Estratégia Concursos

Aula 09

PRF (Policial) Informática - 2023

(Pré-Edital)

Autor:

Diego Carvalho, Renato da Costa,

Equipe Informática e TI

18 de Fevereiro de 2023

Índice

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.

cert.br

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO
DE INCIDENTES DE SEGURANÇA NO BRASIL

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.

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) Pheaking 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 intuitos geralmente comerciais é denominado:

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

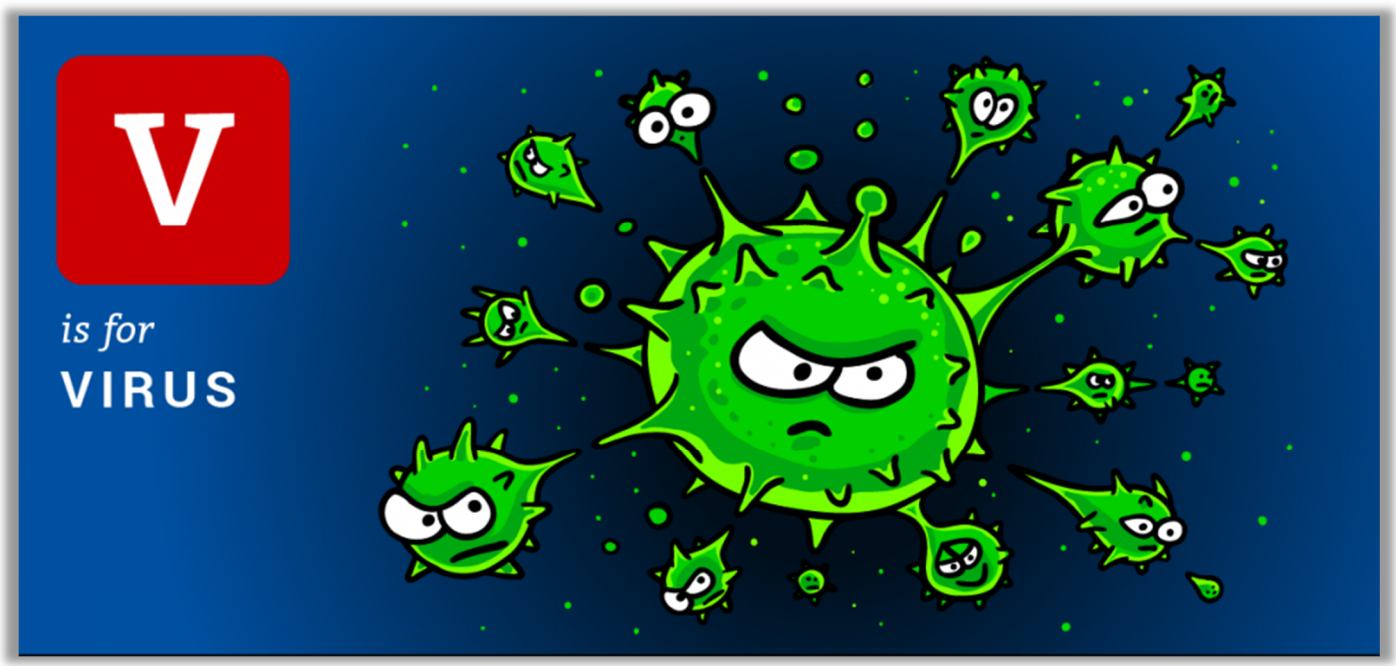
_____

Comentários: os famosos e-mails não solicitados ou indesejados são chamados de 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[1], 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[2]**! Essa informação é

[1] Eles não precisam ser necessariamente destrutivos ou maliciosas para o sistema do usuário. Um vírus pode, por exemplo, simplesmente mostrar uma imagem na tela do computador.

[2] 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.

ATIVAÇÃO	Nessa fase, o vírus é ativado para executar a função pretendida. Como ocorre com a fase de dormência, a fase de ativação pode ser causada por uma variedade de eventos de sistema, incluindo a contagem do número de vezes que essa cópia de vírus fez uma cópia de si mesma.
AÇÃO	Nessa fase, a função é executada. Ela pode ser inofensiva, como uma mensagem na tela, ou danosa, como a destruição de programas e arquivos de dados.

(CBM/SC – 2015) Um dos grandes problemas que afeta quem trabalha com computação, seja usuário avançado ou mesmo doméstico, é a possibilidade de infecção de seu sistema por um vírus. Com o crescimento da internet, cresce também a criminalidade virtual, e nos noticiários muitas vezes se vê algo relacionado ao tema. De acordo com Goodrich e Tamassia (2013), um vírus de computador, ou normalmente como é chamado, vírus, trata-se de um programa de computador, que pode ser replicado pela modificação de outros arquivos e/ou programas, para inserir código capaz de replicação posterior. Segundo os autores, os vírus de um computador, normalmente seguem quatro fases de execução. São elas:

a) Dormente; Propagação; Ativação; e, Ação.
b) Ataque; Penetração; Replicação; e, Liberação.
c) Diversidade; Robustez; Autoexecução; e, Privilégio.
d) Anonimato; Garantia; Autenticidade; e, Disponibilidade.

Comentários: as etapas são Dormência, Propagação, Ativação e Ação (Letra A).

A maioria dos vírus que infectam arquivos de programas executáveis realiza seu trabalho de maneira que sejam específicos para um sistema operacional em particular e, em alguns casos, específicos até mesmo para uma determinada plataforma de hardware. **Dessa forma, eles são projetados para tirar proveito dos detalhes e fraquezas de sistemas particulares. Em outras palavras, em geral um malware que funciona em um sistema não funciona em outro.**

Dito isso, existe uma lenda de que o Linux e o Mac OS são sistemas operacionais imunes a vírus! **Todo Sistema Operacional (SO) pode ser alvo de vírus**. O que ocorre é que – como a grande maioria dos computadores utiliza Windows – a taxa de replicação acaba sendo maior nesse sistema operacional. Ademais, existe maior interesse em se criar softwares maliciosos para esse SO!

(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 despeeeeeenca 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:

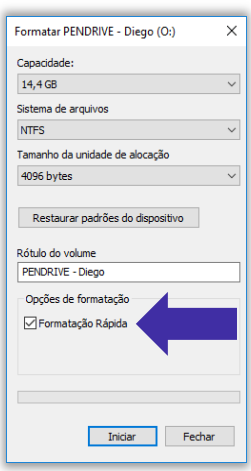
a) Spyware
b) vírus de macro.
c) Trojan Dropper.
d) Backdoor.
e) Worm.

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 Jaru/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


BBC Menu

NEWS | BRASIL

Notícias | Brasil | Internacional | Economia | Saúde | Ciência | Tecnologia | Aprenda Inglês

O vírus mutante e quase perfeito desativado pelo FBI e pela UE

10 abril 2015 Compartilhar

Uma força policial internacional persegue um criminoso que se transforma diante de seus olhos e foge justo quando parece que está prestes a ser capturado.

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 decriptação. Em geral, para realizar a detecção dessas ameaças, os antivírus fazem a decriptação 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.

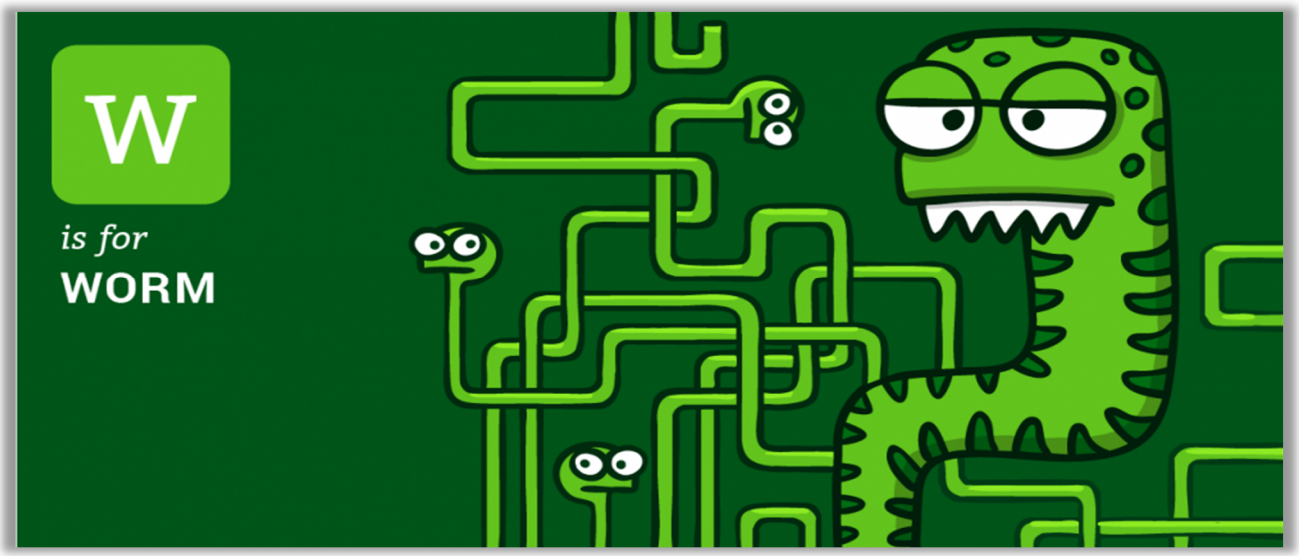
Está correto o que se afirma APENAS em:

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).

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

 # CURIOSIDADE SOBRE WORMS: 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).

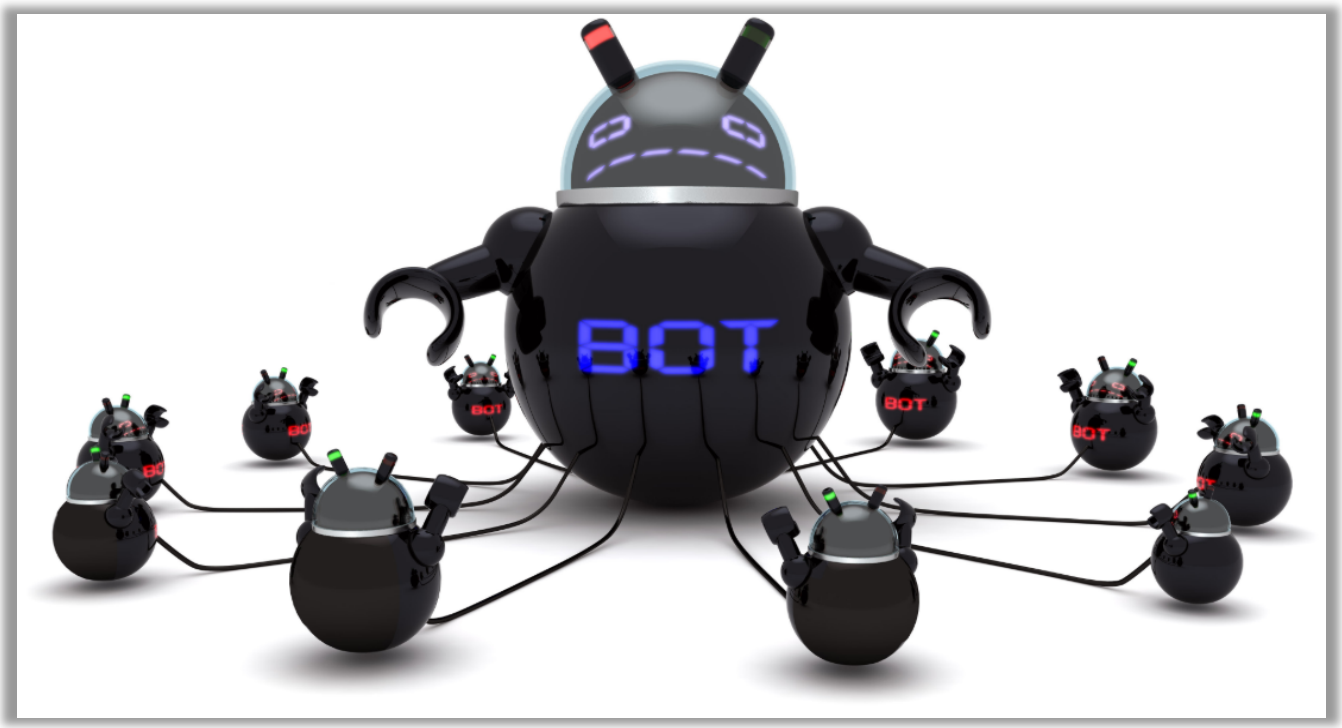
(PC/MG – 2018) O tipo de ameaça à segurança de um computador que consiste em um programa completo que se replica de forma autônoma para se propagar para outros computadores é:

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



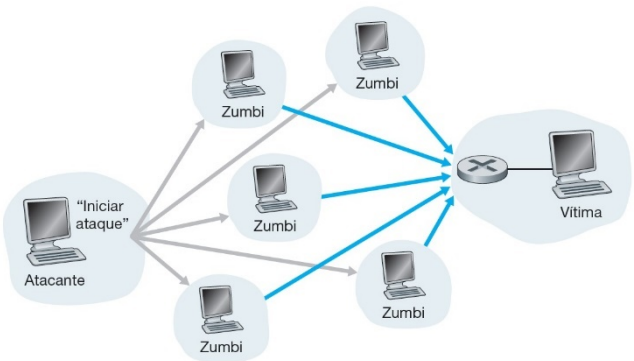
Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do Worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. 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 ROBOT = 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...

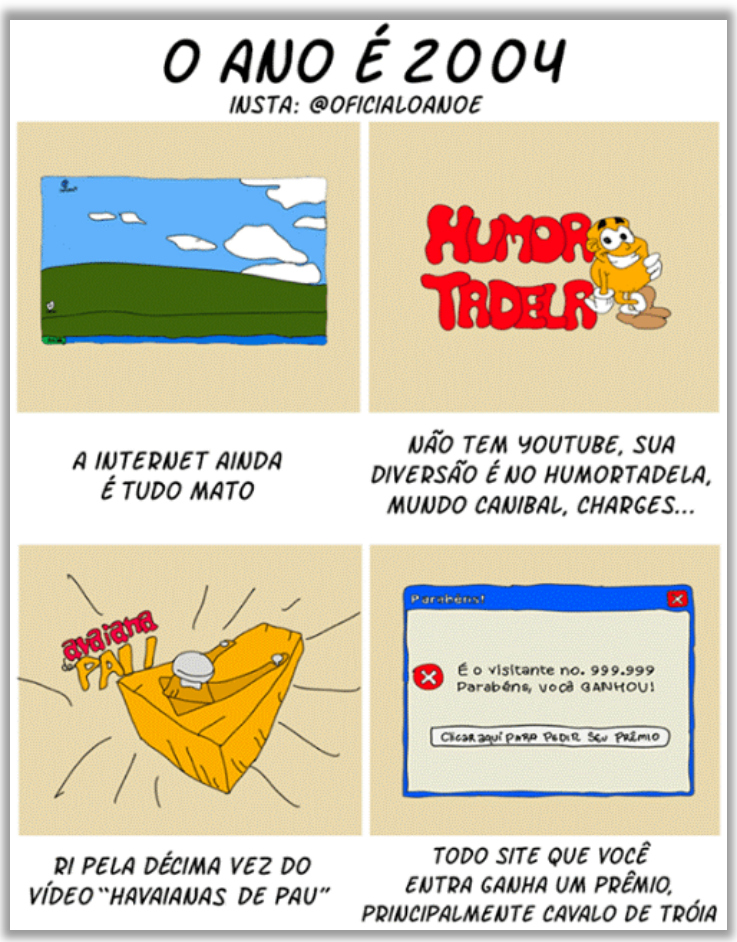
Dentro do cavalo de madeira estavam diversos soldados gregos. Os troianos acharam que os gregos estavam sendo corteses, aceitaram o presente e levaram o cavalo para dentro da cidade fortificada. À noite, os soldados gregos que estavam escondidos dentro do cavalo saíram, dominaram os sentinela e possibilitaram 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.

DROPPER	
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.

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/)

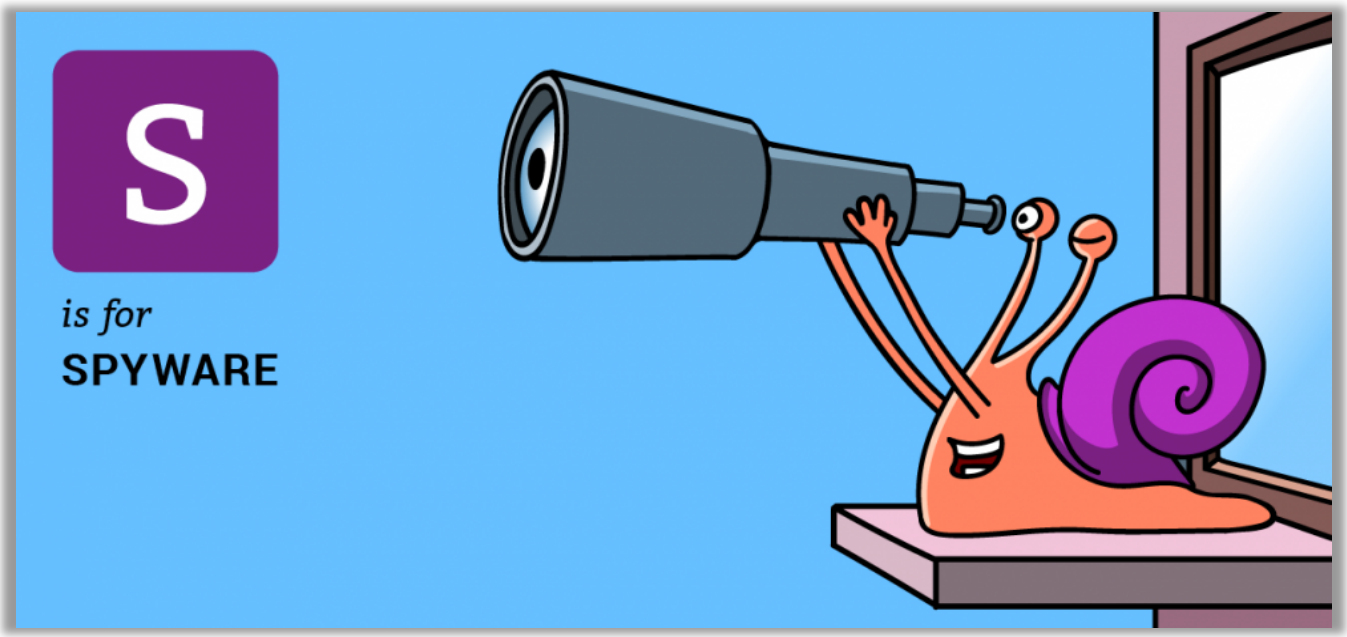
Esse tipo de malware, que parece ser uma coisa (vídeo), mas na realidade é outra (script de mineração), é categorizado como:

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[3] 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 = ESPIÃO

SPYWARE = SOFTWARE ESPIÃO

(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).

[3] 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...

ESCLARECENDO!

