concursos de ti

ebooks e mentoria

ebook

segurança da informação

Sumário

Conceitos Básicos

Definição de Segurança da Informação

Comecemos com o conceito de Informação:

Informação:
Segundo o dicionário, informação significa um conjunto de conhecimento sobre alguém ou alguma coisa.

De acordo com a ISO/IEC 27002:2005, a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.

De acordo com Sócrates Arantes Teixeira Filho, "a informação é um bem, um patrimônio a ser preservado para uma empresa e que tem importância aos negócios."

Informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e precisa ser protegido.

Sendo assim, a segurança da informação busca a proteção das informações tanto quanto a ameaças ligadas a fatores tecnológicos, quanto a fatores não tecnológicos. Focando em garantir a continuidade dos negócios, minimizando possíveis danos e maximizando o retorno do investimento e as oportunidades de negócio.

Segundo a Wikipedia, "*a Segurança da Informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais*" ou ainda "*a proteção contra o uso ou acesso não autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas*."

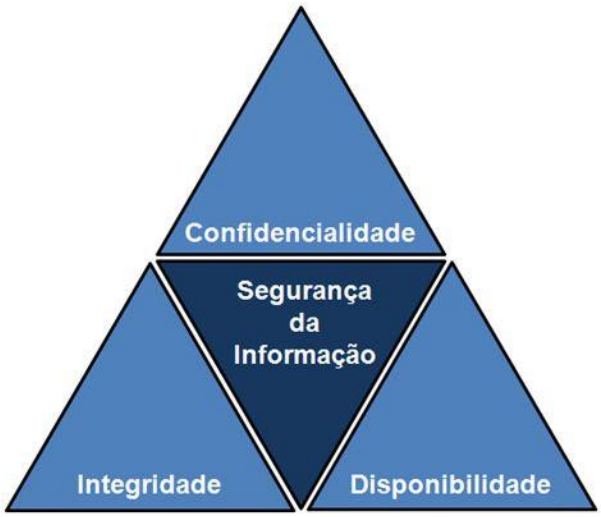
Princípios

Para a ISO/IEC 27002:2005, a segurança da informação consiste na preservação dos princípios básicos da confidencialidade, da integridade e da disponibilidade da informação. Formando, assim, a famosa tríade da segurança da informação:

- **Confidencialidade:** o acesso à informação deve ser obtido apenas por pessoas autorizadas; proteção contra exposição não autorizada;
- **Integridade:** as informações em trânsito ou em um sistema de computador somente podem ser modificadas pelas partes autorizadas; proteção contra modificação não autorizada;

- **Disponibilidade:** as informações podem ser acessadas pelas pessoas autorizadas sempre que for necessário;

Mnemônico: **CID**



Outras propriedades podem estar envolvidas como:
Autenticidade: a origem da informação deve ser identificada e o seu remetente deve ser realmente a pessoa indicada na própria mensagem;
Responsabilidade: capacidade de se responsabilizar um usuário pelos seus atos, no tratamento de informações;
Irretratabilidade e não repúdio: quem enviou uma informação não poderá negar que a enviou;
Confiabilidade: garantia de tolerância a falhas de um sistema de informação;

Obs.: Em inglês o mnemônico CID vira **CIA**. **C**onfidentiality, **I**ntegrity e **A**vailability.

Terminologia

O termo genérico para identificar quem realiza o ataque em um sistema computacional é hacker. Entretanto, temos diversos termos e definições sobre os possíveis atacantes em um sistema computacional.

Hacker: são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos às vítimas, mas sim como um desafio às suas habilidades.

Cracker: são os que invadem sistemas para roubar informações e causar danos às vítimas. Também são aqueles que decifram códigos e destroem proteções de software.

Script Kiddies: também conhecidos como newbies, são inexperientes e novatos que conseguem ferramentas, que podem ser encontradas prontas na internet, e depois as utilizam sem entender o que estão fazendo. São a imensa maioria dos “hackers” na internet e muitos incidentes de segurança são causados por eles.

Cyberpunks: são os hackers dos tempos românticos, aqueles que se dedicam às invasões de sistemas por puro divertimento e desafio. Eles têm extremo conhecimento e são obcecados pela privacidade de seus dados, o que faz com que todas as suas comunicações sejam protegidas por criptografia.

