MALWARE

1 - SPYWARE

2 - VÍRUS

2 - VÍRUS

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

2.1 – VÍRUS DE BOOT

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

2.2 – VÍRUS DE MACRO

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

2.3 – VÍRUS DE POLIMÓRFICO

- ✓ **ALTERA SUA ASSINATURA, MAS MANTÉM SUA FUNCIONALIDADE.**

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

2.3 – VÍRUS DE METAMÓRFICO

- ✓ **ALTERA SUA ASSINATURA E SUA FUNCIONALIDADE.**

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

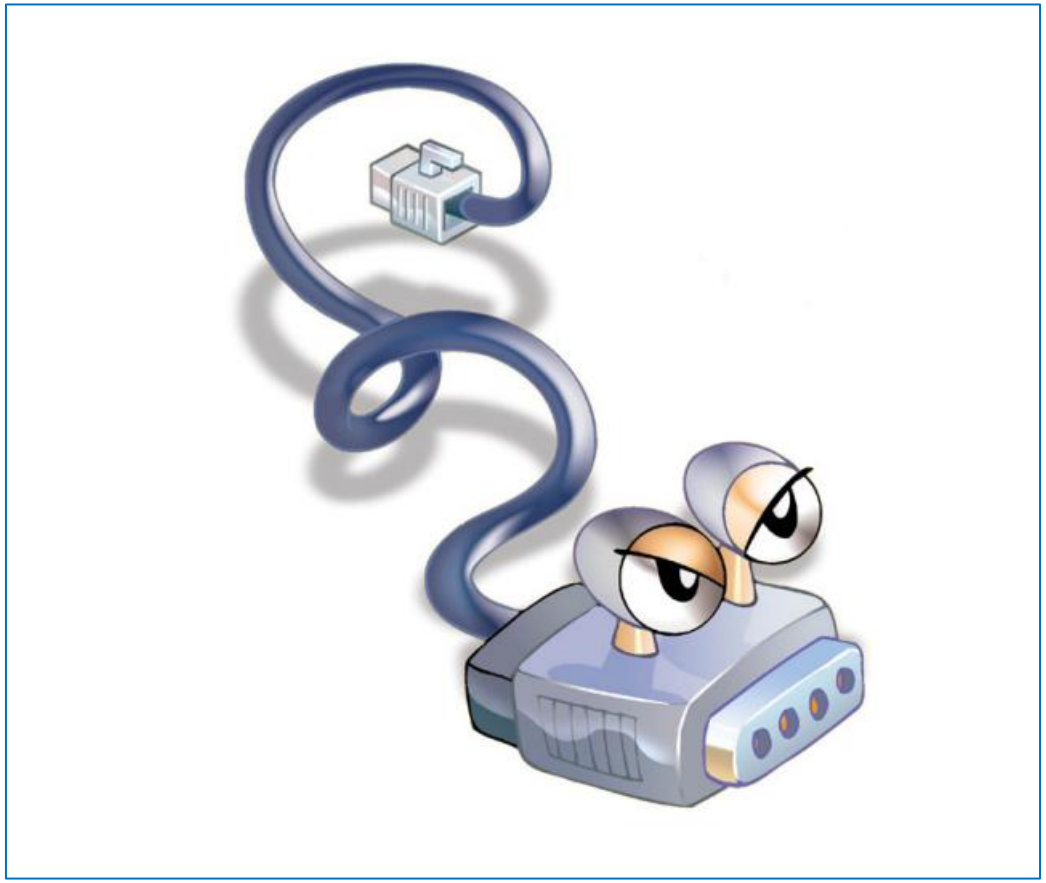
MALWARE

1 - SPYWARE

2 - VÍRUS

3 - WORM

3 - WORM



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

MALWARE

1 - SPYWARE

2 - VÍRUS

3 - WORM

4 - BACKDOOR

4 - BACKDOOR

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

MALWARE

1 - SPYWARE

2 - VÍRUS

3 - WORM

4 - BACKDOOR

5 - TROJAN HORSE

5 – TROJAN HORSE (CAVALO DE TRÓIA)

