SPYWARE

Software espião. Monitora atividades de um sistema e envia informações para terceiros.

- Keylogger – captura teclas
- Screenlogger – captura telas
- Adware – exibe propagandas em programas

OBS: Sniffer, ferramenta de interceptação.

Prefeitura de Jataí GO - 2019

Assinale a alternativa que apresenta o programa espião que envia informações, de forma oculta, do computador do usuário (vítima) para um determinado criminoso.

a)spam
b)spyware
c)engenharia social
d)worm
e) vírus time bomb

CRO AC - 2019

Um exemplo de programa que realiza determinadas ações maliciosas com base nos resultados de uma dada condição lógica é a bomba lógica.

( ) CERTO ( ) ERRADO

Conrerp - 2019

A bomba lógica é um tipo de código malicioso embutido no malware que consegue fazer com que o computador trave ou se torne muito lento, de forma a interromper o trabalho do usuário. Contudo, esse tipo de praga virtual não consegue eliminar dados ou arquivos.

( ) CERTO ( ) ERRADO

CRO AC - 2019

Um exemplo de programa que realiza determinadas ações maliciosas com base nos resultados de uma dada condição lógica é a bomba lógica.

( ) CERTO ( ) ERRADO

PF

A fim de se proteger do ataque de um spyware — um tipo de vírus (malware) que se multiplica de forma independente nos programas instalados em um computador infectado e recolhe informações pessoais dos usuários —, o usuário deve instalar softwares antivírus e antispywares, mais eficientes que os firewalls no combate a esse tipo de ataque.

( ) CERTA ( ) ERRADA

PC PA - 2021

Qual é um tipo de praga virtual que é utilizado para gravar/registrar todas as teclas pressionadas em um teclado de forma secreta, para que a pessoa que utiliza o dispositivo não saiba que está sendo monitorada?

A) Adwares.
B) Worm.
C) Spyware.
D) Keyloggers.
E) Trojan.

Keylogger e Screenlogger são exemplos de

a) Bot, um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

b) Worm, um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente.

c) Spyware, um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

d) Vírus, um programa malicioso que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

e) Worm, 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.

CEGÁS

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

MC - 2022

Keylogger é um programa conhecido por permitir que um invasor acesse um computador diversas vezes.

( ) CERTO ( ) ERRADO

Condesus - 2022

Um spyware capaz de monitorar e enviar, para um hacker, prints e informações referentes ao posicionamento do cursor do mouse na tela do dispositivo é chamado:

A) Keylogger.
B) Adware.
C) Rootkit.
D) Screenlogger.

TRT SP

O usuário de um computador conectado à internet está se queixando que, repentinamente, começaram a aparecer janelas com anúncios na tela do computador. Considerando a possibilidade de que um malware está atacando o computador do usuário, o sintoma relatado aparenta ser a ação de um malware do tipo

a) Backdoor.
b) Adware.
c) Botnet.
d) Spyware.
e) Rootkit.

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.

CAVALO DE TRÓIA (Trojan Horse)

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.

Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Creci GO - 2019

Assinale a alternativa que apresenta o arquivo malicioso que permite que o computador do criminoso acesse remotamente outro computador, obtenha os dados confidenciais da vítima e os envie para o criminoso.

a)Keylogger
b)sniffer
c)cavalo de Troia
d)worm
e)engenharia social

IF PE- 2019

Podemos considerar diversos tipos de Trojans, que são classificados de acordo com sua ação maliciosa e, usualmente, executam-se ao infectar o computador. O Trojan Backdoor tem a capacidade de

a) possibilitar que o computador seja utilizado para navegação anônima e para envio de spam.

b)possibilitar o acesso remoto do atacante ao computador.

c)coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.

d) redirecionar a navegação do usuário para sites específicos.

e)instalar ferramentas de negação de serviço e as utilizar para desferir ataques.

MPE AL

Para realizar a contabilidade de sua pequena empresa, Beth acessou a Internet e fez o download de um programa de calculadora. Ao executar o programa, Beth observou que diversos arquivos foram excluídos do seu computador e, com isso, percebeu que foi vítima de um malware.

O tipo de programa de comando útil, ou aparentemente útil, executado por Beth, contendo código oculto que, quando invocado, realiza alguma função indesejada ou prejudicial, é o

a) adware.
b) backdoors.
c) keylogger.
d) cavalo de Troia.
e) spyware.

BACKDOOR (porta dos fundos)

Backdoor 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.

IF BA - 2019

As pragas virtuais presentes na Internet representam um grande risco para os usuários. São uma ameaça constante e severa, pois variações destas pragas são criadas diariamente por pessoas mal-intencionadas, o que compromete a segurança dos dados pessoais na rede mundial. A respeito dos diferentes tipos de pragas virtuais, assinale a alternativa que indique corretamente o nome da praga de difícil detecção e responsável por conseguir acesso não autorizado e controle remoto a um computador.

a)keyloggers
b)ransomwares
c)backdoors
d)botnets
e)spam

BANRISUL

Considere as afirmações abaixo sobre os diferentes tipos de códigos maliciosos.

I - Técnicas como ofuscação e polimorfismo são utilizadas por atacantes para dificultar a análise de um código malicioso.

