MALWARE

1 - SPYWARE
2 - VÍRUS
3 - WORM
4 - BACKDOOR
5 - TROJAN HORSE
6 - BOT
7 - RANSOMWARE

7 - RANSOMWARE

HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

7 – RANSOMWARE LOCKER

HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

7 – RANSOMWARE CRYPTO

HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

MALWARE

1 - SPYWARE

2 - VÍRUS

3 - WORM

4 - BACKDOOR

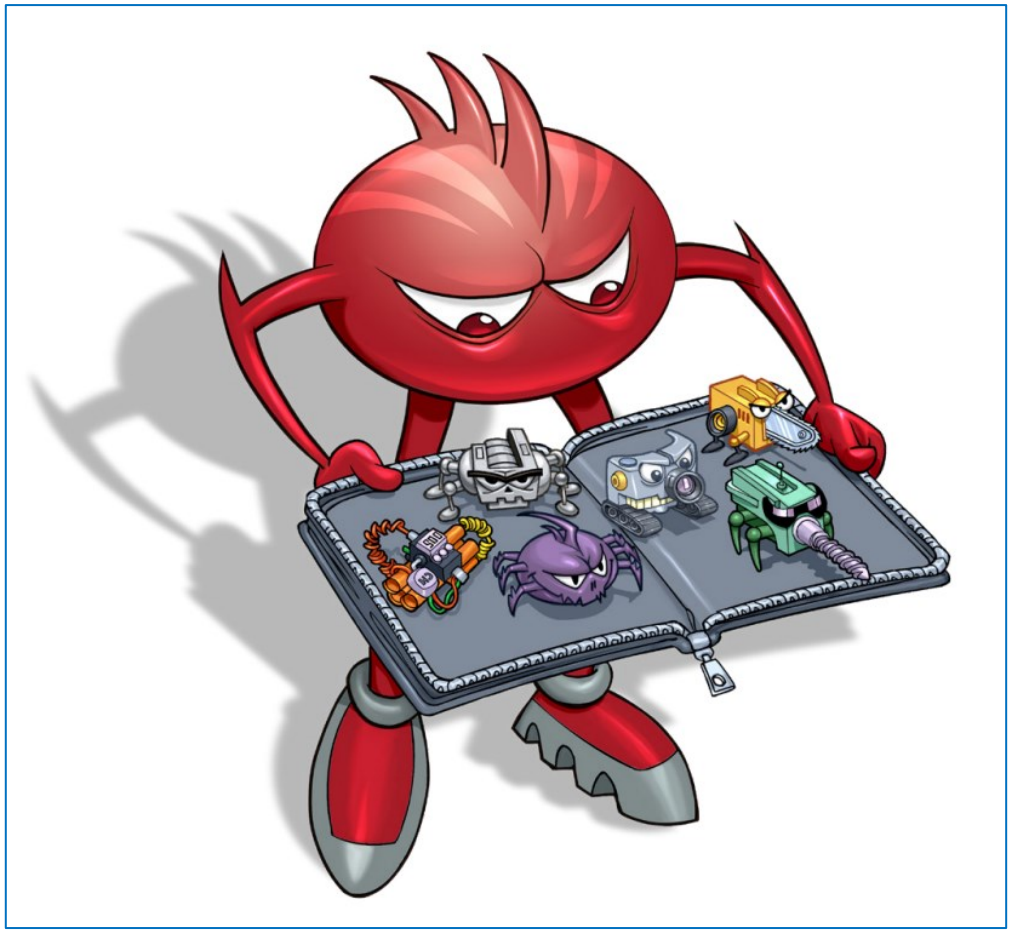
5 - TROJAN HORSE

6 - BOT

7 - RANSOMWARE

8 - ROOTKIT

8 - ROOTKIT

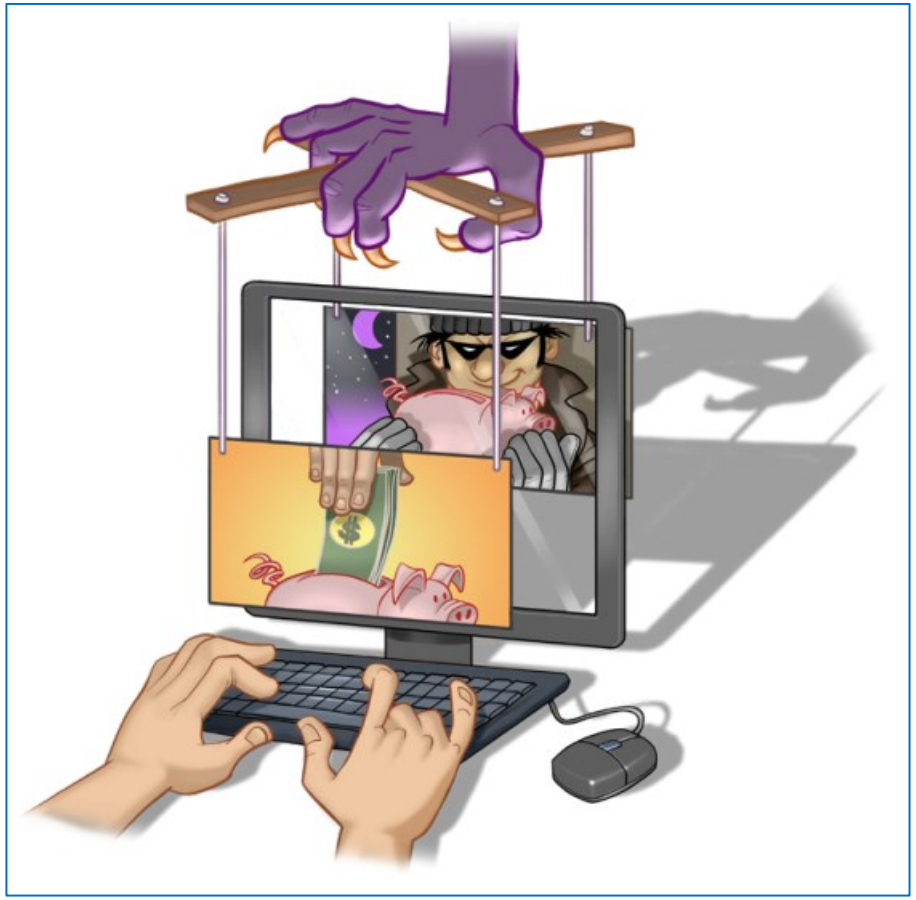


HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

MALWARE

1 - SPYWARE
2 - VÍRUS
3 - WORM
4 - BACKDOOR
5 - TROJAN HORSE
6 - BOT
7 - RANSOMWARE
8 - ROOTKIT
9 - RAT

9 – RAT(REMOTE ACCESS TROJAN)



HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

MALWARE

1 - SPYWARE
2 - VÍRUS
3 - WORM
4 - BACKDOOR
5 - TROJAN HORSE
6 - BOT
7 - RANSOMWARE
8 - ROOTKIT
9 - RAT
10 - SCAREWARE

10 – SCAREWARE

HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

MALWARE

1 - SPYWARE
2 - VÍRUS
3 - WORM
4 - BACKDOOR
5 - TROJAN HORSE
6 - BOT
7 - RANSOMWARE
8 - ROOTKIT
9 - RAT
10 - SCAREWARE
11 - STALKERWARE

11 – STALKERWARE

HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

1) Q3219334 Ano: 2024 Banca: Objetiva ConcursosProva: Objetiva Concursos - FEAES

Em relação aos diversos tipos de vírus de computadores e suas definições, numerar a 2ª coluna de acordo com a 1ª e, após, assinalar a alternativa que apresenta a sequência CORRETA:

