

## **Aula 13**

*BNB (Analista Bancário) Informática -  
2023 (Pré-Edital)*

Autor:

**Diego Carvalho, Renato da Costa,  
Equipe Informática e TI**

30 de Junho de 2023

## Índice

1) Noções Iniciais de Segurança da Informação - Malwares .....	3
2) Segurança da Informação - Malwares - Principais Malwares .....	7
3) Segurança da Informação - Malwares - Outros Malwares .....	36
4) Segurança da Informação - Malwares - Ataques e Golpes .....	49
5) Resumo - Segurança da Informação - Malwares - Resumo .....	74
6) Mapas Mentais - Segurança da Informação - Malwares .....	78
7) Questões Comentadas - Segurança da Informação - Malwares - Cesgranrio .....	82
8) Lista de Questões - Segurança da Informação - Malwares - Cesgranrio .....	92



# MALWARES

## Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXA

**Malwares (Malicious Softwares)** – também chamados de **Softwares Maliciosos** ou **Pragas Virtuais** – são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Eles são inseridos intencionalmente em um sistema computacional com um propósito prejudicial. Algumas das formas como eles podem infectar ou comprometer um computador são:

### FORMAS COMUNS DE INFECÇÃO DE MALWARES

Pela exploração de vulnerabilidades existentes nos programas instalados ou pela auto-execução de mídias removíveis infectadas, como pen-drives;

Pelo acesso a páginas maliciosas, utilizando navegadores vulneráveis ou pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas web ou de outros computadores.

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo.

Além disso, os códigos maliciosos são muitas vezes utilizados como intermediários e possibilitam a prática de golpes virtuais, a realização de ataques e a disseminação de spam (mensagens indesejadas). Em suma: o termo *malware* abrange qualquer tipo de software indesejado, instalado sem o devido consentimento no computador do usuário. As principais categorias de *malware* são: *Vírus*, *Worm*, *Bot*, *Trojan*, *Spyware*, *Backdoor* e *Rootkit*.



## Infecção

A principal porta de entrada para os malwares hoje é a Internet! Ela pode ocorrer por meio da execução de arquivos infectados obtidos de anexos de mensagens eletrônicas, de mídias



removíveis ou dispositivos de memória *flash* (Ex: PenDrive), de páginas web comprometidas, de redes sociais ou diretamente de outros equipamentos. É interessante também tomar muito cuidado ao fazer o download de arquivos com alguns formatos específicos.

## Prevenção

É muito provável que a maioria dos seus dados está gravado em seu computador pessoal e, é por meio dele, que você acessa seus e-mails e redes sociais, e realiza transações bancárias e comerciais. **Por conta disso, mantê-lo seguro é essencial para se proteger dos riscos envolvidos no uso da Internet.** Além disso, ao manter seu computador seguro, você diminui as chances de ele ser indevidamente utilizado para atividades maliciosas.

Por diversas vezes, os atacantes estão interessados em conseguir o acesso a grande quantidade de computadores, independentemente de quais são e das configurações que possuem. **Dessa forma, acreditar que seu computador está protegido, por não apresentar atrativos para um atacante, pode ser um erro gigantesco.** Logo, para manter seu computador pessoal seguro, é importante seguir os seguintes procedimentos:

### PROCEDIMENTOS DE SEGURANÇA

- Manter os programas instalados com as versões mais recentes;
- Ser cuidadoso ao instalar aplicativos desenvolvidos por terceiros;
- Utilizar apenas softwares originais (sem pirataria);
- Manter os programas instalados com todas as atualizações aplicadas;
- Utilizar mecanismos de proteção (antivírus, firewall, etc);
- Ser cuidadoso ao enviar seu computador para serviços de manutenção;
- Utilizar configurações de segurança disponíveis;
- Ser cuidadoso ao manipular arquivos;
- Proteger seus dados (utilizando backup, por exemplo);
- Manter seu computador com data e hora corretas;
- Criar um disco de recuperação de sistema;
- Ser cuidadoso ao utilizar o computador em locais públicos.



**PARA MAIS INFORMAÇÕES, EU RECOMENDO QUE VOCÊS ACESSEM O SITE DO CERT.BR. ESSA AULA TEÓRICA FOI COMPLETAMENTE BASEADA EM SEUS DOCUMENTOS. ACESSEM: [HTTP://WWW.CERT.BR](http://www.cert.br).**



## Terminologia

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



TERMINOLOGIA	DESCRIÇÃO
HACKER	Trata-se de um usuário experiente – exímio programador – que invade sistemas computacionais para provar suas habilidades, ampliar seus conhecimentos, descobrir novas técnicas e demonstrar vulnerabilidades, mas não para causar danos.
CRACKER	Trata-se de um usuário que invade sistemas para roubar informações, violar a integridade de sistemas, além de outras atividades maliciosas – podem também ser associados a indivíduos que decifram códigos indevidamente e destroem proteções de software para pirataria.
SCRIPT KIDDIES	Também chamado de Newbies, essa terminologia é utilizada para o hacker iniciante, que utiliza de ferramentas prontas na internet para realizar ataques a sistemas computacionais.
INSIDERS	Ameaças internas a uma instituição, funcionários descontentes ou insatisfeitos, corruptos ou subornados ou até mesmo enganados.
PHREAKING	É um especialista em telefonia, sua principal atividade é a realização de ligações gratuitas, clonagem e instalação de escutas em telefones fixos ou celulares.
WAREZ	Software pirata distribuído ilegalmente pela internet.
SPAM	Termo usado para se referir aos e-mails não solicitados geralmente enviados para um grande número de pessoas com finalidade comercial.



**(SEAD/AP - 2010)** Quando se trata da Gestão da Segurança da Informação, a terminologia empregada no mundo dos hackers assume papel de importância. A esse respeito, dois termos são a seguir descritos.

- I. É o hacking de sistemas telefônicos, geralmente com o objetivo de fazer ligações gratuitas ou para espionar ligações alheias;
- II. É o software pirata distribuído ilegalmente pela Internet. Esses dois termos são denominados, respectivamente como:

- a) phishing e worm.
- b) phreaking e warez.
- c) war dialer e worm.
- d) phreaking e phishing.
- e) phishing e warez.

**Comentários:** (I) Phreaking é o nome dado ao hacking de sistemas telefônicos; (II) Warez é o famoso software pirata (Letra B).

**(PCDF - 2012)** No mundo cibernético, qual é o termo utilizado para designar quem pratica quebra de proteções de softwares cedidos a título de demonstração usando-os por tempo indeterminado como se fossem cópias legítimas.

- a) worm
- b) hacker
- c) trojan
- d) malware
- e) cracker

**Comentários:** o indivíduo que "quebra" um sistema de segurança indevidamente, geralmente associados à pirataria, é o cracker (Letra E).

**(Câmara De Araraquara - 2016)** O termo técnico, em inglês, que se refere a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas com intuíto geralmente comerciais é denominado:

- a) zombie
- b) worm
- c) spam
- d) wiki

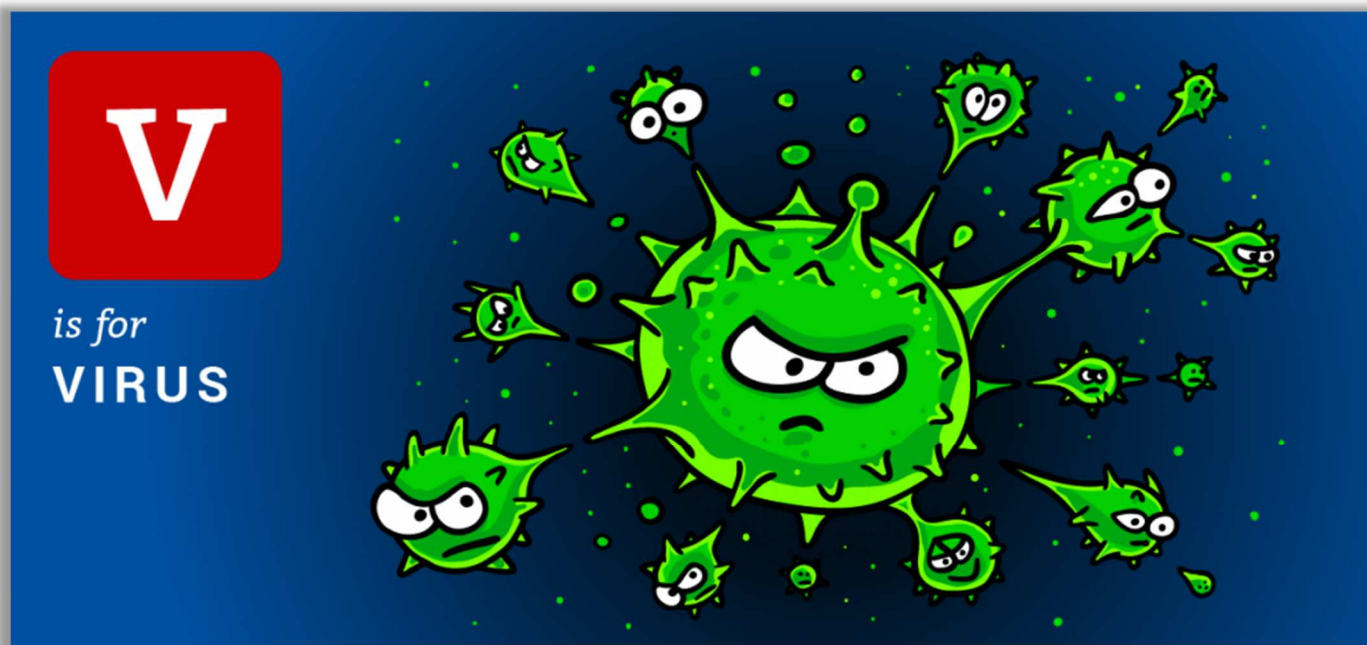
**Comentários:** os famosos e-mails não solicitados ou indesejados são chamados de spam (Letra C).



## Principais Malwares

### Vírus

INCIDÊNCIA EM PROVA: ALTÍSSIMA



Os vírus de computador foram introduzidos na década de 1980, com funções simples que ocasionalmente geravam inconvenientes ou apenas mostravam informações ao usuário. **Atualmente esse tipo de código traz um risco significativo com potencial destrutivo e que demanda grande esforço das organizações para manterem seus sistemas a salvo.** Mas o que é um vírus de computador?

**O vírus é um programa ou parte de um programa, normalmente malicioso<sup>1</sup>, que se propaga infectando, inserindo cópias de si mesmo, anexando-se ou hospedando-se em arquivos ou programas existentes na máquina.** Para que um código malicioso seja considerado um vírus, ele deve ter a capacidade de auto replicação, ou seja, fazer uma cópia de si mesmo e distribuir essa cópia para outros arquivos e programas do sistema infectado.

O principal objetivo de um vírus é replicar-se e contaminar o maior número possível de programas, de maneira a comprometer outros sistemas. **Para tal, o vírus depende da execução do programa ou arquivo hospedeiro para se tornar ativo e dar continuidade à infecção<sup>2</sup>!** Essa informação é

<sup>1</sup> Eles não precisam ser necessariamente destrutivos ou maliciosos para o sistema do usuário. Um vírus pode, por exemplo, simplesmente mostrar uma imagem na tela do computador.

<sup>2</sup> Para que um vírus recebido em um anexo de um e-mail seja ativado é necessário que anexo contaminado seja aberto ou executado. Logo, não é necessária a execução explícita do vírus em si, apenas do arquivo ou programa infectado.

bastante importante: vírus não são autossuficientes, eles necessitam da execução de um hospedeiro para se propagar pelas redes enviando cópias de si mesmo.

Pode-se dizer, então, que um vírus realiza duas tarefas: primeiro, replica-se das mais variadas formas; **segundo, executa seu código malicioso, podendo exercer diversas funcionalidades danosas na máquina infectada** – como exibir uma mensagem na tela do computador, tornar a máquina mais lenta, reiniciar o computador, apagar arquivos fundamentais do disco rígido ou, no limite, causar a destruição total de todos os dados armazenados na máquina.

**(TJ/SE – 2014)** Vírus são programas que podem apagar arquivos importantes armazenados no computador, podendo ocasionar, até mesmo, a total inutilização do sistema operacional.

**Comentários:** perfeito... vírus podem apagar arquivos importantes inutilizando o sistema operacional – cuidado! (Correto).

Um vírus é composto basicamente de três partes: **um mecanismo de infecção, um mecanismo de ativação e uma carga útil**. Vejamos na tabela a seguir como essas partes são definidas:

COMPOSIÇÃO DE UM VÍRUS		
MECANISMO DE INFECÇÃO	MECANISMO DE ATIVAÇÃO	CARGA ÚTIL
Meios ou formas pelas quais um vírus se propaga, habilitando-o a se reproduzir – é também conhecido como Vetor de Infecção.	Evento ou condição que determina quando a carga útil é ativada ou entregue – às vezes, é conhecido como Bomba Lógica.	O que o vírus faz, além de se espalhar. A carga útil pode envolver algum dano ou atividade benigna, porém notável.

**(Polícia Federal – 2018)** Uma das partes de um vírus de computador é o mecanismo de infecção, que determina quando a carga útil do vírus será ativada no dispositivo infectado.

**Comentários:** a questão trata – na verdade – do Mecanismo de Ativação (Errado).

Quando se trata de vírus de computador, eles podem ser classificados em quatro fases de execução: **Dormência, Propagação, Ativação e Ação**. Vejamos:

FASES	DESCRIÇÃO
DORMÊNCIA	Nessa fase, o vírus está ocioso. A certa altura, ele será ativado por algum evento, como uma data, a presença de outro programa ou arquivo, ou a ultrapassagem de algum limite de capacidade de disco. Nem todos os vírus têm esse estágio.
PROPAGAÇÃO	Nessa fase, o vírus instala uma cópia de si mesmo em outros programas ou em certas áreas do sistema no disco. A cópia pode não ser idêntica à versão de propagação; muitas vezes, os vírus mudam de forma para escapar à detecção. Agora, cada programa infectado conterá um clone do vírus, que também entrará em uma fase de propagação.





**(TJ/SE – 2014)** Os computadores com sistema operacional Linux não são afetados por vírus; os que têm sistemas Windows são vulneráveis a vírus, por falhas específicas de kernel.

**Comentários:** nenhum sistema operacional é imune a vírus e o Linux não é uma exceção (Errado).

Alguns tipos de vírus procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Outros tipos de vírus permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas – quando sua carga útil é ativada. **Galera, existem diversos tipos de vírus – vamos vê-los em detalhes nas próximas páginas. Fechado?**

## Vírus de Script

INCIDÊNCIA EM PROVA: ALTÍSSIMA

*Seus lindos, o que vocês acham que é um script?* Um ator, por exemplo, possui um script para saber o que ele deve falar em uma cena. **De forma similar, no mundo da tecnologia da informação, um script é um conjunto de instruções que devem ser executadas.** Por exemplo: páginas web estão lotadas de scripts escritos em uma linguagem chamada JavaScript que têm o intuito de tornar as páginas mais dinâmicas.

Se vocês desabilitarem esses scripts das páginas, vocês vão perceber que as páginas ficarão mais estáticas e sem diversas funcionalidades. Da mesma forma, documentos e arquivos de um computador podem conter scripts. *Querem um exemplo?* **Documentos do MS-Excel podem possuir as famosas macros, que são basicamente scripts que executam alguma funcionalidade no documento. Como assim, Diego?**

Galera, eu posso criar botão em um arquivo do MS-Excel que calcula, por exemplo, a média de valores de produtos vendidos em um supermercado – isso é feito por um macro, que é um tipo de script! **Diferente dos scripts de páginas web, essas macros são scripts escritos em uma linguagem chamada VBScript!** Em suma, vírus de script são softwares maliciosos que podem ser escritos em alguma linguagem de script (Ex: JavaScript ou VBScript).

**Em geral, eles são recebidos quando um usuário acessa uma página web ou faz o download de algum arquivo por-email, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML.** Logo, tomem bastante cuidado com os e-mails que vocês recebem – não saiam abrindo arquivos em anexo sem verificar antes – mesmo que seja recebido de algum remetente conhecido (lembre-se que o computador dele pode estar infectado).

Os vírus de script podem ser automaticamente executados, dependendo da configuração do navegador web ou do programa leitor de e-mails do usuário.



**(IFS/MS – 2016)** Os vírus de scripts, que são os vírus que exploram as linguagens de script, são executados automaticamente pelos softwares de leitura de e-mails, por exemplo.

**Comentários:** eles realmente exploram linguagens de script e são executados automaticamente pelos softwares de leitura de e-mails (Correto).

**(PRF – 2019)** No acesso a uma página web que contenha o código de um vírus de script, pode ocorrer a execução automática desse vírus, conforme as configurações do navegador.

**Comentários:** eles – de fato – podem ser executados automaticamente no acesso a uma página web que contenha o código de um vírus de script (Correto).

## Vírus de Macro

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Nós a-ca-ba-mos de ver o que é uma macro! Nós já sabemos que se trata de um tipo de script, logo os vírus de macro são um tipo específico de vírus de script – escrito em linguagem de macro – **que tenta infectar arquivos manipulados por aplicativos que utilizam essa linguagem como, por exemplo, os arquivos de dados que compõem o Microsoft Office (Excel, Word, PowerPoint, Access, entre outros).** Esse tipo de vírus despeeeeeeeenca em prova!

**Os vírus de macro utilizam técnicas de propagação baseadas em anexos de documentos que executam macros, uma vez que os usuários frequentemente compartilham documentos com recursos de macro habilitados.** Quando um software carrega um arquivo com esse código malicioso, ele executa as instruções do vírus nele contidas, que geralmente são as primeiras instruções executadas.

Galera, vejam a imagem a seguir! **Um dia desses eu recebi um e-mail de um remetente desconhecido falando comigo como se já nos conhecêssemos.** Havia três anexos com formato .mp4, .xlsx, .pptx. Era muito provável que os dois últimos tratassem de vírus de macro, apesar de haver outras possibilidades. *O que eu fiz?* Bloqueei o remetente e exclui a mensagem. Enfim, serviu pelo eu mostrar um caso real para vocês. Jamais abram anexos sem verificar antes!

### VÍRUS DE MACRO

Ele infecta documentos e, não, programas – grande parte das informações em um sistema de computador se encontra na forma de documentos e, não, de programas;

Ele é fácil de se propagar, já que os documentos que eles exploram normalmente são compartilhados – um método muito comum de distribuição é por meio do envio de e-mails;

Como ele infecta documentos de usuário, os tradicionais controles de acesso a sistemas de arquivo são de efetividade limitada para impedir que eles se espalhem;



Eles geralmente infectam arquivos de dados produzidos por suítes de aplicativos de escritório como o Microsoft Office;

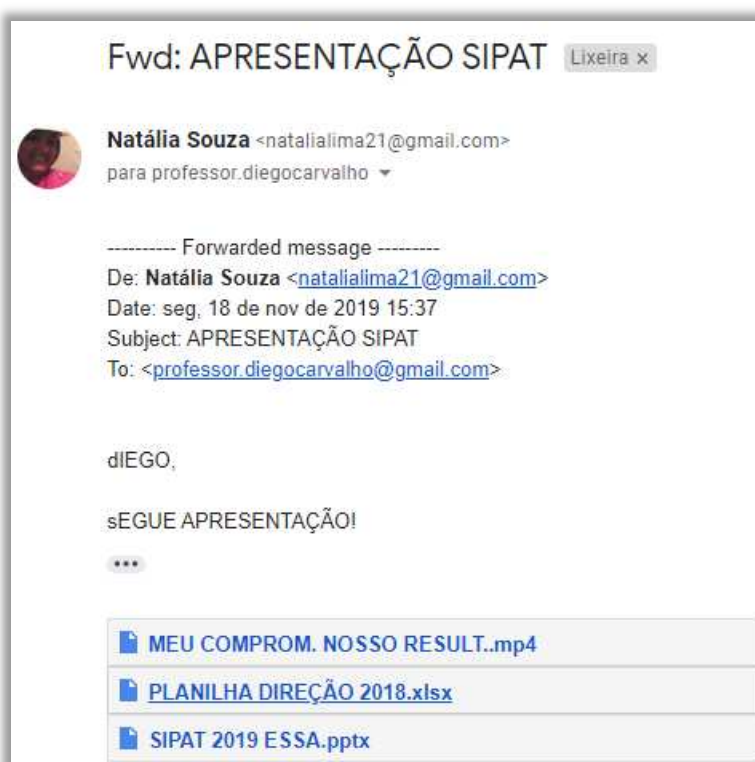
Vírus de Macro costumam alterar ou substituir um conjunto de comandos utilizados por programas para executar ações comuns;

É necessário que o arquivo que contém o vírus de macro seja aberto para que ele execute suas automaticamente instruções maliciosas e infecte outros arquivos no computador;

Eles podem ser bloqueados por meio de uma configuração específica dos programas do MS-Office. Para tal, deve-se bloquear a execução de macros em documentos;

A propagação ocorre quando documentos por ele infectados são remetidos por correio eletrônico para outros usuários;

A assinatura digital de um arquivo por meio da utilização de um certificado digital é possível evitar vírus de macro.



**(TRE/TO – 2011)** Arquivos de dados produzidos por suíte de aplicativos para escritório, por ex. Microsoft Office, costumam ser alvo predileto de contaminação por:

- a) trojans.    b) worms.    c) hijackers.    d) vírus de boot.    e) vírus de macro.

**Comentários:** arquivos de dados de aplicativos de escritório são típicos de contaminação por vírus de macro (Letra E).

**(CLDF – 2018)** Um usuário de um computador relatou para o Administrador do sistema computacional que, ao abrir um arquivo do tipo .DOC recebido por e-mail, o computador utilizado começou a realizar ações erráticas e desordenadas. A partir desse relato, o Administrador concluiu que o computador foi infectado pelo malware do tipo:



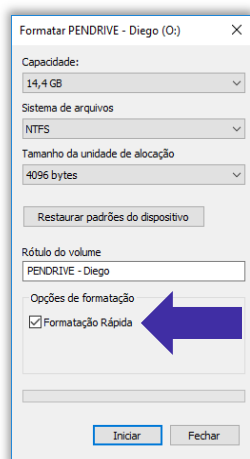
- a) Spyware
- b) vírus de macro.
- c) Trojan Dropper.
- d) Backdoor.
- e) Worm.

**Comentários:** um arquivo de uma suíte de escritório (MS-Word) pode conter macros, que podem conter vírus de macro capazes de realizar ações maliciosas (Letra B).

## Vírus de Boot

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

*Diego, o que é Boot?* Galera, trata-se do procedimento de inicialização do computador durante o carregamento do sistema operacional, logo após a máquina ser ligada! **O Vírus de Boot – também chamado de Vírus de Setor ou Vírus de Setor de Inicialização – é um dos primeiros tipos de vírus conhecidos e infecta a parte de inicialização do sistema operacional, escondendo-se no primeiro setor da memória.**



**Ele é ativado quando o computador é ligado e é carregado na memória antes mesmo do carregamento do sistema operacional.** Os Vírus de Boot afetam o procedimento descrito anteriormente e podem impedir que o sistema operacional seja executado de forma adequada – aliás, eles podem afetar inclusive dispositivos móveis de armazenamento como pendrives!

**A formatação rápida de um pendrive infectado não garante a remoção completa de vírus**, uma vez que alguns malwares conseguem se alojar na MBR (Master Boot Record) – que é o setor de inicialização de dispositivos de armazenamento. Recomenda-se, portanto, não selecionar a opção de Formatação Rápida apresentada na imagem acima.

**(BB – 2011)** Ativado quando o disco rígido é ligado e o sistema operacional é carregado; é um dos primeiros tipos de vírus conhecido e que infecta a partição de inicialização do sistema operacional. Trata-se de:

- a) vírus de boot.
- b) cavalo de Troia.
- c) verme.
- d) vírus de macro.
- e) spam.

