SUMÁRIO

TECNOLOGIA NA EDUCAÇÃO E INFORMÁTICA BÁSICA

SEGURANÇA DA INFORMAÇÃO (NOÇÕES DE VÍRUS E PRAGAS VIRTUAIS, PROCEDIMENTOS DE BACKUP)

O QUE É SEGURANÇA DA INFORMAÇÃO?

Essa é uma pergunta curta, que exige conhecimentos diversos, para que possa ser respondida. Neste tópico, você encontrará as informações necessárias para isso.

As redes de computadores tornaram-se cada vez mais interligadas e complexas. Elas integram, atualmente, muitos dispositivos, que, talvez, você não conheça, mas que estão ali, promovendo a troca de dados entre o seu equipamento e o servidor remoto o qual está acessando. No entanto, é sabido que os criminosos virtuais podem acessar redes de qualquer lugar do mundo.

Neste sentido, os profissionais de Segurança da Informação procuram proteger os dados armazenados e trafegados entre os dispositivos por meio de equipamentos, programas e técnicas direcionadas. Para isso, o treinamento dos usuários também é importante, considerando que eles compreendem o elo mais fraco e vulnerável no que se refere à Segurança da Informação.

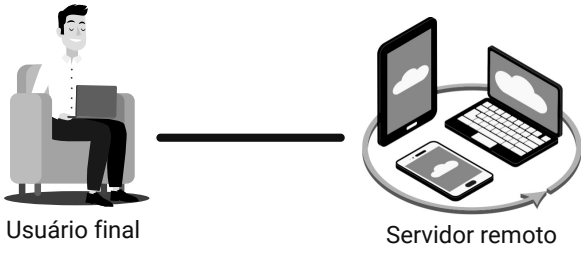


Figura 1. A conexão entre o usuário cliente e o servidor é realizada por diferentes equipamentos, que são transparentes para o usuário final.

Entre o servidor remoto e o usuário final, as informações solicitadas passarão por vários dispositivos de conexão (roteadores, repetidores de sinal, *switches*, *bridges*, *gateways*) antes de serem apresentadas no dispositivo do usuário.

Paradigma cliente-servidor: nós somos clientes e acessamos informações em servidores remotos. As redes de computadores, em concursos públicos, são abordadas, seguindo esse paradigma. Usamos cliente *web* (*browser* ou navegador) para acessar um servidor *web*. Usamos cliente de *e-mail* para acessar um servidor de *e-mail*. Usamos um cliente FTP para acessar um servidor FTP.

Ataques e ameaças à Segurança da Informação

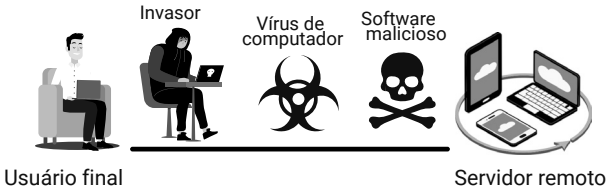


Figura 2. O tráfego de dados, em uma conexão, é um ativo interessante para invasores, vírus de computadores e *softwares* maliciosos.

Invasores tentarão acessar a conexão e capturar os dados trafegados. Os vírus de computador procuram infectar os arquivos e causar danos aos sistemas. Esses softwares maliciosos podem infectar dispositivos e sequestrar arquivos.

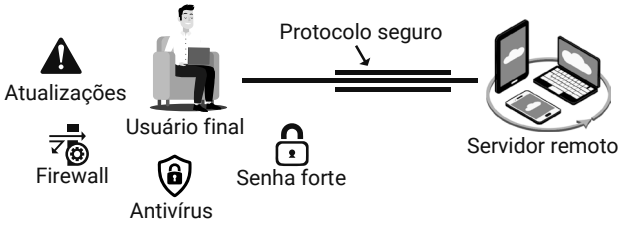


Figura 3. Um protocolo seguro protege o tráfego de dados em uma conexão insegura, criptografando as informações que são enviadas e recebidas.

O usuário deverá utilizar um protocolo seguro para acessar os dados, manter o seu dispositivo atualizado e protegido, utilizar uma senha forte de acordo com as políticas de segurança e práticas recomendadas, entre outras ações. Além disso, deverá utilizar conexões seguras, como as VPN's – *Virtual Private Network* –, para acesso aos serviços remotos (Computação na Nuvem); proteger-se das ameaças e ataques à Segurança da Informação, utilizando medidas de proteção em seu dispositivo, como antivírus, *firewall* e *anti-spyware*).