(1) Vírus de boot.

(2) Vírus de macro.

(3) Vírus stealth.

( ) Corrompe os arquivos de inicialização do sistema operacional, impedindo que ele seja inicializado corretamente.

( ) É um vírus que se camufla do antivírus durante a varredura da memória, impedindo que este o detecte.

( ) São procedimentos gravados pelo usuário para realizar tarefas repetitivas nos arquivos do MS Office e LibreOffice.

A) 3 - 2 - 1.

B) 1 - 3 - 2.

C) 3 - 1 - 2.

D) 2 - 1 - 3.

2) Q2982040 Ano: 2023 Banca: Objetiva Concursos Prova: Objetiva Concursos - Prefeitura de Canoas

Com relação aos perigos existentes ao navegar na internet, os softwares Keyloggers são conhecidos por:

A) Gravar tudo o que é digitado nos computadores invadidos.

B) Filmar utilizando a câmera do usuário do computador.

C) Capturar dados por meio de mensagens recebidas em e-mails.

D) Tirar fotos utilizando a câmera do celular invadido.

E) Deletar todos os arquivos existentes nos computadores invadidos.

3) Q3303893Ano: 2024 Banca: Fundação Carlos Chagas – FCC Prova: FCC - BAHIAGÁS - Analista de Processos Organizacionais

Considere as seguintes características dos códigos maliciosos (malwares) I e II:

I. Propaga-se automaticamente pelas redes, explorando vulnerabilidades nos sistemas e aplicativos instalados e enviando cópias de si mesmo de dispositivo para dispositivo. É responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho de redes e a utilização de dispositivos.