II - Um Spyware pode capturar dados bancários inseridos pelo usuário em um sistema comprometido.

III - Ransomware é um tipo de código malicioso que exige pagamento de resgate para restabelecer o acesso de dados armazenados em um dispositivo.

IV - Backdoor é um código malicioso que permite o retorno de um atacante a um sistema comprometido.

V - RootKit é um código malicioso que tem por objetivo ocultar as atividades do invasor no sistema comprometido.

BANRISUL

Quais estão corretas?

a) Apenas III, IV e V.
b) Apenas I, II, III e IV.
c) Apenas I, II, IV e V.
d) Apenas I, III, IV e V.
e) I, II, III, IV e V.

Creci GO - 2019

Um vírus polimórfico é um vírus que muda a cada infecção, impossibilitando a detecção por sua assinatura.

( ) CERTO ( ) ERRRADO

ROOTKIT

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.

- 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.

AL RO

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 alastrar.

MC - 2022

Rootkit é um programa malicioso conhecido por apresentar propagandas.

( ) CERTO ( ) ERRADO

TCE PA

Um Rootkit, software que permite ao atacante obter controle administrativo na máquina infectada, pode ser removido por qualquer antivírus com base em assinatura, haja vista ser de fácil detecção.

( ) CERTO ( ) ERRADO

TCE PA

A característica de um Rootkit é

a) roubar informações do usuário como senhas e arquivos confidenciais.

b) injetar um código malicioso na máquina infectando os acessos à Internet.

c) camuflar-se para impedir que seu código seja encontrado por um antivírus.

d) enviar spam e códigos maliciosos a todos os usuários autenticados no servidor.

e) omitir arquivos e pastas de usuários, dando a impressão de que foram excluídas.

CRB - 2019

Assinale a alternativa que apresenta os programas que invadem o computador sem que o usuário perceba e modificam o registro do Windows, "sequestrando" o navegador, alterando a página inicial dele e fazendo com que apareçam novas barras e botões.

a)keyloggers
b)backdoors
c)rootkits
d)hijackers
e) macros

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.

UFMT - 2019

A tabela abaixo apresenta um resumo comparativo das ações maliciosas mais comuns de quatro tipos de códigos maliciosos (malware) representados pelas colunas numeradas de 1 a 4.

De acordo com a figura, assinale a alternativa que associa corretamente cada coluna ao tipo de malware caracterizado.

Códigos Maliciosos				
Ações maliciosas mais comuns:				
	1	**2**	**3**	**4**
Altera e/ou remove arquivos	✓		✓	
Consome grande quantidade de recursos		✓		
Furta informações sensíveis			✓	✓
Instala outros códigos maliciosos		✓	✓	
Possibilita o retorno do invasor				
Envia *spam* e *phishing*				
Desfere ataques na Internet		✓		
Procura se manter escondido	✓			✓

UFMT - 2019

a)1-Cavalo de Troia, 2-Worm, 3-Vírus, 4-Spyware
b)1-Vírus, 2-Worm, 3-Cavalo de Troia, 4-Spyware.
c)1-Worm, 2-Spyware, 3-Cavalo de Troia, 4-Vírus.
d)1-Vírus, 2-Cavalo de Troia, 3-Spyware, 4-Worm.

Códigos Maliciosos				
Ações maliciosas mais comuns:				
	1	**2**	**3**	**4**
Altera e/ou remove arquivos	✓		✓	
Consome grande quantidade de recursos		✓		
Furta informações sensíveis			✓	✓
Instala outros códigos maliciosos		✓	✓	
Possibilita o retorno do invasor				
Envia *spam* e *phishing*				
Desfere ataques na Internet		✓		
Procura se manter escondido	✓			✓

Sanasa Campinas - 2019

Considere as características de pragas virtuais, abaixo.

I. 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.

II. É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, ela depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

Sanasa Campinas - 2019

III. É um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para 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.

Os itens I, II e III descrevem corretamente um

a)worm – vírus e spyware.
b)botnet – trojan e rootkit
c)backdoor – worm e adware
d)vírus – spyware e botnet.
e)trojan – vírus e rootkit.

PCBA - 2022

Dado os três conceitos técnicos abaixo, assinale a alternativa que corresponda, respectivamente, a cada um desses conceitos especificamente.

1. Vírus que cria cópias em outras unidades ou nos computadores de uma rede para executar ações maliciosas.
2. Esse malware é como uma porta criada a partir de um programa cuja instalação não foi autorizada pelo usuário, que explora as vulnerabilidades ali existentes e permite que terceiros tenham acesso à máquina.
3. Método que tenta "pescar" vítimas para que cliquem em links ou baixem arquivos com o objetivo de adquirir informações pessoais.

...

PCBA - 2022

...

A) 1.Worm - 2.Backdoor - 3.Phishing
B) 1.Backdoor - 2.Worm - 3.Phishing
C) 1.Worm - 2.Phishing - 3.Backdoor
D) 1.Phishing - 2.Backdoor - 3.Worm
E) 1.Phishing - 2.Worm - 3.Backdoor

OBRIGADO

Prof. Renato da Costa
@prof.renatodacosta