Iniciaremos nossos estudos sobre Segurança da Informação com o tópico VPN. Elas são muito importantes para a comunicação segura e tornaram-se destaque nos últimos anos, por causa do trabalho remoto (*home office*). Empresas e usuários que não utilizavam uma conexão remota segura precisaram adaptar-se aos novos tempos. Em concursos, a tendência é que aumente a frequência de questões sobre esse tema, pois se tornou popular devido à pandemia.

A seguir, conheceremos como é a Computação na Nuvem, suas características, os tipos de nuvem, os serviços oferecidos e as vantagens e desvantagens. Vale ressaltar que esse tópico já foi bastante abordado em alguns concursos, em provas de diversos cargos.

Vírus de computador e *softwares* maliciosos: quem nunca foi vítima, não é mesmo? Esse será o terceiro tópico sobre Segurança da Informação, no qual abordaremos os ataques e ameaças, com destaque para os principais e mais comuns em provas de concursos. Assim como Computação na Nuvem, o tópico "Noções de Vírus, Worms e Pragas Virtuais" também é muito questionado em concursos públicos.

Finalizando o conteúdo de Segurança da Informação, estudaremos os mecanismos de proteção e defesa contra os ataques e ameaças. Existem equipamentos de proteção, no entanto, em concursos públicos, geralmente, são questionados os aplicativos para segurança (antivírus, *firewall*, *anti-spyware* etc.).

Apesar de existirem soluções integradas e avançadas para os problemas de Segurança da Informação, que até usamos em nossos dispositivos, nos concursos públicos, são questionadas as definições oficiais e as configurações padrão dos programas.

NOÇÕES DE VÍRUS, WORMS E PRAGAS VIRTUAIS

Sabe-se que ameaças e riscos de segurança estão presentes no mundo virtual. Assim como existem pessoas boas e más no mundo real, existem usuários com boas ou más intenções no mundo virtual.

Os criminosos virtuais são genericamente denominados como *hackers*, porém o termo mais adequado seria *cracker*. Um *hacker* é um usuário que possui muitos conhecimentos sobre tecnologia, podendo ser nomeado como *White Hat* – *hacker* ético que usa suas habilidades com propósitos éticos e legais –, *Gray Hat* – aquele que comete crimes, mas sem ganho pessoal (geralmente, para exposição de falhas nos sistemas) – e *Black Hat* – aquele que viola a segurança dos sistemas para obtenção de ganhos pessoais.

Amadores ou inexperientes, profissionais ou experientes, todo usuário está sujeito aos riscos inerentes ao uso dos recursos computacionais. São riscos de segurança digital:

- **Ameaças:** vulnerabilidades que existem e podem ser exploradas por usuários;
- **Falhas:** vulnerabilidades existentes nos sistemas, sejam elas propositais ou acidentais;
- **Ataques:** ação que procura denegrir ou suspender a operação de sistemas.

Devido à crescente integração entre as redes de comunicação, conexão com novos e inusitados dispositivos (IoT – *Internet* das Coisas) e criminosos com acesso de qualquer lugar do mundo, as redes de informações tornaram-se particularmente difíceis de se proteger. Profissionais altamente qualificados são formados e contratados pelas empresas com a única função de proteger os sistemas informatizados.

Em concursos públicos, as ameaças e os ataques são os itens mais questionados.

Dica

Você conhece a Cartilha de Segurança CERT? Disponível gratuitamente na *Internet*, ela é a fonte oficial de informações sobre ameaças, ataques, defesas e segurança digital. Ela pode ser acessada pelo link: <https://cartilha.cert.br/>. (Acesso em: 13 nov. 2020).

Ameaças

As ameaças são identificadas como aquelas que possuem potencial para comprometer a oferta ou existência dos ativos computacionais, tais como: informações, processos e sistemas. Um *ransomware* – *software* que sequestra dados, utilizando-se de criptografia e solicita o pagamento de resgate para a liberação das informações sequestradas – é um exemplo de ameaça.

É importante entender que, apesar de a ameaça existir, se não ocorrer uma ação deliberada para sua execução ou se medidas de proteção forem implementadas, ela é eliminada e não se torna um ataque. As ameaças à segurança da informação podem ser classificadas como:

- **Tecnológicas:** quando ocorre mudança no padrão ou tecnologia, sem a devida atualização ou *upgrade*;
- **Humanas:** intencionais ou acidentais, que exploram vulnerabilidades nos sistemas;
- **Naturais:** não intencionais, relacionadas ao ambiente, como as catástrofes naturais.

