Segurança da Informação: Malwares

SEDUC AM – FGV – 2014

Um Assistente Técnico recebe um e-mail com arquivo anexo em seu computador e o antivírus acusa existência de vírus.

Assinale a opção que indica o procedimento de segurança a ser adotado no exemplo acima.

A) Abrir o e-mail para verificar o conteúdo, antes de enviá-lo ao administrador de rede.

B) Executar o arquivo anexo, com o objetivo de verificar o tipo de vírus.

C) Apagar o e-mail, sem abri-lo.

D) Armazenar o e-mail na área de backup, para fins de monitoramento.

E) Enviar o e-mail suspeito para a pasta de spam, visando a analisá-lo posteriormente.

TJ TO – FGV - 2022

Há diversas medidas preventivas para manter os dispositivos computacionais protegidos contra ações de códigos maliciosos, como, por exemplo:

A) utilizar mídias removíveis, como, por exemplo, pen-drives, para a transferência de arquivos;

B) executar simultaneamente diferentes programas antimalware;

C) manter os programas instalados com as versões mais recentes e com todas as atualizações;

D) habilitar a autoexecução de arquivos anexados ao e-mail;

E) utilizar firewall pessoal em vez de antimalware.

TRE PA – FGV – 2011

Se você receber um e-mail de um remetente desconhecido, solicitando que abra um documento anexo, de nome orçamento.doc, o melhor procedimento a tomar é

A) executar o arquivo e depois submetê-lo a um antivírus.

B) apagar permanentemente o e-mail sem executar o arquivo.

C) manter o e-mail em sua caixa de entrada e só executar o arquivo quando não estiver conectado à rede.

D) mover a mensagem para a pasta Lixo Eletrônico, pois nela o antivírus é mais rigoroso.

E) aplicar regras a essa mensagem, deslocando o e-mail para uma pasta apropriada a esse remetente.

MPE-GO – FGV – 2022

João acessou seu computador e recebeu a seguinte mensagem:

> Todos os seus arquivos foram criptografados. Realize o pagamento no link indicado e receba a senha para descriptografar.

A medida de proteção que João deve tomar é instalar um programa que o proteja de ataques do tipo

A) Adware.
B) Keylogger.
C) Ransomware.
D) Vírus.
E) Backdoor.

CGE MA – FGV – 2014

A segurança na Internet constitui atualmente uma das preocupações dos administradores de redes, pelos danos que as pragas virtuais podem causar.

Nesse contexto, analise as descrições a seguir.

I. São malwares que necessitam de uma interação do usuário para infectar uma máquina. O exemplo clássico é um anexo de e-mail contendo um código executável malicioso. Se o usuário receber e abrir tal anexo, o malware será executado na máquina.

II. São malwares capazes de entrar em uma máquina sem qualquer interação do usuário. O exemplo clássico é o de um usuário que está executando uma aplicação de rede frágil para o qual um atacante pode enviar um malware, que varre a Internet em busca de outros hospedeiros que estejam executando a mesma aplicação

de rede vulnerável.

CGE MA – FGV – 2014

...

Essas descrições definem, respectivamente, os seguintes termos:

A) worm e sniffer.

B) vírus e worm.

C) proxy e vírus.

D) spyware e proxy.

E) sniffer e spyware.

IBGE – FGV – 2017

O Antivírus do departamento de tecnologia da informação de uma empresa identificou que um programa de computador invadiu máquinas de funcionários do departamento e abriu portas através das quais é possível controlar os sistemas afetados sem que os usuários percebam.

Esse tipo de ataque ou técnica encontrada pelo Antivírus é o:

A) backdoor;
B) bug;
C) bloatware;
D) dns poisoning;
E) adware.

DPE MT – FGV – 2015

A respeito das ameaças a que uma informação pode ser submetida, analise as afirmativas a seguir.

I. Vírus é um programa que se conecta a um arquivo e replica- se sem a necessidade de sua execução.

II. Worm é um programa que se conecta a um arquivo e replica- se após ser executado.

III. Cavalo de Troia é um programa disfarçado como aplicação útil.

Assinale

A) se somente a afirmativa I estiver correta.

B) se somente a afirmativa II estiver correta.

C) se somente a afirmativa III estiver correta.

D) se somente as afirmativas I e II estiverem corretas.

E) se somente as afirmativas II e III estiverem corretas.

SEPOG RO – FGV – 2017

Um usuário recebe um e-mail anônimo dizendo que o arquivo anexo, fotos.exe, contém algumas fotos antigas desse mesmo usuário. Este usuário então clica no arquivo anexo, mas nada acontece.