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

MALWARE

1 - SPYWARE

2 - VÍRUS

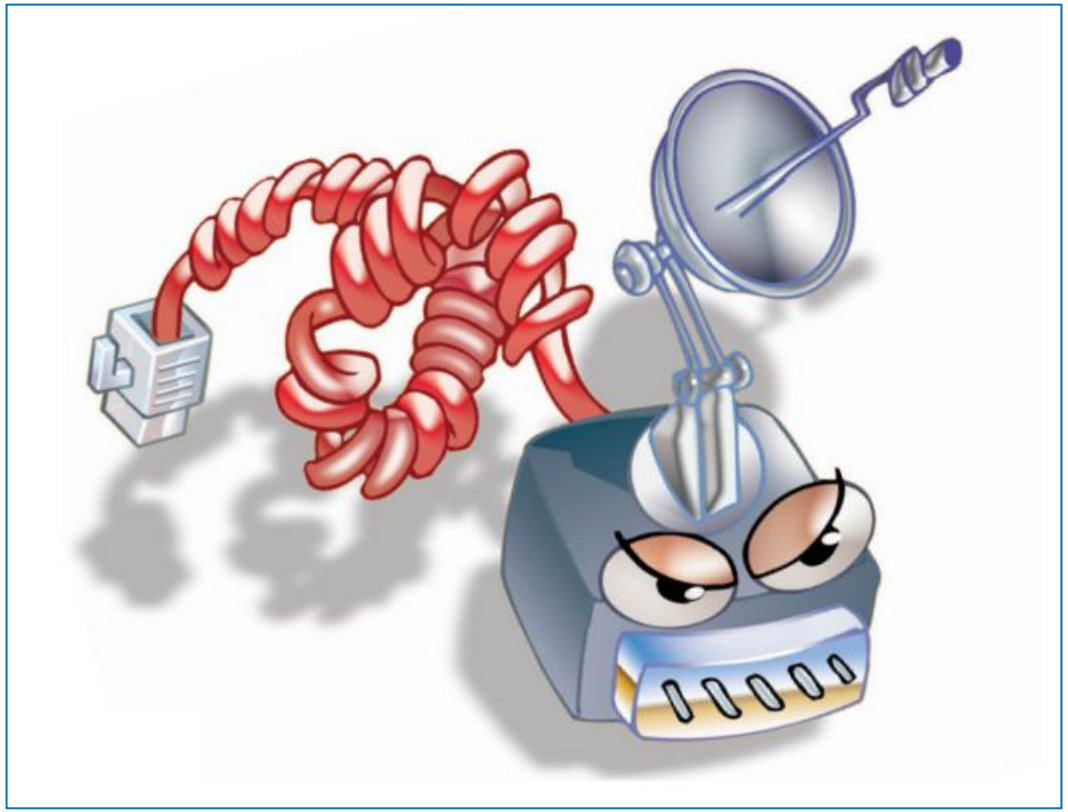
3 - WORM

4 - BACKDOOR

5 - TROJAN HORSE

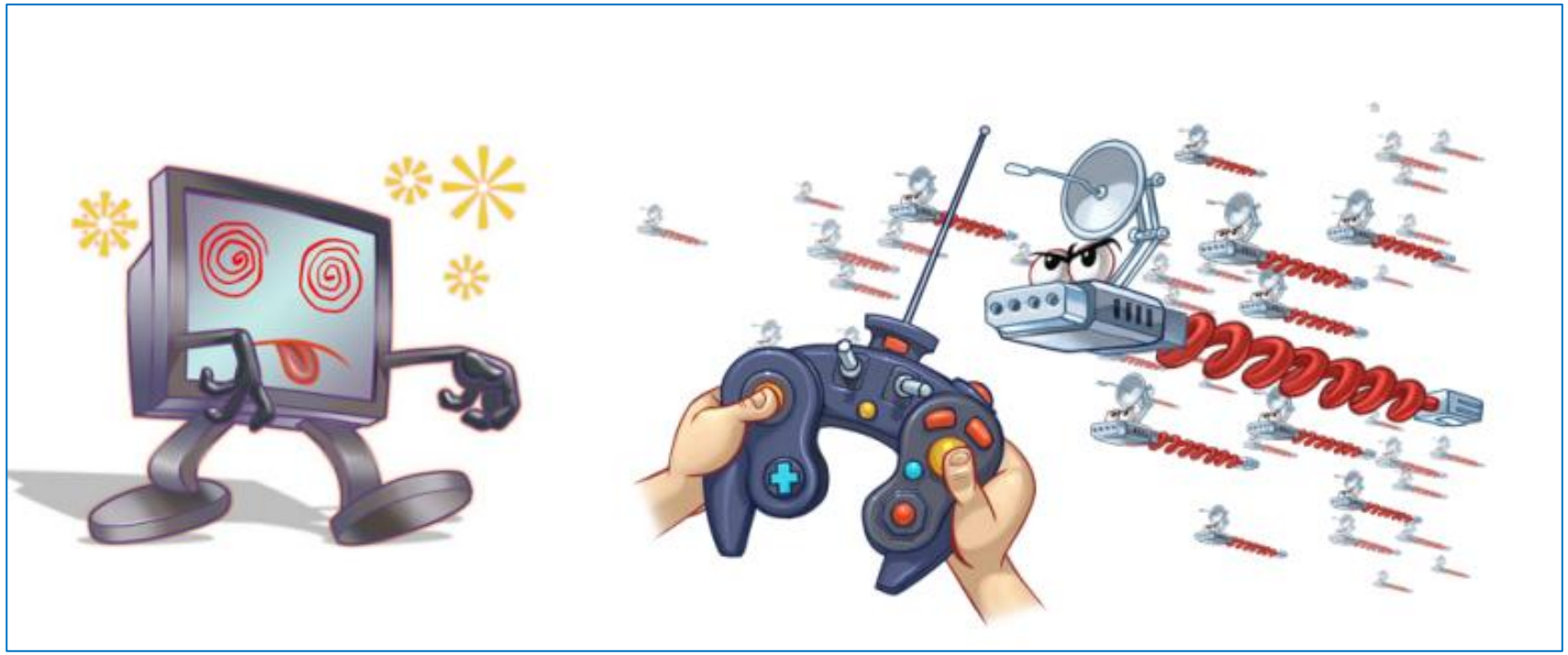
6 - BOT

6 - BOT