**Comentários:** o vírus de boot (também chamado de partida ou inicialização) é ativado quando o disco rígido é ligado e o sistema operacional é carregado (Letra A).



**(CODHAB – 2018)** O vírus de boot é um vírus que age diretamente na inicialização do sistema de computadores conectados à rede. Contudo, ele não é espalhado por meio de dispositivos, como, por exemplo, pen drives.

**Comentários:** eles podem ser espalhados por meio de dispositivos de armazenamento móveis, uma vez que mídias removíveis são atualmente uma das maiores fontes de propagação de vírus (Errado).

## Vírus de Arquivo

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Também chamado de Vírus de Programa ou Vírus Parasitário, trata-se do vírus mais tradicional no cotidiano das pessoas. **Ele infecta arquivos executáveis, sobrescrevendo o código original e causando danos quase sempre irreparáveis.** Em geral, replicam-se ao localizar outros arquivos executáveis, embora possam também infectar arquivos que sejam requisitados para a execução de alguns programas, como os arquivos com as seguintes extensões.



**(SEPLAG/MG – 2013)** Assinale a única alternativa correta, que corresponde a seguinte definição: “Estes tipos de vírus são os que mais causam danos, pois atacam arquivos executáveis (.exe, .com, .ovl, .dll) sobrescrevendo o código original e causando danos quase sempre irreparáveis. Para ser contaminado por este vírus se deve executar um arquivo já infectado.”:

- a) Vírus invisível.
- b) Vírus de macro.
- c) Vírus de boot.
- d) Vírus de programa.

**Comentários:** os vírus que atingem arquivos executáveis são chamados de Vírus de Programa/Arquivo (Letra D).

**(Câmara de Jarú/RO – 2019)** Dos tipos de arquivo abaixo, você evitaria abrir para se proteger da instalação de um vírus o arquivo:

- a) .AWS
- b) .JPEG
- c) .MP3
- d) .EXE
- e) .XLS

**Comentários:** seria interessante evitar abrir arquivos no formato .exe porque essa é a extensão de arquivos executáveis – comuns em vírus de arquivo/programa (Letra D).



## Vírus Polimórfico

INCIDÊNCIA EM PROVA: MÉDIA



**Também chamado de Vírus Mutante, é capaz de assumir múltiplas formas a cada infecção com o intuito de burlar o software de antivírus.** Como ele faz isso, professor? Ele muda sua assinatura, mantendo suas funcionalidades e alterando apenas o seu padrão de bits. A assinatura é uma característica utilizada pelos antivírus para detectar a sua presença. Pode ser um nome, um comportamento ou o tamanho do vírus.

**Os vírus polimórficos são capazes de criar uma nova variante a cada execução, alterando tanto a rotina de encriptação quanto a rotina de decríptação.** Em geral, para realizar a detecção dessas ameaças, os antivírus fazem a decríptação do vírus usando um emulador ou realizam uma análise de padrão do corpo do vírus, uma vez que verificar a assinatura é pouco efetivo em um contexto em que o código muda, mas a semântica, não.

**(CFA – 2010)** Tem a capacidade de gerar réplicas de si mesmo utilizando-se de chaves de encriptação diversas, fazendo com que as cópias finais possuam formas diferentes. A polimorfia visa a dificultar a detecção de utilitários antivírus, já que as cópias não podem ser detectadas a partir de uma única referência do vírus. Tal referência normalmente é um pedaço do código virótico, que no caso dos vírus polimórficos varia de cópia para cópia. O texto do enunciado da questão está se referindo aos vírus:

- a) de scripts.
- b) criptografados.



- c) mutantes.
- d) stealth ou furtivos.

**Comentários:** os vírus que variam de cópia para cópia com formas diferentes são os vírus mutantes/polimórficos (Letra C).

Uma variação do vírus polimórfico é o vírus metamórfico que, diferentemente do vírus polimórfico – se reescreve completamente a cada infecção, podendo mudar seu tamanho e comportamento, aumentando a dificuldade de detecção. Aqui não tem muito o que falar: basta lembrar que o Vírus Polimórfico muda apenas a sua assinatura, mantendo sua funcionalidade, e o Vírus Metamórfico muda sua assinatura e sua funcionalidade.

**(SUGEP – 2018 – Letra B)** O vírus metamórfico muda a cada infecção, se reescrevendo completamente a cada iteração, aumentando a dificuldade de detecção.

**Comentários:** o vírus metamórfico realmente muda a cada infecção, reescrevendo-se e dificultando bastante a sua detecção (Correto).

## Vírus Stealth

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



Vocês já ouviram falar no avião Lockheed Blackbird SR-71? Ele é conhecido por ser o avião mais incrível de toda a história da aviação. Por que ele era tão especial, Diego? **Galera, esse avião tinha uma característica muito peculiar: ele era praticamente invisível a radares, sendo capaz de**

**refletir ou absorver ondas eletromagnéticas.** Por conta disso, ele ganhou a denominação de Avião Furtivo ou Stealth. *Professor, o que isso tem a ver com a aula?*

*Pessoal, vocês acreditam que nós temos um tipo de vírus chamado de Vírus Stealth? Também chamado de Vírus Furtivo, eles são projetados explicitamente para não serem detectados pelo antivírus,* possuindo a capacidade de se remover da memória do computador temporariamente para evitar que o antivírus o detecte. Da mesma forma que o avião stealth era capaz de se esconder de radares, o vírus stealth é capaz de se esconder de antivírus.

**(TCU – 2015)** O vírus do tipo stealth, o mais complexo da atualidade, cuja principal característica é a inteligência, foi criado para agir de forma oculta e infectar arquivos do Word e do Excel. Embora seja capaz de identificar conteúdos importantes nesses tipos de arquivos e, posteriormente, enviá-los ao seu criador, esse vírus não consegue empregar técnicas para evitar sua detecção durante a varredura de programas antivírus.

**Comentários:** a questão trata – na verdade – dos Vírus de Macro (Errado).

## Vírus Time Bomb

INCIDÊNCIA EM PROVA: MÉDIA

Também conhecido como Vírus Bomba Relógio, trata-se de um vírus que – após infectar a máquina – permanece latente (oculto), apenas se replicando. **Além disso, seu código malicioso é programado para ser ativado em um determinado momento específico, executando sua carga útil.** É comumente distribuído como anexo de e-mails e se instalam em computadores pela ação do usuário, ao executar o arquivo.

**Os Time Bombs se instalam silenciosamente e agem apenas em datas ou momentos determinados, que são definidos pelo seu criador.** Alguns vírus conhecidos foram:

- Sexta-feira 13 (ações danosas apenas nas sextas-feiras 13);
- I Love you (ação danosa apenas no dia dos namorados - 12 de junho)
- Chernobyl (ação danosa apenas no dia do acidente nuclear - 25 de abril)

**(MTE – 2014)** Quando ativado na máquina, a principal característica do vírus time bomb é a sua capacidade de remover o conteúdo do disco rígido em menos de uma hora.

**Comentários:** a principal característica do Vírus Time Bomb é sua capacidade de ser ativado em momentos específicos – definidos pelo criador. Não há necessariamente nenhuma relação com a remoção do conteúdo do disco rígido em menos de uma hora (Errado).

## Vírus de E-Mail

INCIDÊNCIA EM PROVA: MÉDIA



**Os vírus propagados por e-mail são recebidos como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado.** Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador. Por essa razão, é importante desabilitar a autoexecução de arquivos anexos em e-mails e verificar a sua extensão.

**(TJ/SE – 2009)** Quanto às medidas sensatas e objetivas de precaução contra a propagação de vírus por e-mail, considere:

- I. Nunca abrir arquivos anexados às mensagens.
- II. Desabilitar, no programa leitor de e-mails, a auto-execução de arquivos anexados às mensagens.
- III. Não anexar arquivos às mensagens.
- IV. Excluir todos os e-mails que forem recebidos com arquivos anexados.

Está correto o que se afirma APENAS em:

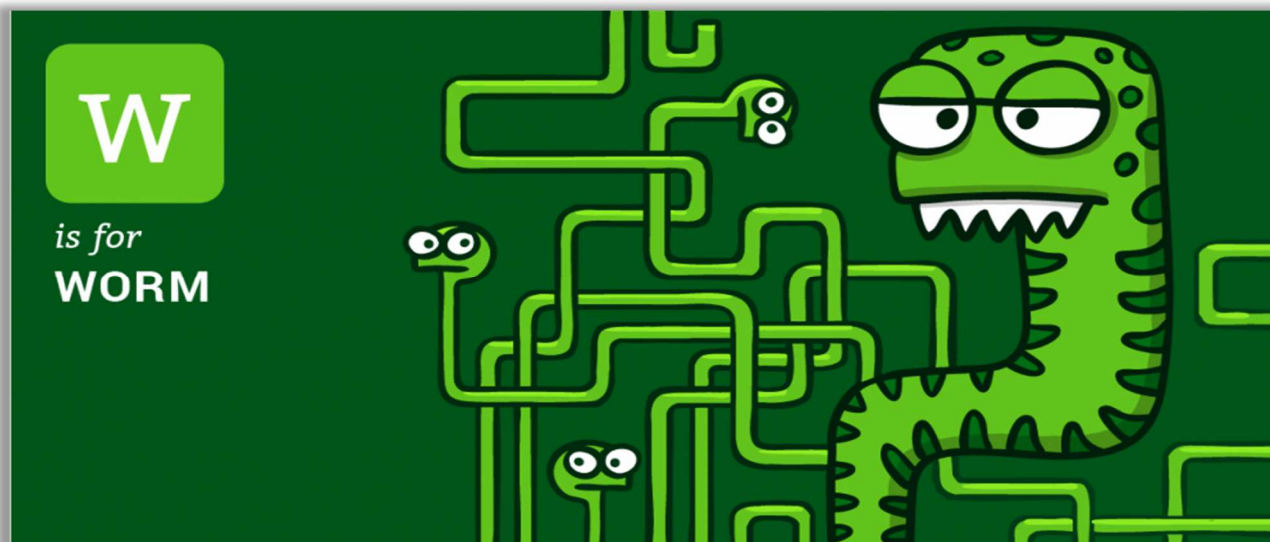
- a) I.
- b) I e II.
- c) II.
- d) II e III.
- e) III e IV.

**Comentários:** (I) Errado, pode-se abrir arquivos anexados às mensagens, mas é importante passar previamente por algum antivírus; (II) Correto, isso é importante para que o leitor de e-mails não faça o download automático sem verificação do arquivo; (III) Errado, isso não é necessário; (IV) Errado, isso não é necessário (Letra C).



## Worm

INCIDÊNCIA EM PROVA: ALTÍSSIMA



Worm (ou Verme) é um programa capaz de se replicar automaticamente, enviando cópias de si mesmo de computador para computador. **Diferente dos vírus, ele não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos através da rede**, mas – sim – pela exploração automática de vulnerabilidades existentes em programas instalados em computadores ou pela execução direta de suas cópias.

Pois é! Nesse primeiro parágrafo, nós temos dois pontos que necessitam de mais atenção: primeiro, worms podem – sim – ser executados diretamente, apesar de não ser a regra; segundo, worms não infectam outros arquivos, eles mesmos são os arquivos. Eles identificam computadores ativos na rede e exploram as conexões ou através da Internet por meio de correio eletrônico, redes sociais, bate papo, entre outros.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores. **O processo de infecção e propagação ocorre em quatro fases: identificação dos computadores alvos; envio das cópias; ativação das cópias; e reinício do processo.**

- **Identificação de computadores-alvo:** também conhecido como *scanning*, após infectar um computador, ele tenta se propagar e continuar o processo de infecção. Para tal, ele necessita identificar os computadores alvos para os quais tentará se copiar;
- **Envio de cópias:** após identificar os alvos, ele efetua cópias de si mesmo e tenta enviá-las para estes computadores anexadas a e-mails, via canais de IRC, via programas de troca de mensagens instantâneas, incluídas em pastas compartilhadas em redes locais, etc;



- **Ativação de cópias:** após realizado o envio da cópia, ele necessita ser executado para que a infecção ocorra, o que pode acontecer imediatamente após ter sido transmitido, diretamente pelo usuário ou condicionado a algum evento específico (como a inserção de uma mídia):
  - imediatamente após a transmissão, pela exploração de vulnerabilidades em programas sendo executados no equipamento alvo no momento do recebimento da cópia;
  - diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu equipamento;
  - pela realização de uma ação específica do usuário, a qual o worm está condicionado como, por exemplo, a inserção de uma mídia removível.

**Os worms são capazes de entrar em uma máquina sem qualquer interação do usuário.** Em geral, podem ser obtidos automaticamente pela rede, recebidos por e-mail, baixados de páginas na web, pelo compartilhamento de arquivos, pelo uso de mídias removíveis infectadas, por meio de redes sociais, por meio de mensagens instantâneas, por conta de uma invasão de um hacker ou pela ação de outro código malicioso.

*E quais são as ações maliciosas mais comuns de um worm?* **Sua ação maliciosa mais comum consiste em 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 do computador.** Além disso, eles podem instalar outros códigos maliciosos no computador, desferir ataques na internet e enviar e-mails sem autorização.

**Sobre ações maliciosas, é importante destacar novamente que worms não infectam arquivos.** Em resumo, os worms são programas autorreplicantes completos e autônomos que não necessitam de um programa hospedeiro para se propagar. Diferentemente dos vírus, esse programa não embute cópias de si mesmo em outros programas ou arquivos – além de não precisarem ser explicitamente executados para se propagar. *Fechado?*



**WORM = VERME**

**ALGUNS DIZEM QUE SEU NOME VEM DE: WRITE ONCE RUN EVERYWHERE**

# CURIOSIDADE SOBRE WORMS: [HTTPS://WWW.YOUTUBE.COM/WATCH?V=SF6MYPWIHHQ](https://www.youtube.com/watch?v=SF6MYPWIHHQ)

# CURIOSIDADE SOBRE WORMS: [HTTPS://WWW.YOUTUBE.COM/WATCH?V=UM9G6TO\\_61W](https://www.youtube.com/watch?v=UM9G6TO_61W)

**(Prefeitura de Apodi/RN – 2019)** Os malwares são programas maliciosos cujo objetivo é roubar informações ou contaminar os computadores. O malware que tem a capacidade de se propagar na rede de computadores é o:

- a) vírus
- b) worm
- c) netmal
- d) trojan.



**Comentários:** o malware que busca se propagar na rede de computadores é o worm (Letra B).

**(PC/MG – 2018)** O tipo de ameaça à segurança de um computador que consiste em um programa completo que se replica de forma autônoma para se propagar para outros computadores é:

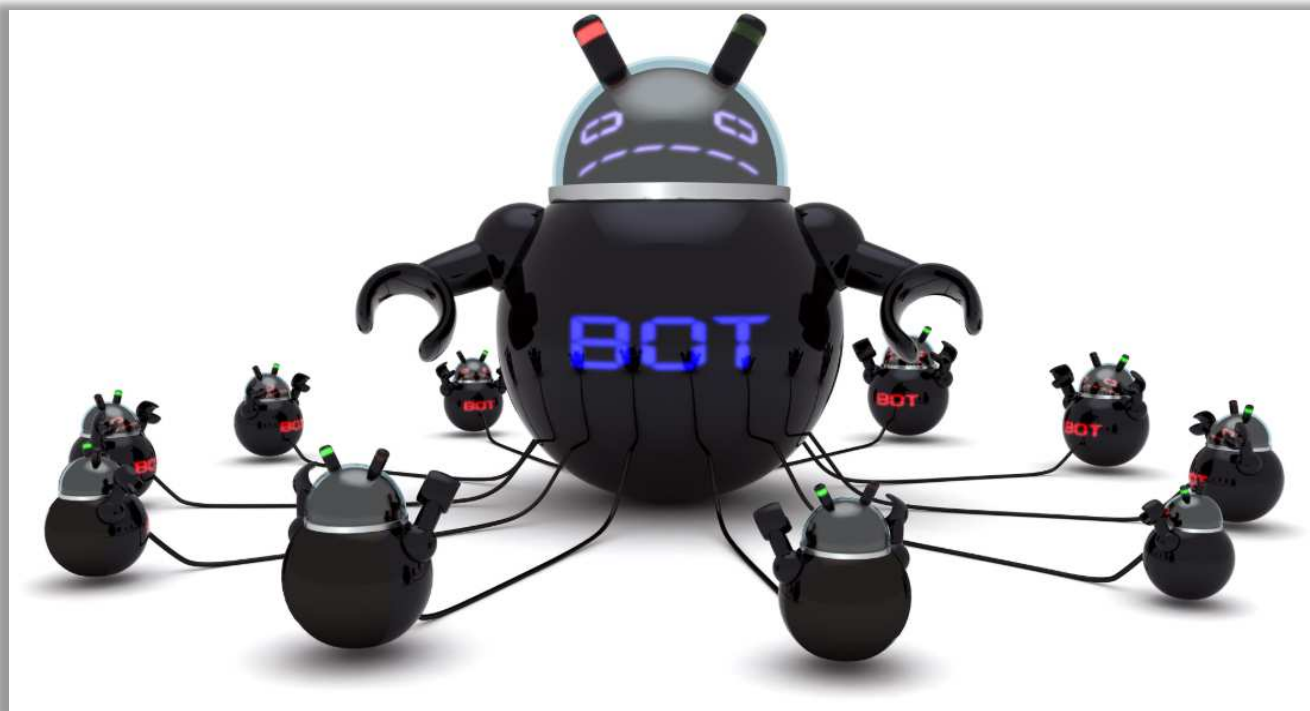
- a) Worm
- b) Vírus
- c) Spyware
- d) Spam.

**Comentários:** programa completo que se replica de forma autônoma só pode ser worm (Letra A).



## Bot e Botnet

INCIDÊNCIA EM PROVA: ALTA



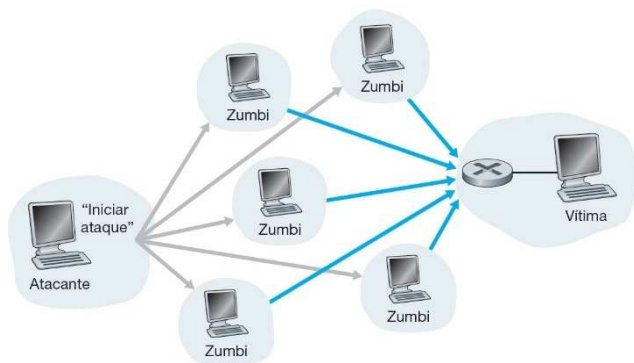
**Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente.** Possui processo de infecção e propagação similar ao do Worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. A comunicação entre o invasor e o computador infectado pode ocorrer via IRC, Servidor Web, Redes P2P, entre outros.

**Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.** Um computador infectado por um bot costuma ser chamado de zumbi, porque ele pode ser controlado remotamente e sem o conhecimento do seu dono. É chamado de Zumbi de Spam quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio de spam.

*Diegão, não entendi muito bem!* Galera, imagine que você está aí todo feliz no seu computador, mas ele possui um bot zumbi instalado. *Sabe o que isso significa?* Significa que alguém pode estar controlando à distância o bot presente no seu computador, podendo realizar diversas atividades maliciosas. **Em alguns casos específicos, o hacker nem quer destruir nada em seu computador, ele quer apenas utilizá-lo para enviar e-mails spam para outras pessoas.**

O ideal para proteger seus dados quando se detecta que ele está infectado por um bot é desconectar o computador da rede o mais rápido possível. **Já uma Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permitem potencializar as ações danosas**

**executadas pelos bots.** Quanto mais zumbis participarem da Botnet, mais potente serão as ações danosas. *Compreendido?*



**O atacante que a controlar – além de usá-la para seus próprios ataques – também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.** As ações maliciosas mais comuns são: ataques de negação de serviço; propagação de códigos maliciosos (inclusive do próprio Bot); coleta de informações de outros computadores; envio de spam; camuflagem da identidade de hackers; etc.

O esquema simplificado apresentado a seguir exemplifica o funcionamento básico de uma botnet (rede de bots):

1. Um atacante propaga um tipo específico de bot na esperança de infectar e conseguir a maior quantidade possível de zumbis;
2. Os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;
3. Quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;
4. Os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;
5. Quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

**Em suma: Bot é um programa que possui mecanismos de replicação, infecção e ações maliciosas similares aos de um worm, entretanto dispõe de mecanismos de comunicação que permitem que ele seja controlado remotamente.** É utilizado para realizar ações repetitivas, se fazendo passar por um ser humano, em que a máquina infectada passa a ser chamada de zumbi e sem o conhecimento do usuário pode ser utilizada para ações maliciosas.



**BOT = DIMINUTIVO DE ROBÔ = ROBÔ; NET = REDE;**

**BOT = ROBÔ; BOTNET = REDE DE ROBÔS**

**(Polícia Federal – 2014)** Computadores infectados por botnets podem ser controlados remotamente bem como podem atacar outros computadores sem que os usuários percebam.

**Comentários:** computadores infectados por bots que formam botnets realmente podem ser controlados remotamente como podem atacar outros computadores sem serem notados (Correto).



## Trojan Horse

INCIDÊNCIA EM PROVA: ALTA



**O Trojan é um software malicioso que age por meio da utilização do princípio do Cavalo de Troia.** Quem se lembra dessa história? Os gregos queriam invadir a cidade de Troia, no entanto essa cidade era cercada por uma grande muralha. Como a invasão de uma cidade fortificada era bastante complexa, os gregos tiveram a ideia de dar um presente aos troianos. *O que era, Diego?* Era uma grande estátua de madeira no formato de um cavalo, mas tinha uma particularidade...

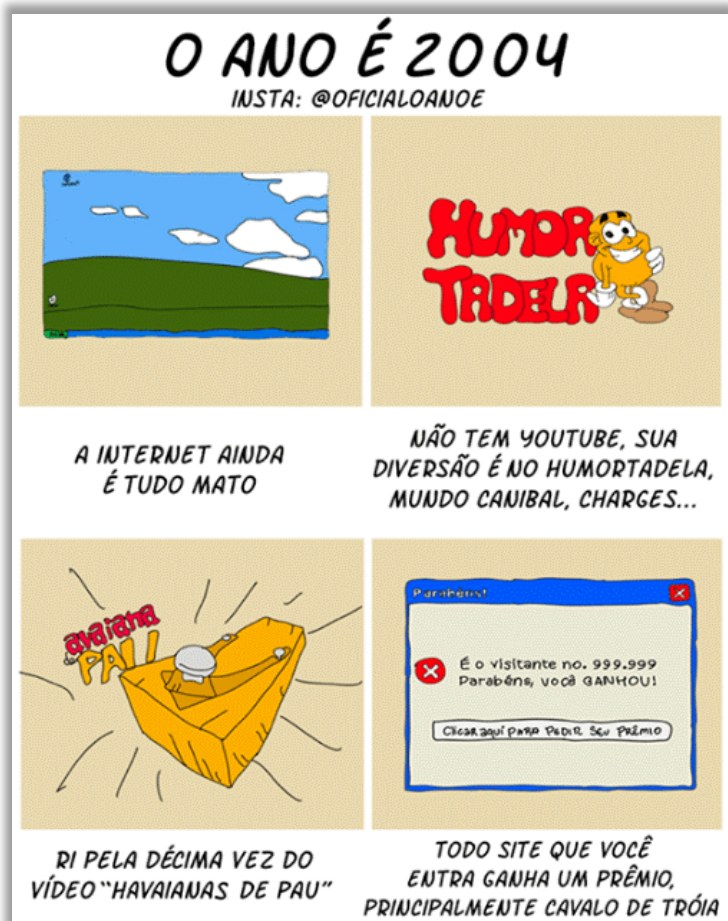
Dentro do cavalo de madeira estavam diversos soldados gregos. Os troianos acharam que os gregos estavam sendo corteses, aceitaram o presente e levaram o cavalo para dentro da cidade fortificada. À noite, os soldados gregos que estavam escondidos dentro do cavalo saíram, dominaram os sentinelas e possibilitaram a entrada do exército grego, levando a cidade à ruína. **Resumo da história: muito cuidado com os "presentes de grego" que vocês aceitam!**

**O Trojan Horse – também chamado de Cavalo de Troia – é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.** Ele é enviado se fazendo passar por um aplicativo útil, mas é capaz de abrir portas de comunicação de um computador para que a máquina possa ser invadida ou monitorada através da Internet.

