Segurança da Informação: Malwares

Prof. Renato da Costa

MALWARES (Softwares Maliciosos)

Códigos maliciosos (malware) são programas especialmente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas instalados;

- pela auto execução de mídias removíveis infectadas, como pen-drives;
- pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;
- 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 diretamente de outros computadores (através compartilhamento de recursos).

CRN PE - 2022

Uma forma de se prevenir contra os códigos maliciosos é não clicar links recebidos por outras pessoas, nem mesmo os recebidos por pessoas confiáveis, uma vez que não podem ser considerados totalmente seguros.

( ) CERTO ( ) ERRADO

MSGAS - 2021

Sobre malware, verifique as assertivas e assinale a correta.

I. Em inglês malware é abreviação de "malicious software".

II. Trata-se de um código malicioso, programa malicioso, software nocivo, software malintencionado ou software malicioso.

III. É um programa de computador destinado a infiltrarse em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

A) Apenas as assertivas II e III são corretas.

B) As assertivas I, II e III são corretas.

C) Apenas as assertivas I e II são corretas.

D) Apenas as assertivas I e III são corretas.

MC - 2022

Malware é qualquer software intencionalmente criado para causar danos a um computador, servidor, cliente ou a uma rede de computadores.

( ) CERTO ( ) ERRADO

Prefeitura de Carnaíba – 2019

Pode-se afirmar que são tipos de códigos maliciosos (malware), EXCETO

a)vírus.
b)worm.
c)spyware.
d)firewall.

Prefeitura de Pedro Rosário – 2019

Malware (abreviação de "software malicioso") é qualquer software desenvolvido para a finalidade de fazer mal a um sistema de computador. A ameaça de software mal-intencionado facilmente pode ser considerada como a maior ameaça à segurança da Internet. Anteriormente, vírus foram, mais ou menos, a única forma de malware. Hoje em dia, a ameaça tem crescido para incluir network-aware worms, cavalos de Tróia, spyware, adware e assim por diante. Existem muitos tipos diferentes de Malware, são exemplos, exceto:

a)Propagação de vírus & Worms.
b)Cavalo de Tróia.
c)Spyware.
d)Machine Learning.

MALWARE		
VÍRUS	Se propaga se anexando a arquivos ou programas existentes na máquina (hospedeiro)	**SE PROPAGA**
WORM	Se propagam através da exploração de vulnerabilidades e de conexões de rede (independente).	**SE PROPAGA**
BOT	Se propagam através da exploração de vulnerabilidades e de conexões de rede (independente).	**SE PROPAGA**
RANSOMWARE	Através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link; ou se propagam através da exploração de vulnerabilidades e de conexões de rede.	**SE PROPAGA**
CAVALO DE TRÓIA		**NÃO SE PROPAGA**
SPYWARE		**NÃO SE PROPAGA**
BACKDOOR		**NÃO SE PROPAGA**
ROOTKIT		**NÃO SE PROPAGA**

VÍRUS

Se propaga se inserindo em arquivos ou programas existentes na máquina, para que seu computador seja infectado depende da execução do programa ou arquivo hospedeiro.

SEDU ES

Vírus é um programa que pode se reproduzir anexando seu código a um outro programa, da mesma forma que os vírus biológicos se reproduzem.

( ) CERTO ( ) ERRADO

CRESS DF - 2021

I Um vírus se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Se um usuário receber um arquivo com vírus e não executar o arquivo, seu computador não será contaminado. II Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro.

As afirmações acima referem-se a vírus, uma das categorias de malware. Considerando as duas afirmações, assinale a alternativa correta.

A) As duas são verdadeiras e a segunda é a justificativa correta da primeira.

B) A primeira é verdadeira e a segunda é falsa.

C) As duas são falsas.

D) A segunda é verdadeira, mas não é a justificativa correta da primeira.

E) A primeira é falsa e a segunda é verdadeira.