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

6.1 - BOTNET



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

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

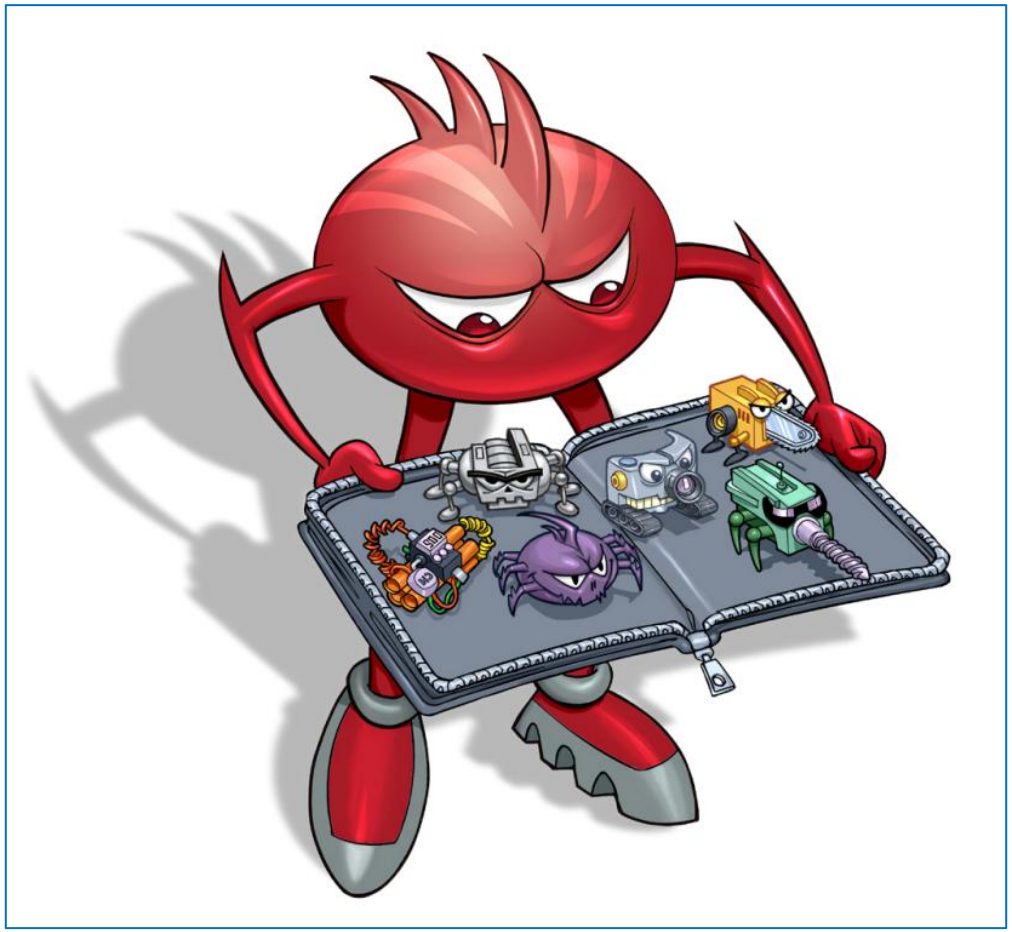
5 - TROJAN HORSE