Insiders: geralmente são funcionários descontentes com seu trabalho, insatisfeitos ou injustiçados que querem prejudicar a organização com as informações que têm ou com os acessos privilegiados que possuem. Esse tipo de funcionário pode ser manipulado pelos concorrentes e ainda há o caso de espionagem industrial que também utiliza muito os insiders.

Coders: são os hackers que resolveram compartilhar seus conhecimentos escrevendo livros ou proferindo palestras e seminários sobre suas proezas. Vieram a público mostrarem suas façanhas no mundo digital.

White hat: também são conhecidos como “hackers do bem” ou “hacker ético”, que utilizam seus conhecimentos para descobrir vulnerabilidades nos sistemas e aplicar as correções necessárias, trabalhando de maneira profissional e legal dentro das organizações.

Black hat: também conhecidos como “crackers”. São os que utilizam seus conhecimentos para invadir sistemas e roubar informações secretas das organizações.

Gray hat: são black hats que fazem o papel de white hats a fim de trabalhar na área de segurança. Muitas vezes, após terminarem um serviço legal e ético dentro de uma organização, os gray hats acabam quebrando a lei e divulgando as vulnerabilidades encontradas na organização. É muito perigoso trabalhar com os gray hats pois estão frequentemente nos dois lados, white hat e black hat.

Ciberterroristas: define hackers que realizam seus ataques contra alvos selecionados cuidadosamente, com o objetivo de transmitir uma mensagem política ou religiosa (hacktivism) para derrubar a rede ou obter informações que podem comprometer a segurança nacional de alguma nação.

Exploit: de acordo com o Wikipedia, “um exploit é um pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto a ocorrer no software ou hardware de um computador ou em algum eletrônico (normalmente computadorizado).”

Ataques a computadores

Etapas de um ataque

Para se executar um ataque a computadores e a redes de computadores, geralmente são cumpridos vários passos listados e detalhados abaixo:

1. Footprinting
2. Varreduras
3. Enumeração de vulnerabilidades
4. Ataque
5. Cobertura dos rastros
6. Manutenção do acesso

Footprinting

- Levantamento das informações do alvo, footprint significa pegada, então a etapa de footprinting seria como achar as “pegadas”, o “caminho das pegadas” do alvo na internet; É uma fase de coleta de informações sobre o alvo. O footprinting pode ser feito manualmente ou por programas; Uma etapa de planejamento de um ataque;

- Nessa etapa pode ocorrer o uso de técnicas como Dumpster Diving (ou Trashing) e Engenharia Social:
    - **Dumpster Diving/Trashing:** atividade na qual o lixo é verificado/revirado em busca de informações sobre a organização ou a rede da vítima, com, por exemplo, nomes de contas e senhas, informações pessoais e confidenciais; Uma característica interessante dessa técnica é que ela é legal, pois as informações são coletadas diretamente do lixo;
    - **Engenharia Social:** técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Tem como objetivo enganar e ludibriar pessoas, fazendo com que elas revelem informações importantes (até mesmo senhas) que possam comprometer a segurança;

Varreduras

- O objetivo dessa etapa é descobrir computadores ativos em uma determinada rede e em quais portas esses sistemas estão rodando.
- Utiliza-se scanners de portas e tenta enumerar os serviços disponíveis assim como sua versão. Nesta etapa o ICMP echo e echo reply são bastante utilizados.
- Alguns softwares que podem ser utilizados nessa etapa são:
    - NMAP
    - Strobe
    - NetCat
    - SuperScan

Enumeração de vulnerabilidades

- Já sabemos os hosts disponíveis e quais portas estão usando. Agora devemos descobrir quais serviços e recursos estão rodando e buscar as vulnerabilidades de cada versão.

Curiosidade:

CVE (common vulnerabilities and exposures): uma iniciativa colaborativa de diversas organizações de tecnologia que criam listas de nomes padronizados para vulnerabilidades e outras exposições de segurança. Busca padronizar vulnerabilidades e riscos conhecidos, facilitando a procura, o acesso e o compartilhamento de dados entre diversos indivíduos e empresas. É uma lista pública de falhas de segurança.

Ataque

- Etapa em que realmente é realizado o ataque. Há diversas alternativas de ataques em que o hacker/cracker busca invadir o sistema, roubar informações, destruir o sistema, aproveitar-se das vulnerabilidades levantadas nas etapas anteriores. Logo abaixo veremos diversas técnicas de ataques.