Sobre as razões que podem explicar esse fato, analise as afirmativas a seguir.

I. O computador do usuário não tem software instalado para a visualização de fotografias.

II. O arquivo anexo era provavelmente algum tipo de vírus que infectou a máquina do usuário.

III. O servidor de e-mails não conseguiu executar o arquivo anexo.

SEPOG RO – FGV – 2017

...

Está correto o que se afirma em

A) I, somente.

B) II, somente.

C) III, somente.

D) I e II, somente.

E) II e III, somente.

DPE MS – FGV – 2019

Com relação aos aplicativos para a segurança da informação, assinale V para a afirmativa verdadeira e F para a falsa.

( ) Firewall é um recurso baseado exclusivamente em software, que se coloca entre computadores e redes, visando impedir acessos indesejados oriundos da rede.

( ) A detecção de vírus por meio de um serviço de computação em nuvem permite a identificação de arquivos maliciosos e indesejados por múltiplos mecanismos de detecção em paralelo.

( ) Antispyware é um software de segurança que tem o objetivo de detectar e remover spywares, sendo ineficaz contra os adwares.

...

DPE MS – FGV – 2019

...

As afirmativas são, respectivamente,

A) F, V e F.

B) F, V e V.

C) V, F e F.

D) V, V e F.

E) F, F e V.

AL RO – FGV – 2018

Um vírus de computador é um software malicioso que pode causar sérios danos ao sistema infectado.

Sobre vírus de computador, assinale a afirmativa correta.

A) Adwares são vírus pacíficos utilizados para examinar as informações alheias.

B) Cavalos de Tróia são geralmente aplicativos simples que escondem funcionalidades maliciosas e alteram o sistema para permitir ataques posteriores.

C) Backdoors são vírus que restringem o acesso ao sistema infectado e cobra um resgate para que o acesso possa ser restabelecido.

D) Spywares são vírus de engenharia social que manipulam pessoas para conseguir informações confidenciais.

E) Worms são arquivos nocivos que infectam um programa e necessita deste programa hospedeiro para se espalhar.

MPE AL – FGV – 2018

Para reduzir o risco de malware, por meio do monitoramento do computador, para evitar que estes programas maliciosos modifiquem configurações do sistema operacional, deve ser usado o seguinte recurso do Windows 10:

A) VBS

B) Windows Firewall.

C) Defender.

D) BitLocker.

E) Credential Guard.

TJ DFT – FGV - 2022

João administra uma rede de computadores com muitos sistemas de informação cujas operações são de acesso restrito, pois contém informações confidenciais. Nos últimos meses, João recebeu diversos relatos de ataques de keylogger e screenlog. Diante desse cenário, João deve proteger a sua rede de ataques do tipo:

A) worm;
B) spyware;
C) botnet;
D) zumbi;
E) remote access trojan.

FUNSAÚDE CE – FGV - 2021

As ameaças virtuais representam riscos a qualquer computador conectado à internet. Os softwares que realizam ações maliciosas, publicidade indevida, coleta de informações pessoais ou alteração da configuração do computador, sem o consentimento do usuário são denominados

A) Trojan.
B) Spywares.
C) Ransonware.
D) Worm.
E) DDoS.

PREFEITURA DE NITERÓI – FGV - 2018

As falhas de segurança em sistemas operacionais ou em aplicativos podem permitir que pessoas não autorizadas acessem informações de computadores e instalem vírus ou aplicativos de controle sobre máquinas remotas.

Essas falhas de segurança são denominadas

A) DDoS.

B) Keylogging.

C) Backdoor.

D) Phishing.

E) Spyware.

COMPESA – FGV - 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.

SEPOG RO – FGV - 2017

Um programador de um sistema com autenticação de usuário, descontente com a empresa que trabalha, incluiu no código uma forma de passar por cima da autenticação convencional documentada, autenticando usuário e senha de forma programática (dentro do próprio código).

Dessa forma, o programador criou um

A) adware.

B) backdoor.

C) keylogger.

D) vírus

E) worm.

IBGE – FGV - 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.

TJ PI – FGV - 2015

Um tipo de ataque que vem se popularizando é o chamado "ransomware", que tem por característica:

A) o envio de e-mails falsos, com a finalidade de obter dados privados de usuário;

B) a combinação de ataques simultâneos a um site a partir de várias máquinas infectadas;

C) o envio de determinadas mensagens a portas específicas, procurando vulnerabilidades em função das respostas obtidas;

D) a quebra de senhas através da combinação de todas as combinações possíveis;

E) o sequestro de dados via criptografia, cobrando um "resgate" para a liberação da chave.