**Em outras palavras, eles podem ser instalados por atacantes que – após invadirem um computador – alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.** Exemplos de trojans são programas

que você recebe ou obtém de sites na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros.

**Estes programas, geralmente, consistem em um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador** – ao contrário dos vírus, ele não se replica automaticamente. O Cavalo de Troia trabalha com um modo de infecção que envolve despertar a curiosidade do usuário para que este o execute e, assim, possa infectar e comprometer o sistema. Galera, a variedade de atividade maliciosa que um Trojan pode fazer é inacreditável...



*Professor, agora estou com medo – o que eu tenho que fazer para evitar que um Trojan seja instalado no meu computador uma vez que você disse que ele parece inofensivo? Pois é! Quem é mais velho como eu (31 anos) se identificará com a imagem ao lado. Você acessava um site e, não mais que de repente, aparecia um pop-up na tela informando que você havia ganhado um prêmio. Para buscá-lo, bastava clicar no botão apresentado. Esse era o momento em que você fazia o download de um trojan capaz de comprometer a segurança do seu computador. Então prestem bastante atenção em tudo que vocês baixam na internet, em especial aqueles arquivos recebidos por e-mail e não baixem softwares piratas! *Estão vendo agora como informática é maravilhoso? Diz aí no fórum se não é a matéria mais legal da vida? Se você não acha, mente no fórum um pouquinho pelo menos para eu ficar feliz :)**

Galera... algumas bancas (em especial, CESPE) consideram o cavalo de troia como um tipo de vírus, podendo ser instalados por outros vírus ou programas – além de poder infectar o ambiente por meio de links durante a navegação ou até mesmo por meio de phishing. *Não adianta brigar com a banca, ok? Bem... como prova de que se trata de um malware extremamente versátil, existem vários tipos de trojans, classificados de acordo com as ações maliciosas que costumam executar.*

TIPO DE TROJAN	DESCRIÇÃO
TROJAN DOWNLOADER	Instala outros códigos maliciosos, obtidos de sites na Internet.
TROJAN	Instala outros códigos maliciosos, embutidos no próprio código do trojan.



<b>DROPPER</b>	
<b>TROJAN BACKDOOR</b>	Inclui backdoors, possibilitando o acesso remoto do atacante ao computador.
<b>TROJAN DOS</b>	Instala ferramentas de negação de serviço e as utiliza para desferir ataques.
<b>TROJAN DESTRUTIVO</b>	Altera ou apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
<b>TROJAN CLICKER</b>	Redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
<b>TROJAN PROXY</b>	Instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.
<b>TROJAN SPY</b>	Instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
<b>TROJAN BANKER</b>	Coleta dados bancários do usuário através da instalação spyware que são ativados quando sites de Internet Banking são acessados – similar ao Trojan Spy, mas com objetivos específicos.



**TROJAN = TROIA; HORSE = CAVALO**

**TROJAN HORSE = CAVALO DE TROIA**

**(TRT/PE – 2018)** Considere o texto abaixo:

*Um grupo de especialistas em segurança encontrou um novo tipo de malware, que está se espalhando massivamente por meio do Facebook Messenger. Trata-se do Digmine, um malware que usa sistemas infectados para extrair a criptomoeda Monero. Esse malware é enviado às vítimas como um link para um arquivo de vídeo, quando na verdade é um script executável que afeta as versões desktop e web do Facebook Messenger, usando o navegador Google Chrome para minerar a moeda Monero no computador.*

(Adaptado de: <https://guiadobitcoin.com.br/>)

Esse tipo de malware, que parece ser uma coisa (vídeo), mas na realidade é outra (script de mineração), é categorizado como:

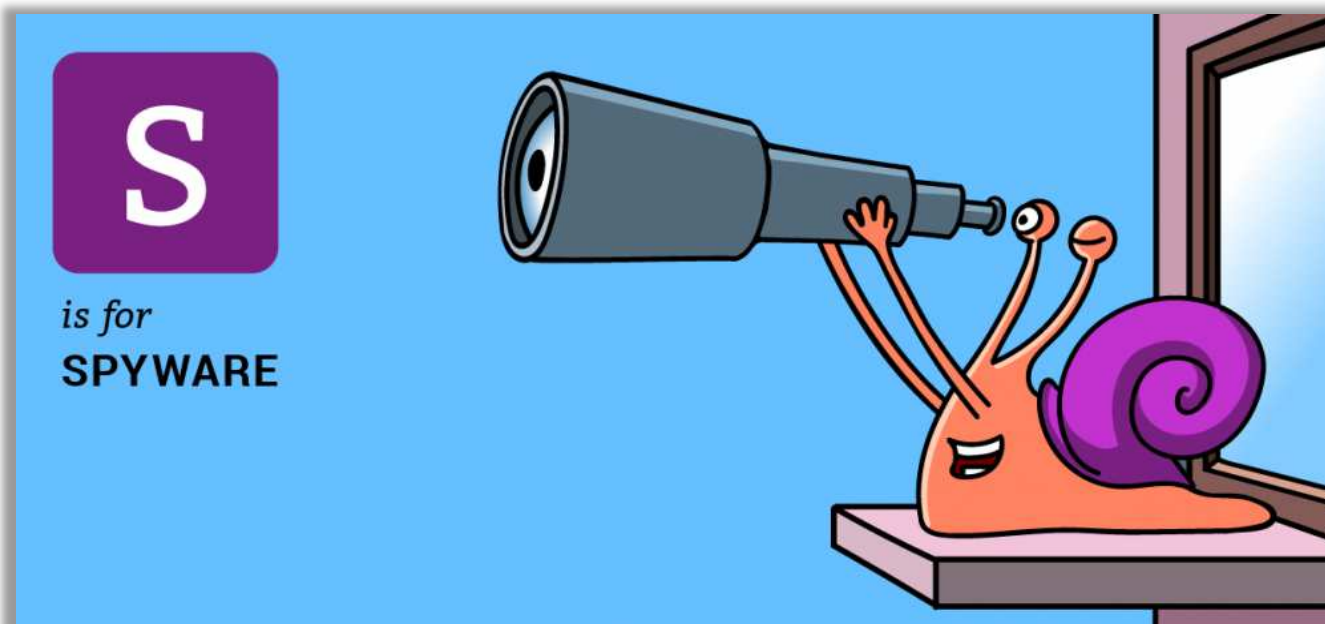
- a) trojan.
- b) backdoor.
- c) adware.
- d) rootkit.
- e) ransomware.

**Comentários:** o malware que parece ser uma coisa legítima, mas é outra coisa maliciosa como um presente de grego é o Trojan (Letra A).



## Spyware

INCIDÊNCIA EM PROVA: ALTÍSSIMA



Um **spyware** é um software espião, capaz de violar a privacidade das informações de usuários, coletando dados da máquina ou da rede e disponibilizando-as a terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

- **Legítimo**: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.
- **Malicioso**: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Como esse é um dos malwares que mais cai em prova, eu resolvi fazer uma **consolidação das principais definições encontradas em prova**. Dessa forma, pode-se dizer que um **Spyware** é:

### DEFINIÇÕES DE SPYWARE

Um programa automático de computador que recolhe informações sobre o usuário e as envia a uma entidade externa na Internet, sem o conhecimento/consentimento do usuário.

Um software malicioso que recolhe informações sobre o usuário do computador e as transmite para alguém externo, sem conhecimento do usuário.

Um programa espião que monitora as atividades de um sistema e envia as informações coletadas para os invasores/terceiros.



Uma praga virtual que se aloja em uma máquina e, quando em ação, produz uma falsa impressão de normalidade, obtendo dados importantes (Ex: senhas).

Um programa automático instalado em um computador, que têm como finalidade capturar informações sobre o usuário e transmiti-las externamente sem a sua prévia autorização.

Uma aplicação que recolhe automaticamente dados sobre atividades e hábitos de um usuário na internet e transmite essa informação a uma entidade externa.

**Diferentemente dos vírus, os spywares precisam ser explicitamente executados pelo usuário para infectar<sup>3</sup> uma máquina (a infecção de vírus é feita pela execução do arquivo hospedeiro).** Ademais, para combatê-los, recomenda-se a utilização de um Anti-Spyware, que são softwares que se destinam a detectar e remover spywares. *Bacana?* Os tipos mais comuns de spywares são os keyloggers, screenloggers e adwares.



**SPY = ESPÃO**

**SPYWARE = SOFTWARE ESPÃO**

**(PC/ES - 2012)** Ter receio de se fazer compras on-line ou de se acessar o sítio de um banco pela Internet justifica-se, atualmente, pela possibilidade de perda de privacidade causada por softwares maliciosos capazes de enviar dados privativos referentes a senhas de acesso a contas bancárias e números de cartão de crédito a outras máquinas conectadas remotamente na Internet.

**Comentários:** todas essas são características de um spyware (Correto).

**(TCE-SP - 2015)** Dentre os tipos de malwares, o spyware se caracteriza por:

- a) capturar as teclas digitadas no computador infectado e enviar as informações para o invasor.
- b) explorar falhas do sistema operacional para controlar o computador infectado.
- c) permitir o acesso contínuo ao computador infectado.
- d) propagar-se automaticamente pela rede enviando cópias para outros computadores.
- e) monitorar as atividades de um sistema e enviar as informações coletadas para o invasor.

**Comentários:** ele monitora as atividades de um sistema e envia as informações coletadas para o invasor. A primeira opção trata do Keylogger, que é um tipo de Spyware, logo também poderia ser uma resposta. No entanto, a última opção é "mais correta". Concurseiro tem que se acostumar com isso infelizmente (Letra E).

<sup>3</sup> Note que eu disse que é necessário que ele seja executado para infectar uma máquina e, não, para se propagar. Vírus se propagam inserindo cópias de si próprios em arquivos; Worms se propagam enviando cópias de si próprios automaticamente pela rede ou e-mail; e spywares não se propagam.



## Backdoor

INCIDÊNCIA EM PROVA: ALTA



**Backdoor (em português, Porta dos Fundos) é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.** Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, ele é utilizado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, **sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.** Há casos, inclusive, de Backdoors incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. *Sinistro, não é?*

Esses casos constituem uma séria ameaça à segurança de um computador que contenha um destes programas instalados, pois – além de comprometerem a privacidade do usuário – também podem ser usados por invasores para acessarem remotamente computadores. **Em suma: esse software malicioso é capaz de abrir Portas TCP para que seja possível que um invasor acesse o computador remotamente.** *Professor, qual é a diferença entre Backdoor e Bot? São muitas...*



BACKDOORS	BOTS
São obtidos somente pela inserção por um invasor ou pela ação de outro código malicioso	Podem ser obtidos de diversas outras maneiras
São instalados via execução de outro código malicioso	São instalados pela sua execução explícita
Não são capazes de se propagar	São capazes de propagar
Buscam possibilitar o retorno do invasor a própria, mantendo-se escondidos	Possuem realizar ataques coordenados a máquinas de terceiros.



**BACK = FUNDO; DOOR = PORTA**

**BACKDOOR = PORTA DOS FUNDOS**

**(COMPESA – 2018)** Os códigos maliciosos fazem inúmeras vítimas e provocam os mais variados prejuízos. Quando esse código se instala na máquina da vítima para permitir conexões remotas, funcionando como um controle remoto, é classificado como:

- a) Adware.
- b) Spyware.
- c) Keylogger.
- d) Worm.
- e) Backdoor.

**Comentários:** dentre os códigos maliciosos apresentados, aquele que permite conexões remotas funcionando como um controle remoto é o backdoor (Letra E).

**(IBGE – 2017)** Curioso, um usuário baixou e instalou em seu computador um suposto jogo erótico que viu em um site desconhecido. O jogo era, na verdade, um software que passou a permitir remotamente o controle do computador do usuário. É possível concluir que esse comportamento é típico de um malware denominado:

- a) vírus
- b) keylogger
- c) adware
- d) worm
- e) backdoor

**Comentários:** um software que passou a permitir controle remoto por parte de um usuário mal intencionado, logo esse comportamento é típico de um backdoor (Letra E).



## Rootkit

INCIDÊNCIA EM PROVA: MÉDIA



Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. **É muito importante ressaltar que o nome rootkit não indica que os programas e as técnicas que o compõem são usados para obter acesso privilegiado a um computador, mas – sim – para mantê-lo.** O conjunto de programas e técnicas fornecido pelos rootkits pode ser usado para:

- Remover evidências em arquivos de logs (arquivos de registro de ações de um sistema);
- Instalar códigos maliciosos (ex: *backdoors*), para assegurar acesso futuro à máquina infectada;
- Esconder atividades/informações (Ex: arquivos, diretórios, processos, chave de registro, etc);
- Mapear potenciais vulnerabilidades em outros computadores, através de varreduras na rede;
- Capturar informações da rede do computador pela interceptação de tráfego.

Rootkits inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, **sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador.** Apesar de ainda serem bastante usados por atacantes, os rootkits atualmente têm sido também tem uma outra função.

Eles são utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção. **Galera, os rootkits são um dos tipos de malware mais sofisticados que existem atualmente.** Por anos, as soluções de segurança têm lutado contra a sua detecção e remoção, principalmente porque eles comprometem o sistema operacional. *Como é, professor?*



Sim, eles comprometem o sistema operacional em um nível tão profundo que podem camuflar sua presença tanto das soluções antimalware quanto do próprio sistema operacional. Ao contrário do malwares tradicionais, os *rootkits* introduzem uma falha fundamental nos computadores que infectam: **eles não comprometem arquivos ou pastas – em vez disso, eles alteram tudo o que o sistema operacional informa de acordo com as necessidades do criador.**

**Quando algum sistema operacional efetua um pedido de leitura de um arquivo, o rootkit intercepta os dados que são requisitados e faz uma filtragem dessa informação, deixando o sistema ler apenas arquivos não infectados.** Dessa forma, ferramentas antimalware ficam impossibilitadas de encontrar o arquivo malicioso no computador. Galera, mesmo que você consiga remover o rootkit, o sistema operacional não volta a sua condição original porque já foi modificado.

**Ao utilizar um rootkit, um criminoso tem privilégios totais de administrador para o seu computador e softwares,** convenientemente acessando logs, monitorando sua atividade, roubando informações e arquivos privados, e mexendo em suas configurações. Sem você saber, todas as suas senhas e informações poderão ser roubadas. É interessante enfatizar também que ele geralmente é formado por um conjunto de arquivos executáveis.

Rootkits podem se instalar em diferentes níveis do sistema. Para cada nível, o rootkit se estabelece de uma forma diferente e requer, portanto, estratégias diferenciadas para ser detectado. À medida em que ficamos mais próximos do hardware, aumenta-se o poder de controle do atacante, assim como a complexidade de sua detecção. **Os principais modos de operação são em Modo Usuário (que se instala em aplicativos) e Modo Kernel<sup>4</sup> (que se instala no núcleo do sistema operacional).**



**Alunos sempre me perguntam no fórum qual é a diferença entre Rootkit e Backdoor.** Eles realmente são bastante parecidos em relação à obtenção, instalação e propagação. No entanto, os rootkit são bem mais avançados e complexos – trata-se de um conjunto de funcionalidades maliciosas capaz de camuflar a presença do invasor, apagar evidências, remover logs e infectar o núcleo do sistema operacional, geralmente implicando a formatação da máquina do usuário.



**ROOT = ADMINISTRADOR (LINUX)**

**ROOTKIT = KIT DO ADMINISTRADOR**

<sup>4</sup> Kernel é o núcleo do sistema operacional, a camada que liga os aplicativos ao hardware – é ele que controla a CPU, a memória, e os dispositivos de entrada e saída.



**(TRT/24 – 2017)** *É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Pode ser usado para: remover evidências em arquivos de logs; instalar outros códigos maliciosos, como backdoors, para assegurar o acesso futuro ao computador infectado; esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede etc.; mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede; capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego; dentre outras possibilidades. No entanto, seu nome não indica que os programas e as técnicas que o compõem são usadas para obter acesso privilegiado a um computador, mas sim para manter o acesso privilegiado.*

(Disponível em: <http://cartilha.cert.br/malware/>)

O texto descreve um tipo de ameaça à segurança das informações conhecido como:

- a) rootkit.
- b) engenharia social.
- c) wardriving.
- d) worm.
- e) bot.

**Comentários:** conjunto de programas e técnicas? Já dá para desconfiar que se trata de um Rootkit. Permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido? Sim, é definitivamente um Rootkit. Engenharia Social é um golpe e, não, um malware; Wardriving não tem relação com o enunciado; Worm não é um conjunto de programas e técnicas e nem busca esconder a presença de um invasor ou código malicioso; e bot também não é um conjunto de programas e técnicas (Letra A).

**(IDAM - 2019)** *“A capacidade de se esconder permite que este tipo de malware permaneça no sistema da vítima por meses, às vezes até anos, deixando que um hacker use o computador para o que bem entender. Mesmo uma máquina que não contém informações valiosas, o que é pouco comum, pode ser útil para produzir bitcoins (moeda digital), enviar spam e participar de ataques DDoS.”* Essa é uma definição do malware denominado:

- a) adware
- b) spyware
- c) keylogger
- d) rootkit

**Comentários:** capacidade de se esconder, permitindo que o hacker use o computador para o que bem entender são características típicas de um rootkit (Correto).



## Tabela Comparativa

# RESUMO DE CÓDIGOS MALICIOSOS

	VÍRUS	WORM	BOT	TROJAN	SPYWARE	BACKDOOR	ROOTKIT
<b>FORMA DE OBTENÇÃO</b>							
Recebido automaticamente pela rede		X	X				
Recebido por <i>e-mail</i>	X	X	X	X	X		
Baixado de <i>sites</i> na Internet	X	X	X	X	X		
Compartilhamento de arquivos	X	X	X	X	X		
Uso de mídias removíveis infectadas	X	X	X	X	X		
Redes sociais	X	X	X	X	X		
Mensagens instantâneas	X	X	X	X	X		
Inserido por um invasor		X	X	X	X	X	X
Ação de outro código malicioso		X	X	X	X	X	X
<b>FORMA DE INSTALAÇÃO</b>							
Execução de um arquivo infectado	X						
Execução explícita do código malicioso		X	X	X	X		
Via execução de outro código malicioso						X	X
Exploração de vulnerabilidades		X	X			X	X
<b>FORMA DE PROPAGAÇÃO</b>							
Inserir cópia de si próprio em arquivos	X						
Envia cópia de si próprio automaticamente pela rede		X	X				
Envia cópia de si próprio automaticamente por email		X	X				
Não se propaga				X	X	X	X
<b>AÇÕES MALICIOSAS MAIS COMUNS</b>							
Altera e/ou remove arquivos	X			X			X
Consome grande quantidade de recursos		X	X				
Furta informações sensíveis			X	X	X		
Instala outros códigos maliciosos		X	X	X			X
Possibilita o retorno do invasor						X	X
Envia <i>spam</i> e <i>phishing</i>			X				
Desfere ataques na Internet		X	X				
Procura se manter escondido	X				X	X	X





## Outros Malwares

### Ransomware

INCIDÊNCIA EM PROVA: ALTÍSSIMA



**Esse tem começado a cair com mais frequência recentemente em provas de concurso, mas é minha aposta nesses novos tempos de moedas digitais.** O *Ransomware* é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, e que exige pagamento de um resgate (*ransom*, em inglês) para restabelecer o acesso ao usuário – trata-se de uma espécie de extorsão virtual.

**Ele pode se propagar de diversas formas, embora as mais comuns sejam:** através de correios eletrônicos com o código malicioso em anexo ou que induzam o usuário a seguir um link; ou explorando vulnerabilidades em sistemas operacionais comprometidos que não tenham recebido as devidas atualizações de segurança. Atualmente, existem dois tipos básicos da praga virtual *ransomware*:

- **Ransomware Locker:** impede que você acesse o equipamento infectado.
- **Ransomware Crypto:** impede que você acesse dados no equipamento infectado.

**Esse segundo tipo utiliza criptografia para impedir que o usuário tenha acesso aos dados.** Além de infectar o equipamento, ele também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também. Para se proteger, recomenda-se manter o sistema operacional e os programas instalados com todas as atualizações aplicadas; ter um antivírus instalado; e ser cuidadoso ao clicar em links ou abrir arquivos.



Fazer backups regularmente também é essencial para proteger os seus dados, pois – se seu equipamento for infectado – a única garantia de que você conseguirá acessá-los novamente é possuir backups atualizados. **Em geral, o pagamento é feito utilizando moedas digitais (Ex: Bitcoin), de modo que se torne não-rastreável, e infelizmente não garante o restabelecimento do acesso aos dados.**

## o bastidor

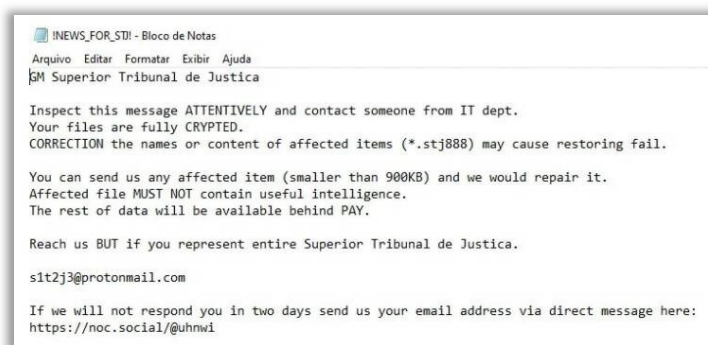
JUSTIÇA

### Hacker cobra resgate de dados sequestrados do STJ

Técnicos do Superior Tribunal de Justiça acabam de encontrar – quinta, dia 5, na hora do almoço – um pedido de resgate dos dados sequestrados por um hacker na terça. O pedido, obtido pelo **Bastidor**, segue a linha comum a ataques dessa natureza, chamados de *ransomware*.

O STJ está refém de criminosos.

**Atualização:** quem aí ficou sabendo do ataque às bases de dados do Superior Tribunal de Justiça (STJ)? Pois é, trata-se de um ransomware (tomem cuidado com seus arquivos!)



**Vejam o texto que os cybercriminosos enviaram com o pedido de resgate:** "Inspeccionem esta mensagem atentamente e contacte alguém do Departamento de TI. Seus arquivos foram completamente criptografados (...). O restante dos dados estará disponível mediante pagamento. Entre em contato apenas se você representar totalmente o Superior Tribunal de Justiça: s1t2j3@protonmail.com".



**RANSOM = RESGATE**

**RANSOMWARE = SOFTWARE DE RESGATE**

**(SERES/PE – 2017)** Praga virtual que informa, por meio de mensagem, que o usuário está impossibilitado de acessar arquivos de determinado equipamento porque tais arquivos foram criptografados e somente poderão ser recuperados mediante pagamento de resgate denomina-se:

- a) ransomware.
- b) trojan.
- c) spyware.
- d) backdoor.
- e) vírus.

**Comentários:** a praga virtual que impossibilita o acesso a arquivos porque eles foram criptografados e somente podem ser recuperados mediante pagamento de um resgate é o ransomware (Letra A).