As empresas precisam fazer uma avaliação das ameaças que possam causar danos ao ambiente computacional dela mesma (Gerenciamento de Risco), implementar sistemas de autenticação (Controlar o Acesso), definir os requisitos de senha forte (Política de Segurança), manter um inventário e realizar o rastreamento de todos os ativos (Gerenciamento de Recursos), além de utilizar sistemas de *backup* e restauração de dados (Gerenciamento de Continuidade de Negócios).

Falhas

As falhas de segurança nos sistemas de informação poderão ser propositais ou involuntárias. Se o programador insere, no código do sistema, uma falha que produza danos ou permita o acesso sem autenticação, temos um exemplo de falha proposital. Já se uma falha for descoberta após a implantação do sistema, sem que tenha sido uma falha proposital, e tenha sido explorada por invasores, temos um exemplo de falha involuntária, inerente ao sistema.

Quando identificadas, as falhas são corrigidas pelas empresas que desenvolveram o sistema por meio da distribuição de notificações e correções de segurança. O Windows Update, serviço da Microsoft para atualização do Windows, distribui, mensalmente, os *patches* (pacotes) de correções de falhas de segurança.

Ataques

Sem dúvidas, o assunto de maior destaque, tanto em concursos como no mundo real, são os ataques. Coordenados ou isolados, os ataques procuram romper as barreiras de segurança definidas na Política de Segurança, com o objetivo de anular o sistema ou capturar dados.

Os ataques podem ser classificados como:

- **Baixa complexidade**: exploram falhas de segurança de forma isolada e são facilmente identificados e anulados;
- **Média complexidade**: combinam duas ou mais ferramentas e técnicas, para obter acesso aos dados, sendo de média complexidade para a solução, gerando impactos na operação dos sistemas, como a indisponibilidade;
- **Alta complexidade**: refinados e avançados, os ataques combinam o acesso às falhas do sistema, novos códigos maliciosos desconhecidos e a distribuição do ataque com redes zumbis, tornando difícil a resolução do problema.

Dica

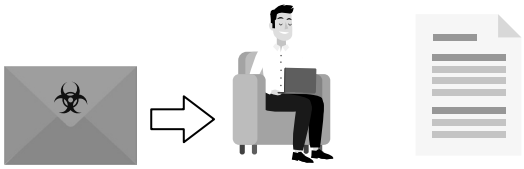
- Ameaças existem e podem afetar ou não os sistemas computacionais;
- Falhas existem e podem ser exploradas ou não pelos invasores;
- Ataques são realizados todo o tempo contra todos os tipos de sistemas.

Vírus de Computador

O vírus de computador é a ameaça digital mais popular. Tem esse nome por se assemelhar a um vírus orgânico ou biológico. O vírus biológico é um organismo que possui um código viral que infecta uma célula de outro organismo. Quando a célula infectada é acionada, o código viral é duplicado e se propaga para outras células saudáveis do corpo. Quanto mais vírus existirem no organismo, menor será o seu desempenho, fazendo com que recursos vitais sejam consumidos, podendo levar o hospedeiro à morte.

O vírus de computador é um código malicioso que infecta arquivos em um dispositivo. Quando o arquivo é executado, o código do vírus é duplicado, propagando-se para outros arquivos do computador. Quanto mais vírus existirem no dispositivo, menor será o seu desempenho, fazendo com que recursos computacionais sejam consumidos, podendo levar o hospedeiro a uma falha catastrófica.

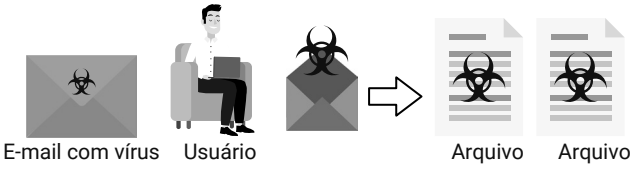
1. E-mail com vírus de computador é enviado para o usuário



2. E-mail é aberto e o arquivo anexo infectado é executado.

3. O código do vírus é copiado para arquivos do computador

4. Ao executar o arquivo infectado, novos arquivos serão infectados.



O vírus de computador poderá entrar no dispositivo do usuário por meio de um arquivo anexado em uma mensagem de *e-mail*, ou por cópia de arquivos existentes em uma mídia removível, como o *pen drive*, recebidos por alguma rede social, baixados de *sites* na *Internet*, entre outras formas de contaminação.