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 propria, 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[4] (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

[4] 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
FORMA DE OBTENÇÃO							
Recebido automaticamente pela rede		X	X				
Recebido por *e-mail*	X	X	X	X	X		
Baixado de *sites* 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
FORMA DE INSTALAÇÃO							
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
FORMA DE PROPAGAÇÃO							
Insere 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
AÇÕES MALICIOSAS MAIS COMUNS							
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 *spam* e *phishing*			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

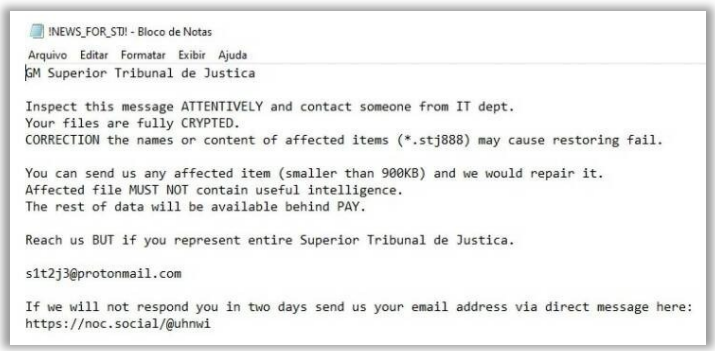
JUSTIÇA

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 *ramsomware*.

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!)...



!NEWS_FOR_ST! - Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

GM Superior Tribunal de Justica

Inspect this message ATTENTIVELY and contact someone from IT dept.
Your files are fully CRYPTED.
CORRECTION the names or content of affected items (*.stj888) may cause restoring fail.

You can send us any affected item (smaller than 900KB) and we would repair it.
Affected file MUST NOT contain useful intelligence.
The rest of data will be available behind PAY.

Reach us BUT if you represent entire Superior Tribunal de Justica.

s1t2j3@protonmail.com

If we will not respond you in two days send us your email address via direct message here:
https://noc.social/@uhnwi

Vejam o texto que os cybercriminosos enviaram com o pedido de resgate: *"Inspecionem 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

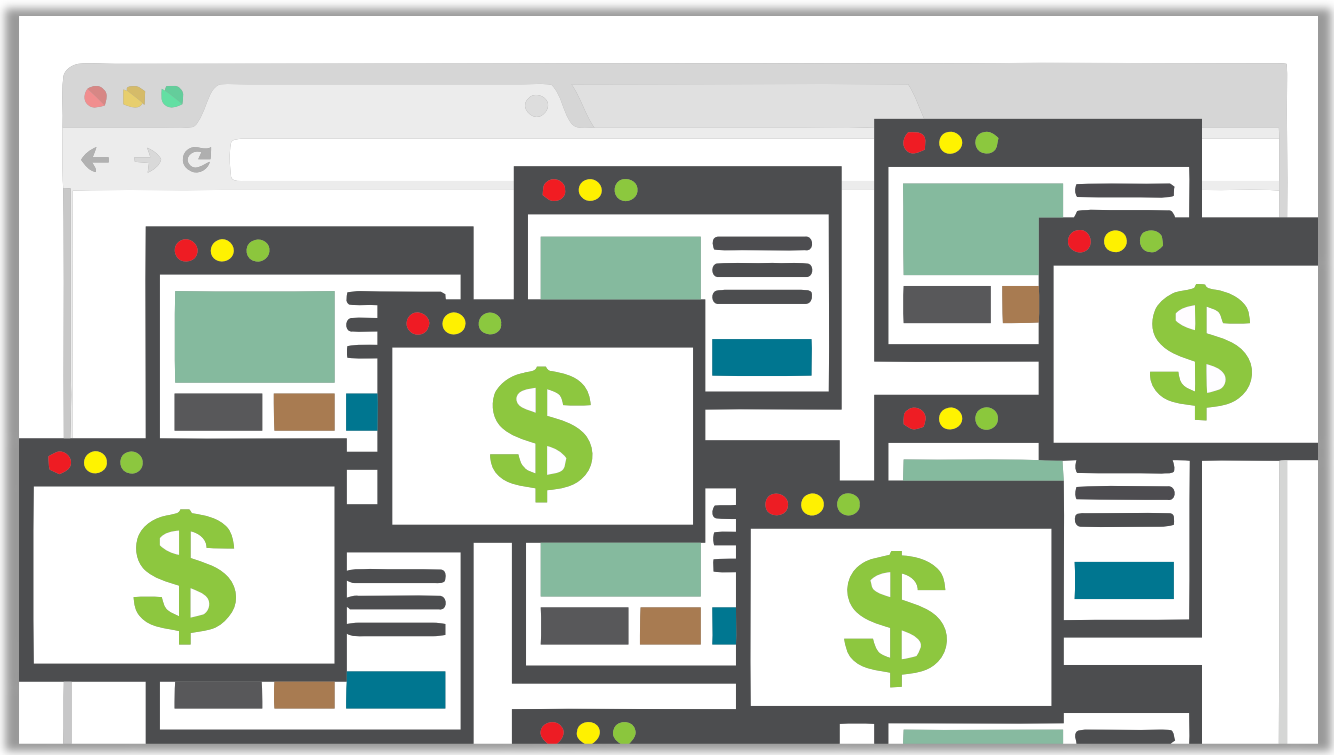
(TRT/AMAZONAS – 2017) Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Existem tipos específicos deste programa, como o que é capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse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

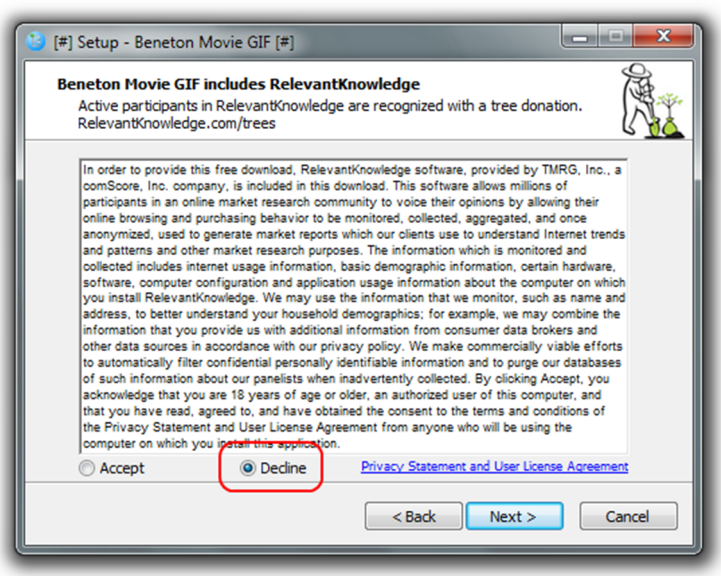
Comentários: o tipo de spyware que é programado para monitorar as atividades de um sistema e enviar para terceiros, armazenando a posição do cursor e a tela do monitor nos momentos de clique do mouse é o Screenlogger (Letra D).

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.

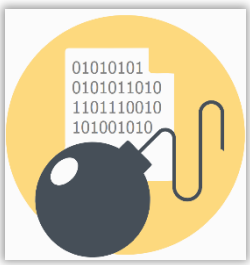
d) Põe em risco as informações que trefegam em rede, apesar de criptografar em HTTPS os pacotes desse ambiente.

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

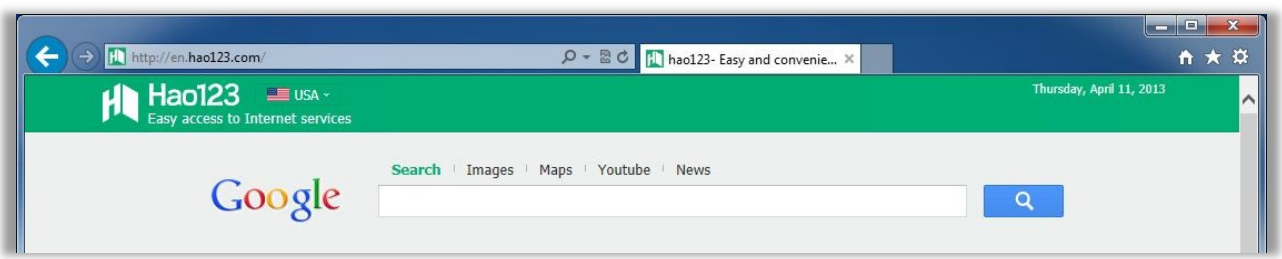
(UFAL – 2016) Exploit é um software malicioso projetado para explorar uma vulnerabilidade existente em um software de computador.

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:

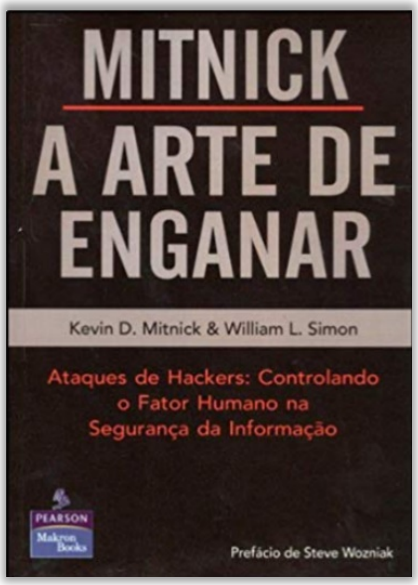
a) Hijacker.
b) Rootkit.
c) Worm.
d) Bootnet.
e) Keylogger.

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

Ataques e Golpes

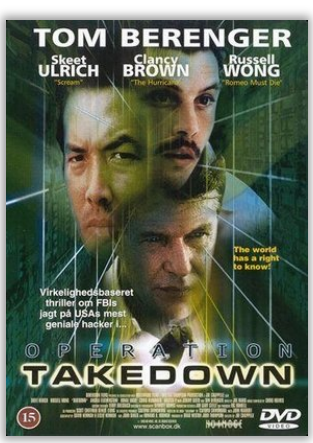
Engenharia Social

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.

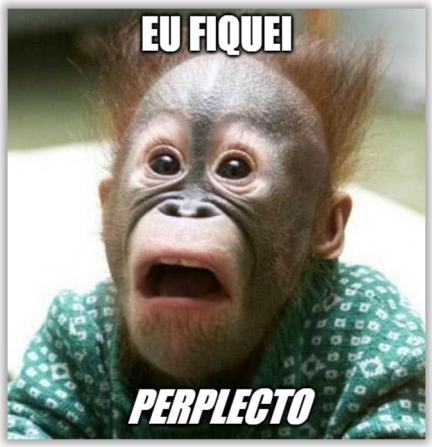


Essa história é contada no filme chamado Take Down (Caçada Virtual)! Eu – ávido por entender como esse hacker conseguiu fazer tudo isso – comprei o livro pensando que descobriria técnicas mirabolantes sobre como *hackear* computadores e sistemas. No entanto, em determinado momento do livro, Mitnick surpreende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


TECNOLOGIA

Telegram enfrenta 'poderoso ataque de negação de serviço'

Aplicativo de mensagens informou que usuários das Américas e de outros países tiveram problemas de conexão, mas dados estavam seguros.

Por G1

12/06/2019 08h33 · Atualizado há 6 meses


Telegram Messenger

@telegram

We're currently experiencing a powerful DDoS attack, Telegram users in the Americas and some users from other countries may experience connection issues.

3,764 8:20 AM - Jun 12, 2019

2,718 people are talking about this

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).

(SEGEP/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.

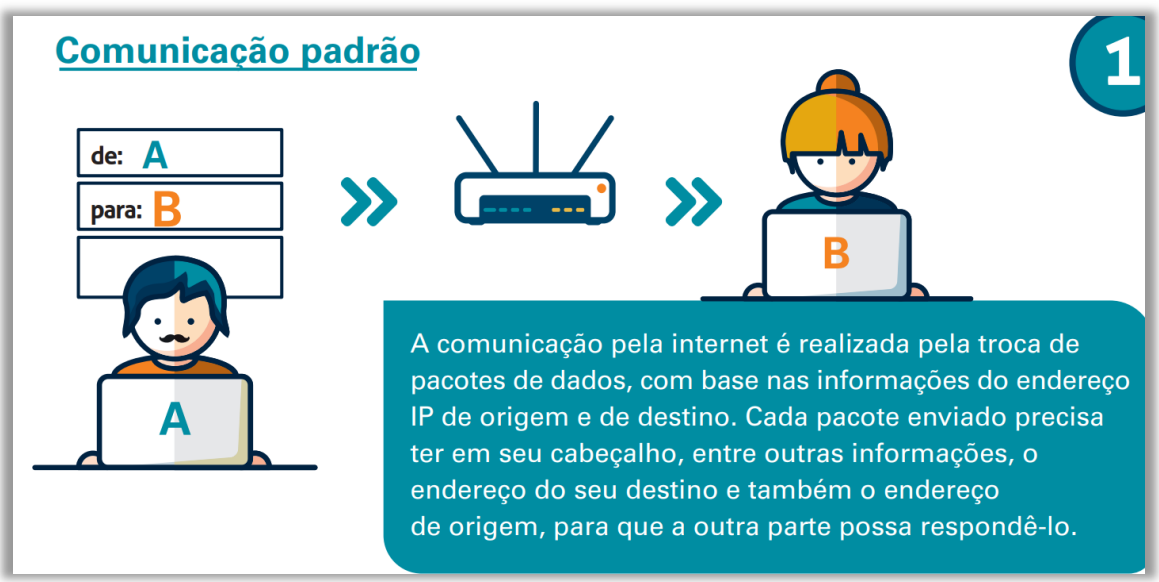
Comentários: bombardear um servidor alvo por meio de um ataque de zumbis de vários computadores, tirando-o do ar, é uma característica de um ataque distribuído de negação de serviço – DDoS (Letra B).

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:

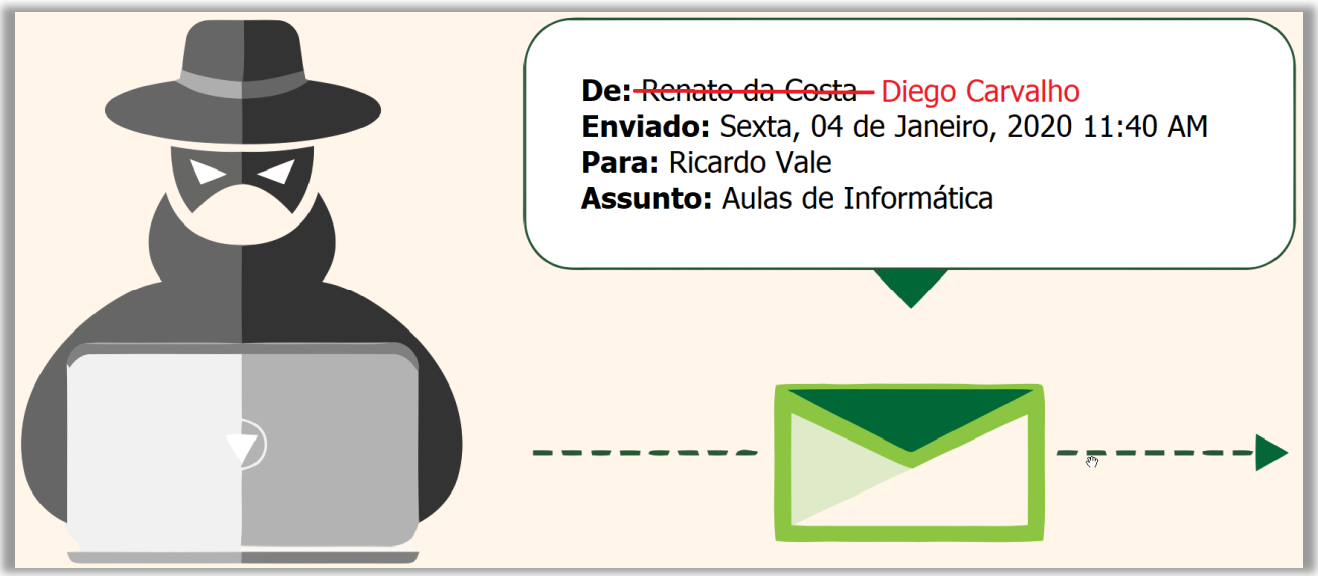
a) combolist.
b) bruteforce.
c) keylogger.
d) sniffer.
e) spoofing.

_____

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 fasificá-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. *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):

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 revisitar 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[1].

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, por exemplo. No entanto, você é redirecionado para uma página cujo endereço é www.bb.net.br e sequer percebe. Galera, existem tipos diferentes de redirecionamento. Vejamos...

TIPOS DE REDIRECIONAMENTO

[1] Há um tipo específico de Pharming chamado DNS Spoofing ou DNS Poisioning, 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:

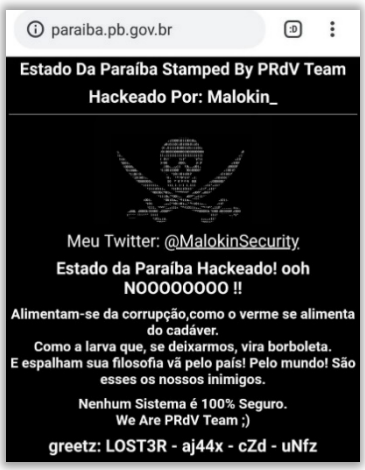
a) SYN Flooding.
b) Pharming.
c) Man-in-The-Middle.
d) DoS.
e) Spoofing.

_____

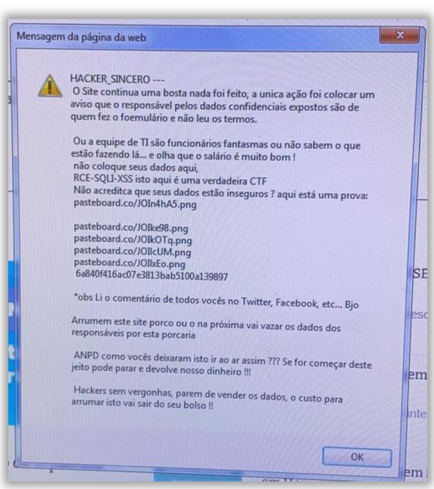
Comentários: o ataque que intercepta a comunicação se fazendo passar por outro usuário é o Man-in-the-Middle (Letra C).

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 furtar 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 você 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 compõe 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 (*Ransom*, 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 (*Script Kiddies*) 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.

RESUMO DE CÓDIGOS MALICIOSOS

	VÍRUS	WORM	BOT	TROJAN	SPYWARE	BACKDOOR	ROOTKIT
FORMA DE OBTENÇÃO							
Recebido automaticamente pela rede		X	X				
Recebido por *e-mail*	X	X	X	X	X		
Baixado de *sites* 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
FORMA DE INSTALAÇÃO							
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
FORMA DE PROPAGAÇÃO							
Insere 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
AÇÕES MALICIOSAS MAIS COMUNS							
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 *spam* e *phishing*			X				
Desfere ataques na Internet		X	X				
Procura se manter escondido	X				X	X	X

MAPA MENTAL

Vírus

Vírus de Script

- SCRIPT = UM CONJUNTO DE INSTRUÇÕES QUE DEVEM SER EXECUTADAS.
- ESCRITO EM LINGUAGEM DE SCRIPT (EX: VBSCRIPT E JAVASCRIPT).
- 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.
- PODE SER AUTOMATICAMENTE EXECUTADO, DEPENDENDO DA CONFIGURAÇÃO DO NAVEGADOR OU DO PROGRAMA LEITOR DE E-MAILS.

Vírus de Macro

- TIPO ESPECÍFICO DE VÍRUS DE SCRIPT.
- ESCRITO EM LINGUAGEM DE MACRO.
- INFECTA DOCUMENTOS QUE USAM ESSA LINGUAGEM (DO EXCEL, DO WORD, DO POWER POINT, ETC).
- QUANDO O SOFTWARE CARREGA UM ARQUIVO, EXECUTA O CÓDIGO MALICIOSO.
- SE PROPAGA FACILMENTE ATRAVÉS DO COMPARTILHAMENTO DE DOCUMENTOS INFECTADOS.