Cobertura dos rastros

- Etapa em que o atacante busca apagar os rastros que o identificam ou que identificam que ele invadiu o sistema. Busca apagar os logs de sistemas, sempre que possível e alterar configurações de sistemas para que não o acusem; entretanto, há situações em que o atacante quer deixar uma mensagem deixando claro que ele invadiu o sistema.

Manutenção do acesso

- O atacante busca instalar, secretamente, programas maliciosos como rootkits para que seja possível, além de esconder os seus rastros (etapa anterior), assegurar a sua presença no computador comprometido. O atacante busca deixar backdoors para que possa sempre voltar quando quiser.

Tipos de ataques

Buffer Overflow

- Consiste em armazenar, em um buffer de tamanho fixo, dados maiores que o seu tamanho. Consequências: funcionamento errôneo do programa; valor da variável X corrompido; travamento do programa; vulnerabilidade a exploits.

- O hacker explora bugs de implementação, nos quais o controle do buffer (memória temporária para armazenamento dos dados) não é feito adequadamente. Assim, o hacker pode enviar mais dados do que o buffer pode manipular, preenchendo o

espaço da pilha de memória. Os dados podem ser perdidos ou excluídos e, quando isso acontece, o hacker pode reescrever no espaço interno da pilha do programa, para fazer com que comandos arbitrários sejam executados.

Sniffing

- É o processo de captura das informações da rede por meio de um software de escuta de rede (sniffer). Esse software é capaz de interpretar as informações transmitidas no meio físico. Atua em modo promíscuo. É um ataque à confidencialidade. Geralmente é um agente passivo. Raramente interfere no funcionamento da rede. A principal característica visível de um sniffer é uma interface em modo promíscuo sem o aval do administrador de rede.

- Técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio de programas específicos chamados de sniffers. Esta técnica pode ser legítima (por administradores de redes para analisar o desempenho e monitorar atividades) ou maliciosa (por atacantes para capturar informações sensíveis).

DoS e DDoS

- Os ataques de DoS fazem com que recursos sejam explorados de maneira agressiva, de modo que usuários legítimos ficam impossibilitados de utilizá-los.

- Um atacante envia vários pacotes ou requisições de serviço de uma vez, com objetivo de sobrecarregar um servidor e, como consequência, impedir o fornecimento de um serviço. Quando o atacante faz o uso de uma bot-net (rede de computadores zumbis sob comando do atacante) para bombardear o servidor com as requisições, fazendo com que o ataque seja feito de forma distribuída, temos o DDoS (Distributed Denial of Service).

Phishing

- É o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. O phishing ocorre por meio do envio de mensagens eletrônicas. Geralmente vem de páginas falsas de comércio eletrônico, internet banking, companhias aéreas, essas mensagens normalmente vêm com formulários ou link para códigos maliciosos ou solicitação de recadastramento.

- A fraude se dá através de mensagens não solicitadas, passando-se por comunicação de uma instituição conhecida e que procura induzir o acesso a páginas fraudulentas, projetadas para furtar dados pessoais e financeiros de usuários. Ocorre por e-mail, mensagem instantânea, SMS, VoIP etc. Procura induzir o usuário a fornecer dados pessoais e financeiros.

    - **Spear phishing:** phishing altamente direcionado. Envia e-mails personalizados a uma pessoa específica.
    - **Vishing:** phishing usando VoIP.
    - **Smishing:** phishing usando mensagens de texto em celulares.

- **Whaling:** phishing que buscam vítimas de alto nível, como executivos seniores em empresas, celebridades, políticos.

Pharming

- É um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS. Quando você tenta acessar um site legítimo, o seu navegador web é redirecionado, de forma transparente, para uma página falsa.

- De acordo com Wikipedia: é o termo atribuído ao ataque baseado na técnica DNS cache poisoning (envenenamento de cache DNS) que, consiste em corromper o DNS (Sistema de Nomes de Domínio ou Domain Name System) em uma rede de computadores, fazendo com que a URL (Uniform Resource Locator ou Localizador Uniforme de Recursos) de um site passe a apontar para um servidor diferente do original. Os golpistas geralmente copiam fielmente as páginas das instituições, criando a falsa impressão que o usuário está no site desejado e induzindo-o a fornecer seus dados privados como login ou números de contas e senha que serão armazenados pelo servidor falso.