## Keyloggers

INCIDÊNCIA EM PROVA: MÉDIA



Galera, vocês se lembram que nós vimos os spywares? Pois é, **keylogger** é um tipo de **spyware** capaz de **capturar e armazenar as teclas digitadas pelo usuário no teclado do computador e enviá-las a um invasor**. Imaginem que tudo que vocês digitam no teclado é armazenado pelo software malicioso e enviado para o atacante, que pode eventualmente capturar senhas ou outras informações relevantes.

Criado inicialmente com a intenção de ser utilizado para auxiliar o suporte técnico e fiscalização, **ele adquire uma característica maliciosa quando é integrado a malwares e usado para coletar informações pessoais**. O uso ilícito tem o objetivo de coletar dados como nomes de usuário e senhas de contas de e-mail, sites de relacionamento, mensageiros instantâneos e qualquer outro serviço que precise de senha para se conectar, inclusive dados de acesso às contas bancárias.



Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking. **Para aumentar a proteção dos seus clientes, alguns bancos online utilizam a tecnologia do teclado virtual, com recursos que reduzem a probabilidade de sucesso desses softwares**. A ideia é que caracteres não sejam digitados pelo teclado físico e, sim, clicados com o auxílio do mouse em um teclado virtual que aparece na tela do computador.





KEY = TECLA; LOGGER = REGISTRADOR  
KEYLOGGER = REGISTRADOR DE TECLA

**(CAU/MG – 2019)** Qual é o software malicioso criado para gravar informações digitadas por um determinado usuário no teclado de um computador, a fim de obter dados sigilosos?

- a) Keylogger
- b) Spam
- c) Firewall
- d) Scan

**Comentários:** malware que grava informações digitadas no teclado (key) de um computador é o Keylogger (Letra A).

**(TRT/10 – 2019)** “Programa que armazena todas as informações que um usuário digitou em um micro infectado por esse tipo de programa”. A afirmativa se refere a:

- a) Adware.
- b) Spyware.
- c) Keylogger.
- d) Screenlogger.

**Comentários:** o programa que armazena informações digitadas por um usuário é o Keylogger (Letra C).

**(TRT-BA – 2013)** Um site de segurança publicou uma notícia informando sobre um tipo de e-mail falso que vem atacando as redes sociais. Trata-se de um falso aviso de segurança informando que a conta será bloqueada caso não seja atualizada. Com aparência semelhante à do Facebook, este tipo de e-mail oferece um link para que a pessoa acesse uma página da rede social para iniciar o processo de atualização dos dados. Na verdade, o que ocorre ao clicar no link é a instalação de um spyware, capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. O spyware capaz de realizar o que está sublinhado no texto, de acordo com a cartilha de segurança para internet do CERT.BR, é denominado:

- a) Adware.
- b) Keylogger.
- c) Rootkit.
- d) Bot.
- e) Trojan.

**Comentários:** o tipo de spyware que captura e armazena teclas digitadas (key) no teclado é o Keylogger (Letra B).



## Screenloggers

INCIDÊNCIA EM PROVA: MÉDIA



Trata-se também de um *spyware* – similar ao *keylogger* – capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. *Vocês se lembram que uma das soluções contra os keyloggers foi a utilização de teclados virtuais? Pois é, o screenlogger foi criado principalmente para capturar as teclas digitadas pelos usuários nesses teclados virtuais.*

*Professor, como ele faz isso? Ele permite capturar uma foto instantânea da tela (Print Screen) e assim observar uma sequência de cliques.* Ele era bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de internet Banking. *Por que era utilizado?* Porque, hoje em dia, é mais raro utilizar teclados virtuais e porque atualmente há diversas maneiras de impedir esse tipo de praga virtual.



SCREEN = TELA; LOGGER = REGISTRADOR

SCREENLOGGER = REGISTRADOR DE TELA

(TRT/AMAZONAS – 2017) Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Existem tipos específicos deste programa, como o que é capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. Este tipo de spyware é denominado de:

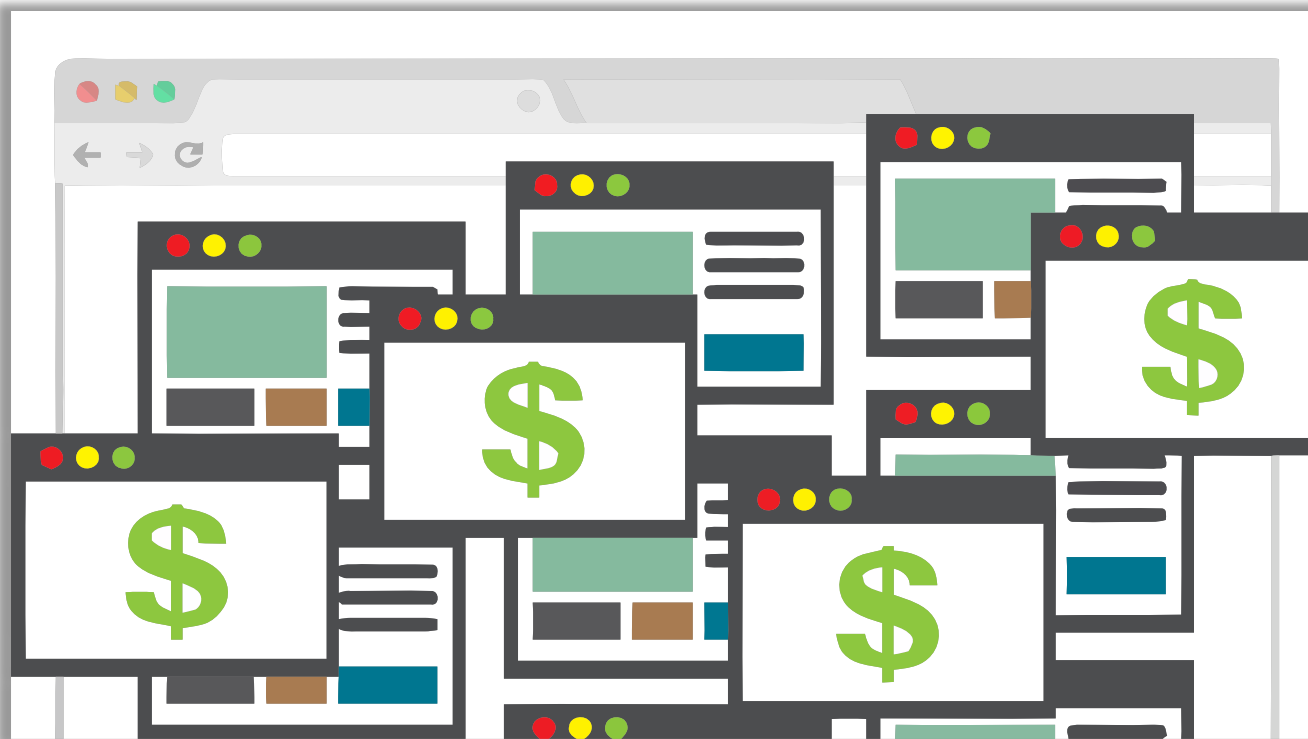
- a) KeyLogger
- b) Mouselogger
- c) Adware
- d) Screenlogger

**Comentários:** o tipo de spyware que é programado para monitorar as atividades de um sistema e enviar para terceiros, armazenando a posição do cursor e a tela do monitor nos momentos de clique do mouse é o Screenlogger (Letra D).

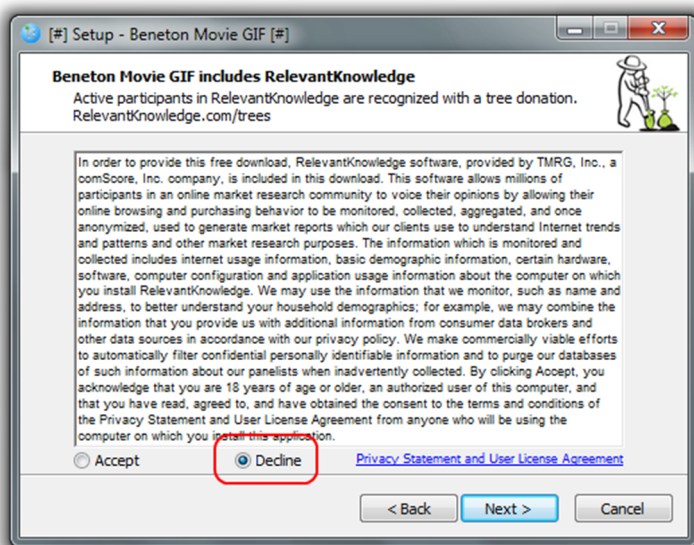


## Adwares

INCIDÊNCIA EM PROVA: ALTA



**Trata-se de um spyware projetado especificamente para apresentar propagandas.** Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas são direcionadas de acordo com a navegação do usuário sem que este saiba que tal monitoramento está sendo feito.



**É um programa executado de forma automática e geralmente instalado sem o consentimento do usuário durante a instalação de outro software.** É utilizado para divulgação de links publicitários, muitas vezes através de pop-ups.

*Quem nunca fez download de um software, não prestou atenção nas instruções de instalação e acabou instalando algum outro software de propaganda que não gostaria de ter instalado? Prestem muita atenção na instalação, como na imagem ao lado!*



**Em suma: consiste em um programa projetado para exibir propagandas e anúncios normalmente sem a autorização do usuário, tornando o computador mais lento e a navegação mais incômoda.** Geralmente vêm em formato de diversos pop-ups e notificações inseridas em outro programa (em geral, um navegador) e pode ser considerado um malware na hipótese de sua propaganda variar de acordo com hábitos de navegação do usuário.



**AD (ADVERTISEMENT) = PROPAGANDA OU ANÚNCIO**

**ADWARE = SOFTWARE DE PROPAGANDA**

**(DETRAN/MA – 2018)** Após acessar um website para o download de músicas da internet foi notado que o navegador internet passou a mostrar janelas pop-up com propagandas de forma infinita, ou seja, após o fechamento de uma janela, outra é apresentada em seguida de forma contínua. Esse efeito é característico do ataque do malware conhecido como:

- a) adware.
- b) spyware.
- c) botnet.
- d) worm.
- e) rootkit.

**Comentários:** janelas de pop-up com propagandas de forma infinita e apresentada de forma contínua é uma característica típica de um adware (Letra A).

**(INPI – 2013)** A principal atividade de programas com códigos maliciosos e que funcionam na função de keylogger é apresentar propagandas não solicitadas pelo usuário, direcionando-o a sítios maliciosos.

**Comentários:** a questão trata de adwares e, não, de keyloggers (Errado).



## Sniffer

INCIDÊNCIA EM PROVA: BAIXA



Por padrão, computadores em uma mesma rede “farejam” e respondem somente pacotes endereçados a eles. **No entanto, é possível utilizar um analisador de pacotes de dados chamado *sniffer* capaz de monitorar, interceptar e registrar tráfego de dados em segmentos de rede de computadores.** Esse software pode ser utilizado de forma legítima ou pode ser utilizado de forma maliciosa. *Diego, você pode explicar melhor? Claro...*

Ele é utilizado de forma legítima por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados. **Ele também pode ser utilizado por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.**

**Nesse último caso, dizemos que ele está configurado em modo promíscuo.** Notem que as informações capturadas por este software malicioso são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las. Os hackers costumam colocar sniffers em locais que ofereçam redes wi-fi inseguras, como cafeterias, hotéis e aeroportos.

**Um sniffer é programa que age monitorando o tráfego na rede, através da captura de pacotes de dados, em busca de informações sensíveis como o endereço dos sites acessados, senhas de acesso, e-mails, entre outros.** No entanto, é bom enfatizar que eles não são necessariamente maliciosos (aliás, em regra eles são legítimos). Este tipo de software é usado com frequência para monitorar e analisar o tráfego de rede para detectar problemas e manter um fluxo eficiente.

**Por outro lado, se utilizados de má-fé, eles podem capturar tudo o que passa por eles, inclusive senhas e nomes de usuários não criptografados.** Além disso, um *sniffer* pode ser instalado em qualquer computador conectado a uma rede local. Ele não precisa ser instalado no próprio aparelho que se deseja monitorar. Em outras palavras, ele pode permanecer oculto durante a conexão em um outro computador conectado à rede local.



**Professor, qual é a diferença entre sniffers e spywares? Eles são bem parecidos, mas há duas diferenças principais:** em primeiro lugar, sniffers são comumente utilizados de forma legítima ou malicioso; spywares geralmente são maliciosos. Em segundo lugar, sniffers podem ser instalados em qualquer máquina conectada à rede local – eles não precisam estar instalados na máquina que desejam monitorar; spywares precisam estar instalados na máquina monitorada.



**SNIFF = FAREJAR**

**SNIFFER = FAREJADOR**

**(TCE/SP – 2015)** Os Sniffers, utilizados para monitorar o tráfego da rede por meio da interceptação de dados por ela transmitidos, não podem ser utilizados por empresas porque violam as políticas de segurança da informação.

**Comentários:** eles não só podem como geralmente são utilizados assim desde que com boa-fé (Errado).

**(CRF/PR – 2019)** Os programas que são considerados como muito parecidos com os spywares e que têm como função principal interceptar e registrar dados trafegados na rede são os:

a) hijackers    b) vírus time bomb    c) sniffers    d) spams    e) de engenharia social.

**Comentários:** o programa responsável por interceptar e registrar dados trafegados é o sniffer (Letra C).

**(BANESTES – 2015)** Um SNIFFER de rede é um programa que:

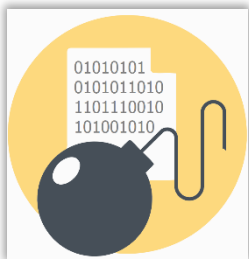
- a) Põe em risco as informações que trefegam em rede, pois captura pacotes desse ambiente.
- b) Não põe em risco as informações que trefegam em rede, pois protege os pacotes desse ambiente.
- c) Não põe em risco as informações que trefegam em rede, pois criptografa em IPSEC os pacotes desse ambiente.
- d) Põe em risco as informações que trefegam em rede, apesar de criptografar em HTTPS os pacotes desse ambiente.
- e) Não pode ser utilizado em protocolos TCP/IP.

**Comentários:** (a) Correto, ele pode pôr as informações em risco por capturar pacotes de dados; (b) Errado, ele compromete pacotes de dados; (c) Errado, ele não criptografa pacotes de dados; (d) Errado, ele não criptografa pacotes de dados; (e) Errado, ele pode – sim – ser utilizado com protocolos da arquitetura TCP/IP (Letra A).



## Bombas Lógicas

INCIDÊNCIA EM PROVA: BAIXA



Trata-se de um software malicioso normalmente instalado por um usuário autorizado, como um administrador da rede, que o mantém no sistema deixando-o programado para causar danos (como excluir arquivos importantes) em um determinado evento, como – por exemplo – um código que monitora o sistema de pagamentos de uma empresa e deleta arquivos críticos para a organização caso um determinado funcionário seja demitido.

Imaginem um camarada que tenha sido demitido por qualquer que seja a razão e, insatisfeito, decide criar uma bomba lógica que apagará arquivos importantes caso ele seja excluído da base de dados da empresa (significando a sua demissão) – de forma que ninguém desconfie que ele foi o responsável pelos danos causados pelo software malicioso. **Esse é geralmente o tipo de situação em que esse malware aparece.**

Lembrando que uma bomba lógica pode ser configurada via disparo positivo ou negativo. Na forma positiva, a carga útil do malware ficará inativa até que um evento específico ocorra; na forma negativa, a carga útil do malware será ativada a não ser que um evento específico ocorra. *Professor, qual é a diferença do vírus Time Bomb para uma Bomba Lógica? A Bomba Lógica pode ser utilizada por outros tipos de malware; já o Vírus Time Bomb é apenas para vírus...*

▪ **(CRQ/SP – 2011)** O programador escreve uma parte do código e o insere secretamente no sistema operacional para utilizá-lo em represália a um possível afastamento involuntário do ambiente de trabalho. Dessa forma, a execução bem-sucedida do programa depende desse programador alimentá-lo diariamente, por meio de uma senha. O tipo de ataque descrito acima é conhecido por:

- a) alçapão.
- b) conexão impostora.
- c) transbordo do buffer.
- d) código móvel.
- e) bomba lógica.

**Comentários:** como a execução bem-sucedida do programa depende de o programador alimentá-lo diariamente, existe uma dependência lógica, logo se trata de uma bomba lógica (Letra E).

**(CRO/AC – 2019)** A bomba lógica tem como característica principal enviar várias requisições de informação para um sistema de computação, com o objetivo de paralisá-lo.

**Comentários:** na verdade, essa é a característica principal de um ataque chamado DDoS (Errado).



## Exploits

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



Trata-se de um software criado por hackers para permitir explorar vulnerabilidades ou brechas de segurança conhecidas de sistemas e assim permitir que atacantes possam praticar ações de invasões sem conhecimentos avançados. Eles geralmente causam instabilidade no sistema para diminuir temporariamente a sua segurança, passando então a executar ordens para roubar informações, invadir acessos bloqueados ou propagar vírus.

Outra coisa interessante é que eles podem explorar de vulnerabilidades zero-day. *Zero o que, Diego?* Zero-day! No contexto de segurança da informação, trata-se de uma vulnerabilidade desconhecida por administradores de um sistema que pode ser explorada por hackers. **O termo zero-day (ou dia zero) é o dia em que o administrador de um sistema descobre essa vulnerabilidade e começa a tomar ações para mitigá-la.**



EXPLOIT = EXPLORAR

EM NOSSO CONTEXTO, UTILIZAR ALGO TIRAR VANTAGENS

**(UFAL – 2016)** Exploit é um software malicioso projetado para explorar uma vulnerabilidade existente em um software de computador.

**Comentários:** o exploit realmente é projetado para explorar vulnerabilidades de um software ou sistema computacional (Correto).

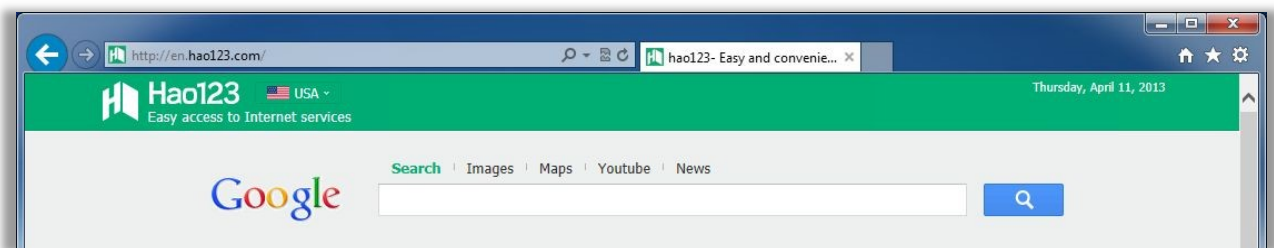


## Hijacker

INCIDÊNCIA EM PROVA: MÉDIA



O Browser Hijacker é um *software* malicioso que modifica o registro do sistema operacional, alterando o funcionamento do navegador, modificando sua página inicial, abrindo páginas automaticamente ou inserindo botões inadvertidamente. Como muitos sites patrocinam o acesso a seu conteúdo, remunerando por cliques em links, o desenvolvedor do Hijacker costuma receber quantias financeiras sempre que estas páginas são abertas.



Essa praga virtual assume o controle do navegador e muda a forma como seu conteúdo é exibido quando você está navegando na web (em geral, modificando os registros do sistema operacional). Quem nunca instalou sem querer o HAO123? Gente, esse maldito *malware* se instala, bagunça seu navegador inteiro e é terrível para desinstalar (eu odeio essa @#&\*# desse software). Eu já tive que formatar meu computador várias vezes por conta de hijackers.



HIJACK = SEQUESTRAR

HIJACKER = SEQUESTRADOR



**(Prefeitura de Rurópolis/PA – 2019)** Os programas que alteram a página inicial do navegador e também são capazes de redirecionar qualquer página visitada para outra, escolhida pelo criador da praga, são denominados de:

- a) sniffers.
- b) snappers.
- c) hijackers.
- d) screenloggers.

---

**Comentários:** alterar página inicial do navegador e redirecionar páginas visitadas são ações maliciosas típicas de um Hijacker (Letra C).

**(TRE/MA - 2015)** Alcebíades queria instalar um software em seu computador rapidamente para modificar umas fotos. Procurou na internet e achou um software freeware. Baixou e instalou, sem perceber que alguns softwares adicionais foram instalados também. Como a prioridade era a rapidez e não a segurança, ele pagou o preço. Sua página inicial do browser foi alterada, sua página de procura principal e redirecionamentos de páginas. Qual destas pragas virtuais ele instalou?

- a) Browser Hijacker.
- b) Trojans.
- c) Spyware.
- d) Worms.

---

**Comentários:** a praga virtual que altera o browser, página principal e redirecionamento é o Browser Hijacker (Letra A).

**(TRT/MA – 2014)** Após a instalação de um programa obtido na internet, o navegador Internet Explorer utilizado por Luis apresenta uma página inicial diferente da configurada por ele, além de exibir pop-up indesejável. A partir dessas informações, pode-se concluir que o tipo de malware que atacou o computador do Luis é:

- a) Hijacker.
- b) Rootkit.
- c) Worm.
- d) Bootnet.
- e) Keylogger.

---

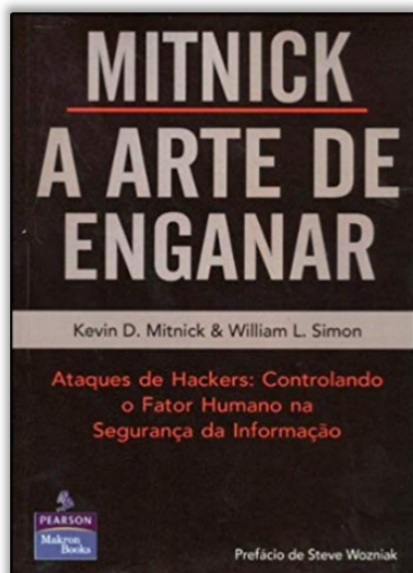
**Comentários:** apresentar página inicial diferente e exibir pop-up indesejável são ações maliciosas típicas de um Hijacker (Letra A).



## Ataques e Golpes

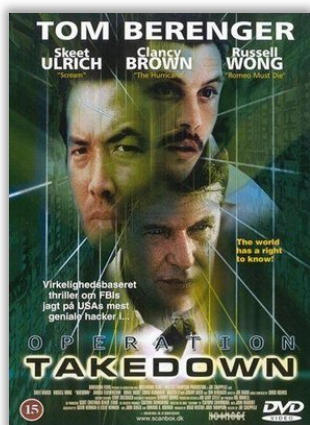
### Engenharia Social

INCIDÊNCIA EM PROVA: MÉDIA



Galera, quando eu tinha uns 14 anos, eu já era fissurado com computadores e ficava encantado com todas as histórias de hackers que invadiam computadores, etc. À época, eu fiquei sabendo de um livro que contava a história do maior hacker de todos os tempos: Kevin Mitnick. **Eu comprei e fui logo ler a história desse cara que *hackeou* computadores e sistemas de diversas empresas de tecnologia e provedores de internet na década de noventa.**

Ele era tão ousado que – para mostrar como ele era competente – ele invadiu o computador pessoal de um dos maiores especialistas em segurança computacional do mundo: Tsutomu Shimomura. Esse cara evidentemente não deixou barato e, no ano seguinte, conseguiu capturá-lo e prendê-lo com a ajuda do FBI. Ele ficou cinco anos preso e depois mais três anos sem poder chegar perto de um computador, celular ou internet.