VÍRUS DE COMPUTADOR	CARACTERÍSTICAS
Vírus de *boot*	● Infectam o setor de *boot* do disco de inicialização ● Cada vez que o sistema é iniciado, o vírus é executado
Vírus de *script*	Armazenados em *sites* na *Internet*, são carregados e executados quando o usuário acessa a página, usando um navegador de *Internet*
Vírus de macro	● As macros são desenvolvidas em linguagem *Visual Basic for Applications* (VBA) nos arquivos do Office, para a automatização de tarefas ● Quando desenvolvido com propósitos maliciosos, é um vírus de macro
Vírus do tipo mutante	O vírus "mutante" ou "polimórfico", a cada nova multiplicação, o novo vírus mantém traços do original, mas é diferente dele
Vírus *time bomb*	São programados para agir em uma determinada data, causando algum tipo de dano no dia previamente agendado
Vírus *stealth*	● Um vírus *stealth* é um código malicioso muito complexo, que se esconde depois de infectar um computador ● Ele mantém cópias dos arquivos que foram infectados para si e, quando um *software* antivírus realiza a detecção, apresenta o arquivo original, enganando o mecanismo de proteção
Vírus *Nimda*	● O vírus *Nimda* explora as falhas de segurança do sistema operacional ● Ele se propaga pelo correio eletrônico e, também, pela *web*, em diretórios compartilhados, pelas falhas de servidor Microsoft IIS e nas trocas de arquivos

Todos os sistemas operacionais são vulneráveis aos vírus de computador. Quando um vírus de computador é desenvolvido por um *hacker*, este procura elaborá-lo para um *software* que tenha uma grande quantidade de usuários iniciantes, o que aumenta as suas chances de sucesso.

O Windows, por exemplo, possui muitos usuários e a maioria deles não tem preocupações com segurança. Por isso, grande parte dos vírus de computadores são desenvolvidos para atacarem sistemas Windows.

O Linux, por sua vez, tem poucos usuários, se comparado ao Windows, e a maioria deles possui muito conhecimento sobre Informática, tornando a ação de vírus nesse sistema uma ocorrência rara.

Já o Android, *software* operacional dos *smartphones* populares, é uma variação do sistema Linux original. Apesar de possuir essa origem nobre, é alvo de milhares de vírus, por causa dos seus usuários, que, na maioria das vezes, não têm rotinas de proteção e segurança de seus aparelhos.

Um vírus de computador poderá ser recebido por *e-mail*, transferido de *sites* na *Internet*, compartilhado em arquivos, através do uso de mídias removíveis infectadas, nas redes sociais e por mensagens instantâneas. Vale lembrar, no entanto, que um vírus necessita ser executado para que entre em ação, pois ele tem

um hospedeiro definido e um alvo estabelecido. Ele se propaga, inserindo cópias de si em outros arquivos, alterando ou removendo arquivos do dispositivo para propagação e autoproteção, a fim de não ser detectado pelo antivírus.

Worms

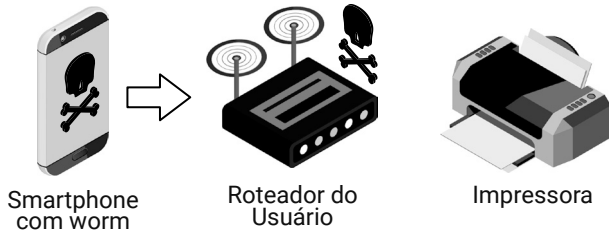
O *worm* é um verme que explora de forma independente as vulnerabilidades nas redes de dispositivos. Geralmente, eles deixam a comunicação na rede lenta, por ocuparem a conexão de dados ao enviarem cópias de seu código malicioso.

Um verme biológico parasita um organismo, consumindo seus recursos e deixando o corpo debilitado. Um verme tecnológico parasita um dispositivo, consumindo seus recursos de memória e conexão de rede, deixando o aparelho e a rede de dados lentos.