Vírus de Arquivo

- VÍRUS DE PROGRAMA OU VÍRUS PARASITÁRIO.
- É O MAIS TRADICIONAL.
- INFECTA ARQUIVOS EXECUTÁVEIS, SOBRESCREVENDO O CÓDIGO ORIGINAL.
- REPLICA-SE AO LOCALIZAR OUTROS ARQUIVOS EXECUTÁVEIS OU INFECTANDO ARQUIVOS QUE FORAM REQUISITADOS PARA A EXECUÇÃO DE UM PROGRAMA.

`.EXE` `.COM` `.VBS` `.OVL` `.DLL` `.CMD` `.PIF` `.SYS` `.SRC` `.BAT` `.ASP`

Vírus de Boot

- VÍRUS DE SETOR OU VÍRUS DE INICIALIZAÇÃO.
- BOOT = PROCEDIMENTO DE INICIALIZAÇÃO DO COMPUTADOR DURANTE O CARREGAMENTO DO SISTEMA OPERACIONAL.
- ESCONDE-SE NO PRIMEIRO SETOR DA MEMÓRIA.
- É ATIVADO QUANDO O COMPUTADOR É LIGADO E É CARREGADO ANTES MESMO DO SISTEMA OPERACIONAL.
- PODE AFETAR DISPOSITIVOS MÓVEIS DE ARMAZENAMENTO. (EX: PENDRIVES)
- A FORMATAÇÃO RÁPIDA DO PENDRIVE NÃO GARANTE A REMOÇÃO COMPLETA DO VÍRUS.

Vírus Stealth

- VÍRUS FURTIVO.
- PROJETADO PARA NÃO SER DETECTADO PELO ANTIVÍRUS.
- É CAPAZ DE SE REMOVER DA MEMÓRIA TEMPORARIAMENTE.

Vírus Timebomb

- VÍRUS BOMBA RELÓGIO.
- APÓS INFECTAR A MÁQUINA, FICA LATENTE (OCULTO), SE REPLICANDO.
- É PROGRAMADO PARA SER ATIVADO EM UM MOMENTO ESPECÍFICO.
- SE INSTALAM NOS COMPUTADORES PELA AÇÃO DO USUÁRIO.

Vírus Polimórfico

- VÍRUS MUTANTE.
- É CAPAZ DE ASSUMIR MÚLTIPLAS FORMAS A CADA INFECÇÃO COM O INTUITO DE BURLAR O ANTIVÍRUS.
- MUDA SUA ASSINATURA, MANTENDO SUAS FUNCIONALIDADES, MAS ALTERANDO O SEU PADRÃO DE BITS.
- ALTERAM A ROTINA DE ENCRIPTAÇÃO E A DE DECRIPTAÇÃO.
- GERA VARIAÇÕES DE SI MESMO UTILIZANDO-SE DE CHAVES DE ENCRIPTAÇÃO DIVERSAS.

Vírus Metamórfico

- É UMA VARIAÇÃO DO VÍRUS POLIMÓRFICO.
- SE REESCREVE COMPLETAMENTE A CADA INFECÇÃO.
- PODE MUDAR DE TAMANHO E DE COMPORTAMENTO.
- MUDA SUA ASSINATURA E SUA FUNCIONALIDADE.

Observações Gerais

- SE PROPAGA ANEXANDO-SE OU HOSPEDANDO-SE EM ARQUIVOS E PROGRAMAS;
- NÃO É AUTOEXECUTÁVEL;
- NÃO É AUTOSUFICIENTE;
- COMPOSTO DE 3 PARTES: MECANISMO DE INFECÇÃO, MECANISMO DE ATIVAÇÃO E CARGA ÚTIL.

@mapasdathai

@mapasdathai

Principais Malwares

Worm

VERME

- CAPAZ DE SE REPLICAR AUTOMATICAMENTE, ENVIANDO CÓPIAS DE SI MESMO.
- CONSOME MUITOS RECURSOS, AFETA O DESEMPENHO DA REDE E PODE LOTAR O DISCO RÍGIDO.
- WORMS 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 P/ 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).

Spywares

SOFTWARE ESPIÃO

- SOFTWARE ESPIÃO 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 P/ APRESENTAR PROPAGANDAS.

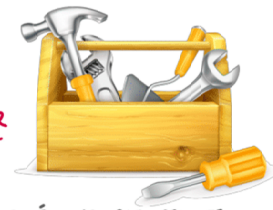
Backdoor

PORTA DOS FUNDOS

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

Rootkit

KIT DO ADMINISTRADOR



- 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 SOFISTICADOS QUE EXISTEM.
- NÃO É USADO P/ OBTER O ACESSO, MAS SIM P/ MANTÊ-LO.
- COMPROMETE O SISTEMA OPERACIONAL, ALTERANDO TUDO QUE ELE INFORMA, DE ACORDO COM O QUE QUER O INVASOR.

Bot

DIMINUTIVO DE ROBOT = ROBÔ

- PROGRAMA QUE DISPÕE 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.

Trojan

CAVALO DE TROIA

- PROGRAMA QUE, ALÉM DE EXECUTAR AS FUNÇÕES PARA AS QUAIS FOI APARENTEMENTE PROJETADO, TAMBÉM EXECUTA FUNÇÕES MALICIOSAS.
- PRECISA EXPLICITAMENTE SER EXECUTADO P/ 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.

Outros Malwares

Ransomware

- EXTORSÃO OU ESTELIONATO VIRTUAL.
- RANSOM = RESGATE.
- TORNA INACESSÍVEIS OS DADOS ARMAZENADOS EM EQUIPAMENTOS E EXIGE PAGAMENTO DE UM RESGATE PARA RESTABELECER O ACESSO AO USUÁRIO.

- RANSOMWARE LOCKER: IMPEDE O ACESSO AO EQUIPAMENTO.
- RANSOMWARE CRYPTO: IMPEDE O ACESSO AOS DADOS UTILIZANDO CRIPTOGRAFIA.

- PREVENÇÃO: FAZER BACKUPS REGULARMENTE.

Bombas lógicas

- SOFTWARE MALICIOSO PROGRAMADO PARA CAUSAR DANOS QUANDO SATISFEITA UMA DETERMINADA CONDIÇÃO (UMA DEPENDÊNCIA LÓGICA).

- EX: EXCLUIR ARQUIVOS SE DETERMINADO USUÁRIO FICAR + DE 30 DIAS SEM EFETUAR LOGIN.

- GERALMENTE SÃO INSTALADAS POR UM USUÁRIO AUTORIZADO, COMO UM ADMINISTRADOR DE REDE.

Sniffer

FAREJADOR

- ANALISADOR DE PACOTES DE DADOS CAPAZ DE MONITORAR, INTERCEPTAR E REGISTRAR TRÁFEGO DE DADOS EM SEGMENTOS DE REDE.

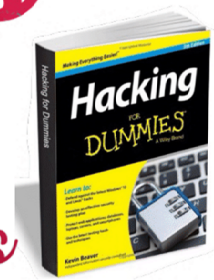
- USO LEGÍTIMO → POR ADMINISTRADORES DE REDES, PARA DETECTAR PROBLEMAS E MONITORAR A REDE.

- USO MALICIOSO → PARA CAPTURAR INFORMAÇÕES SENSÍVEIS QUE ESTEJAM TRAFEGANDO POR MEIO DE CONEXÕES SEM CRIPTOGRAFIA.
  - MODO PROMÍSCUO

Hijacker

- MODIFICA O REGISTRO DO SISTEMA OPERACIONAL, ALTERANDO O FUNCIONAMENTO DO NAVEGADOR.
- MODIFICA A PÁGINA INICIAL, ABRE PÁGINAS AUTOMATICAMENTE, INSERE BOTÕES, ETC.
- O DESENVOLVEDOR DO HIJACKER GERALMENTE GANHA DINHEIRO POR REDIRECIONAR O USUÁRIO PARA PÁGINAS PATROCINADAS.

EX: HAO123 😤



Exploits

- FERRAMENTA CRIADA POR HACKERS, QUE EXPLORAM VULNERABILIDADES DOS SISTEMAS PARA PERMITIR QUE ATACANTES SEM CONHECIMENTO AVANÇADO POSSAM FAZER INVASÕES.

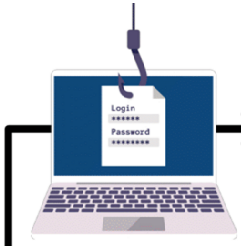
- PODEM EXPLORAR VULNERABILIDADES ZERO-DAY.
  - DESCONHECIDAS PELOS ADMINISTRADORES DE UM SISTEMA

@mapasdathai

Ataques e golpes

Engenharia social

- TÉCNICA POR MEIO DA QUAL UMA PESSOA PROCURA PERSUADIR OUTRA A EXECUTAR DETERMINADAS AÇÕES.
- É UTILIZADA PARA OBTER INFORMAÇÕES SENSÍVEIS DO USUÁRIO, ATRAVÉS DE SUA INGENUIDADE OU DE SUA CONFIANÇA.



Phishing Scan

- O ATACANTE UTILIZA UMA ARMADILHA VIRTUAL PARA OBTER INFORMAÇÕES SENSÍVEIS, COMO SENHAS DE BANCO.

ARMADILHAS COMUNS:

- PÁGINAS FALSAS DE COMÉRCIO ELETRÔNICO OU DE INTERNET BANKING;
- PÁGINAS FALSAS DE REDES SOCIAIS OU DE COMPANHIAS AÉREAS;
- E-MAILS COM FORMULÁRIOS COM CAMPOS P/ DADOS PESSOAIS E FINANCEIROS;
- E-MAILS QUE INDUZEM A CLICAR EM LINKS P/ CÓDIGOS MALICIOSOS;
- SOLICITAÇÃO DE RECADASTRAMENTO.

Força bruta

- ADVINHAR, POR TENTATIVA E ERRO, UM NOME DE USUÁRIO E SENHA.
- MESMO QUE O ATACANTE NÃO DESCUBRA A SENHA, A VÍTIMA PODE TER SUA CONTA BLOQUEADA POR CAUSA DAS VÁRIAS TENTATIVAS SEM SUCESSO.
- DEPENDENDO DE COMO É UTILIZADO, PODE RESULTAR EM UM ATAQUE DE NEGAÇÃO DE SERVIÇO (DoS).

→ FALSIFICAÇÃO / MASCARAMENTO DE IP

IP Spoofing

- TÉCNICA USADA QUANDO O MECANISMO DE AUTENTICAÇÃO DE UMA REDE É BASEADO EM ENDEREÇOS IP.
- O ATACANTE PODE CLONAR O IP DE UM USUÁRIO LEGÍTIMO, E CONSEGUE ACESSO NÃO AUTORIZADO FAZENDO-SE PASSAR POR ELE.
- EM RESUMO, O IP SPOOFING GERA PACOTES COM O ENDEREÇO IP FORJADO.

→ DENIAL OF SERVICE

DoS

- O ATACANTE BUSCA RETIRAR DE OPERAÇÃO UM SERVIÇO, UM COMPUTADOR OU UMA REDE CONECTADA À INTERNET, ESGOTANDO SEUS RECURSOS.
- DDoS - DISTRIBUTED DENIAL OF SERVICE (ATAQUE DISTRIBUÍDO DE NEGAÇÃO DE SERVIÇO): OCORRE QUANDO UM CONJUNTO DE EQUIPAMENTOS É USADO DE FORMA COORDENADA EM UM ATAQUE.

→ FALSIFICAÇÃO / MASCARAMENTO DE E-MAIL

E-mail Spoofing

- O ATACANTE ALTERA CAMPOS DO CABEÇALHO DE UM EMAIL, PARA APARENTAR QUE FOI ENVIADO DE DETERMINADA ORIGEM QUANDO, NA VERDADE, FOI ENVIADO DE OUTRA.
- É POSSÍVEL GRAÇAS A CARACTERÍSTICAS DO PROTOCOLO SMTP, QUE PERMITEM QUE CAMPOS DO CABEÇALHO SEJAM FALSIFICADOS.

Pharming

- TIPO DE PHISHING QUE ENVENENA A TABELA DE CACHE DO SERVIDOR DNS, REDIRECIONANDO O TRÁFEGO PARA SITES FRAUDULENTOS.
- EXEMPLO: VOCÊ DIGITA WWW.BB.COM.BR NA BARRA DE ENDEREÇOS, MAS É REDIRECIONADO PARA O SITE WWW.BB.NET.BR DE FORMA TRANSPARENTE (SEM PERCEBER). NA PÁGINA FALSA O GOLPISTA PODE CAPTURAR SEUS DADOS BANCÁRIOS.

→ BOATO

Hoax

- MENSAGEM QUE POSSUI CONTEÚDO ALARMANTE OU FALSO.
- PODE CONTER CÓDIGOS MALICIOSOS QUE SÃO PROPAGADOS COMO "CORRENTES".
- ESPALHAM DESINFORMAÇÃO NA INTERNET.
- AUMENTAM EXCESSIVAMENTE A CARGA DE SERVIDORES DE E-MAIL E O CONSUMO DA BANDA DE REDE.
- COMPROMETEM A REPUTAÇÃO DE PESSOAS / ENTIDADES REFERENCIADAS NA MENSAGEM.

QUESTÕES COMENTADAS – CESPE

1. **(CESPE / IBAMA – 2022)** O vírus do tipo *ransomware* é um código malicioso que executa tarefas indesejadas no computador, sem o conhecimento do usuário.

Comentários:

Ransomware não é um vírus! Sua função é criptografar dados e pedir um resgate financeiro por eles.

Gabarito: Errado

---

2. **(CESPE / TELEBRAS – 2022)** Em uma rede, a instalação de um firewall e a atualização frequente desse firewall garantem a total proteção da rede contra invasores e dos programas instalados nas estações de trabalho contra vírus e worms.

Comentários:

Em primeiro lugar, firewalls nada podem fazer contra vírus e worms; em segundo lugar, mesmo mecanismos de proteção e segurança atualizados não garantem proteção total em uma rede.

Gabarito: Errado

---

3. **(CESPE / TELEBRAS – 2022)** Um *worm* tem como características a infecção de estações de trabalho, ao invés de arquivos, e a dispersão pela rede, utilizando múltiplas técnicas de replicação.

Comentários:

Perfeito! Não confundam com os vírus, que infectam arquivos em vez de estações de trabalho.

Gabarito: Correto

---

4. **(CESPE / PC-PB – 2022)** Ataque malicioso ao ambiente computacional, realizado por programa ou fragmentos de código não replicável, aparentemente seguro, que, de forma oculta, realiza ações como roubo de senhas e arquivos, é:

a) *spyware*.
b) *ransomware*.
c) cavalo de troia.
d) vírus.
e) *worms*.

Comentários:

Aparentemente seguro, mas que realiza de forma oculta ações maliciosas é função de um Cavalo de Troia (Trojan Horse).

Gabarito: Letra C

---

5. **(CESPE / TCE-RJ – 2022)** Os trojans possuem características totalmente distintas em relação aos vírus; a principal delas é que os trojans não permitem ser controlados à distância pela pessoa que os instalou, diferentemente dos vírus.

Comentários:

Trojan é um dos malwares mais versáteis que existe, sendo um deles o Trojan Backdoor, que possibilita o acesso remoto do atacante a um equipamento.

Gabarito: Errado

---

6. **(CESPE / TCE-RJ – 2022)** Quando instalado e ao ser executado pelo operador do sistema, o rootkit substitui arquivos executáveis importantes do sistema operacional.

Comentários:

Perfeito! Assim que um ataque de rootkit acontece, ele concede acesso de administrador ao sistema operacional enquanto evita ser detectado, permitindo que o atacante substitua arquivos executáveis importantes do sistema operacional.

Gabarito: Correto

---

7. **(CESPE / PGE-RJ – 2022)** O botnet é um vírus projetado especificamente para mostrar, no computador do usuário, propagandas oriundas das redes sociais.

Comentários:

Botnet não é um vírus – trata-se de uma rede de bots (computadores zumbis). A questão se parece mais com adwares.

Gabarito: Errado

---

8. **(CESPE / SERES-PE – 2022)** A praga virtual que bloqueia o computador, impedindo o acesso a seus arquivos, com o objetivo de exigir-se pagamento para liberação é conhecida como:

a) *bot*.
b) *trojan*.

c) *ransomware*.
d) vírus.
e) *worm*.

Comentários:

Bloqueia o computador? Impede acesso a arquivos? Exige pagamento para liberação? Todas essas características nos remetem ao ransomware, que é um malware que faz o sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos.

Gabarito: Letra C

---

9. **(CESPE / SECONT-ES – 2022)** Pharming é o ataque em que são alteradas as informações de endereço armazenadas pelos provedores de serviço de Internet para agilizar a navegação web, com o objetivo de redirecionar o usuário para uma página web falsa.

Comentários:

Perfeito! Pharming é um tipo de crime virtual muito parecido com o phishing, em que o tráfego de um site é manipulado e informações confidenciais são roubadas. O pharming explora a base de funcionamento da navegação na Internet, ou seja, a conversão da sequência de letras que forma um endereço da Internet, como www.google.com, em um endereço IP por um servidor DNS para que ocorra a conexão.

Gabarito: Correto

---

10. **(CESPE / Prefeitura de São Cristóvão-SE – 2022)** Um software malicioso tem a capacidade de infectar o computador e executar nele ações que prejudiquem seu funcionamento, como apagar arquivos pessoais ou instalar outros tipos de vírus.

Comentários:

Perfeito! Softwares maliciosos (malwares) podem executar diversas atividades maliciosas diferentes, sendo uma das mais comuns a execução de ações que prejudiquem o funcionamento de computadores, como deletar arquivos pessoais ou instalar outros tipos de vírus.

Gabarito: Correto

---

11. **(CESPE / MC – 2022)** Diferentemente dos vírus, os worms consomem poucos recursos computacionais e de rede e se propagam por meio da infecção silenciosa de programas ou arquivos, o que dificulta a sua detecção e eliminação.

Comentários:

Opa... worms consomem muitos recursos computacionais e de rede!

Gabarito: Errado

---

12. (CESPE / MC – 2022) Rootkit é um programa malicioso conhecido por apresentar propagandas.

Comentários:

Rootkit é um pacote de software maligno projetado para oferecer acesso não autorizado a um computador ou outro software – a questão trata de Adware.

Gabarito: Errado

---

13. (CESPE / APEX Brasil – 2022) *Malware* é qualquer software intencionalmente criado para causar danos a um computador, servidor, cliente ou a uma rede de computadores.

Comentários:

Perfeito! Malware é um termo amplo que é usado para classificar todo tipo de software malicioso usado para causar prejuízo, que pode ser até financeiro, danificar sistemas, interceptar dados ou simplesmente irritar o usuário, afetando tanto computadores como servidores, clientes, celulares e até redes inteiras.

Gabarito: Correto

---

14. (CESPE / DPDF - 2022) Para detectar um ataque malicioso a um computador e fornecer evidências desse ataque, é correto utilizar um registro de logs externo a esse computador.

Comentários:

A partir de logs, conseguimos saber tudo o que acontece em um computador. Dessa forma, é possível detectar ataques maliciosos por meio deles – como tentativas de acesso indevido.

Gabarito: Correto

---

15. (CESPE / DPE-RO – 2021) Uma significativa parte da prevenção contra determinado ataque cibernético pode ser realizada por meio da minimização dos privilégios de acesso das aplicações, bem como pela sanitização de códigos relacionados aos acessos a bancos de dados. Trata-se de prevenção contra-ataques:

a) de vírus.
b) DDoS.

c) de SQL injection.
d) do tipo phishing.
e) do tipo ransomware.