Spoofing

- É a modificação de campos de identificação de pacotes de forma que o atacante possa atuar se passando por outro host. As alterações no campo de identificação podem ser úteis para: o atacante se disfarçar como se fosse outro usuário da rede; envenenar caches de protocolos, para inserir informações falsificadas para diversos fins (cache poisoning);
  - **ARP Spoofing:** o atacante faz o envenenamento do cache das estações da rede enviando de tempos em tempos, o pacote ARP is-at indicando que o IP de uma máquina com o seu próprio endereço MAC, de forma que o tráfego a ser transmitido ao endereço IP indicado seja todo desviado para a sua máquina.
  - **IP Spoofing**: o atacante altera o endereço IP dos pacotes emitidos de forma que o atacante possa fazer solicitações em nome de outro host conhecido pela rede. Essa forma de spoofing é mais utilizada no ataque do man-in-the-middle.
  - **DNS Spoofing**: o atacante encaminha ao servidor DNS mudando o endereço IP de sites conhecidos de comércio eletrônico ou bancos, para sites falsificados, previamente montados com objetivo coletar as informações do cliente para fazer transações no site verdadeiro.
  - **E-mail Spoofing:** altera 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. Esta técnica é possível devido a características do protocolo SMTP que permitem que campos do cabeçalho, como “From” e “Return-Path”, sejam falsificados.

Evil Twin

- Ataque a redes sem fio, em que o atacante cria um Access Point com as mesmas configurações de um Access Point de acesso livre, como os de aeroportos, shoppings, cafés, de forma que as vítimas possam se conectar a ele ao invés do

Access Point original. Esse Access Point fake repassa as informações para o atacante, logo, este pode roubar senhas e informações dos usuários da rede wireless.

- Criação de um Access Point (AP) igual ao verdadeiro que repassa o tráfego ao atacante.

Cache Poisoning

- Atacante se passa pelo servidor DNS raiz e envia pacotes ao servidor DNS mudando endereços de sites conhecidos. Chama-se "envenenamento" porque assim que a cache de endereços obtém o primeiro endereço falso, pode passar a pedir outros endereços a esse endereço falso, falsificado todo o conteúdo.

Man-in-the-Middle

- É uma espécie de ataque de escuta de rede, em que o atacante atua como um intermediário entre a vítima e o servidor, sem que nenhuma das partes saiba. Com isso, o atacante tem a possibilidade de, além de interceptar, fazer modificações nas transações feitas pelo usuário, além de continuar a sessão após a vítima solicitar o seu encerramento.

SQL Injection

- Uma técnica de ataque que explora vulnerabilidades de segurança que ocorrem na camada de banco de dados de uma aplicação, que ocorrem quando a entrada do usuário ou está incorretamente filtrada, ou não é rígida o suficiente.

- Algumas aplicações não validam entradas de usuários permitindo que hackers executem comandos diretamente no banco de dados de uma aplicação. É uma manipulação de uma instrução SQL através das variáveis que compõem os parâmetros recebidos por um script. Este tipo de ataque consiste em passar parâmetros a mais via barra de navegação do navegador.

Cross Site Scripting (CSS/XSS)

- É um tipo de ataque que é baseado nas vulnerabilidades de aplicações web. Os atacantes conseguem injetar scripts maliciosos no lado do cliente, de forma a burlar as proteções que normalmente estão embutidas nos browsers.

- Ataque baseado em induzir o navegador web do usuário a executar um script malicioso dentro do contexto de um site confiável. A exploração bem sucedida deste permite ao hacker embutir um código malicioso (na forma de JavaScript, geralmente) em campos de entrada, os quais serão inseridos de volta para a resposta do servidor. Isto permite ao hacker a execução de um código arbitrário em um usuário desatento que tenha acesso permitido ao site escolhido como vítima. Coleta informações nos cookies também. A execução é sempre no cliente e para enganar o cliente, devido a uma falha no servidor.

Cross Site Request Forgery (CSRF)

- Consiste em inserir requisições em uma sessão já aberta pelo usuário, explorando a confiança que um site tem do navegador. Atua após a obtenção do cookie gerado

pela aplicação após a autenticação. Por meio do cookie, o servidor acredita estar se comunicando com o usuário real e autenticado. Pode ser inibido por captcha. Este ataque é extremamente difícil de ser detectado, dado que um identificador de sessão correto e válido será incluído na requisição recebida pela aplicação e a requisição partirá do mesmo browser e endereço IP das requisições legítimas. A aplicação web não sabe como separar a requisição correspondente ao ataque das requisições legítimas.