II. Usa técnicas de engenharia social para assustar e enganar o usuário, fazendo-o acreditar na existência de um problema de segurança em seu dispositivo e oferecendo uma solução para corrigi-lo, mas que, na verdade, poderá comprometê-lo. Exemplos são janelas de pop-up que informam que o dispositivo está infectado e, para desinfetá-lo, é preciso instalar um (falso) antivírus, que é, na verdade, um código malicioso.

Os itens I e II referem-se, correta e respectivamente, a

A) rootkit e Scareware.

B) worm e bot.

C) worm e Scareware.

D) botnet e worm.

E) scareware e phishing.

4) Q3077929 ANO: 2023 BANCA: CEBRASPE PROVA: PM PA - OFICIAL

A proteção dos arquivos armazenados em um computador depende tanto das ações do usuário quanto de softwares específicos. Nesse sentido, é correto afirmar que

A) softwares antivírus deixam o computador imune a phishing.

B) firewall, assim como antivírus, é um software que evita que o computador seja contaminado com softwares maliciosos.

C) malwares são softwares de segurança usados para proteger seu sistema contra ameaças virtuais.

D) os vírus não dependem de um hospedeiro ou de uma ação humana para contaminar um computador e se espalhar por ele.

E) ransomware é uma ameaça digital que bloqueia o acesso aos arquivos do computador.

5) Q2676498 ANO: 2023 BANCA: IFMT PROVA: TÉCNICO DE LABORATÓRIO

Leia as sentenças abaixo.

I. programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento.

II. conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um equipamento comprometido.

III. programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

IV. programa que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado.

As sentenças dizem respeito a códigos maliciosos e são, respectivamente, as definições de:

A) Vírus, Worm, Bot e Rootkit.

B) Botnet, Ramsonware, Trojan e Worm.

C) Rootkit, Vírus, Trojan e Botnet.

D) Worm, Rootkit, Backdoor e Bot.

E) Trojan, Worm, Vírus e Rootkit.

6) Q2703171 ANO: 2023 BANCA: CEBRASPE PROVA: POLC AL

RAT (Remote Access Trojan) é um programa que combina as características de trojan e de backdoor, possibilitando ao atacante acessar o equipamento remotamente e executar ações como se fosse o legítimo usuário.

CERTO

7) Q2982372 Ano: 2023 Banca: BRB Assessoria e Concursos Prova: BRB Assessoria e Concursos

Malware, ou “software malicioso,” é um termo mais amplo que descreve qualquer programa ou código malicioso que seja prejudicial aos sistemas. Dentre eles, temos o Adware, que é:

A) É um malware que registra todo pressionamento de tecla do usuário, geralmente armazenando as informações obtidas e enviando-as ao invasor, o qual está procurando por informações sensíveis como nomes de usuário, senhas ou detalhes de cartões de crédito.

B) São um tipo de malware semelhante aos vírus, que se multiplicam a fim de se espalharem para outros computadores através de uma rede, geralmente causando danos e destruindo dados e arquivos.

C) É um software indesejado projetado para jogar anúncios em sua tela, na maioria das vezes dentro de um navegador da web.

D) É o malware que secretamente observa as atividades do usuário do computador sem permissão e passa informações ao autor do software.

E) É um malware que se anexa a outro programa e, quando executado - geralmente inadvertidamente pelo usuário - se reproduz modificando outros programas de computador e infectando-os com seu próprio código.

8) Q3349643 Ano: 2024 Banca: Fundação Carlos Chagas – FCC Prova: CETESB - Analista Administrativo

Um funcionário descobriu que em um equipamento estava instalado um malware projetado para espionar o dono do dispositivo, que não o havia autorizado, não sabia que tal código estava instalado e nem sabia que as informações coletadas estavam sendo enviadas para quem o instalou ou induziu sua instalação. Este malware é:

A) stalkenware.

B) scareware.