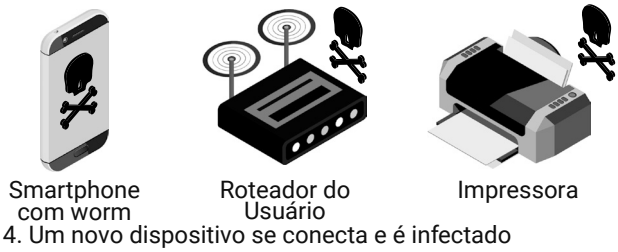
Os worms não precisam ser executados pelo usuário como os vírus de computador e a sua propagação será rápida caso não existam barreiras de proteção que os impeçam.

1. Dispositivo infectado se conecta na rede do usuário

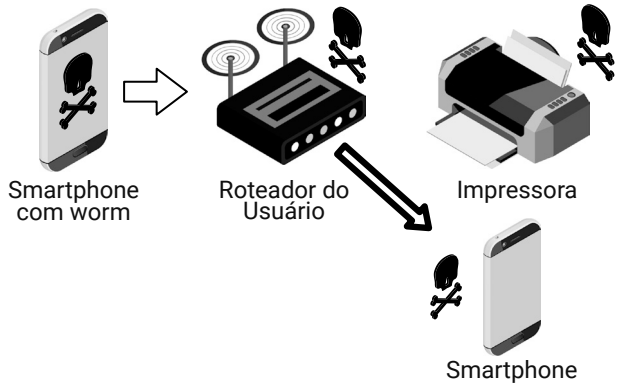
2. Roteador infectado envia o worm para a impressora



3. Impressora infectada demora muito para imprimir



4. Um novo dispositivo se conecta e é infectado



Dica

Os *worms* infectam dispositivos e propagam-se para outros dispositivos de forma autônoma, sem interferência do usuário.

Os *worms* podem ser recebidos automaticamente pela rede, inseridos por um invasor ou por ação de outro código malicioso. Assim como os vírus, ele poderá ser recebido por *e-mail*, transferido de *sites* na *Internet*, compartilhado em arquivos, por meio do uso de mídias removíveis infectadas, nas redes sociais e por mensagens instantâneas.

Com o objetivo de explorar as vulnerabilidades dos dispositivos, os *worms* enviam cópias de si mesmos para outros dispositivos e usuários conectados. Por serem autoexecutáveis, costumam consumir grande quantidade de recursos computacionais, promovendo a instalação de outros códigos maliciosos e iniciando ataques na *Internet* em busca de outras redes remotas.

Pragas Virtuais

As diversas pragas virtuais são, genericamente, chamadas de *malwares* (*softwares* maliciosos), por apresentarem características semelhantes: oferecem alguma vantagem para o usuário, mas realizam ações danosas que acabarão prejudicando-o.

- **Cavalo de Troia ou *Trojan***

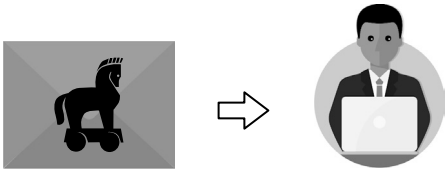
É um código malicioso que realiza operações mal-intencionadas enquanto realiza uma operação desejada pelo usuário, como um jogo *on-line* ou reprodução de um vídeo. Ele é enviado com o conteúdo desejado e, ao ser executado, desativa as proteções do dispositivo, para que o invasor tenha acesso aos arquivos e dados.

Esse nome está, justamente, relacionado com a história do presente dado pelos gregos aos troianos, consistindo em um cavalo de madeira, com soldados em seu interior. Após entrar nas fortificações de Troia, os gregos desativaram as defesas e permitiram o acesso do seu exército.

Importante!

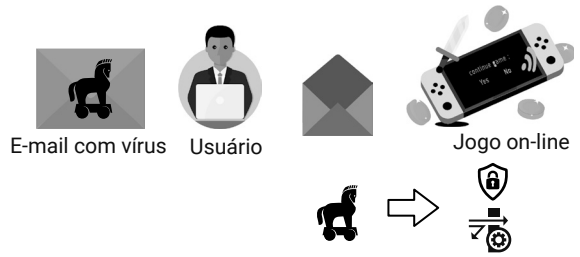
O *Trojan* ou Cavalo de Troia é apresentado, no enunciado de algumas questões de concursos, como um tipo de vírus de computador.