Diferença entre XSS e CSRF:

- XSS tira proveito da confiança que o usuário tem no site. Explora o usuário/navegador.
- CSRF tira proveito da confiança que o site tem no usuário. Explora o site/sessão.

Ransomware

- O malware que, por meio de criptografia, torna inacessíveis os dados armazenados em um equipamento e exige pagamento de resgate para restabelecer o acesso ao usuário. Ransomware é um tipo de malware que cifra os arquivos armazenados no computador da vítima e solicita um resgate para decifrá-los. A forma mais comum de infectar um computador com ransomware é utilizando a técnica de phishing para enganar a vítima, fazendo com que ela clique em um link enviado via e-mail que ache ser confiável.

Ataque do Dicionário

- Método de cracking que consiste em tentar adivinhar uma senha provando todas as palavras do dicionário ou combinação de palavras.

- Um ataque de dicionário é caracterizado pela tentativa de todas as sequências de caracteres de uma lista predefinida normalmente derivada de uma lista de palavras como em um dicionário, daí o nome *ataque de dicionário*.

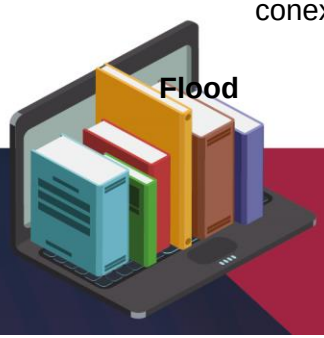
Força Bruta (Brute Force)

- 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. Um ataque de força bruta, dependendo de como é realizado, pode resultar em um ataque de negação de serviço, devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo. Testa exaustivamente todas alternativas.

Smurf

- Uma combinação do DDoS com o IP Spoofing. O atacante envia em uma rede uma série de pacotes ICMP echo request (Ping) em broadcast (para todos da rede), com o endereço IP de origem da estação da vítima. Normalmente, as máquinas irão receber os pacotes e cada uma delas irá responder com um pacote ICMP echo reply endereçado para a vítima. Isso irá sobrecarregar a vítima e interromper sua conexão.

Flood



- Um atacante envia vários pacotes ou requisições de serviço de uma vez, com objetivo de sobrecarregar um servidor e, como consequência, impedir o fornecimento de um serviço.
- Os modos mais conhecidos são:
    - **SYN Flood:** abertura de diversas conexões TCP, com pacote TCP com flag SYN ativado, para sobrecarregar a pilha TCP/IP da vítima;
    - Explora o mecanismo de estabelecimento de conexões TCP, baseado em three-way-handshake.
    - **Ping Flood:** envio de diversos pacotes ICMP echo request (Ping), obrigando a vítima a responder aos pacotes com ICMP echo reply, o que também sobrecarrega a vítima.

Defacement

- Desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página web de um site. As principais formas que um atacante pode utilizar para desfigurar uma página web são: explorar erros da aplicação web; explorar vulnerabilidades do servidor da aplicação web; explorar vulnerabilidades da linguagem de programação ou dos frameworks de desenvolvimento que foram usados para fazer o site; entre outras.

Rainbow Table

- Uma tabela de consulta de hashes pré-calculados. Usada para tentar recuperar o texto original de uma senha através de uma senha digerida (hash), gerada por uma função criptográfica de hashing.

Teardrop

- É uma espécie de DoS mas que envia fragmentos de um pacote IP intencionalmente com erros, de maneira que haja uma superposição dos dados entre dois fragmentos, ocasionando até que a rede da vítima pare de funcionar.

Identity theft

- Furto de identidade, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas.

Advance fee fraud

- Fraude de antecipação de recursos, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Hoax

- Boato, ou hoax, é 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. Boatos trazem diversos problemas, como: conter códigos maliciosos, espalhar desinformação pela internet, ocupar desnecessariamente sua caixa de e-mail, compromete a credibilidade e a reputação de pessoas ou entidades, aumenta o consumo de banda de rede, a carga de servidores de e-mail, entre outros problemas.