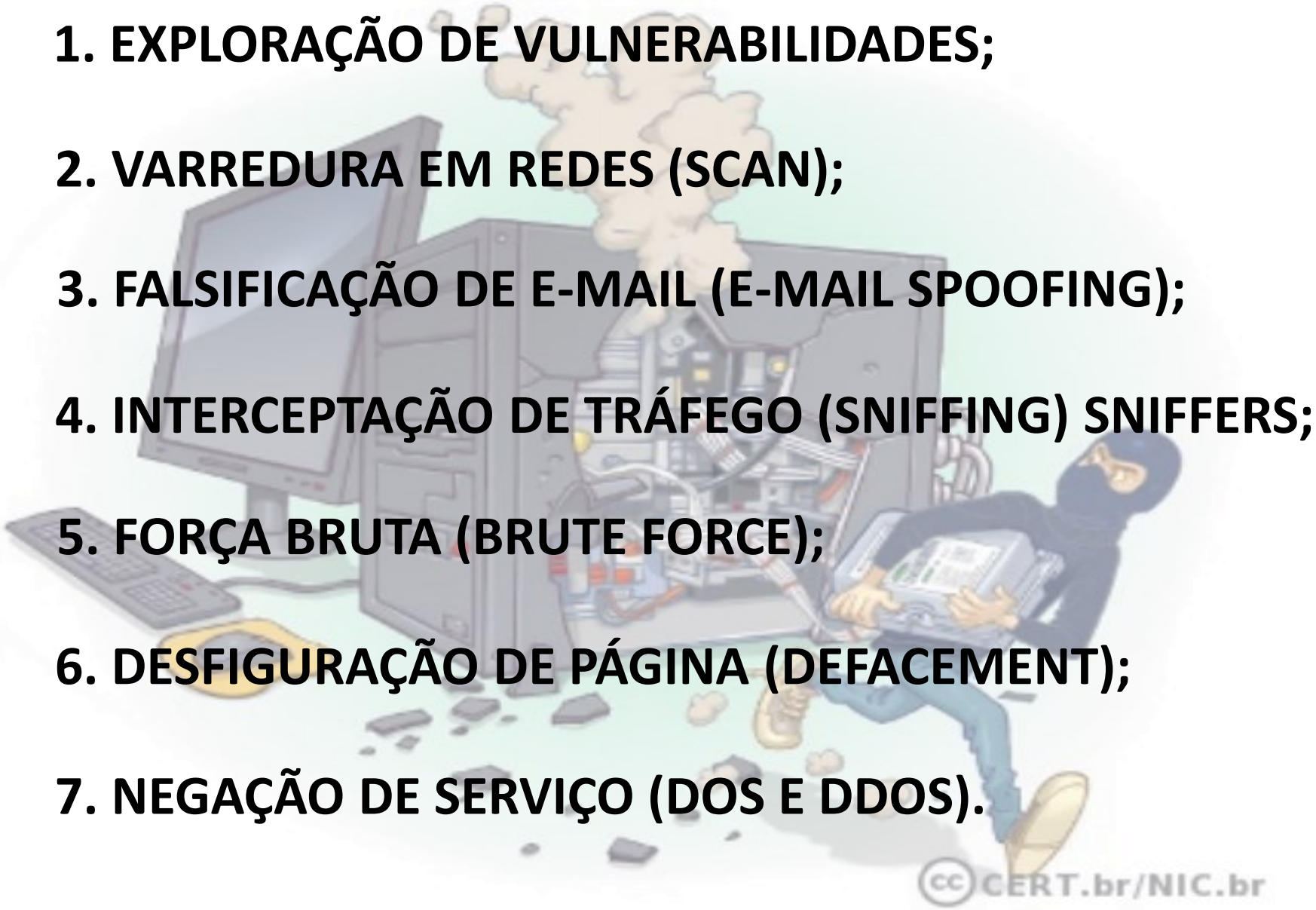
C) worm.

D) zumbi.

E) rat.

ATAQUES

HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF



1. EXPLORAÇÃO DE VULNERABILIDADES;

2. VARREDURA EM REDES (SCAN);

3. FALSIFICAÇÃO DE E-MAIL (E-MAIL SPOOFING);

4. INTERCEPTAÇÃO DE TRÁFEGO (SNIFFING) SNIFFERS;

5. FORÇA BRUTA (BRUTE FORCE);

6. DESFIGURAÇÃO DE PÁGINA (DEFACEMENT);

7. NEGAÇÃO DE SERVIÇO (DOS E DDOS).

9) Q3061188 Ano: 2023 Banca: VUNESP Prova: PC SP - Investigador de Polícia

O(A) _____ é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga. São feitos geralmente para forçar o sistema vítima a reinicializar ou consumir todos os recursos (como memória ou processamento, por exemplo) de forma que ele não possa mais fornecer seu serviço.Assinale a alternativa que preenche corretamente a lacuna do enunciado.

A) spoofing

B) phishing

C) Ataque de negação de serviço (DoS)

D) ransomware

E) engenharia social