1. E-mail com Cavalo de Troia é enviado para o usuário

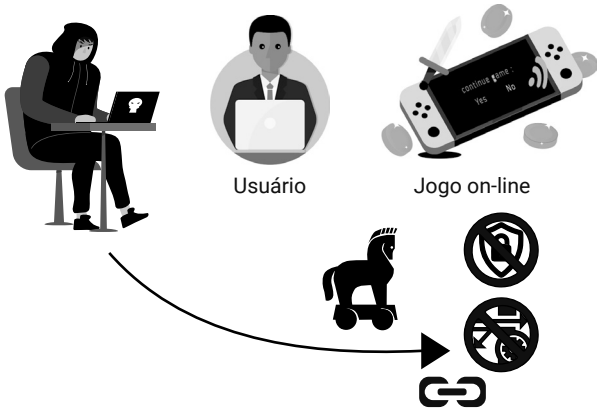


2. E-mail é aberto e o link do jogo on-line é acessado

3. Enquanto o usuário joga, o trojan desativa as proteções



4. Enquanto o usuário joga, o invasor consegue acesso



- ***Spyware***

É um programa malicioso que procura monitorar as atividades do sistema e enviar os dados capturados durante a espionagem para terceiros. Existem *softwares* espiões considerados legítimos (instalados com o consentimento do usuário) e maliciosos (que executam ações prejudiciais à privacidade do usuário).

Os *softwares* espiões podem ser especializados na captura de teclas digitadas (*keylogger*), nas telas e cliques efetuados (*screenlogger*) ou para apresentação de propagandas alinhadas com os hábitos do usuário (*adware*). Eles, geralmente, são instalados por outros programas maliciosos, para aumentar a quantidade de dados capturados.

- ***Bot***

É um programa malicioso que mantém contato com o invasor, permitindo que comandos sejam executados remotamente.

O dispositivo controlado por um *bot* poderá integrar uma rede de dispositivos zumbis, a chamada *botnet*.

Quando o invasor deseja atacar *sites* para provocar Negação de Serviço, ele aciona os *bots* que estão distribuídos nos dispositivos do usuário, para que façam a ação danosa. Além de esconder os rastros da identidade do verdadeiro atacante, os *bots* poderão continuar sua propagação através do envio de cópias para outros contatos do usuário afetado.

- ***Backdoor***

É um código malicioso semelhante ao *bot*, mas que, além de executar comandos recebidos do invasor, realiza ações para desativação de proteções e aberturas de portas de conexão. O invasor, ciente das portas TCP que estão disponíveis, consegue acesso ao dispositivo para a instalação de outros códigos maliciosos e roubo de informações.

Assim como os *spywares*, existem *backdoors* **legítimos** (adicionados pelo desenvolvedor do *software* para funcionalidades administrativas) e **ilegítimos** (para operarem independente do consentimento do usuário).

- ***Rootkit***

É um código malicioso especializado em esconder e assegurar a presença de outros códigos maliciosos para o invasor acessar o sistema. Essas pragas virtuais podem ser incorporadas em outras pragas, para que o código que camufla a presença seja executado, escondendo os rastros do *software* malicioso.

Após a remoção de um *rootkit*, o sistema afetado não se recupera dos dados apagados, sendo necessária uma cópia segura (*backup*) para restauração dos arquivos.

Dica

Cavalo de Troia, *Spyware*, *Bot*, *Backdoor* e *Rootkit* são as pragas digitais mais questionadas em concursos públicos.

Confira, na tabela a seguir, outras pragas digitais que ameaçam a Segurança da Informação e a privacidade dos usuários de sistemas computacionais.

CÓDIGO MALICIOSO	CARACTERÍSTICAS
Bomba lógica	Gatilho para a execução de outros códigos maliciosos que permanece inativa até que um evento acionador seja executado
Ransomware	Sequestrador de dados que criptografa pastas, arquivos e discos inteiros, solicitando o pagamento de resgate para liberação
Scareware	• Simulam janelas do sistema operacional, induzindo o usuário a acionar um comando, fazendo a operação continuar normalmente • O comando iniciará a instalação de códigos maliciosos
Phishing	Fraude que engana o usuário, induzindo-o a informar seus dados pessoais em páginas de captura de dados falsas
Pharming	Ataque aos servidores de DNS para alteração das tabelas de *sites*, direcionando a navegação para *sites* falsos
Negação de Serviço	Ataques na rede que simulam tráfego acima do normal com pacotes de dados formatados incorretamente, fazendo o servidor remoto ocupar-se com os pedidos e erros, negando acesso para outros usuários