Comentários:

O único ataque que está relacionado a acessos a bancos de dados é o SQL Injection. Esse ataque injeta comandos SQL em campos de entrada de dados em determinados sites ou páginas, podendo ter acessos a dados sensíveis.

Gabarito: Letra C

---

16. (CESPE / ALE-CE - 2021) Ao acessar um anexo de email, um usuário teve seus arquivos criptografados e tornados inacessíveis para ele, por meio de uma taque a seu computador. Para torná-los acessíveis, foi exigido pagamento de resgate em bitcoins. Esse de tipo de ataque utiliza um código malicioso conhecido como

a) ransomware.
b) email spoofing.
c) virus.
d) força bruta.
e) trojan ou cavalo de troia.

Comentários:

(a) Correto, trata-se de um ataque de Ransomware; (b) Errado, o email spoofing é uma técnica que consiste em alterar campos do cabeçalho de um e-mail; (c) Errado, vírus é um programa ou parte de um programa; (d) Errado, um ataque de força bruta consiste em adivinhar, por tentativa e erro, um nome de usuário e senha; (e) Errado, o trojan 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.

Gabarito: Letra A

Paulo, servidor de determinado órgão público, recebeu a seguinte mensagem em seu email corporativo.

> ***Assunto:*** *Seu dispositivo está infectado e hackeado.*
>
> *Oi! Eu tenho más notícias para você, há alguns meses tive acesso aos dispositivos que você usa para navegar na web. Instalei um cavalo de troia nos sistemas operacionais de todos os dispositivos que você usa para acessar seu e-mail (celular, computador e tablete).*

Eu bloqueei o cesso aos seus sistemas por meio de criptografia de todas as suas informações, tais como impostos de renda, fotos e arquivos de trabalho, o arquivo curriculum.docx no diretório Meus documentos. Para comprovar, veja a última dará de atualização desse arquivo – está dando agosto deste ano.

Posso publicar todos os seus dados pessoais na nuvem, incluindo os dados financeiros e, ainda, deixar seus arquivos indisponíveis para sempre.

Acho que você não vai querer que isso aconteça, pois será um verdadeiro desastre em sua vida. Vamos resolver assim: você me transfere $ 1.000.00 (em bitcoin equivalente à taxa de câmbio no momento da transferência) e, assim que a transferência for recebida, eu removerei imediatamente o vírus da sua máquina e devolverei seu acesso.

Minha carteira bitcoin para pagamento é 123456789abcdef. Se eu descobrir que você compartilhou esta mensagem com outra pessoa ou avisou à polícia, destruirei seus arquivos e sua privacidade financeira para sempre e todos os seus dados se tornarão públicos.

Considerando essa situação hipotética e assuntos a ela relacionados, julgue os itens a seguir.

17. (CESPE / PC-SE – 2021) Admitindo-se que a infecção por cavalo de Troia realmente tenha ocorrido, é correto afirmar que tal infecção pode ter acontecido por meio de um spear phishing, o que teria sido evitado se na máquina do usuário tivesse um antispyware instalado.

Comentários:

O Spear Phishing é um tipo de phishing que, embora tenha a intenção de roubar dados para fins mal-intencionados, os criminosos virtuais também podem tentar instalar malware no computador do usuário. Logo, a infecção por Cavalo de Troia realmente pode ter ocorrido por conta do Spear Phishing. No entanto, um antispyware não poderia evitar essa infecção e, sim, um antimalware.

Gabarito: Errado

Paulo, servidor de determinado órgão público, recebeu a seguinte mensagem em seu email corporativo.

Assunto: *Seu dispositivo está infectado e hackeado.*

Oi! Eu tenho más notícias para você, há alguns meses tive acesso aos dispositivos que você usa para navegar na web. Instalei um cavalo de troia nos sistemas operacionais de todos os dispositivos que você usa para acessar seu e-mail (celular, computador e tablete).

Eu bloqueei o cesso aos seus sistemas por meio de criptografia de todas as suas informações, tais como impostos de renda, fotos e arquivos de trabalho, o arquivo curriculum.docx no diretório

Meus documentos. Para comprovar, veja a última dará de atualização desse arquivo – está dando agosto deste ano.

Posso publicar todos os seus dados pessoais na nuvem, incluindo os dados financeiros e, ainda, deixar seus arquivos indisponíveis para sempre.

Acho que você não vai querer que isso aconteça, pois será um verdadeiro desastre em sua vida. Vamos resolver assim: você me transfere $ 1.000.00 (em bitcoin equivalente à taxa de câmbio no momento da transferência) e, assim que a transferência for recebida, eu removerei imediatamente o vírus da sua máquina e devolverei seu acesso.

Minha carteira bitcoin para pagamento é 123456789abcdef. Se eu descobrir que você compartilhou esta mensagem com outra pessoa ou avisou à polícia, destruirei seus arquivos e sua privacidade financeira para sempre e todos os seus dados se tornarão públicos.

Considerando essa situação hipotética e assuntos a ela relacionados, julgue os itens a seguir.

18.(CESPE / PC-SE – 2021) Infere-se do email apresentado, especialmente do trecho ''Eu bloqueei o acesso aos seus sistemas por meio de criptografia de todas as suas informações, tais como imposto de renda, fotos e arquivos de trabalho'', que se trata de um ataque por trojan, o qual é um programa que, além de executar as funções para as quais foi aparentemente projetado, torna inacessíveis os dados armazenados, som o conhecimento do usuário.

Comentários:

Bloqueio de acesso via criptografia é uma característica típica do ransomware e, não, de um trojan. Além disso, cavalo de troia não torna inacessíveis dados armazenados.

Gabarito: Errado

19.(CESPE / PC-AL – 2021) A grande diferença entre vírus e 7orms está na forma como eles se propagam: o vírus, ao contrário do worm, não se propaga por meio da inclusão de cópias de si mesmo em outros programas, mas pela execução direta de uma de suas cópias.

Comentários:

Opa... é exatamente o inverso: o worm, ao contrário do vírus, não se propaga por meio da inclusão de cópias de si mesmo em outros programas, mas pela execução direta de uma de suas cópias.

Gabarito: Errado

20.(CESPE / PM-AL – 2021) O registro das atividades, em um computador, normalmente gerado por programas ou serviços e armazenado em arquivos é conhecido como scan de vulnerabilidades.

Comentários:

Na verdade, o scan (varredura) de vulnerabilidades e uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas, é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

O que a questão descreve é o registro de eventos – também chamado de log. Trata-se do registro de atividade gerado por programas e serviços de um computador. Ele pode ficar armazenado em arquivos, na memória do computador ou em bases de dados.

Gabarito: Errado

---

21. **(CESPE / PM-AL – 2021)** Códigos maliciosos capazes de capturar tudo o que for digitado no teclado do usuário são conhecidos como rootkits.

Comentários:

A questão trata de um keylogger – esse é um tipo de spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Não há nenhuma relação com rootkit!

Gabarito: Errado

---

22. **(CESPE / PM-AL – 2021)** Uma infecção por trojan pode ser recebida automaticamente pela rede, sem que nenhum usuário tenha efetuado o envio.

Comentários:

Trojan não se propaga, logo não pode ser recebido automaticamente pela rede. A banca, por vezes, considera trojan como um tipo de vírus, mas como ela não especificou isso na questão, vamos considerar a definição tradicional de trojan.

Gabarito: Errado

---

23. **(CESPE / PM-AL – 2021)** Um worm é um programa capaz de se propagar enviando cópias de si mesmo para outros computadores em uma rede.

Comentários:

Perfeito! Essa é a definição clássica de worm: programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento.

Gabarito: Correto

---

24. (CESPE / DEPEN – 2021) Os vírus do tipo cavalo de troia, também conhecidos como trojans, podem ser instalados por outros vírus e programas, mas também podem infectar o ambiente por meio de links durante a navegação na Internet ou até mesmo por meio de emails falsos (phishing).

Comentários:

Já é uma jurisprudência da banca considerar o cavalo de troia como um tipo de vírus. Nesse contexto, ele realmente pode ser instalado por outros vírus e programas – assim como por meio de links durante a navegação ou e-mails falsos.

Gabarito: Correto

---

25. (CESPE / PM-AL – 2021) O Dropper é um trojan que executa em um site a ação maliciosa de redirecionar o usuário para sites específicos, com a finalidade de aumentar a quantidade de acessos à página.

Comentários:

Quem se lembra da tabelinha de trojans? Pois é, a questão menciona o Trojan Dropper, que instala outros códigos maliciosos, embutidos no próprio código do trojan. Na verdade, a descrição da questão trata do Trojan Clicker, que redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.

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: Errado

---

26. (CESPE / PCDF – 2021) Para que as pragas virtuais denominadas worms ataquem o computador em uso, é necessário que se execute um arquivo do tipo .bat.

Comentários:

Nada melhor do que a justificativa da própria banca: *"Os worms não necessitam infectar outros arquivos para se multiplicar e normalmente se espalham usando recursos da rede. Ele não necessita que o usuário o acione, pois, por ser um programa completo, é autônomo".*

Worms se propagam automaticamente pelas redes explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento. Logo, eles não infectam arquivos e não necessita da execução de nenhum arquivo hospedeiro.

Gabarito: Errado

---

27. (CESPE / PM-TO – 2021) A solução mais efetiva a ser tomada em caso de um usuário que tenha sofrido ataque de Ransomware em seus arquivos é:

a) utilizar um antispyware capaz de bloquear o keylogger e assim monitorar os arquivos afetados e, desse modo, evitar que as informações coletadas desses arquivos sejam enviadas para terceiros.

b) realizar periodicamente backups testados, pois a garantia de que ele conseguirá acessá-los novamente é possuir backups atualizados, uma vez que nesse tipo de ataque o acesso aos arquivos é bloqueado sem a garantia de que o pagamento de um valor será a solução.

c) executar um antivírus nos arquivos infectados com método de detecção por meio de heurística, de modo a eliminar o malware presente nos arquivos.

d) instalar e executar o sistema de firewall, de modo a impedir que o atacante tente explorar o conteúdo dos arquivos afetados e, assim, evitar o acesso não autorizado caso haja algum backdoor neles instalados.

e) executar software que realize a criptografia nos arquivos, de forma a proteger os dados presentes nos arquivos e garantir que seu conteúdo não seja enviado para terceiros.

Comentários:

A solução mais efetiva contra *ransomwares* é realizar periodicamente backups testados, pois a garantia de que ele conseguirá acessá-los novamente é possuir backups atualizados, uma vez que nesse tipo de ataque o acesso aos arquivos é bloqueado sem a garantia de que o pagamento de um valor será a solução. Inclusive, após o ataque de *ransomware* ao Superior Tribunal de Justiça (STJ), vários órgãos ficaram mais alertas com a qualidade e periodicidade dos seus procedimentos de backup.

Gabarito: Letra B

---

28. (CESPE / TCE-RJ – 2021) Os ataques de phishing caracterizam-se pelo envio de mensagens eletrônicas que despertam a atenção de usuários por meio da sugestão de vantagens ou ameaças de prejuízos e também por induzirem os usuários a fornecer dados pessoais e(ou) financeiros.

Comentários:

Perfeito! O ataque de Phishing funciona como uma isca para que usuários fornecendo possíveis vantagens ou eventuais prejuízo, induzindo o usuário a fornecer dados pessoais ou financeiros.

Gabarito: Correto

---

29. (CESPE / Polícia Federal – 2021) Denomina-se *backdoor* a situação em que o usuário sofre um ataque, seus dados são criptografados, ficam inacessíveis e, então, exige-se desse usuário o pagamento de resgato para restabelecimento do acesso a seus dados.

Comentários:

A questão trata do ransomware e, não, de um backdoor! Além disso, ele é um software malicioso e, não, uma situação.

Gabarito: Errado

---

30. (CESPE / PRF – 2021) Ransomware é um programa malicioso de computador que se propaga por meio da inserção de cópias de si mesmo em arquivos criptografados.

Comentários:

Propagação por meio da inserção de cópias de si mesmo em arquivos é uma característica de vírus e, não, de ransomwares – esses se propagam principalmente por meio de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link; ou por meio da exploração de vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança. Além disso, eles não se inserem em arquivos (previamente) criptografados – eles criptografam arquivos de dados.

Gabarito: Errado

---

31. **CESPE / PC-SE – 2020)** Ao redigir um ofício destinado a uma provedora de Internet, um delegado colocou as seguintes informações a respeito de uma possível captura de dados não autorizada pelo usuário de um sistema.

URL correta de acesso ao sistema	https://suaconta.com.br/suaconta.html
URL apresentada ao acessar o sistema	https://crazyserver.com.uk/suaconta.html
Porta	191.125.13.1

O usuário digitava a URL correta de acesso ao sistema no browser, e a página da Web apresentada solicitava o preenchimento dos dados e a inserção de senha do usuário para acesso ao sistema. A respeito da situação hipotética apresentada e dos aspectos técnicos e legais a ela relacionados, julgue o item a seguir.

Nesse caso, utilizava-se a estratégia de phishing para obter dados dos usuários.

Comentários:

Vejam que contexto interessante: o usuário inseria a URL correta na barra de endereço de seu navegador e pressionar ENTER. No entanto, ele era direcionado não para a página correta e, sim, para uma segunda página com um endereço diferente que requisitava o preenchimento de dados do usuário, assim como senha de acesso. Vamos fazer uma pequena revisão agora: *vocês se lembram do DNS (Domain Name System)?*

Trata-se de um sistema e um protocolo que permite converter endereço lógico (chamado IP) em endereço léxico (nome de domínio) e vice-versa. Em outras palavras, como é difícil memorizar endereços lógicos, nós memorizamos apenas seu endereço léxico. *E quem faz a conversão de um para o outro?* DNS! Agora observem que o usuário escreveu um endereço léxico correto, mas foi direcionado para um segundo endereço léxico diferente. *O que pode ter acontecido?*

Pode ter ocorrido um ataque de *pharming*, que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS. Neste caso, quando você tenta acessar um site legítimo, o seu navegador web é redirecionado, de forma transparente, para uma página falsa. Agora vem a pegadinha da questão: *pharming* é um tipo específico de *phishing* e, por essa razão, a questão está correta – eu acho uma pegadinha um pouco injusta com o aluno!

Gabarito: Correto

---

32. (CESPE / TJ-PA – 2020) Texto 4A3-I: Em um espaço público ABC, um hacker instalou um ponto de acesso gratuito à Internet, do tipo wi-fi sem senha, e deu à rede o identificador ABCfree. O hacker configurou essa rede de modo que usuários que a ela se conectassem e tentassem acessar sítios de mídias sociais fossem direcionados para páginas clonadas, nas quais as credenciais de acesso dos usuários eram solicitadas. De posse dessas credenciais, um programa criado pelo hacker estabelecia conexões reais com as mídias sociais e interceptava transparentemente todas as comunicações dos usuários nas plataformas, acessando indevidamente todo o seu conteúdo.

A técnica de interceptação e acesso indevido às comunicações privadas de terceiros descrita no texto 4A3-I constitui um ataque cibernético do tipo:

a) man-in-the-middle.
b) SIM cloning.
c) IP spoofing.
d) ping of death.
e) DoS (denial of service).

Comentários:

O hacker configurou essa rede de modo que usuários que a ela se conectassem fossem direcionados para páginas clonadas, nas quais as credenciais de acesso dos usuários eram solicitadas. De posse dessas credenciais, ele estabelecia conexões reais. *O que isso significa?* Significa que o hacker interceptava conexões de usuários, direcionava para uma página clonada para roubar seus dados e acesso e depois ele mesmo acessava os dados.

É por essa razão que nós dizemos insistentemente para tomar muito cuidado com conexões wi-fi públicas, especialmente se ela não pedir nenhuma senha. Trata-se de um típico ataque de Man in the Middle (Homem no Meio), em que um atacante se posiciona entre um usuário e um aplicativo para espionar ou se passar por uma das partes, fazendo com que pareça uma troca normal de informações.

(b) SIM Cloining é um ataque para clonagem de Cartão SIM; (c) IP Spoofing é a falsificação de endereços IP; (d) Ping of Death é um tipo de ataque de negação de serviço; (e) DoS é um ataque de negação de serviço – nenhum deles tem relação com interceptação de dados em redes por terceiros.

Gabarito: Letra A

---

33. (CESPE / TJ-PA – 2020) Assinale a opção que indica o tipo de ataque mais comumente utilizado como precursor para viabilizar ataques de ransomware contra estações de trabalho de usuários:

a) DDoS (distributed denial of service)
b) procedimento de defacement
c) ataque de phishing
d) keylogger
e) vírus

Comentários:

(a) Errado, esse é um ataque de negação de serviço distribuído – não permite viabilizar nenhum ransomware; (b) Errado, defacement é um ataque de desfiguração de uma página web – não permite viabilizar nenhum ransomware; (c) Correto. Por meio de um ataque de phishing, um usuário pode acabar clicando em um link que leva a instalação de um software malicioso, como o ransomware; (d) Errado, keyllogger é um spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador e enviá-las a um invasor – não permite viabilizar nenhum ransomware; (e) Errado, vírus é um 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 – não permite viabilizar nenhum ransomware.

Gabarito: Letra C

---

34. (CESPE / TJ-PA – 2020) Um vírus do tipo polimórfico é um vírus que se:

a) conecta a arquivos executáveis e se replica quando o programa infectado é executado.
b) aloja na memória principal como parte de um programa residente no sistema.
c) transforma a cada infecção, o que impossibilita a detecção pela assinatura do vírus.
d) espalha quando o sistema é inicializado, por infectar um registro-mestre de inicialização.
e) reescreve a cada interação, podendo mudar seu comportamento e aparência, o que aumenta a dificuldade de detecção.

Comentários:

(a) Errado, isso seria um vírus de programa/arquivo; (b) Errado, isso seria válido para qualquer tipo de vírus; (c) Correto, vírus polimórfico são capazes de criar uma nova variante a cada execução, mudando a sua assinatura para dificultar a detecção pelo antivírus; (d) Errado, isso seria um vírus de boot; (e) Errado, se ele muda seu comportamento, trata-se de um vírus metamórfico. Lembrando que vírus polimórfico muda apenas a sua assinatura, mantendo sua funcionalidade, e o vírus metamórfico muda sua assinatura e sua funcionalidade.

Gabarito: Letra C

---

35. **(CESPE / CGE - CE – 2019)** Após o envio de um e-mail pelo emissor a determinado destinatário, ocorreu uma ação maliciosa e o e-mail foi lido por terceiro. Nessa situação, a ação maliciosa é do tipo:

a) sniffing
b) spoofing
c) brute force
d) defacement
e) denial of service.

Comentários:

Se o e-mail foi lido por terceiro, houve alguma interceptação. O Sniffing é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers. Eles podem ser maliciosos, capturando informações sensíveis. (b) Spoofing é uma técnica de mascaramento de E-Mail, IP ou MAC; (c) Força Bruta é uma técnica de tentativa e erro; (d) Defacement é uma técnica de desfiguração de uma página web; (e) Denial of Service é uma técnica de negação de serviços.

Gabarito: Letra A

---

36. **(CESPE / TCE-PB – 2018)** Entre os vários tipos de programas utilizados para realizar ataques a computadores, aquele capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo entre computadores, é conhecido como:

a) Botnet.
b) Spyware.
c) Backdoor.
d) Trojan.
e) Worm.

Comentários:

(a) Errado, eles não se propagam; (b) Errado, eles não se propagam; (c) Errado, eles não se propagam; (d) Errado, eles não se propagam; (e) Correto, eles realmente se propagam automaticamente pelas redes, enviando cópias de si mesmo entre computadores.