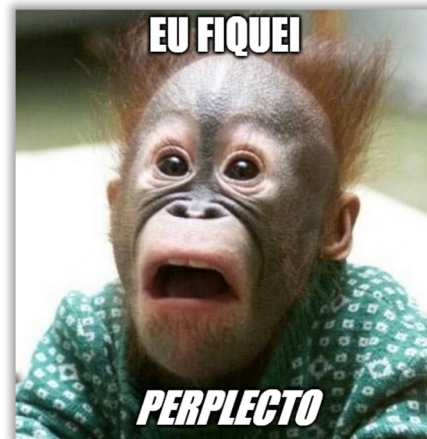
Essa história é contada no filme chamado Take Down (Caçada Virtual)! Eu – ávido por entender como esse hacker conseguiu fazer tudo isso – comprei o livro pensando que descobriria técnicas mirabolantes sobre como *hackear* computadores e sistemas. No entanto, em determinado momento do livro, Mitnick surpreende e diz:

Mitnick: *Vocês sabem qual é a melhor técnica para descobrir uma senha?*

E ele respondeu: *Perguntando!*



Galera, leiam o subtítulo do livro na página anterior. Ele diz: “Ataques de Hackers: controlando o fator humano na Segurança da Informação”. É claro que existem técnicas para invadir sistemas, mas tantas outras envolvem mais o fator humano do que o fator computacional! **A Engenharia Social é uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações por má-fé.** Trata-se de uma técnica utilizada por golpistas para tentar explorar a confiança, ingenuidade, ganância, vaidade ou boa-fé de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes.



**Ela é utilizada para obter informações importantes do usuário, através de sua ingenuidade ou da confiança.** Quem está mal-intencionado geralmente utiliza telefone, e-mails ou salas de bate-papo para obter as informações que necessita. Por exemplo: algum desconhecido liga para a sua casa e se diz do suporte técnico do seu provedor de internet. Nessa ligação, ele te convence de que sua conexão está com problemas e pede sua senha para corrigir.

Duvide desse tipo de abordagem e contate o provedor caso algum técnico ligue para sua casa pedindo dados confidenciais a seu respeito (senhas, números de cartões, etc.) avisando-o do ocorrido. **Em suma: Engenharia Social é um conjunto de práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações/sistemas, através da persuasão e se aproveitando da ingenuidade ou confiança das pessoas.** Um exemplo comum é o *Phishing*.

**(BB – 2013)** Analise o diálogo apresentado a seguir.

- Sr. José, bom dia: Aqui fala o suporte técnico do seu provedor de Internet. O senhor está feliz com o nosso atendimento?
- Sim, bastante.
- Sr. José, constatamos uma ligeira redução na velocidade da sua conexão e por isso gostaríamos de confirmar alguns dados para poder estar melhorando o serviço que lhe prestamos. É possível?
- Pois não!
- O seu endereço é rua do Bastião, 37?
- Sim.
- O seu e-mail é jose.arrose@empresa.com.br?
- Sim.
- Muito obrigado, Sr. José, seus dados foram confirmados e podemos continuar nossa entrevista. O seu histórico de cliente bom pagador gerou um benefício. A sua velocidade de conexão será aumentada sem qualquer acréscimo na sua mensalidade. Bons clientes, melhores serviços. O senhor aceita esse prêmio por bom relacionamento?
- Sim.
- Sr. José, podemos fazer isso imediatamente, nossos recursos de acesso remoto incorporaram novas funcionalidades que permitem que eu mesmo, com um simples comando no meu computador, modifique a configuração do seu modem e troque essa velocidade. O senhor autoriza essa manobra? São 10 M em lugar do seus 2 M atuais.
- Sim.
- O senhor, então, pode ditar sua senha de acesso, por favor?
- 4 5 2 8 4 7 9 3.
- Muito obrigado, Sr. José. Aguarde uns 30 min e verifique como estarão mais rápidos os seus acessos. O seu provedor agradece.

Esse diálogo caracteriza um ataque à segurança da informação conhecido por:

- a) port scanner
- b) cavalo de troia
- c) spyware
- d) técnica de entrevista
- e) engenharia social

**Comentários:** trata-se claramente de engenharia social – inclusive como o exemplo de um provedor de internet que demos na teoria (Letra E).

**(ANP – 2016)** Uma hacker ameaçou divulgar na Web informações sigilosas de uma empresa após ter conseguido acesso a seus sistemas de informação. Para conseguir o acesso, ela telefonou para uma das secretárias da diretoria, passando-se por esposa de um dos diretores. Em seguida, ela disse à secretária que seu marido tinha sofrido um acidente e estava hospitalizado. Porém, antes de ficar inconsciente, o diretor lhe havia pedido que entrasse em contato com a empresa a fim de que uma de suas secretárias solicitasse a mudança do seu login e da sua senha, pois ele havia perdido sua agenda no acidente e temia que alguém pudesse invadir os sistemas da empresa, uma vez que esses dados, por descuido seu, estavam anotados na agenda perdida. Em seguida, a suposta esposa forneceu os novos login e senha à secretária.

Esse tipo de ataque para obtenção de informações é chamado de:

- a) informações livres
- b) engenharia social
- c) varredura de vulnerabilidades
- d) dumpster diving
- e) ataque físico

**Comentários:** (a) Errado. Informações Livres é uma técnica de análise de informações que podem ser obtidas livremente na internet sem a necessidade de ações intrusivas; (b) Correto. Engenharia Social é uma técnica de obtenção de informações explorando vulnerabilidades humanas e sociais dos funcionários de uma organização; (c) Errado. Varredura de Vulnerabilidades é uma técnica de envio de tipos de pacotes com o objetivo de obter informações relevantes para um ataque sobre um computador ou uma rede; (d) Errado. Dumpster Diving é uma técnica de vasculhar o lixo (sim, lixo mesmo) de empresas e pessoas com o objetivo de encontrar algo de valor; (e) Errado. Ataque Físico é basicamente o roubo de equipamentos ou dispositivos de armazenamento realizado diretamente em uma organização (Letra B).

**(CFO/DF – 2017)** Não revelar informações confidenciais para outra pessoa, via telefone, sem confirmar sua legitimidade é uma das formas de evitar a engenharia social.

**Comentários:** essa é uma forma clássica de engenharia social (Correto).



## Força Bruta

INCIDÊNCIA EM PROVA: BAIXA



Galera, deixa eu contar uma historinha para vocês! Era uma vez, um professor de informática que estava viajando para curtir as férias. No fim da viagem, antes de ir para o aeroporto, ele fechou sua mala e – bastante inteligente que é – trancou seus documentos dentro. Na hora do check-in, ele lembrou que os documentos estavam dentro da mala, mas esqueceu a maldita da senha desse cadeado embutido que vem em algumas malas. *O que ele teve que fazer?* Testar todas as possibilidades de combinação desses três números até descobrir a senha correta que abre a mala. **Esse é um exemplo de força bruta e eu sou um exemplo de professor mané** (sim, o professor sou eu!).

**Um Ataque de 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.** Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta.

Mesmo que o atacante não consiga descobrir a sua senha, você pode ter problemas ao acessar a sua conta caso ela tenha sofrido um ataque de força bruta, pois muitos sistemas bloqueiam as contas quando há várias tentativas de acesso sem sucesso. **Apesar dos ataques de força bruta poderem ser realizados manualmente, em geral eles são realizados com o uso de ferramentas facilmente obtidas na Internet.** As tentativas de adivinhação são baseadas em:

- dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- listas de palavras comumente usadas (Ex: personagens de filmes, nomes de times, etc);
- substituições óbvias de caracteres, como trocar "a" por "@" e "o" por "0";
- sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx";
- informações pessoais (Ex: nome, sobrenome, datas e números de documentos).

**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.** Vamos ver exatamente o que é um ataque de negação de serviço no próximo tópico, mas é basicamente um ataque massivo que resulta na interrupção de um serviço. *Bacana? Praticar...*

**(CODEBA – 2016)** Um grupo de hackers chamado DarkSide tem como objetivo executar processos e acessar sites, computadores e serviços em nome e com os privilégios de um



usuário da rede. Para isso, os integrantes do DarkSide tentam adivinhar, por tentativa e erro, um nome de usuário da rede e sua respectiva senha.

De acordo com a Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (cert.br), a técnica utilizada pelos integrantes da DarkSide é:

- a) varredura em redes, ou scan.
- b) interceptação de tráfego, ou sniffing.
- c) ataque de força bruta, ou brute force.
- d) falsificação de e-mail, ou e-mail spoofing.
- e) negação de serviço, ou DoS (Denial of Service).

**Comentários:** tentar adivinhar – por tentativa e erro – um nome de usuário da rede e sua respectiva senha é um exemplo típico de ataque de força bruta (Letra C).

**(Câmara de Ponte Nova/MG – 2018)** A maioria dos computadores, tanto pessoais quanto corporativos, hoje em dia, trabalha conectada à internet. Por isso, eles se tornam vulneráveis a vários tipos de ataques. Um desses ataques 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 desse usuário.

O ataque que contém essa técnica, conforme o <cert.br>, é chamado de:

- a) defacement.
- b) sniffing.
- c) força bruta.
- d) e-mail spoofing.

**Comentários:** adivinhar – por tentativa e erro – um nome de usuário e senha para executar processos e acessar sites, computadores e serviços em nome de um usuário é um ataque de força bruta (Letra C).

**(UFBA – 2017)** Um exemplo de ataque por força bruta (brute force) seria adivinhar, por tentativa e erro, um nome de usuário e senha, por exemplo, e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios desse usuário.

**Comentários:** é mais uma vez a mesma descrição do mesmo ataque de força bruta (Correto).



## Denial of Service (DoS)

INCIDÊNCIA EM PROVA: MÉDIA



**Negação de serviço (Denial of Service – DoS) é uma técnica pela qual um atacante busca retirar de operação um serviço, um computador ou uma rede conectada à Internet.** Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (*Distributed Denial of Service – DDoS*).

**O objetivo destes ataques não é invadir nem coletar informações, mas – sim – exaurir recursos e causar indisponibilidades.** Nesse caso, todas as pessoas que dependem do serviço são prejudicadas, visto que ficam impossibilitadas de acessar ou realizar as operações desejadas. Em geral, os alvos ficaram impedidos de oferecer serviços durante o ataque, mas voltam a operar normalmente ao final sem vazamento de informações ou comprometimento de sistemas.

Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. **No entanto, a grande maioria dos computadores participa dos ataques sem sequer ter conhecimento.** Por vezes, eu computador pode estar infectado (por exemplo, com Worms) ou fazendo parte de botnets. Ataques de negação de serviço podem ser realizados de diversas maneiras, tais como:

- Pelo envio de grande quantidade de requisições para um serviço, consumindo os recursos necessários ao seu funcionamento (processamento, número de conexões simultâneas, memória e espaço em disco, por exemplo) e impedindo que as requisições dos demais usuários sejam atendidas;
- Pela geração de grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível qualquer acesso a computadores ou serviços desta rede; ou pela exploração de vulnerabilidades existentes em programas, que podem fazer com que um determinado serviço fique inacessível.

**(IF/MG – 2016)** A respeito da segurança de redes, o ataque conhecido por tornar inacessíveis os serviços providos pela vítima e usuários legítimos, e normalmente



nenhum tipo de informação é roubado ou alterado e nem é feito um acesso não autorizado à vítima é o:

- a) Sniffer.
- b) Wepattack.
- c) Man-in-the-middle.
- d) Endereçamento MAC.
- e) DoS (Denial of Service).

---

**Comentários:** ataque conhecido por tornar inacessíveis os serviços providos pela vítima e usuários legítimos é a descrição típica de um ataque de negação de serviço ou *denial of service* (Letra E).

**(SEGE/MA – 2016)** Um cracker passou a controlar diversos computadores remotamente após infectá-los com um tipo de programa malicioso chamado bot. Por meio desse programa, ele enviou instruções para desferir ataques maciços para tirar de operação serviços, computadores e redes conectadas à internet. Assim, conseguiu enviar grande quantidade de requisições para um serviço, tirando-o de operação. Conseguiu também gerar grande tráfego de dados para uma rede, ocupando toda a banda disponível, até conseguir sua queda. Esse tipo de ataque é conhecido como:

- a) Ping of Death.
- b) Sniffing.
- c) Spoofing.
- d) Defacement.
- e) DoS.

---

**Comentários:** desferir maciços ataques para tirar serviços, computadores ou redes de operação é um exemplo típico de um ataque de negação de serviço ou *denial of service* – DoS (Letra E).

**(FUNAI – 2016)** Há ataques que consistem em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Há muitas variantes desse tipo de ataque. Em uma delas o agressor invade muitos computadores e instala neles um software zumbi. Quando recebem a ordem para iniciar o ataque, os zumbis bombardeiam o servidor-alvo, tirando-o do ar. Esse tipo de ataque é conhecido como:

- a) NGSV.
- b) DDoS.
- c) ServBlock.
- d) Worm.
- e) Cavalo de Tróia.

---

**Comentários:** bombardear um servidor alvo por meio de um ataque de zumbis de vários computadores, tirando-o do ar, é uma característica de um ataque distribuído de negação de serviço – DDoS (Letra B).

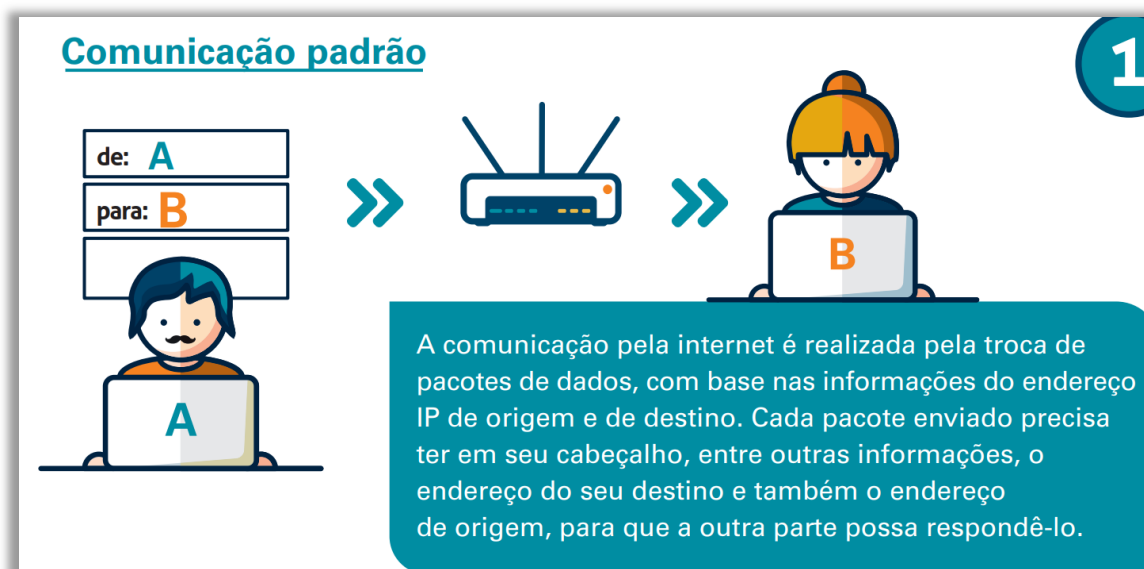


## IP Spoofing

INCIDÊNCIA EM PROVA: BAIXA

O IP Spoofing (Falsificação/Mascaramento de IP) é uma técnica de invasão comumente empregada quando o mecanismo de autenticação de uma rede é baseado em endereços IP, isto é, quando a identificação de um usuário é realizada baseado em seu número de endereço IP. **Nesse caso, um atacante pode clonar o IP de um usuário legítimo, mascarando-se e fazendo-se passar pelo usuário autorizado, podendo ganhar acessos não autorizados na rede.**

### COMUNICAÇÃO PADRÃO



### TÉCNICA DE SPOOFING



**(DPE/RJ - 2014)** Muitos ataques utilizam uma técnica chamada IP spoofing, tanto individualmente para conseguir acesso a outros hosts bem como em conjunto com outras ferramentas de ataque. Basicamente, IP spoofing gera pacotes?

- a) para o endereço de broadcast da rede destino.
- b) com o endereço IP de origem forjado.
- c) para o endereço de destino de loopback.
- d) com cabeçalhos inválidos ou corrompidos.
- e) para endereços multicast.

---

**Comentários:** o IP Spoofing gera pacotes com o Endereço IP de origem forjada/mascarada (Letra B).

**(EBSERH – 2015)** Ataque que objetiva mascarar pacotes IP utilizando endereços de remetentes falsos. Esse tipo de ataque é definido como:

- a) Honeypot.
- b) IP Flooding.
- c) SYN Flooding.
- d) IP Spoofing.
- e) DNS Spoofing.

---

**Comentários:** mascarar pacotes utilizando remetentes falsos é um típico ataque de IP Spoofing (Letra D).

**(FUNASG – 2015)** Uma rede de computadores foi atacada com um vírus que cria endereços de rede falsos e permite que um usuário interno cause dano à rede sem ser descoberto com facilidade. Esse tipo de ameaça é denominado:

- a) combolist.
- b) bruteforce.
- c) keylogger.
- d) sniffer.
- e) spoofing.

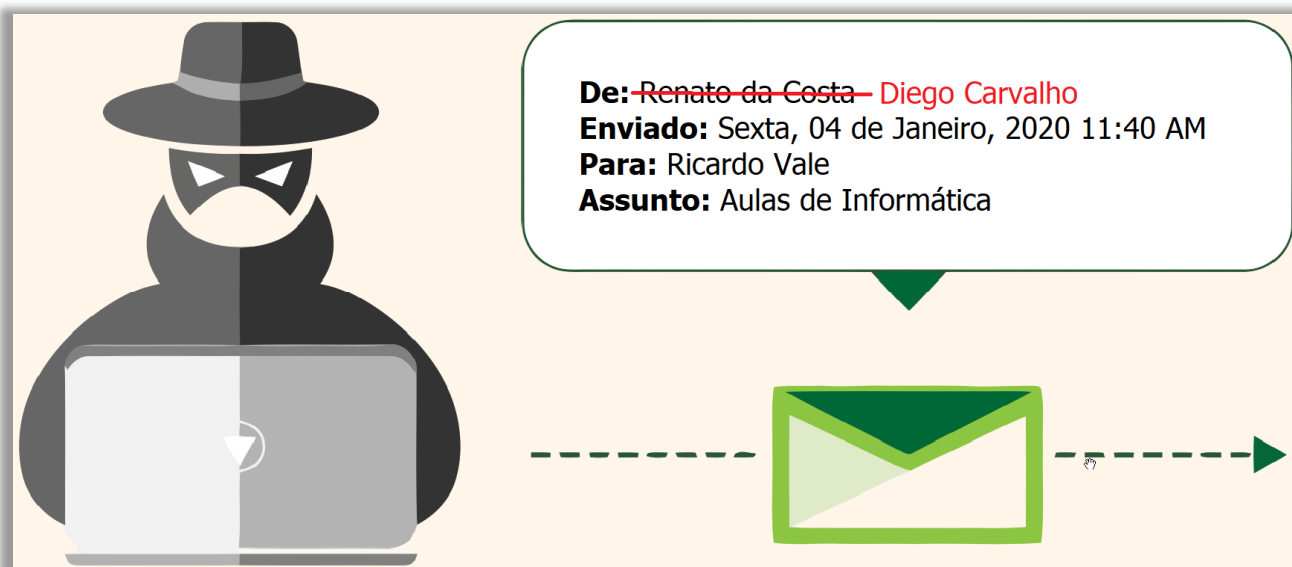
---

**Comentários:** vírus que cria endereços de rede – também chamados de IP – falsos, permitindo que um usuário cause danos à rede sem ser descoberto com facilidade é basicamente um de IP Spoofing (Letra E).



## E-mail Spoofing

INCIDÊNCIA EM PROVA: ALTA



**E-Mail Spoofing (Falsificação/Mascaramento de E-Mail)** é uma técnica que consiste em alterar 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. Essa técnica é possível devido a características do protocolo SMTP (*Simple Mail Transfer Protocol*) que permitem que campos do cabeçalho sejam falsificados.

**Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de spam e em golpes de phishing.** Atacantes utilizam-se de endereços de e-mail coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas. Exemplos de e-mails com campos falsificados são aqueles recebidos como sendo:

- de alguém conhecido, solicitando que você clique algum link ou execute algum arquivo em anexo;
- do seu banco, solicitando que você siga um link fornecido na própria mensagem e informe dados da sua conta bancária;
- do administrador do serviço de e-mail que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie.

**Você também pode já ter observado situações em que o seu próprio endereço de e-mail foi indevidamente utilizado.** Alguns indícios são, por exemplo, quando você recebe respostas de e-mails que você nunca enviou; quando recebe e-mails aparentemente enviados por você mesmo,



sem que você tenha feito isto; ou quando recebe mensagens de devolução de e-mails que você nunca enviou, reportando erros como usuário desconhecido e caixa de entrada lotada.

Galera, existem diversos tipos de Spoofing! Nós já estudamos o IP Spoofing e E-Mail Spoofing, existem também ARP Spoofing, MAC Spoofing, DNS Spoofing, entre outros.

**(Câmara de Boa Vista - 2014)** A respeito de ataques na internet, pode-se afirmar que e-mail spoofing:

- a) é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.
- b) é uma técnica que consiste em espionar os dados de emails trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers.
- c) é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à internet.
- d) é uma técnica que consiste em alterar 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.

**Comentários:** (a) Errado, o item trata de spam; (b) Errado, o item trata de sniffing; (c) Errado, o item trata de negação de serviço; (d) Correto, essa é a definição correta de e-mail spoofing (Letra D).

**(Câmara de Boa Vista - 2014)** Qual é o nome da técnica que consiste em alterar 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?

- a) Spoofing
- b) Sniffing
- c) Brute Force
- d) Defacement

**Comentários:** a técnica que altera cabeçalhos de um e-mail para falsificá-lo é o Spoofing – mais precisamente, E-mail Spoofing (Letra A).



## Phishing Scam

INCIDÊNCIA EM PROVA: ALTÍSSIMA



O Phishing Scam é uma fraude em que o golpista tenta enganar um usuário para obtenção de dados pessoais e financeiros que permitam a aplicação de um golpe, combinando técnicas computacionais e de engenharia social. Um exemplo de *phishing* é um e-mail que possa induzir o usuário a clicar em um link falso levando-o para uma página clonada ou para um arquivo malicioso. O *Phishing* ocorre por meio do envio de mensagens eletrônicas que:

- Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular; ou que procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de malwares; e do preenchimento de formulários contidos na mensagem ou em páginas Web.

Para atrair a atenção do usuário, as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento. Galera, todos vocês já devem ter sido alvos de algum tipo de Phishing alguma vez na vida – eu mesmo vou mostrar alguns casos que aconteceram comigo. Por enquanto, vamos ver alguns exemplos de situações envolvendo esse golpe:



- **Páginas falsas de comércio eletrônico ou Internet Banking:** você recebe um e-mail em nome de um site de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um link. Ao fazer isto, você é direcionado para uma página falsa, semelhante ao site que você realmente deseja acessar, onde são solicitados dados pessoais e financeiros.
- **Páginas falsas de redes sociais ou de companhias aéreas:** você recebe uma mensagem contendo um link para o site da rede social ou da companhia aérea que você utiliza. Ao clicar, você é direcionado para uma página falsa em que são solicitados o seu nome de usuário e a sua senha que, ao serem fornecidos, serão enviados aos golpistas.
- **Mensagens contendo formulários:** você recebe uma mensagem contendo um formulário com campos para a digitação de dados pessoais e financeiros. A mensagem solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações. Ao preencher os campos e confirmar o envio, seus dados são transmitidos para os golpistas.
- **Mensagens contendo links para códigos maliciosos:** você recebe um e-mail que tenta induzi-lo a clicar em um link, para baixar e abrir/executar um arquivo. Ao clicar, é apresentada uma mensagem de erro ou uma janela pedindo que você salve o arquivo. Após salvo, quando você o abrir ou o executar, será instalado um código malicioso em seu computador.
- **Solicitação de recadastramento:** você recebe uma mensagem, supostamente enviada pelo grupo de suporte da instituição de ensino que frequenta ou da empresa em que trabalha, informando que o serviço de e-mail está passando por manutenção e que é necessário o recadastramento. Para isto, é preciso que você forneça dados como nome de usuário e senha.