Advanced Persistent Threats (APT)

- Ameaça Persistente Avançada, consiste em um conjunto de processos de hacking contínuos e invisíveis que são comumente orquestrados por pessoas com uma finalidade específica. As APT costumam atacar organizações e/ou países por motivos comerciais ou políticos (guerra cibernética, espionagem industrial, combate ao terrorismo, ciberterrorismo, etc). Normalmente requerem alto grau de sigilo. O termo avançada significa que são utilizadas técnicas sofisticadas de malwares, o termo persistente significa que há um sistema de controle e comando que está continuamente monitorando e extraindo dados de um alvo específico. Os ataques APT funcionam em três etapas: Planejamento, Engenharia Social e Aprofundamento da Invasão. Um exemplo famoso do uso de APT foi o famoso worm Stuxnet, que foi criado para atingir o programa nuclear iraniano.

Ataque do aniversário (Birthday attack)

- É um ataque conhecido contra funções de hash e se baseia em problema estatístico ligado a uma população: é muito mais fácil achar uma pessoa com a mesma data de aniversário de outra pessoa qualquer, do que achar uma que tenha nascido em um mesmo dia que você ou uma pessoa específica tenha nascido. Este ataque pode ser usado para abusar da comunicação entre duas ou mais partes. O ataque depende da maior probabilidade de colisões encontradas entre as tentativas de ataque aleatórias e um grau fixo de permutações. Com um ataque de aniversário, é possível encontrar uma colisão de uma função hash em $\sqrt{2^n} = 2^{n/2}$, com 2^n sendo a segurança de resistência de pré-imagem clássica.

Brushing

- Não é necessariamente um ataque, mas uma técnica enganosa às vezes utilizada no comércio eletrônico (e-commerce) para aumentar as classificações de um vendedor criando pedidos falsos. Um vendedor golpista pega os dados de alguém na internet e cria uma conta falta no marketplace no nome da vítima. Em seguida, efetua a compra de um determinado produto na própria loja virtual e despacha a "mercadoria", que no caso é algo geralmente de valor irrisório. Quando a mercadoria chega na casa do suposto cliente, o vendedor deixa um comentário positivo e ainda ganha o selo de "comprador verificado", o que lhe dá mais credibilidade. É o envio de mercadorias não solicitadas com o objetivo de registrar compras falsas.
- Sites que sofrem com essa fraude são Alibaba, Amazon, entre outros. Em 2019, consumidores da Amazon foram alertados sobre essa fraude e em 2020 milhares de casas no mundo inteiro receberam pacotes de sementes com descrições falsas, como brincos, direto da China.

Hijack

- Uma tradução literal de hijack seria sequestro e esse tipo de ataque efetuado por um hijacker (sequestrador) consiste no uso de spywares que se instalam furtivamente em computadores por meio de protocolos, como ActiveX, ou no momento da instalação de programas gratuitos e suspeitos. Atuam nos navegadores/browsers mais populares da internet e podem modificar registros do Windows, modificar a página inicial do navegador, fazer aparecer novas barras e botões, alterarem o

mecanismo de busca padrão, fazer páginas abrirem sem parar na tela contra a vontade do usuário, realmente “sequestrarem” o navegador.

- Todas essas alterações no seu navegador são realizadas para linkarem publicidade e, na maioria das vezes, pornografia. A ideia dos hijackers é forçar o usuário a visitar páginas que ele não quer, gerando tráfego e publicidade para esses sites. O desenvolvedor desse hijack é pago por cada visita e clique nessas páginas com publicidade que são abertas.

Malwares

A palavra malware vem de Malicious Software e abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um sistema. Malware é gênero e agora vamos para as espécies:

Vírus
programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de computador. O vírus executa diversas atividades. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

- **Vírus Polimórficos:** são capazes de criar uma nova variante a cada execução, mudam a sua assinatura para dificultar a detecção pelo antivírus.
- **Vírus Metamórficos:** são capazes de mudar o próprio corpo, evitam gerar instâncias parecidas com a anterior. Reescrevem-se completamente, mudando a assinatura, o tamanho e até o próprio comportamento.

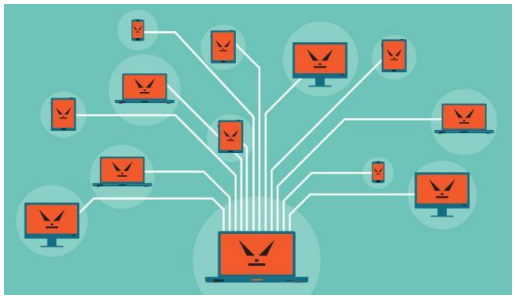
Worm
programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo. É autorreplicante, não precisa de outro programa para se propagar. Consome recursos e degrada o desempenho de redes e computadores. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de software instaladas em computadores.