Gabarito: Letra E

---

37. **(CESPE / PM-MA – 2018)** Fazer becape regularmente é uma conduta que permite minimizar os danos decorrentes de um ataque do tipo ransomware locker, que impede o acesso ao equipamento infectado, visto que o pagamento do resgate não garante acesso aos dados.

Comentários:

Perfeito! Fazer becapes com regularidade é recomendável nos casos de um ataque por um ransomware locker, uma vez que esse malware impede o usuário de acessar o equipamento infectado. O becape é essencial para proteger seus dados visto que – se o equipamento for infectado – a única garantia de acessar os dados é ter um becape atualizado.

Gabarito: Correto

---

38. (CESPE / PM-MA – 2018) A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

A situação III caracteriza-se mais como vírus do que como um worm, pois os vírus são responsáveis por consumir muitos recursos, ao passo que os worms permitem o retorno de um invasor ao computador comprometido.

Comentários:

Na verdade, worms são responsáveis por consumir muitos recursos e backdoors permitem o retorno de um invasor ao computador comprometido.

Gabarito: Errado

---

39. (CESPE / PM-MA – 2018) A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

O ataque descrito na situação I é o ransomware, que, geralmente usando criptografia, torna inacessíveis os dados armazenados em um equipamento.

Comentários:

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. Logo, parece ser o caso da situação I.

Gabarito: Correto

40.(CESPE / PM-MA – 2018) A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

A situação II pode ter ocorrido por meio de bot, um programa que dispõe de determinados mecanismos de comunicação com o invasor, os quais permitem que o computador invadido seja controlado remotamente, propagando a infecção de forma automática e explorando vulnerabilidades existentes em programas instalados.

Comentários:

Bots são softwares maliciosos que dispõem de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Logo, é realmente possível que sejam bots!

Gabarito: Correto

---

41. (CESPE / PM-MA – 2018) A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

As três situações apresentadas poderiam ter sido evitadas se um antiadware atualizado e funcional estivesse instalado nos computadores em questão, uma vez que esse é um tipo de programa capaz de evitar infecções e ataques.

Comentários:

Na verdade, o Antiadware não é utilizado no combate a nenhum dos problemas gerados nas situações descritas, visto que ele é responsável por combater adwares – o que não é o caso de nenhuma das três situações.

Gabarito: Errado

---

42. (CESPE / PC-MA – 2018) Determinado tipo de vírus eletrônico é ativado quando um documento por ele infectado é aberto, podendo então, nesse momento, infectar não apenas outros documentos, mas também um gabarito padrão de documento, de modo que cada novo documento criado sob esse gabarito seja infectado. Tal vírus, cuja propagação ocorre quando documentos por ele infectados são remetidos por correio eletrônico para outros usuários, é conhecido como:

a) vírus de setor de carga (boot sector).

b) vírus de programa.
c) vírus de macro.
d) backdoor.
e) hoax.

Comentários:

Vírus ativado quando um documento é aberto? Podendo infectar outros documentos? Podendo afetar um gabarito padrão de documentos (também chamado de template)? Propagação ocorre quando documentos são remetidos por correio eletrônico? Tudo nos remete ao Vírus de Macro!

Gabarito: Letra C

---

43. (CESPE / Polícia Federal – 2018) No processo conhecido como scanning, o worm, em sua fase de propagação, procura outros sistemas para infectar.

Comentários:

O processo de scanning é também chamado de identificação de computadores-alvo em que o worm tenta se propagar. Para tal, ele necessita identificar – por meio de um scanning – os computadores alvos para os quais tentará se copiar. O início da redação da questão é um pouco confuso porque parece dizer que a propagação é uma fase do scanning, o que não é verdadeiro. Enfim... o examinador deu uma deslizada nesse ponto e a questão ficou sem sentido, mas o gabarito se manteve. Para subsidiar a questão, vejamos o que diz William Stallings:

A primeira função executada na fase de propagação de um verme de rede é procurar outros sistemas para infectar, um processo conhecido como escaneamento (scanning) ou impressão digital. Para tais vermes, que exploram vulnerabilidades de software em serviços de rede acessíveis remotamente, é preciso identificar sistemas potenciais que executam o serviço vulnerável e então infectá-los. Em seguida, normalmente, o código do verme agora instalado nas máquinas infectadas repete o mesmo processo de escaneamento até criar uma grande rede distribuída de máquinas infectadas.

Gabarito: Correto

---

44. (CESPE / Polícia Federal – 2018) Os softwares de spyware têm como principal objetivo adquirir informações confidenciais de empresas e são usados como uma forma de espionagem empresarial.

Comentários:

O spyware é um software malicioso utilizado principalmente com pessoas físicas para avaliar seu hábito de uso e roubar informações pessoais. *Pode ser utilizado em empresas para espionagem empresarial?* Sim, mas esse não é seu objetivo principal.

Gabarito: Errado

---

45. (CESPE / BANCO DA AMAZÔNIA – 2018) Os vírus do tipo hoax são facilmente detectados pelas ferramentas de antivírus que utilizam técnicas de detecção por assinaturas, pois fazem uso de macros já conhecidas de vírus.

Comentários:

Não existe Vírus de Hoax. Hoax é um boato, não há nada na bibliografia que trate de Vírus de Hoax.

Gabarito: Errado

---

46. (CESPE / PM-AL – 2018) Spywares são programas instalados em computadores pessoais, capazes de identificar e remover determinados vírus, como, por exemplo, Hoax e Trojan.

Comentários:

Na verdade, a questão trata de antivírus e, não, de spywares.

Gabarito: Errado

---

47. (CESPE / BNB – 2018) Se um rootkit for removido de um sistema operacional, esse sistema não voltará à sua condição original, pois as mudanças nele implementadas pelo rootkit permanecerão ativas.

Comentários:

Rootkits são capazes de realizar diversas ações maliciosas que são extremamente difíceis de identificar, uma vez que ele geralmente apaga os rastros de suas operações. Existem maneiras de detectá-lo, mas é bastante complexo de identificar o que ele fez no sistema operacional. Logo, o procedimento mais indicado para um rootkit identificado é formatar e reinstalar o sistema. Embora seja drástico, este é o único método comprovado de remover completamente os rootkits.

Gabarito: Correto

---

48. (CESPE / BNB – 2018) Para evitar a contaminação de um arquivo por vírus, é suficiente salvá-lo com a opção de compactação.

Comentários:

Compactar um arquivo apenas reduz seu tamanho – não há nenhum efeito de prevenção à contaminação por vírus.

Gabarito: Errado

---

49. (CESPE / Polícia Federal – 2018) Situação hipotética: Ao processar um código executável malicioso que havia recebido como anexo de um email, Mateus percebeu que um malware havia infectado seu aparelho e que, automaticamente, havia sido enviada uma mensagem idêntica, com um anexo malicioso idêntico, a todos os contatos de sua lista de endereços, a partir do seu aparelho. Assertiva: Essa situação é um exemplo clássico de infecção de vírus de computador.

Comentários:

Perfeito! Exemplo clássico, clássico, clássico de infecção por vírus de computador. Você recebe um e-mail com anexo, abre sem fazer verificações e o vírus insere cópias de si mesmo em outros arquivos podendo enviá-lo automaticamente para pessoas da sua lista de contatos e potencialmente infectando outros usuários (o ideal é ter um backup atualizado).

Gabarito: Correto

---

50. (CESPE / Polícia Federal – 2018) Um ataque de ransomware comumente ocorre por meio da exploração de vulnerabilidades de sistemas e protocolos; a forma mais eficaz de solucionar um ataque desse tipo e recuperar os dados "sequestrados" (criptografados) é a utilização de técnicas de quebra por força bruta da criptografia aplicada.

Comentários:

De fato, um ataque de ransomware comumente ocorre por meio da exploração de vulnerabilidades de sistemas e protocolos. No entanto, técnicas de quebra por força bruta não são eficazes porque a criptografia utilizada poderia levar séculos para ser quebrada, mesmo utilizando alto poder computacional para testar todas as opções de chave.

Gabarito: Errado

---

51. (CESPE / Polícia Federal – 2018) A infecção de um sistema por códigos maliciosos pode ocorrer por meio da execução de arquivos infectados obtidos de anexos de mensagens eletrônicas, de mídias removíveis, de páginas web comprometidas, de redes sociais ou diretamente de outros equipamentos.

Comentários:

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.

Gabarito: Correto

---

52. (CESPE / Polícia Federal – 2018) A superexposição de dados pessoais nas redes sociais facilita o furto de identidade ou a criação de identidade falsa com dados da vítima, identidades essas que podem ser usadas para atividades maliciosas tais como a realização de transações financeiras fraudulentas, a disseminação de códigos maliciosos e o envio de mensagens eletrônicas falsas por email ou redes sociais.

Comentários:

Esse é um caso típico de Furto de Identidade (Identity Theft): ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. 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 – é muito comum nos casos em que pessoas se expõem exageradamente em redes sociais! Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar 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.

Gabarito: Correto

---

53. (CESPE / Polícia Federal – 2018) Formatos comuns de arquivos, como, por exemplo, .docx ou .xlsx, são utilizados como vetor de infecção por ransomware, um tipo de software malicioso que encripta os dados do usuário e solicita resgate.

Comentários:

Galera, eu vou ser honesto com vocês: se eu tivesse feito essa prova, eu marcaria errado com convicção! Extensões de ferramentas de escritório são bastante utilizadas por diversos malwares porque são frequentemente compartilhadas por e-mail ou dispositivos de armazenamento móvel, e porque geralmente contêm dados valiosos para usuários, como uma monografia ou relatório comercial que demandou bastante esforço para ser desenvolvido.

No entanto, para executar tarefas, elas precisam estar habilitadas para macros – e .docx e .xlsx não são extensões habilitadas para macros, portanto não poderiam executar ou infectar nada. Como o gabarito definitivo foi verdadeiro, eu vou dizer qual é a minha teoria para justificar esse gabarito: um atacante pode criar um ransomware e inserir ao final do nome do arquivo a extensão .docx ou .xlsx.

Notem que o arquivo em si não precisa estar nesse formato, basta colocar essa extensão no final do nome do arquivo. Dessa forma, o usuário poderá pensar que se trata de um documento ou planilha inofensiva e, assim, ele poderá baixar o arquivo e executá-lo – infectando seu computador.

Gabarito: Correto

---

54. (CESPE / Polícia Federal – 2018) Cavalos de Troia são exemplos de vírus contidos em programas aparentemente inofensivos e sua ação danosa é mascarada pelas funcionalidades do hospedeiro.

Comentários:

Como eu disse em aula, algumas questões insistem em tratar cavalos de troia (trojans) como um tipo de vírus, então não vamos brigar com a banca! Um trojan comumente é escondido dentro de um programa/arquivo aparentemente inofensivo, logo sua ação danosa acaba sendo mascarada pelas funcionalidades do programa/arquivo hospedeiro. Você acha que está executando um programa inofensivo, mas as ações danosas do trojan contido nesse programa são mascaradas pelas funcionalidades do programa original.

Gabarito: Correto

---

55. (CESPE / FUB – 2018) Worms são programas maliciosos que se propagam por meio da inclusão silenciosa de cópias de si mesmos em outros programas que, ao serem executados, processam também os códigos maliciosos e infectam outros programas e sistemas.

Comentários:

Cópias de si mesmo em outros programas? Opa... isso é um vírus e, não, um worm! Um worm é um programa capaz de se replicar automaticamente, enviando cópias de si mesmo de computador para computador.

Gabarito: Errado

---

56. (CESPE / EMAP – 2018) O ano de 2017 foi marcado por incidentes de sequestro, em diversos países, de dados de instituições, que eram encriptados; sendo essas instituições, em seguida, contatadas pelos atacantes, que solicitavam bitcoins em troca da liberação da chave criptográfica. Esses ataques foram executados por malwares categorizados como ransomwares.

Comentários:

Dados sequestrados e encriptados em que atacantes solicitavam moedas digitais em troca da liberação de acesso aos dados? Essa é uma característica típica de um ransomware!

Gabarito: Correto

---

57. (CESPE / STJ – 2018) Ransomware é um tipo de malware que cifra os arquivos armazenados no computador da vítima e solicita um resgate para decifrá-los.

Comentários:

Perfeito! Ransomware é um tipo de software nocivo que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate – geralmente em criptomoedas – para que o acesso possa ser restabelecido. Caso não ocorra o mesmo, arquivos podem ser perdidos e até mesmo publicados.

Gabarito: Correto

---

58. (CESPE / STJ – 2018) Spoofing é uma técnica que permite ocultar a origem do endereço IP, sendo utilizada em qualquer protocolo da camada de aplicação, mas não na camada de enlace da rede.

Comentários:

O IP Spoofing é o tipo mais comum de Spoofing, mas existem outros tipos como ARP Spoofing e MAC Spoofing – esse último opera na camada de enlace.

Gabarito: Errado

---

59. (CESPE / BNB – 2018) Se um rootkit for removido de um sistema operacional, esse sistema não voltará à sua condição original, pois as mudanças nele implementadas pelo rootkit permanecerão ativas.

Comentários:

O rootkit é capaz de modificar o sistema operacional em um nível tão profundo que a sua remoção não é suficiente para retornar o sistema operacional a sua condição original – a solução geralmente é formatar o sistema operacional.

Gabarito: Correto

---

60. (CESPE / TRT/7 – 2017) Assinale a opção que apresenta um tipo de malware capaz de registrar as teclas que são digitadas em uma estação de trabalho, fazer capturas de tela e até mesmo acessar arquivos em drives locais e(ou) compartilhados.

a) boot
b) cavalo de troia
c) macro
d) melissa

Comentários:

TIPO DE TROJAN	DESCRIÇÃO
TROJAN DESTRUTIVO	Altera ou apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
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.

O enunciado trata de keyloggers e screenloggers, que são tipos de spyware. No entanto, existem Cavalos de Troia do Tipo Spy, que instalam spywares. Ademais, o Trojan Destrutivo altera ou apaga arquivos e diretórios. Logo, a questão trata (mesmo que indiretamente) de Cavalo de Troia. Não é difícil acertar essa questão porque as opções não deixam dúvidas!

Gabarito: Letra B

---

61. (CESPE / CBM-AL – 2017) O backdoor é uma ferramenta maliciosa usada por hackers para invadir um computador e ter acesso aos arquivos e programas da máquina invadida sem autorização do seu usuário.

Comentários:

Essa questão foi anulada por gerar uma dupla interpretação. O backdoor permite o retorno de um invasor a um computador comprometido. Logo, se considerarmos que ele se refere à primeira invasão, seria errado porque os invasores utilizam outros recursos para invadir e acessar arquivos e programas; se considerarmos que ele se refere a uma invasão posterior, o item estaria CERTO, pois a função do backdoor é justamente permitir a invasão das máquinas e o acesso a seus dados.

Gabarito: Anulada

---

62. (CESPE / TRE-TO – 2017) O malware que, por meio de criptografia, torna inacessíveis os dados armazenados em um equipamento e exige pagamento de resgate para restabelecer o acesso ao usuário é do tipo:

a) ransomware.
b) backdoor.
c) cavalo de troia.

d) spyware.
e) rootkit.

Comentários:

Torna dados inacessíveis por meio de criptografia exigindo resgate para restabelecer o acesso? Trata-se do ransomware.

Gabarito: Letra A

---

63. (CESPE / TRT7 – 2017) O ataque que amplia o número de acessos a um servidor, gerando indisponibilidade de recursos aos usuários, é denominado:

a) phishing.
b) DoS.
c) spoofing.
d) adware.

Comentários:

O ataque que amplia o número de acessos a um servidor com o intuito de gerar indisponibilidade é denominado DoS (Denial of Service) ou Negação de Serviço.

Gabarito: Letra B

---

64. (CESPE / DPU – 2016) Malwares são mecanismos utilizados para evitar que técnicas invasivas, como phishing e spams, sejam instaladas nas máquinas de usuários da Internet.

Comentários:

Na verdade, malwares são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Além disso, a redação da questão não faz sentido, uma vez que phishing e spams não são instaláveis.

Gabarito: Errado

---

65. (CESPE / INSS – 2016) A infecção de um computador por vírus enviado via correio eletrônico pode se dar quando se abre arquivo infectado que porventura esteja anexado à mensagem eletrônica recebida.

Comentários:

O vírus é um 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. Logo, a infecção de um computador por vírus enviado via correio eletrônico realmente pode se dar quando se abre arquivo infectado que porventura esteja anexado à mensagem eletrônica recebida.

Gabarito: Correto

---

66. (CESPE / ANVISA – 2016) Códigos maliciosos podem ter acesso aos dados armazenados no computador e executar ações em nome dos usuários, de acordo com as permissões de operação de cada um destes.

Comentários:

De fato, uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e geralmente podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

Gabarito: Correto

---

67. (CESPE / FUB – 2016) Enquanto estiver conectado à Internet, um computador não será infectado por worms, pois este tipo de praga virtual não é transmitido pela rede de computadores.

Comentários:

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.

Gabarito: Errado

---

68. (CESPE / TCE-PA – 2016) A criação de discos de recuperação de sistema é útil no caso de as instalações serem malsucedidas, mas não no caso de perda de arquivos causada por infecções de vírus ou malwares.

Comentários:

Um disco de recuperação tem a finalidade de restaurar dados do sistema, caso ocorra falha da unidade de disco rígido, exclusão acidental, instalações malsucedidas, problema com o sistema ou

perda de arquivos causada por infecções de vírus ou não. Caso um malware exclua arquivos de um computador, esses arquivos poderão ser restaurados por meio de discos de recuperação.

Gabarito: Errado

---

69. (CESPE / TRE/GO – 2015) Botnet é uma rede formada por inúmeros computadores zumbis e que permite potencializar as ações danosas executadas pelos bots, os quais são programas similares ao worm e que possuem mecanismos de controle remoto.

Comentários:

Botnet é realmente uma rede formada por inúmeros computadores zumbis e que permite potencializar as ações danosas executadas pelos bots, os quais são programas similares worm, mas que possuem mecanismos de controle remoto.

Gabarito: Correto

---

70. (CESPE / FUB – 2015) Vírus é um programa autossuficiente capaz de se propagar automaticamente pelas redes enviando cópias de si mesmo de um computador para outro.

Comentários:

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! Vírus não são autossuficientes, eles necessitam da execução de um hospedeiro para se propagar pelas redes enviando cópias de si mesmo.

Gabarito: Errado

---

71. (CESPE / TCE-RN – 2015) O objetivo do vírus Nimda é identificar as falhas de segurança existentes nos sistemas operacionais para contaminar computadores de empresas e propagar-se.

Comentários:

Nimda é um vírus que surgiu em setembro de 2003, e infectou milhões de computadores em apenas 3 dias. Este programa malicioso ataca por e-mail, através de sites, drives compartilhados. Quando enviado por e-mail, chega com o arquivo anexado readme.exe. Ele é capaz de se propagar através dos diretórios compartilhados das redes Windows, de empresas ou domésticas, infectando arquivos executáveis nestes diretórios.

Gabarito: Correto

---

72. (CESPE / TJDFT - 2015) Vírus do tipo boot, quando instalado na máquina do usuário, impede que o sistema operacional seja executado corretamente.

Comentários:

Boot é o procedimento de inicialização do computador durante o carregamento do sistema operacional, logo após a máquina ser ligada! O Vírus de Boot é um dos primeiros tipos de vírus conhecidos e infecta a parte de inicialização do sistema operacional, escondendo-se no primeiro setor da memória e impedindo que o sistema operacional seja executado corretamente.