*Professor, estou assustado. Como eu faço para me prevenir de cair em golpes semelhantes a esses apresentados anteriormente? Vejamos as formas de prevenção:*

#### PREVENÇÃO

Fique atento a mensagens recebidas em nome de alguma instituição que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links.

Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (Ex: se você não tem conta em um banco, não há porque recadastrar dados ou atualizar módulos de segurança).

Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos.

Não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada.

Seja cuidadoso ao acessar links – procure digitar o endereço diretamente no navegador web.



Verifique o link apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o link real para o *phishing*. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso.

Utilize mecanismos de segurança, como programas *antimalware*, *firewall* pessoal e filtros *antiphishing*.

Verifique se a página utiliza conexão segura. Sites de comércio eletrônico ou Internet Banking confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados.

Verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador web será diferente do endereço correspondente ao site verdadeiro.

Acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

Galera, eu recebi um e-mail um dia desses do Bradesco! Eu achei estranho e fui ver o que era porque eu realmente tenho conta no Bradesco. Vejam só a imagem abaixo:



Notem que o título já é estranho, porque “você” está escrito com erro! Outra coisa importante de observar é o endereço do remetente: [banco.bradesco@netmail2.bradesco.com.br](mailto:banco.bradesco@netmail2.bradesco.com.br). *Galera, isso parece ser um e-mail real do Bradesco?* Não, está esquisito! O banco não envia e-mails aos clientes sem autorização prévia. Eu entrei no site do banco e procurei pela seção de segurança. Logo, ficou claro que se tratava de uma tentativa de *phishing*...

Atualmente, as próprias instituições financeiras colocam em suas páginas web informações sobre como se proteger de e-mails falsos.



Vejam essa lista de recomendações extremamente útil da empresa Clavis – Segurança da Informação sobre golpes no período de COVID-19 (Novo Coronavírus):

An infographic divided into two main sections. The left section is titled 'Phishing' and 'ENTENDA O QUE É', explaining that phishing is an attempt to acquire information like usernames, passwords, and credit card details by pretending to be a trustworthy entity in an electronic communication. It warns that phishing attacks can result in exposure and loss of critical information and advises not to click on links in emails, SMS, or social media posts from unknown sources. The right section is titled 'GOLPES DO CORONAVÍRUS' and lists six common scams: 01 Netflix - Liberação de acesso grátis; 02 Aplicativos rastreadores de doença pelo mundo; 03 Álcool gel da Ambev. Registre-se; 04 Kit gratuito com máscara e álcool gel dado pelo governo; 05 Fabricação de vacina Covid-19; 06 Agende teste do Coronavírus em casa. Both sections conclude with a warning to not click on suspicious links and to contact the security team if in doubt. The Clavis logo is at the bottom right.

Por fim, é importante mencionar um tipo específico de phishing chamado *Spear Phishing*. Trata-se de um golpe proveniente de e-mail ou comunicação eletrônica, direcionado a um indivíduo, organização ou empresa específicos. Embora tenha a intenção de roubar dados para fins mal-intencionados, **os criminosos virtuais também podem tentar instalar malware no computador do usuário – e é isso que o diferencia do phishing comum.**



**(Prefeitura de Jardim de Piranhas/RN – 2019)** O nome da técnica de fraude online que é utilizada por criminosos, os quais utilizam armadilhas virtuais como e-mails falsos, websites ou, até mesmo, mensagens, para roubar senhas de banco e demais informações pessoais, usando-as de maneira fraudulenta, é o:

- a) Worm                      b) Keylogger                      c) Ransomware                      d) Phishing.

**Comentários:** fraude online que utiliza armadilhas virtuais como e-mails falsos, websites ou até mesmo mensagens para roubar senhas de banco e informações pessoais é típico de Phishing (Letra D).

**(SEFAZ/BA – 2019)** Um Auditor recebeu uma mensagem de e-mail, aparentemente de seu banco, com um link para verificar a existência de uma dívida de cartão de crédito não paga. Preocupado com a situação, clicou no link e forneceu os dados de seu cartão de crédito para pagar a suposta conta. Dias depois percebeu na fatura do seu cartão que foram feitas diversas compras online em sites de comércio eletrônico na Internet. A situação descrita permite concluir que esse Auditor foi vítima de:

- a) rot                      b) backdoor                      c) worm                      d) phishing                      e) ransomware

**Comentários:** link solicitando fornecimento de dados de cartão é típico de phishing (Letra D).

**(Prefeitura de Valinhos/SP – 2019)** Frequentemente, os usuários de Correio Eletrônico recebem mensagens contendo frases como “atualize seus dados bancários” ou, então, “parabéns, você é o novo milionário”, cujo objetivo é capturar informações como senhas de banco e demais informações pessoais para utilizá-las de maneira fraudulenta. Esse tipo de crime, que cresce em ritmo acelerado, é chamado:

- a) Accounting  
b) Backdoor  
c) Download  
d) Phishing  
e) Redirecting

**Comentários:** (a) Errado, esse conceito não existe no contexto de segurança da informação; (b) Errado, isso é um malware e, não, um crime; (c) Errado, esse é o processo de transferir dados geralmente de um servidor; (d) Correto, e-mails com informações falsas que induzem o usuário a clicar em links para capturar informações pessoais ou financeiras é típico de phishing; (e) Errado, esse é o processo de redirecionar um usuário de uma página para outra (Letra D).



## Pharming

INCIDÊNCIA EM PROVA: ALTA



Para entender a mecânica de um ataque de Pharming e como eles são realizados, precisamos explorar como os servidores DNS (Domain Name System) funcionam. A tarefa do DNS é converter nomes de domínio em endereços IP, o que representa a localização real do site, permitindo que o navegador da Internet se conecte ao servidor em que o site está hospedado. **O método mais comum de executar esse ataque é por meio do envenenamento de cache.**

**Quando você digita o endereço de um site, seu navegador cria um cache (memória rápida) de DNS para que você não precise retornar ao servidor toda vez que quiser visitar um site.** O Pharming é um tipo de Phishing que "envenena" a tabela de cache do navegador web, corrompendo-o por meio da alteração de IPs e redirecionando o tráfego da Internet para sites fraudulentos para capturar informações e permitir a ação de golpistas<sup>1</sup>.

**Neste caso, quando você tenta acessar um site legítimo, o seu navegador é redirecionado para uma página falsa de forma transparente, isto é, sem que você esteja ciente.** Logo, você digita no navegador [www.bb.com.br](http://www.bb.com.br), por exemplo. No entanto, você é redirecionado para uma página cujo endereço é [www.bb.net.br](http://www.bb.net.br) e sequer percebe. Galera, existem tipos diferentes de redirecionamento. Vejamos...

### TIPOS DE REDIRECIONAMENTO

<sup>1</sup> Há um tipo específico de Pharming chamado DNS Spoofing ou DNS Poisoning, que – em vez de envenenar a tabela de cache do Navegador – envenena o próprio Servidor DNS de um provedor de internet para atingir inúmeros usuários em larga escala.



Por meio do comprometimento do servidor de DNS do provedor que você utiliza;

Pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;

Pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou modem de banda larga.

### PREVENÇÃO

Desconfie se, ao digitar uma URL, for redirecionado para outro site, o qual tenta realizar alguma ação suspeita, como abrir um arquivo ou tentar instalar um programa;

Desconfie imediatamente caso o site de comércio eletrônico ou Internet Banking que você está acessando não utilize conexão segura. Sites confiáveis de comércio eletrônico e Internet Banking sempre usam conexões seguras quando dados pessoais e financeiros são solicitados;

Observe se o certificado apresentado corresponde ao do *site* verdadeiro.

**Em suma: Pharming é um ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original.** É um tipo específico de Phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS. Nesse caso, quando o usuário tenta acessar um site legítimo, o seu navegador web é redirecionado, de forma transparente, para uma página falsa.

**(HCPA – 2016)** Assinale a alternativa que apresenta um método utilizado como base para o ataque de segurança chamado de pharming:

- a) Envenenamento de cache de DNS.
- b) Negação de serviço distribuída.
- c) Código malicioso escondido em arquivos.
- d) Troca de endereços nos cabeçalhos IP das mensagens.
- e) Troca de portas nos cabeçalhos TCP das mensagens.

**Comentários:** pharming envenena o cache (memória) do serviço de DNS – nenhum dos outros itens faz qualquer sentido (Letra A).

**(TJ/AC – 2012)** Pharming é um ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original.

**Comentários:** esse ataque realmente busca corromper o DNS e redirecionar o usuário para uma página de um servidor diferente do original (Correto).



## Hoax

INCIDÊNCIA EM PROVA: MÉDIA



O Hoax (Boato) 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. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido ou tentativas de golpes, como correntes de e-mail e pirâmides financeiras.

### CONTEÚDO DE HOAX

Conter códigos maliciosos, espalhar desinformação pela internet ou ocupar – desnecessariamente – espaço nas caixas de e-mails dos usuários.

Comprometer a credibilidade e a reputação de pessoas ou entidades referenciadas na mensagem.

Comprometer a credibilidade e a reputação da pessoa que o repassa, pois, ao fazer isto, esta pessoa estará supostamente endossando ou concordando com o conteúdo da mensagem.

Aumentar excessivamente a carga de servidores de e-mail e o consumo de banda de rede, necessários para a transmissão e o processamento das mensagens.

Indicar, no conteúdo da mensagem, ações a serem realizadas e que, se forem efetivadas, podem resultar em sérios danos.

Em geral, boatos se propagam pela boa vontade e solidariedade de quem os recebe, pois há uma grande tendência das pessoas em confiar no remetente, não verificar a procedência e não conferir a veracidade do conteúdo da mensagem. Para que você possa evitar a distribuição de



boatos é muito importante conferir a procedência dos e-mails e, mesmo que tenham como remetente alguém conhecido, é preciso certificar-se de que a mensagem não é um boato.

**(CRBM/6 – 2018)** A principal característica do vírus Hoax é que ele é utilizado para “pescar” senhas e(ou) dados financeiros dos usuários, como, por exemplo, do cartão de crédito.

**Comentários:** a questão trata de phishing e, não, hoax (Errado).

**(IF/BA - 2014)** A Internet propicia muitas facilidades e tornou-se indispensável na atualidade. Ela expõe, porém, seus usuários a muitas ameaças. Uma das principais ameaças dos usuários da Internet são os vírus, que existem em diversas categorias. A categoria de vírus que visa a difundir histórias enganosas ou boatos é o:

- a) Backdoor.
- b) Cavalo de Troia.
- c) Hoax.
- d) Phishing.
- e) Spyware.

**Comentários:** a questão trata de hoax – eles podem ser espalhados por meio de vírus (Letra C).

**(TRT/24 – 2011)** O usuário do computador recebe uma mensagem não solicitada, geralmente de conteúdo alarmista, a fim de assustá-lo e convencê-lo a continuar a corrente interminável de e-mails para gerar congestionamento na rede. Trata-se de um ataque denominado:

- a) Hoax.
- b) Worms.
- c) Trojans.
- d) Spam.
- e) Backdoors.

**Comentários:** mensagem não solicitada no e-mail com conteúdo alarmista a fim de assustar ou convencer sobre algo é típico de hoax (Letra A).



## Man in the Middle

INCIDÊNCIA EM PROVA: BAIXA



O Man in the Middle é um ataque em que os dados trocados entre duas partes (Ex: você e o seu banco) são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. Durante o ataque, a comunicação é interceptada pelo atacante e retransmitida. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação.

**(BANPARÁ– 2018 – Item II)** O ataque do homem-do-meio refere-se à forma de ataque em que uma comunicação entre duas pessoas é interceptada por uma terceira. O atacante simplesmente recebe e, opcionalmente, repassa as informações do transmissor para o receptor, sem que ambos percebam que a comunicação não está sendo, de fato, direta.

**Comentários:** essa é a definição impecável do ataque Man in The Middle (Correto).

**(TRF4 – 2019)** Em redes de computadores, é o tipo de ataque em que o espião intercepta a comunicação entre dois usuários, de forma que o usuário A comunique-se com ele mesmo pensando ser o usuário B, e o usuário B também o faz, pensando ser o usuário A. Trata-se de:

- a) SYN Flooding.
- b) Pharming.
- c) Man-in-The-Middle.
- d) DoS.
- e) Spoofing.

**Comentários:** o ataque que intercepta a comunicação se fazendo passar por outro usuário é o Man-in-the-Middle (Letra C).

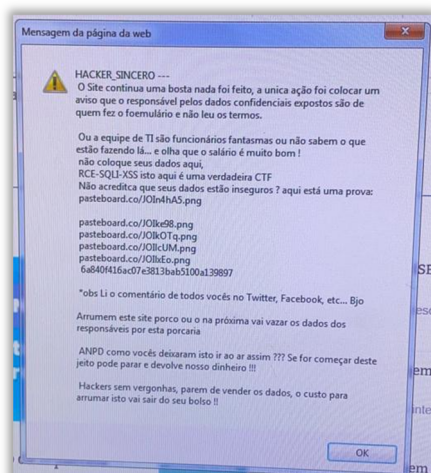


## Defacement

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



**Desfiguração de página (Defacement ou Pichação) é uma técnica que consiste em alterar o conteúdo da página web.** Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente os atacantes alteram a página principal do site, porém páginas internas também podem ser alteradas. As principais formas que um atacante, neste caso também chamado de *Defacer*, pode utilizar para desfigurar uma página web são:



- explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web;
- invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site;
- explorar erros da aplicação Web ou vulnerabilidades do servidor de aplicação web;
- ou furtar senhas de acesso à interface Web usada para administração remota.

**(TRE/RJ – 2012)** É possível executar um ataque de desfiguração (*defacement*) — que consiste em alterar o conteúdo da página web de um sítio — aproveitando-se da vulnerabilidade da linguagem de programação ou dos pacotes utilizados no desenvolvimento de aplicação web.

**Comentários:** o *defacement* realmente consiste em alterar o conteúdo da página web de um sítio (Correto).



## Furto de Identidade

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

**O Furto de Identidade (Identity Theft) é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas.** Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade. No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos.

Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de e-mail e envie mensagens se passando por você ou falsifique os campos de e-mail, fazendo parecer que ele foi enviado por você. **Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtrar a sua identidade, pois mais dados ele tem disponíveis e mais convincente ele pode ser.**

Além disto, o golpista pode usar outros tipos de golpes e ataques para coletar informações sobre você, inclusive suas senhas, como códigos maliciosos, ataques de força bruta e interceptação de tráfego. **Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito.** Além disto, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

*E como me prevenir, professor?* A melhor forma de impedir que sua identidade seja furtada é evitar que o impostor tenha acesso aos seus dados e às suas contas de usuário. Além disto, para evitar que suas senhas sejam obtidas e indevidamente usadas, é muito importante que você seja cuidadoso, tanto ao usá-las quanto ao elaborá-las. É necessário também que você fique atento a alguns indícios que podem demonstrar que sua identidade está sendo indevidamente usada por golpistas:

### PRINCIPAIS INDÍCIOS

Você começa a ter problemas com órgãos de proteção de crédito;

Você recebe o retorno de e-mails que não foram enviados por você;

Você verifica nas notificações de acesso que a sua conta de e-mail ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando;

Ao analisar o extrato da sua conta bancária ou do seu cartão de crédito você percebe transações que não foram realizadas por você;

Você recebe ligações telefônicas, correspondências e e-mails se referindo a assuntos sobre os quais você não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por você.

**(FHSTE/RS – 2019)** 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.

**Comentários:** essa seria a perfeita definição de Furto de Identidade (Correto).



## Fraude de Antecipação de Recursos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

**A Fraude de Antecipação de Recursos (Advance Fee Fraud) 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.** Por meio do recebimento de mensagens eletrônicas ou do acesso a sites fraudulentos, a pessoa é envolvida em alguma situação ou história mirabolante.

**Em geral, essa situação justifica a necessidade de envio de informações pessoais ou a realização de algum pagamento adiantado para a obtenção de um benefício futuro.** Após fornecer os recursos solicitados a pessoa percebe que o tal benefício prometido não existe, constata que foi vítima de um golpe e que seus dados/dinheiro estão em posse de golpistas. Existem variações desse golpe: Golpe da Nigéria, Loteria Internacional, Crédito Fácil, Noiva Russa, entre outros.

GOLPE	DESCRIÇÃO
GOLPE DA NIGÉRIA	A vítima recebe uma mensagem eletrônica em nome de alguém ou de alguma instituição, na qual é solicitado que ela atue como intermediária em uma transferência de fundos.
LOTERIA INTERNACIONAL	A vítima recebe um e-mail informando que foi sorteado em uma loteria internacional, mas que para receber o prêmio a que tem direito, precisa fornecer seus dados pessoais e informações sobre a sua conta bancária.
CRÉDITO FÁCIL	Você recebe um e-mail contendo uma oferta de empréstimo ou financiamento com taxas de juros muito inferiores às praticadas no mercado. Após o seu crédito ser supostamente aprovado você é informado que necessita efetuar um depósito bancário para o ressarcimento das despesas.
OFERTA DE EMPREGO	Você recebe uma mensagem em seu celular contendo uma proposta tentadora de emprego. Para efetivar a contratação, no entanto, é necessário que você informe detalhes de sua conta bancária.
DOAÇÃO DE ANIMAIS	Você deseja adquirir um animal de uma raça bastante cara e, ao pesquisar por possíveis vendedores, descobre que há sites oferecendo estes animais para doação. Após entrar em contato, é solicitado que você envie dinheiro para despesas de transporte.
NOIVA RUSSA	Alguém deixa um recado em sua rede social contendo insinuações sobre um possível relacionamento amoroso entre vocês. Esta pessoa mora em outro país, geralmente a Rússia, e após alguns contatos iniciais sugere que vocês se encontrem pessoalmente, mas, para que ela possa vir até o seu país, necessita ajuda financeira para as despesas de viagem.

Eu já recebi diversas mensagens no fórum me perguntando se alguém realmente cai nesses golpes (principalmente no golpe da noiva russa). Galera, cai demaaaaaaaais... absolutamente todos os dias! Como diz aquele antigo ditado: *"O golpe tá aí, cai quem quer"*! Eu só enfatizo em relação outros golpes que é preciso tomar muito cuidado com nossos pais e avós porque eles tendem a ser mais ingênuos quanto a isso! **Vamos ver como nos prevenir desse tipo de fraude...**



A melhor maneira é identificar algumas características: alguém oferecendo quantias astronômicas de dinheiro; alguém solicitando sigilo nas transações; alguém solicitando que você a responda rapidamente; alguém apresentando palavras como "urgente" e "confidencial" no campo de assunto; alguém apresentando erros gramaticais e de ortografia (muitas mensagens são escritas por meio do uso de programas tradutores e podem apresentar diversos erros).

**Além disto, adotar uma postura preventiva pode, muitas vezes, evitar que você seja vítima de golpes.** Por isto, é muito importante que você: questione-se por que justamente você, entre os inúmeros usuários da Internet, foi escolhido para receber o benefício proposto na mensagem e como chegaram até você; desconfie de situações onde é necessário efetuar algum pagamento com a promessa de futuramente receber um valor maior.

**Além desses, a principal dica para evitar esse tipo de golpe é aplicar a sabedoria popular de ditados como: "Quando a esmola é demais, o santo desconfia"!** Vale alertar que mensagens deste tipo nunca devem ser respondidas, pois isto pode servir para confirmar que o seu endereço de e-mail é válido. Esta informação pode ser utilizada, por exemplo, para incluí-lo em listas de spam ou de possíveis vítimas em outros tipos de golpes.

**(FUNPAPA – 2018)** Assinale a alternativa que descreve uma situação que pode ocorrer com uma vítima de um ataque conhecido como Fraude de antecipação de recursos (Advance fee fraud):

- a) A vítima recebe uma mensagem eletrônica em nome de alguém ou de alguma instituição, na qual é solicitado que ela atue como intermediária em uma transferência de fundos.
- b) A vítima recebe ligações telefônicas, correspondências e e-mails se referindo a assuntos sobre os quais ela não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por ela.
- c) Ao analisar o extrato da sua conta bancária ou do seu cartão de crédito, a vítima percebe transações que não foram realizadas por ela.
- d) O golpista cria um site fraudulento com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias.
- e) A vítima tenta receber a mercadoria sem realizar o pagamento ou o realiza por meio de transferência efetuada de uma conta bancária ilegítima ou furtada.

**Comentários:** (a) Correto, esse é um caso de Golpe da Nigéria; (b) Errado, esse é um caso de Furto de Identidade; (c) Errado, esse é um caso de Furto de Identidade; (d) Errado, esse é um caso de Pharming; (e) Errado, isso não seria uma vítima e, sim, um golpista (Letra A).



## RESUMO

### DEFINIÇÃO DE MALWARE

Códigos maliciosos (Malwares, do inglês *Malicious Softwares*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

### FORMAS COMUNS DE INFECÇÃO DE MALWARES

Pela exploração de vulnerabilidades existentes nos programas instalados ou pela auto-execução de mídias removíveis infectadas, como pen-drives;

Pelo acesso a páginas maliciosas, utilizando navegadores vulneráveis ou pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas web ou de outros computadores.



### DEFINIÇÃO DE VÍRUS

Programa ou parte de um programa, normalmente malicioso, que se propaga infectando, inserindo cópias de si mesmo, anexando-se ou hospedando-se em arquivos ou programas existentes na máquina.

TIPOS DE VÍRUS	DESCRIÇÃO
VÍRUS DE SCRIPT	Escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML.
VÍRUS DE MACRO	Tipo específico de vírus de script normalmente recebido ao acessar páginas web ou por e-mail e que tenta infectar arquivos manipulados por aplicativos que utilizam essas linguagens mencionadas anteriormente como os arquivos que compõem o Microsoft Office.
VÍRUS DE BOOT	Também conhecido como Vírus de Setor de Carga ou Vírus de Setor de Inicialização, ele é ativado quando o computador é ligado e é carregado na memória antes do sistema operacional.
VÍRUS DE ARQUIVO	Também conhecido como Vírus de Programa ou Parasitário, trata-se do vírus mais tradicional e comum. Ele infecta e causa danos ao se conectarem a arquivos executáveis (.exe, .com, .dll, etc), sobrescrevendo o código original e causando danos quase sempre irreparáveis.
VÍRUS POLIMÓRFICO	Também conhecido como Vírus Mutante, é capaz de assumir múltiplas formas a cada infecção com o intuito de burlar o software de antivírus.
VÍRUS METAMÓRFICO	Trata-se de um vírus que se transforma a cada infecção, mas que – diferentemente do polimórfico – se reescreve completamente a cada infecção, podendo mudar seu tamanho e comportamento, aumentando a dificuldade de detecção.
VÍRUS STEALTH	Projetados explicitamente para não serem detectados pelo antivírus e têm a capacidade de se remover da memória temporariamente para evitar que o antivírus o detecte.
VÍRUS TIMEBOMB	Conhecido como Vírus Bomba Relógio, trata-se de um vírus que – após infectar a máquina – permanece latente (oculto), apenas se replicando, e seu código malicioso é programado para ser ativado em um determinado momento específico, executando sua carga útil.