Trojan Horses/ Cavalos de Tróia

executa, além de suas funções, funções clandestinas, pois trata-se de software que executa também atividades não previstas. “Cavalo” deve ser executado. Mas dentro ele traz consigo vírus, worm, keylogger ou qualquer outro arquivo malicioso. Distingue-se de um vírus ou de um worm por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente.

Bot e botnet

De modo similar ao worm, o bot é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador. Dispõe de mecanismos de comunicação com o invasor permitindo que o bot seja controlado remotamente. Normalmente o bot se conecta a um servidor IRC e entra em um canal determinado, esperando instruções do invasor. É igual a um worm, mas mantém comunicação com o invasor. Botnets são redes formadas por computadores infectados com bots.

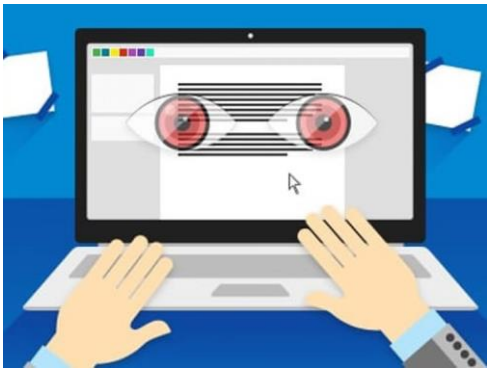


Spyware

é uma violação à confidencialidade. Monitora as atividades de um sistema e envia as informações coletadas para terceiros. É um espião.

Keyloggers

Captura e armazena as teclas digitadas. Há também Screenlogger e Mouselogger, que são variações que gravam a tela inteira ou o caminho do mouse, respectivamente. Muito utilizado em computadores de uso público, como lan-houses, bibliotecas e universidades.



Adware

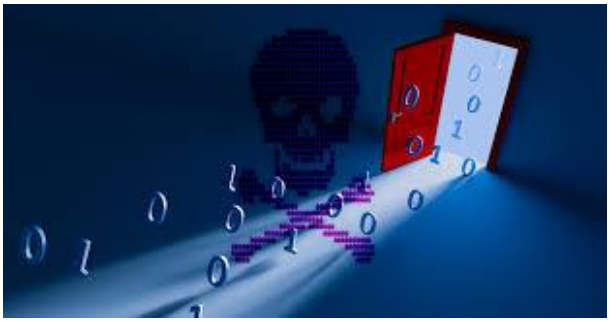
projetado para apresentar propagandas, seja através de um browser, seja através de algum outro programa instalado em um computador. Tem sido incorporado a software, serviços e, principalmente, a aplicativos gratuitos de celular. Não é um vírus, é legítimo e legal porém invasivo. E nada impede a execução de serviços ilegítimos em background, aí já passa a ser ilegal. Adware vem de advertising (propaganda) e software.

Bomba Lógica

executa atividades sob determinada condição. “Explode” geralmente por inanição. Alguém fica alimentando para não explodir, por exemplo, funcionários insatisfeitos. Quando para de alimentar, explode (por exemplo, quando o funcionário é demitido). Depende de hospedeiro.

Backdoor

programas que permitem o retorno de um invasor a um computador comprometido. A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto. Sua existência não pressupõe invasão mas é uma brecha. Alguns softwares alegam necessidade administrativa, deixar portas abertas. É uma "porta dos fundos" destrancada que permite uma invasão.



Rootkit

um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder os seus rastros e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece esses mecanismos é conhecido como rootkit. Ele apaga os seus rastros, não tem nada a ver com acesso root. Na verdade, a confusão se faz pois ele não é utilizado para obter acesso privilegiado, mas manter.

Stuxnet

É um worm de computador projetado especificamente para atacar o sistema operacional SCADA desenvolvido pela Siemens e usado para controlar as centrífugas de enriquecimento de urânio iranianas. Foi descoberto em junho de 2010 pela empresa bielorrussa desenvolvedora de antivírus VirusBlokAda. É o primeiro worm descoberto que espiona e reprograma sistemas industriais.Ele foi especificamente escrito para atacar o sistema de controle industrial SCADA, usado para controlar e monitorar processos industriais.