Gabarito: Correto

---

73. (CESPE / TELEBRAS - 2015) Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.

Comentários:

Sniffer não utiliza técnica de mascaramento, essa é uma característica de ataques ativos e o Sniffer é passivo. A questão tenta confundir com o Spoof, que é um ataque de mascaramento. Ademais, Sniffer não é anexado a arquivos – ele é uma técnica de escuta de dados.

Gabarito: Errado

---

74. (CESPE / TELEBRAS - 2015) Worms, assim como os vírus, são autorreplicáveis e necessitam ser executados pelos usuários para se propagarem e infectarem os computadores de uma rede.

Comentários:

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 execução direta de suas cópias, ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Gabarito: Errado

---

75. (CESPE / FUB – 2015) O phishing é um procedimento que possibilita a obtenção de dados sigilosos de usuários da Internet, em geral, por meio de falsas mensagens de email.

Comentários:

Perfeito! Trata-se de um golpe fraudulento que permite capturar dados sigilosos de usuários por meio do envio de mensagens falsas de e-mail.

Gabarito: Correto

---

76. (CESPE / TELEBRAS – 2015) Uma das formas de manter o aparelho de telefone celular livre de vírus é deixar o *bluetooth* habilitado constantemente, para que ele possa identificar possíveis anexos maliciosos às mensagens recebidas.

Comentários:

Pelo contrário, deixar o bluetooth habilitado constantemente pode comprometer a segurança do celular, permitindo possíveis ataques ou ações maliciosas.

Gabarito: Errado

---

77. (CESPE / STJ – 2015) Os hoaxes são conhecidos como histórias falsas recebidas por email, muitas delas de cunho dramático ou religioso, com o objetivo de atrair a atenção da pessoa e então direcioná-la para algum sítio, oferecendo-lhe algo ou solicitando-lhe que realize alguma ação que possa colocar em risco a segurança de seus dados.

Comentários:

Hoaxes realmente são mensagens com conteúdo alarmante ou falso, no entanto seu objetivo não é, necessariamente, obter dados pessoais do usuário – por essa razão, a questão foi anulada.

Gabarito: Anulada

---

78. (CESPE / TCE-RN – 2015) A principal diferença entre crackers e hackers refere-se ao modo como esses malfeitores da área de segurança da informação atacam: os crackers são mais experientes e realizam ataques sem utilizar softwares, ao passo que os hackers utilizam códigos maliciosos associados aos softwares para realizar ataques ao ciberespaço.

Comentários:

Hacker é aquele 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 é aquele 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. Não existe nenhuma relação com a utilização de softwares ou não para realizar ataques ao ciberespaço.

Gabarito: Errado

79.(CESPE / MDIC – 2014) O comprometimento do desempenho de uma rede local de computadores pode ser consequência da infecção por um worm.

Comentários:

Perfeito! Uma das ações maliciosas mais típicas de um worm é sua massiva replicação, comprometendo o desempenho da rede e, em geral, deixando-a lenta.

Gabarito: Correto

80.(CESPE / MDIC – 2014) Um backdoor (porta dos fundos) é um programa de computador utilizado pelo administrador de rede para realizar a manutenção remota da máquina de um usuário.

Comentários:

Na verdade, eles são programas maliciosas utilizados por atacantes para permitir seu acesso remoto à máquina a fim de cometer ações capazes de comprometer o sistema.

Gabarito: Errado

81.(CESPE / CADE – 2014) O computador utilizado pelo usuário que acessa salas de bate-papo não está vulnerável à infecção por worms, visto que esse tipo de ameaça não se propaga por meio de programas de chat.

Comentários:

Opa... se propaga, sim! Hoje em dia, é bem rara a utilização de salas de bate-papo. No entanto, quando isso era mais comum, era uma grande fonte de vulnerabilidade à infecção por worms.

Gabarito: Errado

82.(CESPE / CADE – 2014) Os vírus de computador podem apagar arquivos criados pelo editor de texto, no entanto são incapazes de infectar partes do sistema operacional, já que os arquivos desse sistema são protegidos contra vírus.

Comentários:

Vírus de computador são capazes – sim – de infectar partes do sistema operacional, uma vez que nem eles estão protegidos softwares maliciosos.

Gabarito: Errado

83.(CESPE / Polícia Federal – 2014) Phishing é um tipo de malware que, por meio de uma mensagem de email, solicita informações confidenciais ao usuário, fazendo-se passar por uma entidade confiável conhecida do destinatário.

Comentários:

Essa seria uma descrição impecável de phishing, caso não afirmasse que se trata de um... malware. Na verdade, trata-se de um golpe ou fraude! Maaaaaas... a banca considerou correta :(

Gabarito: Correto

84.(CESPE / Polícia Federal – 2014) Os hjackers são exemplos de códigos maliciosos que, sem que os usuários percebam, invadem computadores e, por exemplo, modificam o registro do Windows.

Comentários:

A questão trata claramente de hijackers, no entanto o examinador escreveu esse termo de forma errada. Os alunos ficaram em dúvida se se tratava de hackers ou hijackers e, por essa razão, a questão foi anulada. Lembrando que, de fato, ele pode modificar os registros do Windows.

Gabarito: Anulada

85.(CESPE / FUB – 2014) Computadores podem ser infectados por vírus mesmo que não estejam conectados à Internet.

Comentários:

Claro que podem – um computador pode ser infectado por um pendrive, por exemplo!

Gabarito: Correto

---

86. (CESPE / MEC – 2014) A ação de worms pode afetar o desempenho de uma rede de computadores.

Comentários:

Perfeito! A principal ação maliciosa de um worm é afetar o desempenho de uma rede de computador por conta da grande quantidade de cópias de si mesmo consumindo recursos.

Gabarito: Correto

---

87. (CESPE / MTE – 2014) Os antivírus são ferramentas capazes de detectar e remover os códigos maliciosos de um computador, como vírus e worms. Tanto os vírus quanto os worms são capazes de se propagarem automaticamente por meio da inclusão de cópias de si mesmo em outros programas, modificando-os e tornando-se parte deles.

Comentários:

Apenas vírus se propagam incluindo cópias de si mesmo em outros programas – worms se propagam enviando cópias de si mesmo de um computador para outro em uma rede.

Gabarito: Errado

---

88. (CESPE / TELEBRÁS – 2013) Cavalo de troia é um tipo de programa que se instala sem conhecimento do usuário. Por meio desse programa, o invasor pode ter acesso a arquivos do computador e copiá-los, além de poder formatar o disco rígido.

Comentários:

Ele vem "de presente" sem o conhecimento do usuário junto com algum arquivo "legítimo". Por meio dele, o invasor realmente pode ter acesso a arquivos do computador e copiá-los, além de formatar o disco rígido e outras atividades maliciosas.

Gabarito: Correto

---

89. (CESPE / CNJ – 2013) Vírus de macro infectam arquivos criados por softwares que utilizam linguagem de macro, como as planilhas eletrônicas Excel e os documentos de texto Word. Os danos variam de alterações nos comandos do aplicativo à perda total das informações.

Comentários:

Perfeito! Vírus de macro realmente infectam arquivos criados por softwares que utilizam linguagens de macro – como VBA (Visual Basic for Applications). Além disso, os exemplos mais comuns são os softwares que escritório (Ex: MS-Excel e MS-Word), que tem como produtos planilhas eletrônicas e documentos de texto. Por fim, eles de fato podem alterar comandos da aplicação ou remover informações.

Gabarito: Correto

---

90. (CESPE / CNJ – 2013) Vírus de script registram ações dos usuários e são gravados no computador quando da utilização de um pendrive infectado.

Comentários:

Vírus de Script não registram ações dos usuários – essa é uma ação maliciosa típica de spywares como keyloggers ou screenloggers.

Gabarito: Errado

---

91. (CESPE / TJDFT – 2013) Backdoor é uma forma de configuração do computador para que ele engane os invasores, que, ao acessarem uma porta falsa, serão automaticamente bloqueados.

Comentários:

Backdoor é, na verdade, um software malicioso que engana os usuários de modo que permita a invasão de atacantes sem nenhum tipo de bloqueio – é exatamente o oposto do descrito no item.

Gabarito: Errado

---

92. (CESPE / TJDFT – 2013) Worm é um software que, de forma semelhante a um vírus, infecta um programa, usando-o como hospedeiro para se multiplicar e infectar outros computadores.

Comentários:

Worm é realmente um software (malicioso), no entanto ele não infecta programas para utilizá-lo como hospedeiro. Na verdade, ele pode se autorreplicar na rede sem a necessidade de um hospedeiro. Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Gabarito: Errado

---

93. (CESPE / TRT10 – 2013) Os programas, documentos ou mensagens passíveis de causar prejuízos aos sistemas podem ser incluídos na categoria de malwares, que podem ser divididos em três subgrupos: vírus propriamente ditos, worms e trojans ou cavalos de troia.

Comentários:

Existem diversas categorias de malwares, no entanto o examinador quis citar apenas três no item. *Há algo de errado nisso?* Não, lembrem-se de que um item somente está errado se contiver um erro. *Qual é o erro do enunciado?* Nenhum! Os programas, documentos ou mensagens passíveis de causar prejuízos aos sistemas podem ser incluídos na categoria de malwares, que podem ser divididos em três subgrupos: vírus propriamente ditos, worms e trojans (cavalos de troia).

Gabarito: Correto

94.(CESPE / TRT10 – 2013) Arquivos anexados a mensagens de email podem conter vírus, que só contaminarão a máquina se o arquivo anexado for executado. Portanto, antes de se anexar um arquivo a uma mensagem para envio ou de se executar um arquivo que esteja anexado a uma mensagem recebida, é recomendável, como procedimento de segurança, executar um antivírus para identificar possíveis contaminações.

Comentários:

Vírus realmente só contaminam uma máquina caso sejam executados. Além disso, é de fato recomendadíssimo executar um antivírus em anexos de e-mail para identificar possíveis contaminações.

Gabarito: Correto

95.(CESPE / TRT10 – 2013) O vírus de computador é assim denominado em virtude de diversas analogias poderem ser feitas entre esse tipo de vírus e os vírus orgânicos.

Comentários:

Perfeito! Questão meio óbvia... vírus de computador e vírus orgânicos/biológicos realmente possuem muitas coisas em comum e, por essa razão, o segundo inspirou o nome do primeiro.

Gabarito: Correto

---

96. (CESPE / MPU – 2013) Phishing é a técnica de criar páginas falsas, idênticas às oficiais, para capturar informações de usuários dessas páginas.

Comentários:

Coisa linda esse item! Phishing é exatamente isso – uma técnica de criar páginas falsas, idênticas às páginas oficiais, para capturar informações de usuários dessas páginas. *Professor, isso não seria Pharming?* Não, ambos apresentam sites bastante parecidos, mas o Pharming envolve o redirecionando para outro endereço! Em outras palavras, caso você insira o endereço verdadeiro, continuará sendo enviado para o site falso (Ex: *www.bb.com.com* > *www.bb.net.br*).

Gabarito: Correto

97.(CESPE / PRF – 2013) Ao contrário de um vírus de computador, que é capaz de se autorreplicar e não necessita de um programa hospedeiro para se propagar, um worm não pode se replicar automaticamente e necessita de um programa hospedeiro.

Comentários:

Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos hospedeiros, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Gabarito: Errado

---

98. (CESPE / IBAMA – 2013) Ao salvar o arquivo em um disco removível, seu conteúdo será protegido contra vírus de macro, pois esse tipo de vírus ataca apenas arquivos no disco rígido.

Comentários:

Não faz o menor sentido! Vírus de Macro atacam arquivos em qualquer mídia de armazenamento, inclusive discos removíveis.

Gabarito: Errado

---

99. (CESPE / BACEN – 2013) A recepção de respostas de mensagens que nunca foram enviadas ou que têm como destinatário o próprio remetente são indícios de falsificação de e-mail.

Comentários:

Também chamada de E-mail Spoofing, a Falsificação de E-mail tem realmente como indício a recepção de respostas de mensagens que nunca foram enviadas ou como destinatário o próprio remetente. No primeiro caso, o usuário pode achar que ele de fato enviou o e-mail e acabar caindo em algum golpe.

Gabarito: Correto

---

100. (CESPE / BACEN – 2013) Em relação à forma de infecção de computadores, vírus e worms são recebidos automaticamente pela rede, ao passo que trojans e backdoors são inseridos por um invasor.

Comentários:

Vírus não são recebidos automaticamente pela rede – worms, são. O restante do enunciado está perfeito!

Gabarito: Errado

---

101. (CESPE / Telebras – 2013) Malwares do tipo rootkit são difíceis de ser detectados por antivírus ou outros softwares de segurança; além disso, eles usam técnicas avançadas para infiltrar programas em processos ativos na memória do computador.

Comentários:

Perfeito! Rootkits são extremamente difíceis de ser detectados e eles realmente utilizam técnicas avançadas para infiltrar em processos do sistema operacional e executar suas ações em memória unido a esses processos.

Gabarito: Correto

---

102. (CESPE / SEGESP-AL – 2013) Um computador que apresenta reinicializações inexplicáveis ou lentidões excessivas no processamento de comandos pode estar infectado com algum malware, como vírus ou spyware.

Comentários:

Uma dica para vocês: quando uma questão utiliza o verbo "poder", ela facilita bastante a nossa vida! Acredito que todos vocês tiveram certeza em relação ao vírus, mas ficaram com dúvida em relação ao spyware. De fato, é muito improvável que spywares danifiquem um computador causando reinicializações inexplicáveis ou lentidões excessivas no processamento de comandos. Agora eu pergunto: *é impossível que ele faça isso?* Não! Se não é impossível, é possível, logo pode! Para um examinador marcar uma questão dessa como errada, ele vai ter que me provar que é impossível essas ações maliciosas por meio de um spyware.

Gabarito: Correto

---

103. (CESPE / PC-DF – 2013) Malware é qualquer tipo de software que pode causar algum impacto negativo sobre a informação, podendo afetar sua disponibilidade, integridade e confidencialidade. Outros softwares são produzidos para oferecer proteção contra os ataques provenientes dos malwares. Os vírus, ao se propagarem, inserem cópias de seu próprio código em outros programas, enquanto os worms se propagam pelas redes, explorando, geralmente, alguma vulnerabilidade de outros softwares.

Comentários:

Perfeito! Vírus precisam de outro programa para se propagar enquanto worms podem se propagar pelas redes sem infectar outros programas.

Gabarito: Correto

---

104. (CESPE / PC-DF – 2013) O uso de recursos de tecnologias da informação e das comunicações encontra-se difundido e disseminado em toda sociedade. Nesse contexto, ações de investigação criminal necessitam estar adaptadas para identificar e processar evidências digitais de modo a produzir provas materiais. Para tanto, existem diversos tipos de exames técnico-científicos

utilizados em investigações. Computadores infectados com vírus não podem ser examinados em uma investigação, pois o programa malicioso instalado compromete a integridade do sistema operacional.

Comentários:

Ué, claro que podem! Você sempre pode examinar um computador – esse item não faz qualquer sentido. Que viagem...

Gabarito: Errado

---

105. (CESPE / PC-DF – 2013) Rootkit é um tipo de praga virtual de difícil detecção, visto que é ativado antes que o sistema operacional tenha sido completamente inicializado.

Comentários:

Rootkit realmente tem detecção extremamente difícil e – no modo kernel – pode ser ativado antes que o próprio sistema operacional tenha sido completamente inicializado.

Gabarito: Correto

---

106. (CESPE / CPRM – 2013) A compactação de arquivos evita a contaminação desses arquivos por vírus, worms e pragas virtuais.

Comentários:

Compactar um arquivo não tem qualquer efeito para evitar sua contaminação por malwares – ele apenas reduzirá o tamanho do arquivo.

Gabarito: Errado

---

107. (CESPE / ANS – 2013) A contaminação por pragas virtuais ocorre exclusivamente quando o computador está conectado à Internet.

Comentários:

Lembrem-se sempre das mídias removíveis, que são um grande vetor de malwares. Logo, computadores não precisam estar conectados à internet.

Gabarito: Errado

---

108. (CESPE / Telebras – 2013) Cavalo de troia é um tipo de programa que se instala sem conhecimento do usuário. Por meio desse programa, o invasor pode ter acesso a arquivos do computador e copiá-los, além de poder formatar o disco rígido.

Comentários:

Perfeito! Ele se instala sem conhecimento do usuário? Sim, o usuário acha que está instalando um programa legítimo, mas está instalando também um software malicioso. *O invasor pode ter acesso a arquivos do computador e copiá-los, além de poder formatar o disco rígido?* Cavalos de Troia são extremamente versáteis, podendo realizar uma infinidade de ações maliciosas, incluindo acessar arquivos do computador e copiá-los, além de poder formatar o disco rígido.

Gabarito: Correto

---

109. (CESPE / TRT10 – 2013) A transferência de arquivos para pendrives constitui uma forma segura de se realizar becape, uma vez que esses equipamentos não são suscetíveis a malwares.

Comentários:

Opa... são extremamente suscetíveis a malwares.

Gabarito: Errado

---

110. (CESPE / Câmara dos Deputados – 2012) Os worms, assim como os vírus, infectam computadores, mas, diferentemente dos vírus, eles não precisam de um programa hospedeiro para se propagar.

Comentários:

Perfeito! Ambos infectam computadores, mas vírus precisam de um programa hospedeiro para se propagar e worms, não.

Gabarito: Correto

---

111. (CESPE / TJ-AC – 2012) Vírus é um programa de computador malicioso capaz de se propagar automaticamente por meio de redes, mas necessita ser explicitamente executado para se propagar.

Comentários:

Vírus é um programa de computador malicioso? Sim! *Capaz de se propagar automaticamente por meio de redes?* Não, vírus se propagam inserindo cópias de si mesmo em arquivos e, não, através de redes. *Necessita ser explicitamente executado para se propagar?* Sim! Logo, questão errada...

Maaaas... pasmem: o examinador deu gabarito como correto! Ignorem o examinador e confiem no que estudamos – essa questão está muito errada, apesar do gabarito oficial.

Gabarito: Correto

---

112. (CESPE / TJ-AC – 2012) Os rootkits são um conjunto de programas que oferecem mecanismos para esconder o invasor, assegurando a sua presença em um computador invadido.

Comentários:

Perfeito! 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.

Gabarito: Correto

---

113. (CESPE / Câmara dos Deputados – 2012) Um arquivo do tipo PDF não carrega código malicioso, como cavalo de troia.

Comentários:

Opa... eles podem carregar código malicioso, sim! Eles podem conter elementos dinâmicos, logo podem abrigar scripts que podem conter softwares maliciosos.

Gabarito: Errado

---

114. (CESPE / Câmara dos Deputados – 2012) O Cavalo de Troia, ou Trojan Horse, é um tipo de programa de computador, geralmente enviado por email, que, quando executado, permite que o remetente tenha acesso ao computador infectado, sempre que este estiver conectado à rede.

Comentários:

Como eu sempre digo, trojans são malwares extremamente versáteis! Um dos tipos de trojan é o Trojan Backdoor, capaz de incluir um backdoor que possibilita o acesso remoto do atacante ao computador.

Gabarito: Correto

---

115. (CESPE / Câmara dos Deputados – 2012) O termo phishing designa a técnica utilizada por um fraudador para obter dados pessoais de usuários desavisados ou inexperientes, ao empregar informações que parecem ser verdadeiras com o objetivo de enganar esses usuários.

Comentários:

Perfeito! Phishing é uma forma de fraude eletrônica caracterizada por tentativas de adquirir dados pessoais ou financeiros de diversos tipos enganando usuários desavisados ou inexperientes.

