, pode enviar instruções para que ele realize diversas atividades, tais como:

- Iniciar ataques na Internet;
- Executar um ataque de negação de serviço;
- Roubar dados do computador onde é executado;
- Enviar e-mails de phishing;
- Enviar spam.

Botnets

Botnets são redes formadas por centenas ou milhares de computadores infectados com bots.

Um invasor que controla uma botnet pode utilizá-la para aumentar a potência dos seus ataques, por exemplo, para enviar milhares de e-mails de phishing ou spam, desferir ataques de negação de serviço, etc.

Identificar a presença de um bot em um computador não é fácil.

Normalmente, o bot é projetado para realizar as instruções passadas pelo invasor sem que o usuário perceba. Embora alguns programas antivírus permitam detectar a presença de bots, isto nem sempre é possível.

Keyloggers

Keylogger é um programa capaz de capturar e armazenar a informação das teclas digitadas pelo usuário em um computador.

Dentre as informações capturadas podem estar um texto de e-mail, dados da declaração de imposto de renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário como, por exemplo, após o acesso a um site específico de comércio eletrônico ou Internet Banking.

Normalmente, o keylogger contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de e-mail).

As instituições financeiras desenvolveram teclados virtuais para evitar que os keyloggers pudessem capturar informações sensíveis de clientes. Como resposta, foram desenvolvidos os screenloggers, que são capazes de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

Normalmente, o keylogger vem como parte de um programa spyware ou cavalo de tróia.

Desta forma, é necessário que este programa seja executado para que o keylogger se instale em um computador.

Geralmente, tais programas vêm anexados a e-mails ou estão disponíveis em sites na Internet.

Defesa contra malware

De nada adianta reconhecer um malware e não saber proteger-se. Desse modo, a proteção contra malwares oferece uma segunda camada de segurança essencial para seu computador ou rede

Alguns passos simples podem ajudar a proteger-se contra todas as formas de malware:

- **Programa de antivírus -** A maioria dos conjuntos de antivírus captura as formas mais comuns de malware. Contudo, os criminosos virtuais desenvolvem e implantam novas ameaças diariamente. Portanto, o segredo de uma solução antivírus eficaz é manter as assinaturas atualizadas. Uma assinatura é como uma impressão digital. Identifica as características de um código malicioso.

  Uma proteção antivírus bem projetada apresenta algumas características. Ela verifica todos os programas recém-baixados para garantir que estejam livres de malware. Ela verifica o computador periodicamente para detectar e combater todos os malwares que possam ter sido introduzidos. Ela é atualizada regularmente para reconhecer as ameaças mais recentes.

  Uma boa proteção antivírus também é capaz de reconhecer e alertar sobre as ameaças de malware anteriormente desconhecidas com base em recursos técnicos (como tentar se "ocultar" em um computador) característicos de malware. Além disso, os softwares antivírus eficientes detectam e alertam sobre sites suspeitos, especialmente sites que possam ter sido desenvolvidos para "phishing" (uma técnica que induz os usuários a revelar as suas senhas ou números de conta).
- **Software atualizado -** Muitas formas de malware atingem os seus objetivos explorando as vulnerabilidades do software, no sistema operacional e nos aplicativos. Embora as vulnerabilidades do sistema operacional sejam a principal fonte de problemas, as vulnerabilidades dos aplicativos atuais representam o maior risco. Infelizmente, embora os fornecedores de sistemas operacionais estejam cada vez mais propensos a realizar correções, a maioria dos fornecedores de aplicativos não está.

Conclusão

A existência dos malwares é uma realidade é pode ter resultados catastróficos. Durante a pandemia, inúmeras pessoas foram vítimas de diversos tipos de ataques originados por vulnerabilidades aproveitadas por algum descuido. Desse modo é importante esforçar-se para conhecer o modus operandis desses malwares e, consequentemente, proteger-se.

Embora nenhuma protecção é absoluta. É importante combinar consciencialização pessoal e ferramentas de protecção bem desenvolvidas para garantir que seu computador e todos os nossos activos de TI, estejam o mais protegido possível.

Fique atento a e-mails que pedem suas senhas. Ou e-mails que parecem vir de amigos, mas que têm somente uma mensagem como "Olha esse site incrível!", seguido de um link.

Portanto, lembre-se sempre da seguinte máxima: “Não existem almoços grátis