TIPOS DE MALWARES	DESCRIÇÃO
WORM	Worm (ou Verme) é um programa capaz de se replicar automaticamente, enviando cópias de si mesmo. Diferente dos vírus, ele não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos através da rede, mas – sim – pela exploração automática de vulnerabilidades existentes em programas instalados em computadores ou pela execução direta de suas cópias.
BOT	Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do Worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.
BOTNET	Rede formada por centenas ou milhares de computadores zumbis e que permitem potencializar as ações danosas executadas pelos bots.
CAVALO DE TROIA	O Trojan é um programa que age utilizando o princípio do Cavalo de Troia, em um arquivo é enviado se fazendo passar por um aplicativo útil, como um “presente de grego”, mas que na verdade possui funcionalidades maliciosas escondidas. Muitas vezes, o trojan abre portas de comunicação para que através da Internet a máquina possa ser invadida ou monitorada.
RANSOMWARE	Trata-se de um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente utilizando criptografia, e que exige pagamento de um resgate ( <i>Ransom</i> , em inglês) para restabelecer o acesso ao usuário – trata-se de uma espécie de extorsão virtual.
SPYWARE	Software espião, capaz de violar a privacidade das informações de usuários, coletando dados da máquina ou da rede e disponibilizando-as a terceiros. Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas.
KEYLOGGER	Trata-se de um spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador e enviá-las a um invasor.
SCREENLOGGER	Trata-se de um spyware – similar ao keylogger – capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.
ADWARE	Trata-se de um spyware projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos quando as propagandas são direcionadas.
SNIFFER	Um Sniffer é programa que age monitorando o tráfego na rede, através da captura de pacotes de dados, em busca de informações sensíveis como o endereço dos sites acessados, senhas de acesso, e-mails, etc.
BACKDOOR	Um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
ROOTKIT	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
BOMBAS LÓGICAS	Trata-se de um software malicioso normalmente instalado por um usuário autorizado, como um administrador da rede, que o mantém no sistema deixando-o programado para causar danos (como excluir arquivos importantes) em um determinado evento, como por exemplo o caso de ficar mais de 30 dias sem efetuar login.
EXPLOITS	Trata-se de um software criado por hackers para permitir explorar vulnerabilidades conhecidas de sistemas e assim permitir que iniciantes ( <i>Script Kiddies</i> ) possam praticar ações de invasões sem conhecimentos avançados.
HIJACKER	O Hijacker (sequestro, em inglês) é um software malicioso que modifica o registro do sistema operacional, alterando o funcionamento do navegador, modificando sua página inicial, abrindo páginas automaticamente, inserindo botões inadvertidamente.



TIPOS DE ATAQUES	DESCRIÇÃO
ENGENHARIA SOCIAL	Trata-se de uma técnica muito utilizada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança.
FORÇA BRUTA	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. Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta.
NEGAÇÃO DE SERVIÇO	Negação de serviço (Denial of Service – DoS) é uma técnica pela qual um atacante busca retirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (Distributed Denial of Service – DDoS).
IP SPOOFING	O IP Spoofing (Falsificação/Mascaramento de IP) é uma técnica de invasão comumente empregada quando o mecanismo de autenticação de uma rede é baseado em endereços IP, isto é, quando a identificação de um usuário é realizada baseado em seu número de endereço IP.
E-MAIL SPOOFING	Técnica que consiste em alterar 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. Essa técnica é possível devido a características do protocolo SMTP (Simple Mail Transfer Protocol) que permitem que campos do cabeçalho sejam falsificados.
PHISHING SCAM	Fraude em que o golpista tenta enganar um usuário para obtenção de dados pessoais e financeiros que permitam a aplicação de um golpe, combinando técnicas computacionais e de engenharia social. Um exemplo de phishing é um e-mail que possa induzir o usuário a clicar em um link falso levando-o para uma página clonada ou um arquivo malicioso.
PHARMING	Ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original. É um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS. Nesse caso, quando o usuário tenta acessar um site legítimo, o navegador web é redirecionado, de forma transparente, para uma página falsa.
HOAX	Trata-se de 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.
MAN IN THE MIDDLE	Trata-se de um ataque em que os dados trocados entre duas partes são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. Durante o ataque, a comunicação é interceptada pelo atacante e retransmitida. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação.
DEFACEMENT	Trata-se de uma técnica que consiste em alterar o conteúdo da página web. Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente os atacantes alteram a página principal do site, porém páginas internas também podem ser alteradas.

 **PARA MAIS DICAS:** [WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO](https://www.instagram.com/professordiego-carvalho)

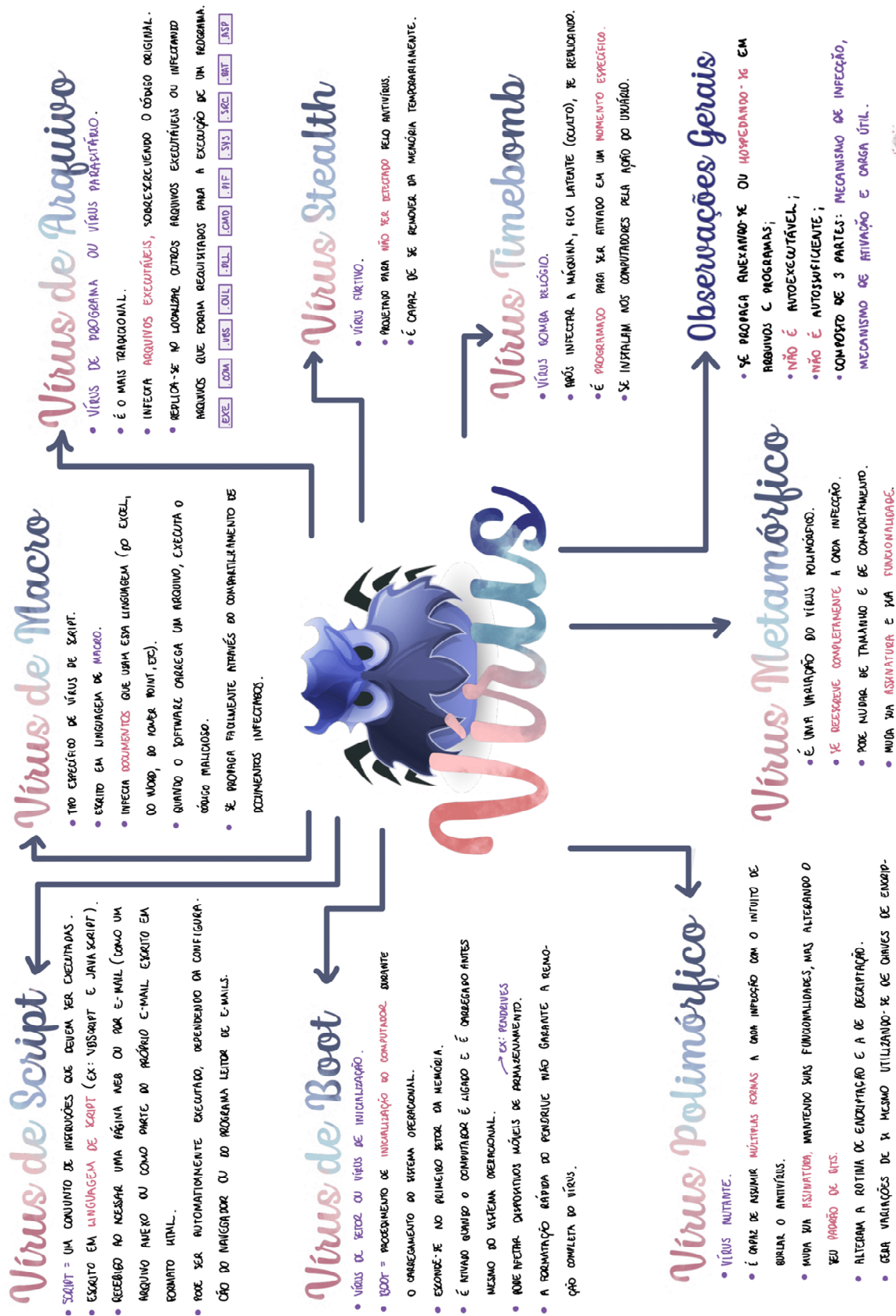


# RESUMO DE CÓDIGOS MALICIOSOS

	VÍRUS	WORM	BOT	TROJAN	SPYWARE	BACKDOOR	ROOTKIT
<b>FORMA DE OBTENÇÃO</b>							
Recebido automaticamente pela rede		X	X				
Recebido por <i>e-mail</i>	X	X	X	X	X		
Baixado de <i>sítes</i> na Internet	X	X	X	X	X		
Compartilhamento de arquivos	X	X	X	X	X		
Uso de mídias removíveis infectadas	X	X	X	X	X		
Redes sociais	X	X	X	X	X		
Mensagens instantâneas	X	X	X	X	X		
Inserido por um invasor		X	X	X	X	X	X
Ação de outro código malicioso		X	X	X	X	X	X
<b>FORMA DE INSTALAÇÃO</b>							
Execução de um arquivo infectado	X						
Execução explícita do código malicioso		X	X	X	X		
Via execução de outro código malicioso						X	X
Exploração de vulnerabilidades		X	X			X	X
<b>FORMA DE PROPAGAÇÃO</b>							
Inserir cópia de si próprio em arquivos	X						
Envia cópia de si próprio automaticamente pela rede		X	X				
Envia cópia de si próprio automaticamente por email		X	X				
Não se propaga				X	X	X	X
<b>AÇÕES MALICIOSAS MAIS COMUNS</b>							
Altera e/ou remove arquivos	X			X			X
Consome grande quantidade de recursos		X	X				
Furta informações sensíveis			X	X	X		
Instala outros códigos maliciosos		X	X	X			X
Possibilita o retorno do invasor						X	X
Envia <i>spam</i> e <i>phishing</i>			X				
Desfere ataques na Internet		X	X				
Procura se manter escondido	X				X	X	X



## MAPA MENTAL



@mapasdashai





- CAPAZ DE SE REPLICAR AUTOMATICAMENTE, ENVIANDO CÓPIAS DE SI MESMO.
- CONSUME MUITOS RECURSOS, AFETA O DESEMPENHO DA REDE E PODE LENTAR O DISCO RÍGIDO.
- VORMS NÃO INFECTAM ARQUIVOS. SÃO AUTÔNOMOS.
- SÃO CAPAZES DE ENTRAR EM UMA MÁQUINA SEM QUALQUER INTERAÇÃO COM O USUÁRIO.

#### PROCESSO DE INFECÇÃO E PROPAGAÇÃO

- 1ª FASE: SCANNING (IDENTIFICAÇÃO DOS COMPUTADORES - ALVO E OS QUAIS TENTARÁ SE COPIAR);
- 2ª FASE: ENVIO DE CÓPIAS;
- 3ª FASE: ATIVAÇÃO DAS CÓPIAS (EM REGRA, PRECISA SER EXECUTADO PARA QUE A INFECÇÃO OCORRA).



#### Bot

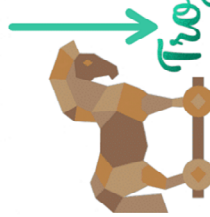
- PROGRAMA QUE QUOTE DE MECANISMOS DE COMUNICAÇÃO COM O INVASOR QUE PERMITEM QUE A MÁQUINA INVADIDA SEJA CONTROLADA REMOTAMENTE.
- SE PROPAGA AUTOMATICAMENTE EXPLORANDO VULNERABILIDADES DOS PROGRAMAS.
- COMPUTADOR INFECTADO = ZUMBI.
- BOTNET = REDE DE ZUMBIS PRONTA PARA EXECUTAR AÇÕES EM MASSA SOB COMANDO DO INVASOR.



#### Software Espião

- SOFTWARE ESPION QUE COLETA DADOS DA MÁQUINA OU DA REDE E DISPONIBILIZA-OS A TERCEIROS.
- PODE SER LEGÍTIMO OU MALICIOSO, DEPENDENDO DA FORMA COMO FOI INSTALADO.
- PRECISA SER EXPLICITAMENTE EXECUTADO PELO USUÁRIO.
- KEYLOGGER: CAPTURA AS TECLAS DIGITADAS PELO USUÁRIO.
- SCREENLOGGER: CAPTURA A POSIÇÃO DO CURSOR E A TELA APRESENTADA NO MOMENTO EM QUE O MOUSE É CLICADO.
- ADWARE: PROJETADO PARA APRESENTAR PROPAGANDAS.

# Principais Malwares



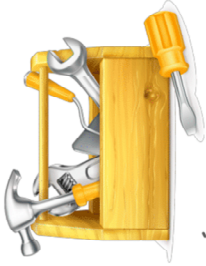
#### Trojan

- PROGRAMA QUE, ALÉM DE EXECUTAR AS FUNÇÕES PARA AS QUAIS FOI APARENTEMENTE PROJETADO, TAMBÉM EXECUTA FUNÇÕES MALICIOSAS.
- PRECISA EXPLICITAMENTE SER EXECUTADO PARA SER INSTALADO.
- NÃO SE PROPAGA.
- PODE SER CONSIDERADO UM TIPO DE VÍRUS.
- SUA ATUAÇÃO MALICIOSA É EXTREMAMENTE VERSÁTIL, PODENDO REALIZAR ATIVIDADES TÍPICAS DE OUTROS MALWARES.
- TIPOS DE TROJAN: DOWNLOADER, DROPPER, BACKDOOR, DOS, DESTRUTIVO, CLICKER, PROXY, SPY E BANKER.



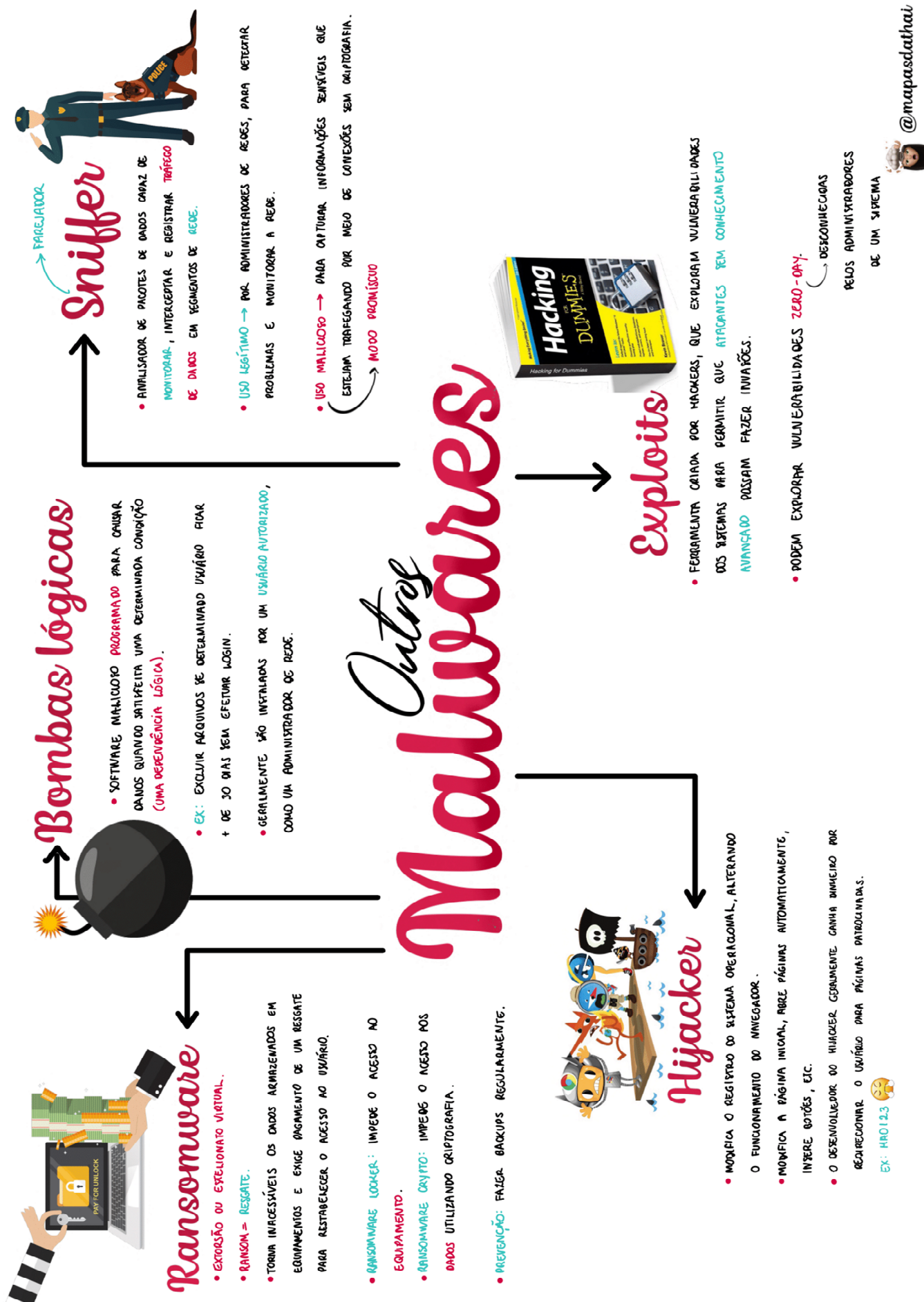
#### Backdoor

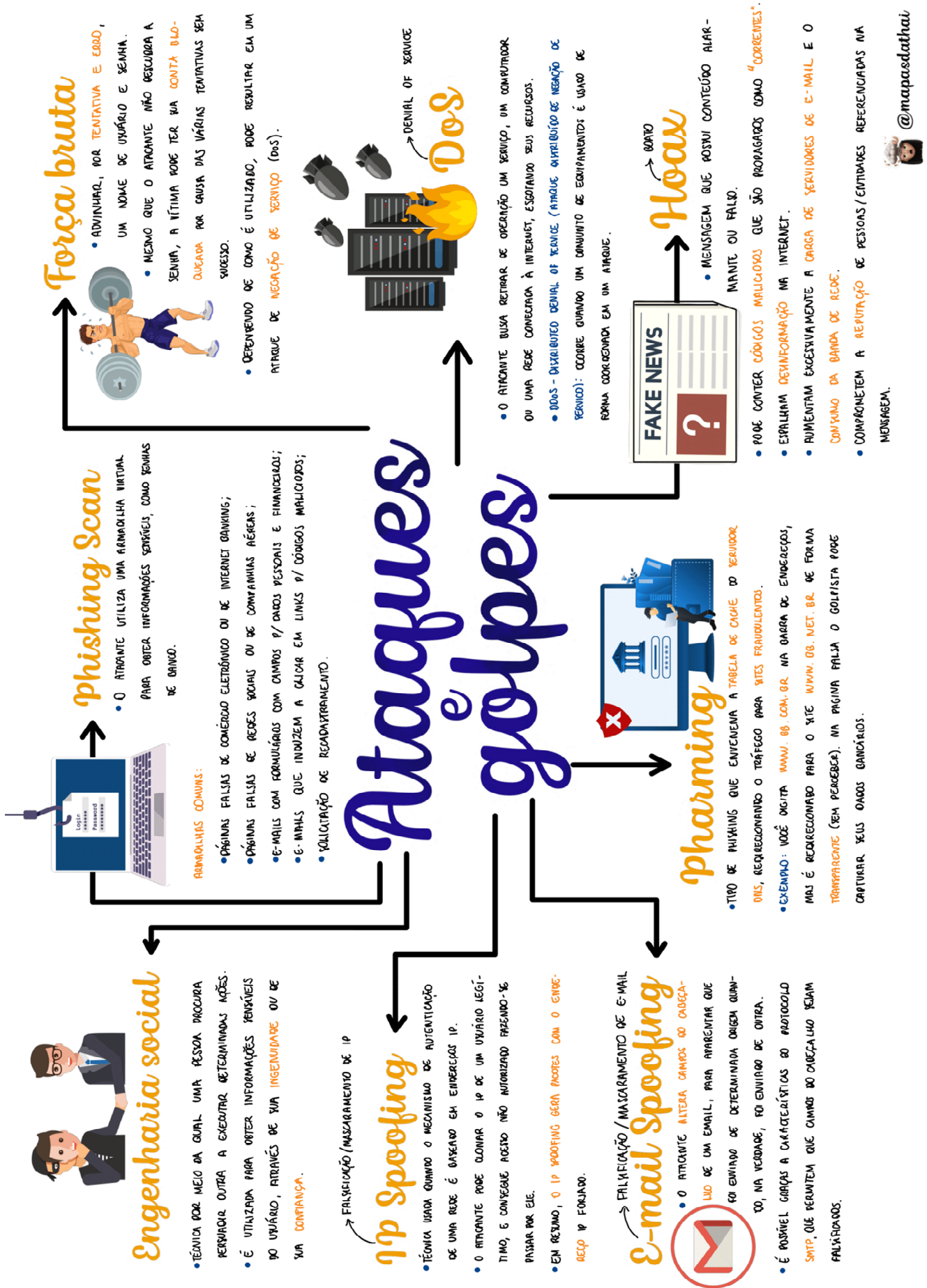
- PROGRAMA QUE PERMITE O RETORNO DE UM INVASOR A UM COMPUTADOR COMPROMETIDO.
- PODE SER INCLUÍDO POR OUTROS CÓDIGOS MALICIOSOS QUE TÊMAM PREVIAMENTE INFECTADO O COMPUTADOR OU POR INVASORES QUE EXPLORAM VULNERABILIDADES NOS PROGRAMAS INSTALADOS NA MÁQUINA.
- GARANTE ACESSO REMOTO FUTURO. (ABRE AS PORTAS TOP)



#### Rootkit

- CONJUNTO DE PROGRAMAS E TÉCNICAS QUE PERMITE ESCONDER E ASSEGURAR A PRESENÇA DE UM INVASOR OU DE OUTRO CÓDIGO MALICIOSO EM UM COMPUTADOR.
- É UM DOS MALWARES MAIS SORFISICADOS QUE EXISTEM.
- NÃO É USADO PARA OBTENÇÃO DE ACESSO, MAS SIM PARA MANTÊ-LO.
- COMPROMETE O SISTEMA OPERACIONAL, ALTERANDO TUDO QUE ELE FORNECE, DE ACORDO COM O QUE QUER O INVASOR.





@mapasdashai



## QUESTÕES COMENTADAS – CESGRANRIO

1. (CESGRANRIO / BB – 2021) Muitos códigos maliciosos aproveitam-se de um recurso do Windows 10 que possibilita a execução de um programa presente em um dispositivo de armazenamento USB imediatamente após a sua conexão ao computador. Esse recurso, que pode ser desativado, é conhecido como:
- a) inicialização automática.
  - b) execução automática.
  - c) reprodução automática.
  - d) atualização automática.
  - e) configuração automática.

### Comentários:

O recurso que permite a execução imediata de um programa presente em um dispositivo USB após a sua conexão ao computador (plug & play) é chamado de Reprodução Automática. Ele realmente pode ser desativado para impedir a ação de malwares – aliás, esse é o padrão atualmente.

**Gabarito:** Letra C

2. (CESGRANRIO / BB – 2021) Os bancos investem em recursos de segurança para minimizar os riscos de fraude nas operações bancárias através de Internet Banking. Os usuários, porém, precisam estar atentos aos golpistas que procuram persuadir vítimas em potencial a acessar sites falsos e a fornecer informações sensíveis. Esse ataque é conhecido como:
- a) botnet.
  - b) injection.
  - c) spyware.
  - d) phishing.
  - e) ransomware.

### Comentários:

Esse tipo de ataque é conhecido como **phishing**. O phishing é uma tentativa de golpe no qual os criminosos tentam obter informações confidenciais, como senhas, números de conta bancária e informações de cartão de crédito, através da criação de sites falsos que imitam as páginas de login de sites legítimos. Os golpistas também costumam enviar e-mails que instam as vítimas a acessar esses sites fraudulentos.