Tempo de vida de um vírus:

- Fase latente – vírus inativo, será ativado por algum evento.
- Fase de propagação – vírus coloca cópias idênticas de si mesmo em outros arquivos.
- Fase de disparo – o vírus é ativado para realizar a função a qual ele foi planejado (assim como na fase latente será ativado a partir de eventos quaisquer, tais como uma data, contagem do número de vezes de replicação, etc.).
- Fase de execução – A função é realizada.

TIPOS DE VÍRUS:

- Vírus de boot
- Vírus de programa/arquivo
- Vírus de macro
- Vírus polimórfico/mutante
- Vírus stealth/furtivo
- Vírus time-bomb
- Vírus Fileless

CRF RJ

Acerca dos tipos de vírus, analise as seguintes afirmativas.

I. Os vírus de arquivos infectam arquivos de programas e arquivos criados por usuários.

II. Os vírus de macro são vírus que tem seu código fonte (linhas de comando) criptografado, ou seja, os caracteres da programação são alterados para outros caracteres.

III. Os vírus de boot infectam os arquivos de inicialização do sistema, escondendo-se no primeiro setor do disco e são carregados na memória antes do sistema operacional.

De acordo com as afirmativas acima, marque a alternativa correta.

a) Apenas as afirmativa I está correta.
b) Apenas as afirmativas I e II estão corretas.
c) Apenas as afirmativas I e III estão corretas.
d) Apenas as afirmativas II e III estão corretas.

PC MA

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

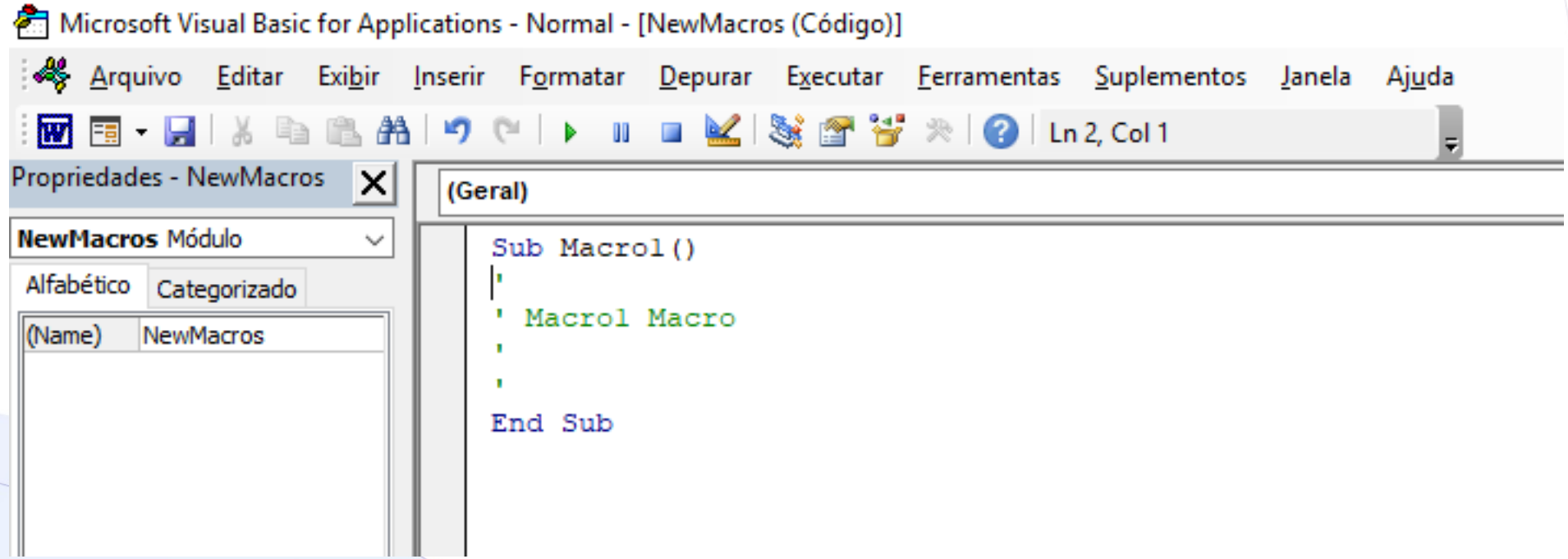
a) vírus de programa.
b) vírus de macro.
c) backdoor.
d) hoax.
e) vírus de setor de carga (boot sector).