Gabarito: Correto

---

116. (CESPE / FNDE – 2012) Trojans ou cavalos de troia são programas capazes de multiplicar-se mediante a infecção de outros programas maiores. Eles não têm o objetivo de controlar o sistema, porém tendem a causar efeitos indesejados. Já os worms causam efeitos altamente destrutivos e irreparáveis. Ao contrário dos trojans, os worms utilizam o email como principal canal de disseminação, mas não possuem a capacidade de produzir cópias de si mesmos ou de algumas de suas partes.

Comentários:

Trojans não são capazes de se propagar/multiplicar; worms não causam efeitos altamente destrutivos e irreparáveis – eles geralmente consomem recursos da rede; além disso, worms possuem a capacidade de produzir cópias de si mesmos ou de algumas de suas partes.

Gabarito: Errado

---

117. (CESPE / FNDE – 2012) Embora sejam considerados programas espiões, os spywares também são desenvolvidos por empresas com o objetivo de coletar legalmente informações acessíveis de usuários.

Comentários:

Perfeito, existem spywares legítimos!

Gabarito: Correto

---

118. (CESPE / MPE-PI – 2012) Worms são programas maliciosos que se autorreplicam em redes de computadores anexados a algum outro programa existente e instalado em computadores da rede.

Comentários:

Worms não são anexados a programas – quem precisa de um programa hospedeiro é o vírus.

Gabarito: Errado

---

119. (CESPE / Banco da Amazônia – 2012) Os vírus do tipo mutante são capazes de modificar a estrutura de arquivos, para dificultar sua detecção por antivírus.

Comentários:

Perfeito! Os vírus mutantes – também chamados de polimórficos – são capazes de assumir múltiplas formas a cada infecção com o intuito de burlar o software de antivírus.

Gabarito: Correto

---

120. (CESPE / IFB – 2011) Os ataques de negação de serviços são feitos por meio de abuso da ingenuidade ou confiança do usuário.

Comentários:

Na verdade, a questão trata de Engenharia Social e, não, Negação de Serviço. Esse termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança.

Gabarito: Errado

LISTA DE QUESTÕES – CESPE

1. **(CESPE / IBAMA – 2022)** O vírus do tipo *ransomware* é um código malicioso que executa tarefas indesejadas no computador, sem o conhecimento do usuário.

2. **(CESPE / TELEBRAS – 2022)** Em uma rede, a instalação de um firewall e a atualização frequente desse firewall garantem a total proteção da rede contra invasores e dos programas instalados nas estações de trabalho contra vírus e worms.

3. **(CESPE / TELEBRAS – 2022)** Um *worm* tem como características a infecção de estações de trabalho, ao invés de arquivos, e a dispersão pela rede, utilizando múltiplas técnicas de replicação.

4. **(CESPE / PC-PB – 2022)** Ataque malicioso ao ambiente computacional, realizado por programa ou fragmentos de código não replicável, aparentemente seguro, que, de forma oculta, realiza ações como roubo de senhas e arquivos, é:

   a) *spyware*.
   b) *ransomware*.
   c) cavalo de troia.
   d) vírus.
   e) *worms*.

5. **(CESPE / TCE-RJ – 2022)** Os trojans possuem características totalmente distintas em relação aos vírus; a principal delas é que os trojans não permitem ser controlados à distância pela pessoa que os instalou, diferentemente dos vírus.

6. **(CESPE / TCE-RJ – 2022)** Quando instalado e ao ser executado pelo operador do sistema, o rootkit substitui arquivos executáveis importantes do sistema operacional.

7. **(CESPE / PGE-RJ – 2022)** O botnet é um vírus projetado especificamente para mostrar, no computador do usuário, propagandas oriundas das redes sociais.

8. **(CESPE / SERES-PE – 2022)** A praga virtual que bloqueia o computador, impedindo o acesso a seus arquivos, com o objetivo de exigir-se pagamento para liberação é conhecida como:

   a) *bot*.
   b) *trojan*.
   c) *ransomware*.
   d) vírus.
   e) *worm*.

9. **(CESPE / SECONT-ES – 2022)** Pharming é o ataque em que são alteradas as informações de endereço armazenadas pelos provedores de serviço de Internet para agilizar a navegação web, com o objetivo de redirecionar o usuário para uma página web falsa.

10. **(CESPE / Prefeitura de São Cristóvão-SE – 2022)** Um software malicioso tem a capacidade de infectar o computador e executar nele ações que prejudiquem seu funcionamento, como apagar arquivos pessoais ou instalar outros tipos de vírus.

11. **(CESPE / MC – 2022)** Diferentemente dos vírus, os worms consomem poucos recursos computacionais e de rede e se propagam por meio da infecção silenciosa de programas ou arquivos, o que dificulta a sua detecção e eliminação.

12. **(CESPE / MC – 2022)** Rootkit é um programa malicioso conhecido por apresentar propagandas.

13. **(CESPE / APEX Brasil – 2022)** *Malware* é qualquer software intencionalmente criado para causar danos a um computador, servidor, cliente ou a uma rede de computadores.

14. **(CESPE / DPDF - 2022)** Para detectar um ataque malicioso a um computador e fornecer evidências desse ataque, é correto utilizar um registro de logs externo a esse computador.

15. **(CESPE / DPE-RO – 2021)** Uma significativa parte da prevenção contra determinado ataque cibernético pode ser realizada por meio da minimização dos privilégios de acesso das aplicações, bem como pela sanitização de códigos relacionados aos acessos a bancos de dados. Trata-se de prevenção contra-ataques:

a) de vírus.
b) DDoS.
c) de SQL injection.
d) do tipo phishing.
e) do tipo ransomware.

16. **(CESPE / ALE-CE - 2021)** Ao acessar um anexo de email, um usuário teve seus arquivos criptografados e tornados inacessíveis para ele, por meio de uma taque a seu computador. Para torná-los acessíveis, foi exigido pagamento de resgate em bitcoins. Esse de tipo de ataque utiliza um código malicioso conhecido como

a) ransomware.
b) email spoofing.
c) virus.
d) força bruta.
e) trojan ou cavalo de troia.

Paulo, servidor de determinado órgão público, recebeu a seguinte mensagem em seu email corporativo.

Assunto: *Seu dispositivo está infectado e hackeado.*

Oi! Eu tenho más notícias para você, há alguns meses tive acesso aos dispositivos que você usa para navegar na web. Instalei um cavalo de troia nos sistemas operacionais de todos os dispositivos que você usa para acessar seu e-mail (celular, computador e tablete).

Eu bloqueei o cesso aos seus sistemas por meio de criptografia de todas as suas informações, tais como impostos de renda, fotos e arquivos de trabalho, o arquivo curriculum.docx no diretório Meus documentos. Para comprovar, veja a última dará de atualização desse arquivo – está dando agosto deste ano.

Posso publicar todos os seus dados pessoais na nuvem, incluindo os dados financeiros e, ainda, deixar seus arquivos indisponíveis para sempre.

Acho que você não vai querer que isso aconteça, pois será um verdadeiro desastre em sua vida. Vamos resolver assim: você me transfere $ 1.000.00 (em bitcoin equivalente à taxa de câmbio no momento da transferência) e, assim que a transferência for recebida, eu removerei imediatamente o vírus da sua máquina e devolverei seu acesso.

Minha carteira bitcoin para pagamento é 123456789abcdef. Se eu descobrir que você compartilhou esta mensagem com outra pessoa ou avisou à polícia, destruirei seus arquivos e sua privacidade financeira para sempre e todos os seus dados se tornarão públicos.

Considerando essa situação hipotética e assuntos a ela relacionados, julgue os itens a seguir.

17. (CESPE / PC-SE – 2021) Admitindo-se que a infecção por cavalo de Troia realmente tenha ocorrido, é correto afirmar que tal infecção pode ter acontecido por meio de um spear phishing, o que teria sido evitado se na máquina do usuário tivesse um antispyware instalado.

Paulo, servidor de determinado órgão público, recebeu a seguinte mensagem em seu email corporativo.

Assunto: *Seu dispositivo está infectado e hackeado.*

Oi! Eu tenho más notícias para você, há alguns meses tive acesso aos dispositivos que você usa para navegar na web. Instalei um cavalo de troia nos sistemas operacionais de todos os dispositivos que você usa para acessar seu e-mail (celular, computador e tablete).

Eu bloqueei o cesso aos seus sistemas por meio de criptografia de todas as suas informações, tais como impostos de renda, fotos e arquivos de trabalho, o arquivo curriculum.docx no diretório Meus documentos. Para comprovar, veja a última dará de atualização desse arquivo – está dando agosto deste ano.

Posso publicar todos os seus dados pessoais na nuvem, incluindo os dados financeiros e, ainda, deixar seus arquivos indisponíveis para sempre.

Acho que você não vai querer que isso aconteça, pois será um verdadeiro desastre em sua vida. Vamos resolver assim: você me transfere $ 1.000.00 (em bitcoin equivalente à taxa de câmbio no momento da transferência) e, assim que a transferência for recebida, eu removerei imediatamente o vírus da sua máquina e devolverei seu acesso.

Minha carteira bitcoin para pagamento é 12345678 9abcdef. Se eu descobrir que você compartilhou esta mensagem com outra pessoa ou avisou à polícia, destruirei seus arquivos e sua privacidade financeira para sempre e todos os seus dados se tornarão públicos.

Considerando essa situação hipotética e assuntos a ela relacionados, julgue os itens a seguir.

18. **(CESPE / PC-SE – 2021)** Infere-se do email apresentado, especialmente do trecho ''Eu bloqueei o acesso aos seus sistemas por meio de criptografia de todas as suas informações, tais como imposto de renda, fotos e arquivos de trabalho'', que se trata de um ataque por trojan, o qual é um programa que, além de executar as funções para as quais foi aparentemente projetado, torna inacessíveis os dados armazenados, som o conhecimento do usuário.

19. **(CESPE / PC-AL – 2021)** A grande diferença entre vírus e 4orms está na forma como eles se propagam: o vírus, ao contrário do worm, não se propaga por meio da inclusão de cópias de si mesmo em outros programas, mas pela execução direta de uma de suas cópias.

20. **(CESPE / PM-AL – 2021)** O registro das atividades, em um computador, normalmente gerado por programas ou serviços e armazenado em arquivos é conhecido como scan de vulnerabilidades.

21. **(CESPE / PM-AL – 2021)** Códigos maliciosos capazes de capturar tudo o que for digitado no teclado do usuário são conhecidos como rootkits.

22. **(CESPE / PM-AL – 2021)** Uma infecção por trojan pode ser recebida automaticamente pela rede, sem que nenhum usuário tenha efetuado o envio.

23. **(CESPE / PM-AL – 2021)** Um worm é um programa capaz de se propagar enviando cópias de si mesmo para outros computadores em uma rede.

24. **(CESPE / DEPEN – 2021)** Os vírus do tipo cavalo de troia, também conhecidos como trojans, podem ser instalados por outros vírus e programas, mas também podem infectar o ambiente por meio de links durante a navegação na Internet ou até mesmo por meio de emails falsos (phishing).

25. **(CESPE / PM-AL – 2021)** O Dropper é um trojan que executa em um site a ação maliciosa de redirecionar o usuário para sites específicos, com a finalidade de aumentar a quantidade de acessos à página.

26. **(CESPE / PCDF – 2021)** Para que as pragas virtuais denominadas worms ataquem o computador em uso, é necessário que se execute um arquivo do tipo .bat.

27. **(CESPE / PM-TO – 2021)** A solução mais efetiva a ser tomada em caso de um usuário que tenha sofrido ataque de Ransomware em seus arquivos é:

a) utilizar um antispyware capaz de bloquear o keylogger e assim monitorar os arquivos afetados e, desse modo, evitar que as informações coletadas desses arquivos sejam enviadas para terceiros.

b) realizar periodicamente backups testados, pois a garantia de que ele conseguirá acessá-los novamente é possuir backups atualizados, uma vez que nesse tipo de ataque o acesso aos arquivos é bloqueado sem a garantia de que o pagamento de um valor será a solução.

c) executar um antivírus nos arquivos infectados com método de detecção por meio de heurística, de modo a eliminar o malware presente nos arquivos.

d) instalar e executar o sistema de firewall, de modo a impedir que o atacante tente explorar o conteúdo dos arquivos afetados e, assim, evitar o acesso não autorizado caso haja algum backdoor neles instalados.

e) executar software que realize a criptografia nos arquivos, de forma a proteger os dados presentes nos arquivos e garantir que seu conteúdo não seja enviado para terceiros.

28. **(CESPE / TCE-RJ – 2021)** Os ataques de phishing caracterizam-se pelo envio de mensagens eletrônicas que despertam a atenção de usuários por meio da sugestão de vantagens ou ameaças de prejuízos e também por induzirem os usuários a fornecer dados pessoais e(ou) financeiros.

29. **(CESPE / Polícia Federal – 2021)** Denomina-se *backdoor* a situação em que o usuário sofre um ataque, seus dados são criptografados, ficam inacessíveis e, então, exige-se desse usuário o pagamento de resgato para restabelecimento do acesso a seus dados.

30. **(CESPE / PRF – 2021)** Ransomware é um programa malicioso de computador que se propaga por meio da inserção de cópias de si mesmo em arquivos criptografados.

31. **CESPE / PC-SE – 2020)** Ao redigir um ofício destinado a uma provedora de Internet, um delegado colocou as seguintes informações a respeito de uma possível captura de dados não autorizada pelo usuário de um sistema.

URL correta de acesso ao sistema	https://suaconta.com.br/suaconta.html
URL apresentada ao acessar o sistema	https://crazyserver.com.uk/suaconta.html
Porta	191.125.13.1

O usuário digitava a URL correta de acesso ao sistema no browser, e a página da Web apresentada solicitava o preenchimento dos dados e a inserção de senha do usuário para acesso ao sistema. A respeito da situação hipotética apresentada e dos aspectos técnicos e legais a ela relacionados, julgue o item a seguir.

Nesse caso, utilizava-se a estratégia de phishing para obter dados dos usuários.

32. (CESPE / TJ-PA – 2020) Texto 4A3-I: Em um espaço público ABC, um hacker instalou um ponto de acesso gratuito à Internet, do tipo wi-fi sem senha, e deu à rede o identificador ABCfree. O hacker configurou essa rede de modo que usuários que a ela se conectassem e tentassem acessar sítios de mídias sociais fossem direcionados para páginas clonadas, nas quais as credenciais de acesso dos usuários eram solicitadas. De posse dessas credenciais, um programa criado pelo hacker estabelecia conexões reais com as mídias sociais e interceptava transparentemente todas as comunicações dos usuários nas plataformas, acessando indevidamente todo o seu conteúdo.

A técnica de interceptação e acesso indevido às comunicações privadas de terceiros descrita no texto 4A3-I constitui um ataque cibernético do tipo:

a) man-in-the-middle.
b) SIM cloning.
c) IP spoofing.
d) ping of death.
e) DoS (denial of service).

33. (CESPE / TJ-PA – 2020) Assinale a opção que indica o tipo de ataque mais comumente utilizado como precursor para viabilizar ataques de ransomware contra estações de trabalho de usuários:

a) DDoS (distributed denial of service)
b) procedimento de defacement
c) ataque de phishing
d) keylogger
e) vírus

34. (CESPE / TJ-PA – 2020) Um vírus do tipo polimórfico é um vírus que se:

a) conecta a arquivos executáveis e se replica quando o programa infectado é executado.
b) aloja na memória principal como parte de um programa residente no sistema.
c) transforma a cada infecção, o que impossibilita a detecção pela assinatura do vírus.

d) espalha quando o sistema é inicializado, por infectar um registro-mestre de inicialização.
e) reescreve a cada interação, podendo mudar seu comportamento e aparência, o que aumenta a dificuldade de detecção.

35. **(CESPE / CGE - CE – 2019)** Após o envio de um e-mail pelo emissor a determinado destinatário, ocorreu uma ação maliciosa e o e-mail foi lido por terceiro. Nessa situação, a ação maliciosa é do tipo:

a) sniffing
b) spoofing
c) brute force
d) defacement
e) denial of service.

36. **(CESPE / TCE-PB – 2018)** Entre os vários tipos de programas utilizados para realizar ataques a computadores, aquele capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo entre computadores, é conhecido como:

a) Botnet.
b) Spyware.
c) Backdoor.
d) Trojan.
e) Worm.

37. **(CESPE / PM-MA – 2018)** Fazer becape regularmente é uma conduta que permite minimizar os danos decorrentes de um ataque do tipo ransomware locker, que impede o acesso ao equipamento infectado, visto que o pagamento do resgate não garante acesso aos dados.

38. **(CESPE / PM-MA – 2018)** A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

A situação III caracteriza-se mais como vírus do que como um worm, pois os vírus são responsáveis por consumir muitos recursos, ao passo que os worms permitem o retorno de um invasor ao computador comprometido.

39. (CESPE / PM-MA – 2018) A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

O ataque descrito na situação I é o ransomware, que, geralmente usando criptografia, torna inacessíveis os dados armazenados em um equipamento.

40. (CESPE / PM-MA – 2018) A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

A situação II pode ter ocorrido por meio de bot, um programa que dispõe de determinados mecanismos de comunicação com o invasor, os quais permitem que o computador invadido seja controlado remotamente, propagando a infecção de forma automática e explorando vulnerabilidades existentes em programas instalados.

41. (CESPE / PM-MA – 2018) A seguir são apresentadas três situações hipotéticas.

I Um usuário, após sequestro de seus dados, recebeu a informação de que, para reavê-los, seria necessário realizar um pagamento ao sequestrador.

II Um usuário recebeu informação, por meio do setor de segurança da informação do seu órgão, de que seu computador, sem seu conhecimento, havia sido usado em um ataque a uma rede de outro órgão.

III Em um dado momento do dia, um usuário notou que sua máquina estava consumindo mais recursos de memória do que o habitual e, ao executar no computador um programa de proteção, obteve a seguinte mensagem: "arquivo xpto infectado com o worm xyz".

Com referência a essas situações hipotéticas e à segurança da informação, julgue o item subsequente.

As três situações apresentadas poderiam ter sido evitadas se um antiadware atualizado e funcional estivesse instalado nos computadores em questão, uma vez que esse é um tipo de programa capaz de evitar infecções e ataques.

42. (CESPE / PC-MA – 2018) Determinado tipo de vírus eletrônico é ativado quando um documento por ele infectado é aberto, podendo então, nesse momento, infectar não apenas outros documentos, mas também um gabarito padrão de documento, de modo que cada novo documento criado sob esse gabarito seja infectado. Tal vírus, cuja propagação ocorre quando documentos por ele infectados são remetidos por correio eletrônico para outros usuários, é conhecido como:

a) vírus de setor de carga (boot sector).
b) vírus de programa.
c) vírus de macro.
d) backdoor.
e) hoax.

43. (CESPE / Polícia Federal – 2018) No processo conhecido como scanning, o worm, em sua fase de propagação, procura outros sistemas para infectar.

44. (CESPE / Polícia Federal – 2018) Os softwares de spyware têm como principal objetivo adquirir informações confidenciais de empresas e são usados como uma forma de espionagem empresarial.

45. (CESPE / BANCO DA AMAZÔNIA – 2018) Os vírus do tipo hoax são facilmente detectados pelas ferramentas de antivírus que utilizam técnicas de detecção por assinaturas, pois fazem uso de macros já conhecidas de vírus.

46. **(CESPE / PM-AL – 2018)** Spywares são programas instalados em computadores pessoais, capazes de identificar e remover determinados vírus, como, por exemplo, Hoax e Trojan.