**Gabarito:** Letra D



**3. (CESGRANRIO / PETROBRAS – 2009)** Os itens a seguir relacionam-se corretamente à Internet, EXCETO:

- a) Phishing é uma técnica usada para induzir usuários de computador a revelar informações pessoais ou financeiras, como uma senha de conta bancária.
- b) Com o Microsoft Word, é possível inserir controles de formulário HTML em uma página da Web para criar formulários de coleta ou fornecimento de dados.
- c) Os vírus de e-mail são anexados às mensagens enviadas e o firewall, ao determinar o conteúdo da mensagem, pode, portanto, proteger o computador contra esses tipos de vírus.
- d) World Wide Web é uma rede de computadores na Internet que fornece informação em forma de hipertexto, podendo usar um software chamado browser para descarregar essas informações de servidores de sites e mostrá-las na tela do usuário.
- e) Um upload consiste em se fazer uma cópia de um arquivo de um computador para algum servidor na Internet

**Comentários:**

Firewall é um hardware e/ou software que controla o tráfego em uma rede – ele não determina o conteúdo de mensagens nem protege computadores contra vírus de e-mail. Todos os outros itens da questão estão perfeitos!

**Gabarito:** Letra C

**4. (CESGRANRIO / UNIRIO – 2016)** Os responsáveis por procedimentos de Segurança da Informação devem-se preocupar com usuários mal intencionados, muitas vezes responsáveis por geração de prejuízos empresariais disseminando malwares, roubando senhas ou realizando outra ação qualquer de invasão dos sistemas da empresa. Um exemplo típico é o programador competente, mas mau caráter, que produz programa malicioso capaz de propagar-se automaticamente pela rede de computadores da empresa em que trabalha, por meio de cópias de computador para computador, provocando, por exemplo, lentidão na rede, desaparecimento de arquivos, etc. Os males que esse tipo de programa produz ainda seriam mais graves se dispusesse, como outros malwares, de mecanismos de comunicação que proporcionassem seu controle remoto pelo agente invasor. Esse tipo de programa malicioso é conhecido como:

- a) Adware
- b) Spyware
- c) Keylogger
- d) Vírus
- e) Worm



### Comentários:

(a) Errado, adware não causa lentidão na rede nem se propaga automaticamente; (b) Errado, spyware não causa lentidão na rede nem se propaga automaticamente; (c) Errado, keylogger não causa lentidão na rede nem se propaga automaticamente; (d) Errado, vírus não causa lentidão na rede nem se propaga automaticamente – suas ações maliciosas mais comuns são alterar e/ou remover arquivos em geral de forma escondida; (e) Correto, worm pode causar lentidão na rede devido ao consumo excessivo de recursos além de se propagar automaticamente.

**Gabarito:** Letra E

**5. (CESGRANRIO / ANP – 2016)** Uma hacker ameaçou divulgar na Web informações sigilosas de uma empresa após ter conseguido acesso a seus sistemas de informação. Para conseguir o acesso, ela telefonou para uma das secretárias da diretoria, passando-se por esposa de um dos diretores. Em seguida, ela disse à secretária que seu marido tinha sofrido um acidente e estava hospitalizado. Porém, antes de ficar inconsciente, o diretor lhe havia pedido que entrasse em contato com a empresa a fim de que uma de suas secretárias solicitasse a mudança do seu login e da sua senha, pois ele havia perdido sua agenda no acidente e temia que alguém pudesse invadir os sistemas da empresa, uma vez que esses dados, por descuido seu, estavam anotados na agenda perdida. Em seguida, a suposta esposa forneceu os novos login e senha à secretária. Esse tipo de ataque para obtenção de informações é chamado de:

- a) informações livres
- b) engenharia social
- c) varredura de vulnerabilidades
- d) dumpster diving
- e) ataque físico

### Comentários:

(a) Errado. Informações Livres é uma técnica de análise de informações que podem ser obtidas livremente na internet sem a necessidade de ações intrusivas; (b) Correto. Engenharia Social é uma técnica de obtenção de informações explorando vulnerabilidades humanas e sociais dos funcionários de uma organização; (c) Errado. Varredura de Vulnerabilidades é uma técnica de envio de tipos de pacotes com o objetivo de obter informações relevantes para um ataque sobre um computador ou uma rede; (d) Errado. Dumpster Diving é uma técnica de vasculhar o lixo (sim, lixo mesmo) de empresas e pessoas com o objetivo de encontrar algo de valor; (e) Errado. Ataque Físico é basicamente o roubo de equipamentos ou dispositivos de armazenamento realizado diretamente em uma organização.

**Gabarito:** Letra B



6. (CESGRANRIO / BB – 2015) Os escriturários de uma agência foram chamados para uma reunião com um profissional da área de segurança da informação de um banco. O objetivo dessa reunião era informá-los de que houve uma falha nos procedimentos de segurança da rede de computadores da agência, o que permitiu a propagação de um programa malicioso bastante perigoso. Durante a reunião, o profissional de segurança disse que o programa em questão permite monitorar a movimentação do mouse por sobre a tela de uma aplicação bancária, com o objetivo de descobrir a senha digitada por um usuário que esteja usando um teclado virtual.

Ele completou sua explanação dizendo que esse tipo de código malicioso é chamado de:

- a) vírus
- b) trojan clicker
- c) spyware
- d) botnet
- e) trojan backdoor

#### Comentários:

*Permite monitorar a movimentação do mouse sobre a tela de uma aplicação bancária? Busca descobrir a senha digitada por um usuário que esteja usando um teclado virtual? Galera, a questão trata do screenlogger, que é um tipo de spyware: capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking. Ressalva: a questão poderia ter utilizado o termo "instalação" em vez de "propagação" para ficar mais adequado, visto que spywares não se propagam.*

**Gabarito:** Letra C

7. (CESGRANRIO / BB – 2013) Há características importantes que distinguem os códigos maliciosos denominados worm daqueles denominados trojan. Uma dessas características é a:

- a) autorreplicação automática pela rede
- b) instalação por execução de arquivo infectado
- c) contaminação através de redes sociais
- d) contaminação por compartilhamento de arquivos
- e) instalação por execução explícita do código malicioso

#### Comentários:

Uma diferença básica é que worms são capazes de propagar automaticamente e trojans, não; ademais, trojans não são recebidos automaticamente pela rede e worms são.



**Gabarito:** Letra A

8. (CESGRANRIO / CEF – 2012) Firewall é um software ou hardware que verifica informações vindas da Internet ou de uma outra rede. Dentre os ataques que **NÃO** são neutralizados por um firewall, inclui-se o ataque de:

- a) golpe de phishing
- b) ping of death
- c) rootkits
- d) hackers
- e) worms

**Comentários:**

Firewalls são capazes de neutralizar ataques de ping of death, rootkits, hackers ou worms, no entanto não são capazes de neutralizar o golpe de phishing. Lembrando que o phishing é um tipo de fraude eletrônica projetada para roubar informações particulares que sejam valiosas para cometer um roubo ou fraude posteriormente, logo ele não pode fazer nada.

**Gabarito:** Letra A

9. (CESGRANRIO / PETROBRAS – 2012) Arquivos de texto armazenados no computador de um usuário, a pedido de um servidor da web, permitindo que um site armazene informações no computador do usuário e depois as recupere, chamam-se:

- a) vírus
- b) cookies
- c) worms
- d) cavalos de troia
- e) sniff

**Comentários:**

(a) Errado, vírus não é um arquivo texto e nada tem a ver com a descrição do enunciado; (b) Correto, cookies são pequenos arquivos de texto armazenados no computador de um usuário, a pedido de um servidor da web, permitindo que um site armazene informações no computador do usuário e depois as recupere; (c) Errado, worms são softwares maliciosos; (d) Errado, cavalos de troia são softwares maliciosos; (e) Errado, sniff é uma técnica de interceptação de tráfego.

**Gabarito:** Letra B



**10. (CESGRANRIO / TRANSPETRO – 2012)** Os softwares navegadores de internet podem utilizar ferramentas externas para executar vários tipos de serviços. Essas ferramentas são gerenciadas pelos navegadores como complementos, também denominados:

- a) browsers
- b) plugins
- c) servers
- d) spammers
- e) webmotors

**Comentários:**

As ferramentas externas para executar diversos tipos de serviço são os denominados plugins!

**Gabarito:** Letra B

**11. (CESGRANRIO / FINEP – 2011)** O navegador de internet da Microsoft (Internet Explorer 8) oferece um recurso que permite ao usuário navegar na Web sem deixar registros sobre essa navegação, ajudando a impedir que outra pessoa que possa utilizar seu computador veja quais páginas foram visitadas por ele. Esse recurso é denominado navegação:

- a) Banned
- b) Hidden
- c) InPrivate
- d) SmartScreen
- e) Phishing Filter

**Comentários:**

O recurso de navegação que impede que outra pessoa que possa utilizar seu computador veja quais páginas foram visitadas por ele é a Navegação InPrivate – em outros navegadores, esse recurso pode ter outros nomes como Navegação Privada ou Navegação Anônima.

**Gabarito:** Letra C

**12. (CESGRANRIO / BB – 2010)** O Filtro do SmartScreen da Microsoft é um recurso do Internet Explorer que ajuda a detectar sites de Phishing e sites de:

- a) Malware.
- b) Ringware.
- c) Spyware.
- d) Threads.
- e) Worms.



### Comentários:

Se um site parecer suspeito, você provavelmente não deverá baixar aplicativos dele, nem fornecer informações pessoais ou sobre sua conta. Porém, às vezes, é difícil dizer se um site é legítimo ou não. O SmartScreen o ajuda a identificar sites considerados de phishing e **malware** e também ajuda você a tomar decisões conscientes sobre o download de aplicativos.

**Gabarito:** Letra A

**13. (CESGRANRIO / IBGE – 2009)** Sobre os aspectos de segurança dos sistemas computacionais, são feitas as afirmativas abaixo.

- I – A palavra “windows” é um exemplo de senha forte.
- II – Ransomware é um tipo de malware.
- III – Os Trojans são antivírus que protegem as macros do Excel contra vírus.

Está(ão) correta(s) a(s) afirmativa(s):

- a) I, apenas.
- b) II, apenas.
- c) III, apenas.
- d) I e II, apenas.
- e) I, II e III.

### Comentários:

(I) Errado, essa palavra é pequena, não possui números ou caracteres especiais, logo é um exemplo de senha fraca; (II) Correto, ransomware é realmente um tipo de malware que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário; (III) Errado, trojans são softwares maliciosos e, não, antivírus.

**Gabarito:** Letra B

**14. (CESGRANRIO / BANCO CENTRAL – 2009)** Um dos crimes que mais causam prejuízos às pessoas e às instituições é a fraude. Utilizando-se da Internet, fraudadores têm enviado e-mails com mensagens que induzem o usuário a fornecer dados pessoais e financeiros.

Esse tipo de fraude, que se dá mediante o envio de mensagem não solicitada, supostamente de uma instituição conhecida, como um banco, e que procura induzir o acesso a páginas fraudulentas, projetadas para furtar dados pessoais e financeiros, constitui a prática de:



- a) spam.
- b) phishing.
- c) worm.
- d) adware.
- e) spyware.

#### Comentários:

Fraude que se dá mediante o envio de mensagem não solicitada supostamente de uma instituição conhecida (Ex: Banco) e que procurar induzir o acesso a páginas fraudulentas com estética idêntica às da instituição verdadeira com o intuito de furtar dados pessoais e financeiros é também conhecida como *phishing*.

**Gabarito:** Letra B

**15. (CESGRANRIO / PETROBRAS – 2011)** Considerados pragas digitais, os rootkits são malwares que, ao se instalarem no computador alvo,

- a) apagam as principais informações do firmware da máquina infectada.
- b) camuflam a sua existência e fornecem acesso privilegiado ao computador infectado.
- c) desinstalam ou corrompem os aplicativos office configurados no computador infectado.
- d) modificam as configurações de TCP/IP do computador infectado, impedindo o acesso à Internet.
- e) multiplicam-se indefinidamente até ocupar todo o espaço disponível no disco rígido.

#### Comentários:

(a) Errado, eles apagam ou alteram arquivos que prejudicam o funcionamento do sistema operacional; (b) Correto, eles inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os rootkits atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção; (c) Errado, eles não costumam infectar aplicativos do Office; (d) Errado, essa não é uma das características de um rootkit; (e) Errado, eles não se propagam.

**Gabarito:** Letra B

**16. (CESGRANRIO / PETROBRAS – 2011)** Os códigos maliciosos desenvolvem a cada dia novos métodos de proliferação. A praga que utiliza a rede de comunicação de dados para se proliferar entre sistemas de computação vulneráveis é o:



- a) worm
- b) logic bomb
- c) cavalo de tróia
- d) flooder
- e) spyware

#### Comentários:

O malware que se prolifera congestionando uma rede de comunicação é o worm (verme).

**Gabarito:** Letra A

**17. (CESGRANRIO / FUNASA – 2009)** Qual dos itens abaixo NÃO representa um mecanismo de segurança?

- a) Assinatura digital
- b) Software anti-spyware
- c) Sistema biométrico
- d) Firewall
- e) Worm

#### Comentários:

Todos são mecanismos de segurança, exceto worm (que é um malware – software malicioso).

**Gabarito:** Letra E

**18. (CESGRANRIO / BASA – 2015)** Como é classificado o código malicioso que instala um servidor de proxy, de modo a permitir que um computador seja utilizado para navegação anônima e envio de spam?

- a) Spyware
- b) Cavalo de troia
- c) Worm
- d) Bot
- e) Backdoor

#### Comentários:

Spyware, Worm, Bot e Backdoor não instalam um servidor de Proxy. O Cavalo de Troia é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Existem



diferentes tipos de trojans classificados de acordo com as ações maliciosas que costumam executar ao infectar um computador. Alguns desses tipos são:

TIPO DE TROJAN	DESCRIÇÃO
TROJAN DOWNLOADER	Instala outros códigos maliciosos, obtidos de sites na Internet.
TROJAN DROPPER	Instala outros códigos maliciosos, embutidos no próprio código do trojan.
TROJAN BACKDOOR	Inclui backdoors, possibilitando o acesso remoto do atacante ao computador.
TROJAN DOS	Instala ferramentas de negação de serviço e as utiliza para desferir ataques.
TROJAN DESTRUTIVO	Altera ou apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
TROJAN CLICKER	Redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
TROJAN PROXY	Instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.
TROJAN SPY	Instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
TROJAN BANKER	Coleta dados bancários do usuário através da instalação spyware que são ativados quando sites de Internet Banking são acessados – similar ao Trojan Spy, mas com objetivos específicos.

**Gabarito:** Letra B



## LISTA DE QUESTÕES – CESGRANRIO

1. **(CESGRANRIO / BB – 2021)** Muitos códigos maliciosos aproveitam-se de um recurso do Windows 10 que possibilita a execução de um programa presente em um dispositivo de armazenamento USB imediatamente após a sua conexão ao computador. Esse recurso, que pode ser desativado, é conhecido como:  
  
a) inicialização automática.  
b) execução automática.  
c) reprodução automática.  
d) atualização automática.  
e) configuração automática.
2. **(CESGRANRIO / BB – 2021)** Os bancos investem em recursos de segurança para minimizar os riscos de fraude nas operações bancárias através de Internet Banking. Os usuários, porém, precisam estar atentos aos golpistas que procuram persuadir vítimas em potencial a acessar sites falsos e a fornecer informações sensíveis. Esse ataque é conhecido como:  
  
a) botnet.  
b) injection.  
c) spyware.  
d) phishing.  
e) ransomware.
3. **(CESGRANRIO / PETROBRAS – 2009)** Os itens a seguir relacionam-se corretamente à Internet, EXCETO:  
  
a) Phishing é uma técnica usada para induzir usuários de computador a revelar informações pessoais ou financeiras, como uma senha de conta bancária.  
  
b) Com o Microsoft Word, é possível inserir controles de formulário HTML em uma página da Web para criar formulários de coleta ou fornecimento de dados.  
  
c) Os vírus de e-mail são anexados às mensagens enviadas e o firewall, ao determinar o conteúdo da mensagem, pode, portanto, proteger o computador contra esses tipos de vírus.  
  
d) World Wide Web é uma rede de computadores na Internet que fornece informação em forma de hipertexto, podendo usar um software chamado browser para descarregar essas informações de servidores de sites e mostrá-las na tela do usuário.  
  
e) Um upload consiste em se fazer uma cópia de um arquivo de um computador para algum servidor na Internet



4. **(CESGRANRIO / UNIRIO – 2016)** Os responsáveis por procedimentos de Segurança da Informação devem-se preocupar com usuários mal intencionados, muitas vezes responsáveis por geração de prejuízos empresariais disseminando malwares, roubando senhas ou realizando outra ação qualquer de invasão dos sistemas da empresa. Um exemplo típico é o programador competente, mas mau caráter, que produz programa malicioso capaz de propagar-se automaticamente pela rede de computadores da empresa em que trabalha, por meio de cópias de computador para computador, provocando, por exemplo, lentidão na rede, desaparecimento de arquivos, etc. Os males que esse tipo de programa produz ainda seriam mais graves se dispusesse, como outros malwares, de mecanismos de comunicação que proporcionassem seu controle remoto pelo agente invasor. Esse tipo de programa malicioso é conhecido como:

- a) Adware
- b) Spyware
- c) Keylogger
- d) Vírus
- e) Worm

5. **(CESGRANRIO / ANP – 2016)** Uma hacker ameaçou divulgar na Web informações sigilosas de uma empresa após ter conseguido acesso a seus sistemas de informação. Para conseguir o acesso, ela telefonou para uma das secretárias da diretoria, passando-se por esposa de um dos diretores. Em seguida, ela disse à secretária que seu marido tinha sofrido um acidente e estava hospitalizado. Porém, antes de ficar inconsciente, o diretor lhe havia pedido que entrasse em contato com a empresa a fim de que uma de suas secretárias solicitasse a mudança do seu login e da sua senha, pois ele havia perdido sua agenda no acidente e temia que alguém pudesse invadir os sistemas da empresa, uma vez que esses dados, por descuido seu, estavam anotados na agenda perdida. Em seguida, a suposta esposa forneceu os novos login e senha à secretária. Esse tipo de ataque para obtenção de informações é chamado de:

- a) informações livres
- b) engenharia social
- c) varredura de vulnerabilidades
- d) dumpster diving
- e) ataque físico

6. **(CESGRANRIO / BB – 2015)** Os escriturários de uma agência foram chamados para uma reunião com um profissional da área de segurança da informação de um banco. O objetivo dessa reunião era informá-los de que houve uma falha nos procedimentos de segurança da rede de computadores da agência, o que permitiu a propagação de um programa malicioso bastante perigoso. Durante a reunião, o profissional de segurança disse que o programa em questão permite monitorar a movimentação do mouse por sobre a tela de uma aplicação bancária, com o objetivo de descobrir a senha digitada por um usuário que esteja usando um teclado virtual.



Ele completou sua explanação dizendo que esse tipo de código malicioso é chamado de:

- a) vírus
- b) trojan clicker
- c) spyware
- d) botnet
- e) trojan backdoor

7. (CESGRANRIO / BB – 2013) Há características importantes que distinguem os códigos maliciosos denominados worm daqueles denominados trojan. Uma dessas características é a:

- a) autorreplicação automática pela rede
- b) instalação por execução de arquivo infectado
- c) contaminação através de redes sociais
- d) contaminação por compartilhamento de arquivos
- e) instalação por execução explícita do código malicioso

8. (CESGRANRIO / CEF – 2012) Firewall é um software ou hardware que verifica informações vindas da Internet ou de uma outra rede. Dentre os ataques que **NÃO** são neutralizados por um firewall, inclui-se o ataque de:

- a) golpe de phishing
- b) ping of death
- c) rootkits
- d) hackers
- e) worms

9. (CESGRANRIO / PETROBRAS – 2012) Arquivos de texto armazenados no computador de um usuário, a pedido de um servidor da web, permitindo que um site armazene informações no computador do usuário e depois as recupere, chamam-se:

- a) vírus
- b) cookies
- c) worms
- d) cavalos de troia
- e) sniff

10. (CESGRANRIO / TRANSPETRO – 2012) Os softwares navegadores de internet podem utilizar ferramentas externas para executar vários tipos de serviços. Essas ferramentas são gerenciadas pelos navegadores como complementos, também denominados:

- a) browsers
- b) plugins
- c) servers



- d) spammers
- e) webmotors

**11. (CESGRANRIO / FINEP – 2011)** O navegador de internet da Microsoft (Internet Explorer 8) oferece um recurso que permite ao usuário navegar na Web sem deixar registros sobre essa navegação, ajudando a impedir que outra pessoa que possa utilizar seu computador veja quais páginas foram visitadas por ele. Esse recurso é denominado navegação:

- a) Banned
- b) Hidden
- c) InPrivate
- d) SmartScreen
- e) Phishing Filter

**12. (CESGRANRIO / BB – 2010)** O Filtro do SmartScreen da Microsoft é um recurso do Internet Explorer que ajuda a detectar sites de Phishing e sites de:

- a) Malware.
- b) Ringware.
- c) Spyware.
- d) Threads.
- e) Worms.

**13. (CESGRANRIO / IBGE – 2009)** Sobre os aspectos de segurança dos sistemas computacionais, são feitas as afirmativas abaixo.

- I – A palavra “windows” é um exemplo de senha forte.
- II – Ransomware é um tipo de malware.
- III – Os Trojans são antivírus que protegem as macros do Excel contra vírus.

Está(ão) correta(s) a(s) afirmativa(s):

- a) I, apenas.
- b) II, apenas.
- c) III, apenas.
- d) I e II, apenas.
- e) I, II e III.

**14. (CESGRANRIO / BANCO CENTRAL – 2009)** Um dos crimes que mais causam prejuízos às pessoas e às instituições é a fraude. Utilizando-se da Internet, fraudadores têm enviado e-mails com mensagens que induzem o usuário a fornecer dados pessoais e financeiros.



Esse tipo de fraude, que se dá mediante o envio de mensagem não solicitada, supostamente de uma instituição conhecida, como um banco, e que procura induzir o acesso a páginas fraudulentas, projetadas para furtar dados pessoais e financeiros, constitui a prática de:

- a) spam.
- b) phishing.
- c) worm.
- d) adware.
- e) spyware.

**15. (CESGRANRIO / PETROBRAS – 2011)** Considerados pragas digitais, os rootkits são malwares que, ao se instalarem no computador alvo,

- a) apagam as principais informações do firmware da máquina infectada.
- b) camuflam a sua existência e fornecem acesso privilegiado ao computador infectado.
- c) desinstalam ou corrompem os aplicativos office configurados no computador infectado.
- d) modificam as configurações de TCP/IP do computador infectado, impedindo o acesso à Internet.
- e) multiplicam-se indefinidamente até ocupar todo o espaço disponível no disco rígido.

**16. (CESGRANRIO / PETROBRAS – 2011)** Os códigos maliciosos desenvolvem a cada dia novos métodos de proliferação. A praga que utiliza a rede de comunicação de dados para se proliferar entre sistemas de computação vulneráveis é o:

- a) worm
- b) logic bomb
- c) cavalo de tróia
- d) flooder
- e) spyware

**17. (CESGRANRIO / FUNASA – 2009)** Qual dos itens abaixo NÃO representa um mecanismo de segurança?

- a) Assinatura digital
- b) Software anti-spyware
- c) Sistema biométrico
- d) Firewall
- e) Worm

**18. (CESGRANRIO / BASA – 2015)** Como é classificado o código malicioso que instala um servidor de proxy, de modo a permitir que um computador seja utilizado para navegação anônima e envio de spam?

- a) Spyware



- b) Cavalo de troia
- c) Worm
- d) Bot
- e) Backdoor



## GABARITO – CESGRANRIO

1. LETRA C
2. LETRA D
3. LETRA C
4. LETRA E
5. LETRA B
6. LETRA C
7. LETRA A
8. LETRA A
9. LETRA B
10. LETRA B
11. LETRA C
12. LETRA A
13. LETRA B
14. LETRA B
15. LETRA B
16. LETRA A
17. LETRA E
18. LETRA B



# ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



1 Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



2 Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



3 Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



4 Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



5 Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



6 Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



7 Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



8 O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.