PREFEITURA MUNICIPAL DE VITÓRIA ES

Um programa do tipo vírus é, tipicamente, capaz de se duplicar e se inserir em programas ou em arquivos. Alguns vírus são escritos nas linguagens de comando de programas como editores de texto.

( ) CERTO ( ) ERRADO

OBS: MACRO – Criada em aplicativos de escritório, tais como editores de texto, planilhas eletrônicas, softwares de apresentação, correspondem a uma sequência de comandos para automatização de tarefas, podendo ser associada a um atalho de teclado, botão ou evento, a depender do aplicativo.



BANCO DO BRASIL

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.

Banrisul - 2019

Um Escriturário recebeu por e-mail um arquivo infectado com vírus. Esse vírus

a)já infectou o computador, assim que a mensagem foi recebida.

b)infectará o computador, se o Escriturário executar (abrir) o arquivo.

c)infectará o computador, se o Escriturário abrir a mensagem de e-mail.

d)não infectará o computador, pois todas as ferramentas de e-mail são programadas para remover vírus automaticamente.

e)infectará o computador, se o Escriturário baixar o arquivo, mesmo que ele não o execute.

TCU

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.

( ) CERTO ( ) ERRADO

MTE

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.

( ) CERTO ( ) ERRADO

STJ

Fileless malware tem por principal característica a ocultação do endereço de entrada localizado no setor de início do ponto de montagem do sistema de arquivo do disco rígido.

( ) CERTO ( ) ERRADO

WORM (Verme)

Diferentemente do vírus não se insere em arquivos ou programas existentes na máquina, sendo capaz de se propagar automaticamente cópias pela rede, enviando cópias de si mesmo de computador para computador.

Write
Once
Read
Many

Congestionam a rede!!!

Prefeitura de Cruz das Almas BA - 2019

Malware são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

A alternativa que contém o programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador, é denominado

a)Worm.
b) Backdoor.
c)Keylogger.
d)Ransomware.
e)Cavalo de Troia.

CRT 04 - 2021

O verme (worm) consegue fazer com que um computador infectado consiga, por meio da Internet, infectar outros computadores.

( ) CERTO ( ) ERRADO

Crea GO - 2019

Um worm é um programa disfarçado que invade os sistemas com um único objetivo: publicidade. Esse tipo de vírus é inofensivo e não causa nenhum tipo de problema para a rede de computadores.

( ) CERTO ( ) ERRADO

IFSP

Qual a diferença entre vírus e worms?

a) Não há diferença, ambos se referem ao mesmo tipo de malware
b) Worms não tem o poder de se auto-duplicar
c) Worms não precisam de um arquivo hospedeiro para infectar
d) Vírus não precisam de um arquivo hospedeiro para infectar
e) Vírus não tem o poder de se auto-duplicar

UFRPE

Existem diversos tipos de códigos maliciosos (vírus, worm, trojan etc.), com diferentes características. É correto afirmar que um worm:

a) executa as funções para as quais foi aparentemente projetado, além de executar outras funções.

b) é uma rede formada por centenas ou milhares de equipamentos zumbis.

c) é capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de um equipamento para outro.

d) permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.

e) possui mecanismos de comunicação com o invasor que permitem que este seja controlado.

Bot (Robot)

Dispõe de mecanismos de comunicação com o invasor que permite o controle do computador remotamente, tornando a máquina uma "máquina zumbi". Se propaga de maneira similar ao worm.
Um conjunto de computadores infectados por um Bot caracteriza uma Botnet, o aumento de máquinas infectadas contribui para maior eficácia e impacto nos ataques.