47. **(CESPE / BNB – 2018)** Se um rootkit for removido de um sistema operacional, esse sistema não voltará à sua condição original, pois as mudanças nele implementadas pelo rootkit permanecerão ativas.

48. **(CESPE / BNB – 2018)** Para evitar a contaminação de um arquivo por vírus, é suficiente salvá-lo com a opção de compactação.

49. **(CESPE / Polícia Federal – 2018)** Situação hipotética: Ao processar um código executável malicioso que havia recebido como anexo de um email, Mateus percebeu que um malware havia infectado seu aparelho e que, automaticamente, havia sido enviada uma mensagem idêntica, com um anexo malicioso idêntico, a todos os contatos de sua lista de endereços, a partir do seu aparelho. Assertiva: Essa situação é um exemplo clássico de infecção de vírus de computador.

50. **(CESPE / Polícia Federal – 2018)** Um ataque de ransomware comumente ocorre por meio da exploração de vulnerabilidades de sistemas e protocolos; a forma mais eficaz de solucionar um ataque desse tipo e recuperar os dados "sequestrados" (criptografados) é a utilização de técnicas de quebra por força bruta da criptografia aplicada.

51. **(CESPE / Polícia Federal – 2018)** A infecção de um sistema por códigos maliciosos pode ocorrer
- por meio da execução de arquivos infectados obtidos de anexos de mensagens eletrônicas, de mídias removíveis, de páginas web comprometidas, de redes sociais ou diretamente de outros equipamentos.

52. **(CESPE / Polícia Federal – 2018)** A superexposição de dados pessoais nas redes sociais facilita o furto de identidade ou a criação de identidade falsa com dados da vítima, identidades essas que podem ser usadas para atividades maliciosas tais como a realização de transações financeiras fraudulentas, a disseminação de códigos maliciosos e o envio de mensagens eletrônicas falsas por email ou redes sociais.

53. **(CESPE / Polícia Federal – 2018)** Formatos comuns de arquivos, como, por exemplo, .docx ou .xlsx, são utilizados como vetor de infecção por ransomware, um tipo de software malicioso que encripta os dados do usuário e solicita resgate.

54. **(CESPE / Polícia Federal – 2018)** Cavalos de Troia são exemplos de vírus contidos em programas aparentemente inofensivos e sua ação danosa é mascarada pelas funcionalidades do hospedeiro.

55. **(CESPE / FUB – 2018)** Worms são programas maliciosos que se propagam por meio da inclusão silenciosa de cópias de si mesmos em outros programas que, ao serem executados, processam também os códigos maliciosos e infectam outros programas e sistemas.

56. (CESPE / EMAP – 2018) O ano de 2017 foi marcado por incidentes de sequestro, em diversos países, de dados de instituições, que eram encriptados; sendo essas instituições, em seguida, contatadas pelos atacantes, que solicitavam bitcoins em troca da liberação da chave criptográfica. Esses ataques foram executados por malwares categorizados como ransomwares.

57. (CESPE / STJ – 2018) Ransomware é um tipo de malware que cifra os arquivos armazenados no computador da vítima e solicita um resgate para decifrá-los.

58. (CESPE / STJ – 2018) Spoofing é uma técnica que permite ocultar a origem do endereço IP, sendo utilizada em qualquer protocolo da camada de aplicação, mas não na camada de enlace da rede.

59. (CESPE / BNB – 2018) Se um rootkit for removido de um sistema operacional, esse sistema não voltará à sua condição original, pois as mudanças nele implementadas pelo rootkit permanecerão ativas.

60. (CESPE / TRT/7 – 2017) Assinale a opção que apresenta um tipo de malware capaz de registrar as teclas que são digitadas em uma estação de trabalho, fazer capturas de tela e até mesmo acessar arquivos em drives locais e(ou) compartilhados.

a) boot
b) cavalo de troia
c) macro
d) melissa

61. (CESPE / CBM-AL – 2017) O backdoor é uma ferramenta maliciosa usada por hackers para invadir um computador e ter acesso aos arquivos e programas da máquina invadida sem autorização do seu usuário.

62. (CESPE / TRE-TO – 2017) O malware que, por meio de criptografia, torna inacessíveis os dados armazenados em um equipamento e exige pagamento de resgate para restabelecer o acesso ao usuário é do tipo:

a) ransomware.
b) backdoor.
c) cavalo de troia.
d) spyware.
e) rootkit.

63. (CESPE / TRT7 – 2017) O ataque que amplia o número de acessos a um servidor, gerando indisponibilidade de recursos aos usuários, é denominado:

a) phishing.

b) DoS.
c) spoofing.
d) adware.

64. **(CESPE / DPU – 2016)** Malwares são mecanismos utilizados para evitar que técnicas invasivas, como phishing e spams, sejam instaladas nas máquinas de usuários da Internet.

65. **(CESPE / INSS – 2016)** A infecção de um computador por vírus enviado via correio eletrônico pode se dar quando se abre arquivo infectado que porventura esteja anexado à mensagem eletrônica recebida.

66. **(CESPE / ANVISA – 2016)** Códigos maliciosos podem ter acesso aos dados armazenados no computador e executar ações em nome dos usuários, de acordo com as permissões de operação de cada um destes.

67. **(CESPE / FUB – 2016)** Enquanto estiver conectado à Internet, um computador não será infectado por worms, pois este tipo de praga virtual não é transmitido pela rede de computadores.

68. **(CESPE / TCE-PA – 2016)** A criação de discos de recuperação de sistema é útil no caso de as instalações serem malsucedidas, mas não no caso de perda de arquivos causada por infecções de vírus ou malwares.

69. **(CESPE / TRE/GO – 2015)** Botnet é uma rede formada por inúmeros computadores zumbis e que permite potencializar as ações danosas executadas pelos bots, os quais são programas similares ao worm e que possuem mecanismos de controle remoto.

70. **(CESPE / FUB – 2015)** Vírus é um programa autossuficiente capaz de se propagar automaticamente pelas redes enviando cópias de si mesmo de um computador para outro.

71. **(CESPE / TCE/RN – 2015)** O objetivo do vírus Nimda é identificar as falhas de segurança existentes nos sistemas operacionais para contaminar computadores de empresas e propagar-se.

72. **(CESPE / TJDFT - 2015)** Vírus do tipo boot, quando instalado na máquina do usuário, impede que o sistema operacional seja executado corretamente.

73. **(CESPE / TELEBRAS - 2015)** Sniffers são programas aparentemente inofensivos cuja principal característica é utilizar a técnica de mascaramento. A técnica em questão permite, por exemplo, que um sniffer seja anexado a um jogo, que, por sua vez, ao ser instalado em um computador, coletará informações bancárias do usuário.

74. **(CESPE / TELEBRAS - 2015)** Worms, assim como os vírus, são autorreplicáveis e necessitam ser executados pelos usuários para se propagarem e infectarem os computadores de uma rede.

75. **(CESPE / FUB – 2015)** O phishing é um procedimento que possibilita a obtenção de dados sigilosos de usuários da Internet, em geral, por meio de falsas mensagens de email.

76. **(CESPE / TELEBRAS – 2015)** Uma das formas de manter o aparelho de telefone celular livre de vírus é deixar o *bluetooth* habilitado constantemente, para que ele possa identificar possíveis anexos maliciosos às mensagens recebidas.

77. **(CESPE / STJ – 2015)** Os hoaxes são conhecidos como histórias falsas recebidas por email, muitas delas de cunho dramático ou religioso, com o objetivo de atrair a atenção da pessoa e então direcioná-la para algum sítio, oferecendo-lhe algo ou solicitando-lhe que realize alguma ação que possa colocar em risco a segurança de seus dados.

78. **(CESPE / TCE-RN – 2015)** A principal diferença entre crackers e hackers refere-se ao modo como esses malfeitores da área de segurança da informação atacam: os crackers são mais experientes e realizam ataques sem utilizar softwares, ao passo que os hackers utilizam códigos maliciosos associados aos softwares para realizar ataques ao ciberespaço.

79. **(CESPE / MDIC – 2014)** O comprometimento do desempenho de uma rede local de computadores pode ser consequência da infecção por um worm.

80. **(CESPE / MDIC – 2014)** Um backdoor (porta dos fundos) é um programa de computador utilizado pelo administrador de rede para realizar a manutenção remota da máquina de um usuário.

81. **(CESPE / CADE – 2014)** O computador utilizado pelo usuário que acessa salas de bate-papo não está vulnerável à infecção por worms, visto que esse tipo de ameaça não se propaga por meio de programas de chat.

82. **(CESPE / CADE – 2014)** Os vírus de computador podem apagar arquivos criados pelo editor de texto, no entanto são incapazes de infectar partes do sistema operacional, já que os arquivos desse sistema são protegidos contra vírus.

83. **(CESPE / Polícia Federal – 2014)** Phishing é um tipo de malware que, por meio de uma mensagem de email, solicita informações confidenciais ao usuário, fazendo-se passar por uma entidade confiável conhecida do destinatário.

84. **(CESPE / Polícia Federal – 2014)** Os hjackers são exemplos de códigos maliciosos que, sem que os usuários percebam, invadem computadores e, por exemplo, modificam o registro do Windows.

85. **(CESPE / FUB – 2014)** Computadores podem ser infectados por vírus mesmo que não estejam conectados à Internet.

86. **(CESPE / MEC – 2014)** A ação de worms pode afetar o desempenho de uma rede de computadores.

87. **(CESPE / MTE – 2014)** Os antivírus são ferramentas capazes de detectar e remover os códigos maliciosos de um computador, como vírus e worms. Tanto os vírus quanto os worms são capazes de se propagarem automaticamente por meio da inclusão de cópias de si mesmo em outros programas, modificando-os e tornando-se parte deles.

88. **(CESPE / TELEBRÁS – 2013)** Cavalo de troia é um tipo de programa que se instala sem conhecimento do usuário. Por meio desse programa, o invasor pode ter acesso a arquivos do computador e copiá-los, além de poder formatar o disco rígido.

89. **(CESPE / CNJ – 2013)** Vírus de macro infectam arquivos criados por softwares que utilizam linguagem de macro, como as planilhas eletrônicas Excel e os documentos de texto Word. Os danos variam de alterações nos comandos do aplicativo à perda total das informações.

90. **(CESPE / CNJ – 2013)** Vírus de script registram ações dos usuários e são gravados no computador quando da utilização de um pendrive infectado.

91. **(CESPE / TJDFT – 2013)** Backdoor é uma forma de configuração do computador para que ele engane os invasores, que, ao acessarem uma porta falsa, serão automaticamente bloqueados.

92. **(CESPE / TJDFT – 2013)** Worm é um software que, de forma semelhante a um vírus, infecta um programa, usando-o como hospedeiro para se multiplicar e infectar outros computadores.

93. **(CESPE / TRT10 – 2013)** Os programas, documentos ou mensagens passíveis de causar prejuízos aos sistemas podem ser incluídos na categoria de malwares, que podem ser divididos em três subgrupos: vírus propriamente ditos, worms e trojans ou cavalos de troia.

94. **(CESPE / TRT10 – 2013)** Arquivos anexados a mensagens de email podem conter vírus, que só contaminarão a máquina se o arquivo anexado for executado. Portanto, antes de se anexar um arquivo a uma mensagem para envio ou de se executar um arquivo que esteja anexado a uma mensagem recebida, é recomendável, como procedimento de segurança, executar um antivírus para identificar possíveis contaminações.

95. **(CESPE / TRT10 – 2013)** O vírus de computador é assim denominado em virtude de diversas analogias poderem ser feitas entre esse tipo de vírus e os vírus orgânicos.

96. **(CESPE / MPU – 2013)** Phishing é a técnica de criar páginas falsas, idênticas às oficiais, para capturar informações de usuários dessas páginas.

97. **(CESPE / PRF – 2013)** Ao contrário de um vírus de computador, que é capaz de se autorreplicar e não necessita de um programa hospedeiro para se propagar, um worm não pode se replicar automaticamente e necessita de um programa hospedeiro.

98. **(CESPE / IBAMA – 2013)** Ao salvar o arquivo em um disco removível, seu conteúdo será protegido contra vírus de macro, pois esse tipo de vírus ataca apenas arquivos no disco rígido.

99. **(CESPE / BACEN – 2013)** A recepção de respostas de mensagens que nunca foram enviadas ou que têm como destinatário o próprio remetente são indícios de falsificação de e-mail.

100. **(CESPE / BACEN – 2013)** Em relação à forma de infecção de computadores, vírus e worms são recebidos automaticamente pela rede, ao passo que trojans e backdoors são inseridos por um invasor.

101. **(CESPE / Telebras – 2013)** Malwares do tipo rootkit são difíceis de ser detectados por antivírus ou outros softwares de segurança; além disso, eles usam técnicas avançadas para infiltrar programas em processos ativos na memória do computador.

102. **(CESPE / SEGESP-AL – 2013)** Um computador que apresenta reinicializações inexplicáveis ou lentidões excessivas no processamento de comandos pode estar infectado com algum malware, como vírus ou spyware.

103. **(CESPE / PC-DF – 2013)** Malware é qualquer tipo de software que pode causar algum impacto negativo sobre a informação, podendo afetar sua disponibilidade, integridade e confidencialidade. Outros softwares são produzidos para oferecer proteção contra os ataques provenientes dos malwares. Os vírus, ao se propagarem, inserem cópias de seu próprio código em outros programas, enquanto os worms se propagam pelas redes, explorando, geralmente, alguma vulnerabilidade de outros softwares.

104. **(CESPE / PC-DF – 2013)** O uso de recursos de tecnologias da informação e das comunicações encontra-se difundido e disseminado em toda sociedade. Nesse contexto, ações de investigação criminal necessitam estar adaptadas para identificar e processar evidências digitais de modo a produzir provas materiais. Para tanto, existem diversos tipos de exames técnico-científicos utilizados em investigações. Computadores infectados com vírus não podem ser examinados em uma investigação, pois o programa malicioso instalado compromete a integridade do sistema operacional.

105. **(CESPE / PC-DF – 2013)** Rootkit é um tipo de praga virtual de difícil detecção, visto que é ativado antes que o sistema operacional tenha sido completamente inicializado.

106. **(CESPE / CPRM – 2013)** A compactação de arquivos evita a contaminação desses arquivos por vírus, worms e pragas virtuais.

107. **(CESPE / ANS – 2013)** A contaminação por pragas virtuais ocorre exclusivamente quando o computador está conectado à Internet.

108. (CESPE / Telebras – 2013) Cavalo de troia é um tipo de programa que se instala sem conhecimento do usuário. Por meio desse programa, o invasor pode ter acesso a arquivos do computador e copiá-los, além de poder formatar o disco rígido.

109. (CESPE / TRT10 – 2013) A transferência de arquivos para pendrives constitui uma forma segura de se realizar becape, uma vez que esses equipamentos não são suscetíveis a malwares.

110. (CESPE / Câmara dos Deputados – 2012) Os worms, assim como os vírus, infectam computadores, mas, diferentemente dos vírus, eles não precisam de um programa hospedeiro para se propagar.

111. (CESPE / TJ-AC – 2012) Vírus é um programa de computador malicioso capaz de se propagar automaticamente por meio de redes, mas necessita ser explicitamente executado para se propagar.

112. (CESPE / TJ-AC – 2012) Os rootkits são um conjunto de programas que oferecem mecanismos para esconder o invasor, assegurando a sua presença em um computador invadido.

113. (CESPE / Câmara dos Deputados – 2012) Um arquivo do tipo PDF não carrega código malicioso, como cavalo de troia.

114. (CESPE / Câmara dos Deputados – 2012) O Cavalo de Troia, ou Trojan Horse, é um tipo de programa de computador, geralmente enviado por email, que, quando executado, permite que o remetente tenha acesso ao computador infectado, sempre que este estiver conectado à rede.

115. (CESPE / Câmara dos Deputados – 2012) O termo phishing designa a técnica utilizada por um fraudador para obter dados pessoais de usuários desavisados ou inexperientes, ao empregar informações que parecem ser verdadeiras com o objetivo de enganar esses usuários.

116. (CESPE / FNDE – 2012) Trojans ou cavalos de troia são programas capazes de multiplicar-se mediante a infecção de outros programas maiores. Eles não têm o objetivo de controlar o sistema, porém tendem a causar efeitos indesejados. Já os worms causam efeitos altamente destrutivos e irreparáveis. Ao contrário dos trojans, os worms utilizam o email como principal canal de disseminação, mas não possuem a capacidade de produzir cópias de si mesmos ou de algumas de suas partes.

117. (CESPE / FNDE – 2012) Embora sejam considerados programas espiões, os spywares também são desenvolvidos por empresas com o objetivo de coletar legalmente informações acessíveis de usuários.

118. (CESPE / MPE-PI – 2012) Worms são programas maliciosos que se autorreplicam em redes de computadores anexados a algum outro programa existente e instalado em computadores da rede.

119. **(CESPE / Banco da Amazônia – 2012)** Os vírus do tipo mutante são capazes de modificar a estrutura de arquivos, para dificultar sua detecção por antivírus.

120. **(CESPE / IFB – 2011)** Os ataques de negação de serviços são feitos por meio de abuso da ingenuidade ou confiança do usuário.

GABARITO – CESPE

1. ERRADO
2. ERRADO
3. CORRETO
4. LETRA C
5. ERRADO
6. CORRETO
7. ERRADO
8. LETRA C
9. CORRETO
10. CORRETO
11. ERRADO
12. ERRADO
13. CORRETO
14. CORRETO
15. LETRA C
16. LETRA A
17. ERRADO
18. ERRADO
19. ERRADO
20. ERRADO
21. ERRADO
22. ERRADO
23. CORRETO
24. CORRETO
25. ERRADO
26. ERRADO
27. LETRA B
28. CORRETO
29. ERRADO
30. ERRADO
31. CORRETO
32. LETRA A
33. LETRA C
34. LETRA C
35. LETRA A
36. LETRA E
37. CORRETO
38. ERRADO
39. CORRETO
40. CORRETO
41. ERRADO
42. LETRA C
43. CORRETO
44. ERRADO
45. ERRADO
46. ERRADO
47. CORRETO
48. ERRADO
49. CORRETO
50. ERRADO
51. CORRETO
52. CORRETO
53. CORRETO
54. CORRETO
55. ERRADO
56. CORRETO
57. CORRETO
58. ERRADO
59. CORRETO
60. LETRA B
61. ANULADA
62. LETRA A
63. LETRA B
64. ERRADO
65. CORRETO
66. CORRETO
67. ERRADO
68. ERRADO
69. CORRETO
70. ERRADO
71. CORRETO
72. CORRETO
73. ERRADO
74. ERRADO
75. CORRETO
76. ERRADO
77. ANULADA
78. ERRADO
79. CORRETO
80. ERRADO
81. ERRADO
82. ERRADO
83. CORRETO
84. ANULADA
85. CORRETO
86. CORRETO
87. ERRADO
88. CORRETO
89. CORRETO
90. ERRADO
91. ERRADO
92. ERRADO
93. CORRETO
94. CORRETO
95. CORRETO
96. CORRETO
97. ERRADO
98. ERRADO
99. CORRETO
100. ERRADO
101. CORRETO
102. CORRETO
103. CORRETO
104. ERRADO
105. CORRETO
106. ERRADO
107. ERRADO
108. CORRETO
109. ERRADO
110. CORRETO
111. CORRETO
112. CORRETO
113. ERRADO
114. CORRETO
115. CORRETO
116. ERRADO
117. CORRETO
118. ERRADO
119. CORRETO
120. ERRADO

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.