TJ RS

Como se denomina o tipo de malware capaz de se propagar de forma autônoma, isso é, sem intervenção humana, explorando vulnerabilidades ou falhas de configuração de softwares instalados em computadores e que pode ser controlado remotamente por um atacante?

a) Virus
b) Spyware
c) Backdoor
d) Bot
e) Verme

PROCON RJ

Com o objetivo de impedir a atividade de programas maliciosos, sites da área bancária e financeira têm implementado um mecanismo de segurança que gera uma imagem com combinações de quatro dígitos aleatórios e que deverão ser digitadas pelos usuários para validação das transações, como exemplificado na figura .

Esse mecanismo é conhecido por:

A) sniffer
B) captcha
C) hijacker
D) phishing
E) spoofing

RANSOMWARE

Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

O ransomware pode se propagar de diversas formas, embora as mais comuns sejam:

- através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link;
- explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Como ocorre a infecção?

O *ransomware* pode se propagar de diversas formas, embora as mais comuns sejam:

- através de *e-mails* com o código malicioso em anexo ou que induzam o usuário a seguir um *link*;
- explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

O mais importante é evitar ser infectado, veja a seguir como se proteger.

Existem dois tipos de ransomware:

- Ransomware Locker: impede que você acesse o equipamento infectado.

- Ransomware Crypto: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

O que é o WannaCry?

O ransomware WannaCry visa redes que usam SMBv1, um protocolo que ajuda PCs a se comunicarem com impressoras e outros dispositivos conectados na rede. Essa versão, que vem de 2003, deixa computadores expostos a hackers, uma vulnerabilidade chamada MS17-010. A Microsoft lançou um patch para corrigi-la em março para as versões do Windows que ainda têm suporte, mas qualquer pessoa que não tenha instalado o patch tornou-se um alvo fácil para os hackers que criaram o WannaCry.

Conhecido também como WanaCrypt0r 2.0 ou WCry, o WannaCry tira proveito de PCs que usam Windows para criptografar arquivos e impedir que os usuários os acessem, a menos que paguem US$ 300 em bitcoins em 3 dias. Depois disso, o preço dobra.

https://www.avast.com/pt-br/c-wannacry

TRT PE

Um dos malwares mais nocivos e difundidos atualmente é o ransomware, que atua por meio de algumas formas. O mais comum deles é o que permite o acesso ao equipamento infectado, mas impede o acesso aos dados armazenados. Esse tipo de ransomware é conhecido como

a) Locker.
b) Scareware.
c) Doxware.
d) Leakware.
e) Crypto.

IBGE - 2019

O tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, usando geralmente criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário é o:

a) Backdoor;
b) Cavalo de troia (trojan);
c) Ransomware;
d)Spyware;
e)Keylogger.

OBS: BITCOIN - é uma criptomoeda descentralizada, sendo uma forma de dinheiro eletrônico.

ANO	BITCOIN	DÓLAR	REAL
2009	1 BTC	U$ 0.0001	R$ 0.001
2010	1 BTC	U$ 0.07	R$ 0.21
2011	1 BTC	U$ 15,00	R$ 40,00
2012	1 BTC	U$ 7,00	R$ 21,00
2013	1 BTC	U$ 100,00	R$ 300,00
2014	1 BTC	U$ 600,00	R$ 1.800
2015	1 BTC	U$ 220,00	R$ 700,00
2016	1 BTC	U$ 600,00	R$ 1,800
2017 (JAN)	1 BTC	U$ 1.000	R$ 3.200
2017 (DEZ)	1 BTC	U$ 7.100	R$ 35.000
2018*	1 BTC	U$ 8.500	R$ 55.500

bitcoinvestimento.blogspot.com

PF

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.

( ) CERTA ( ) ERRADA

PRF - 2021

Ransomware é um programa malicioso de computador que se propaga por meio da inserção de cópias de si mesmo em arquivos criptografados.

( ) CERTA ( ) ERRADA