6 - BOT

7 - RANSOMWARE

8 - ROOTKIT

8 - ROOTKIT

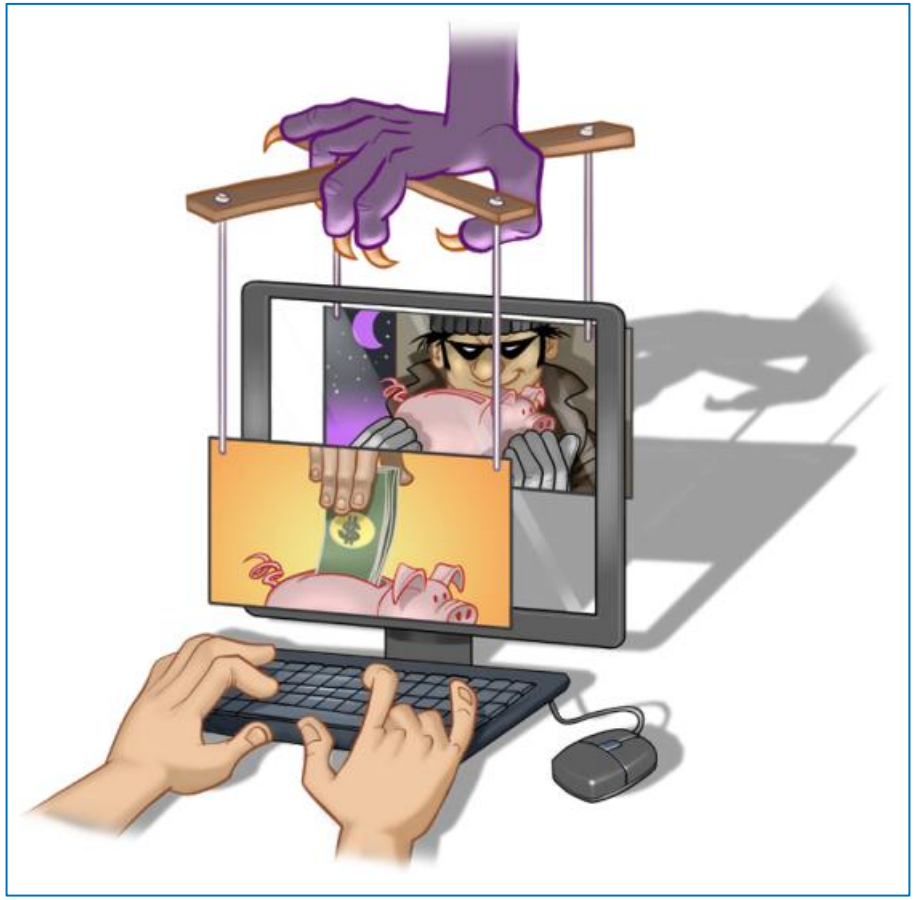


HTTPS://CARTILHA.CERT.BR/FASCICULOS/CODIGOS-MALICIOSOS/FASCICULO-CODIGOS-MALICIOSOS.PDF

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

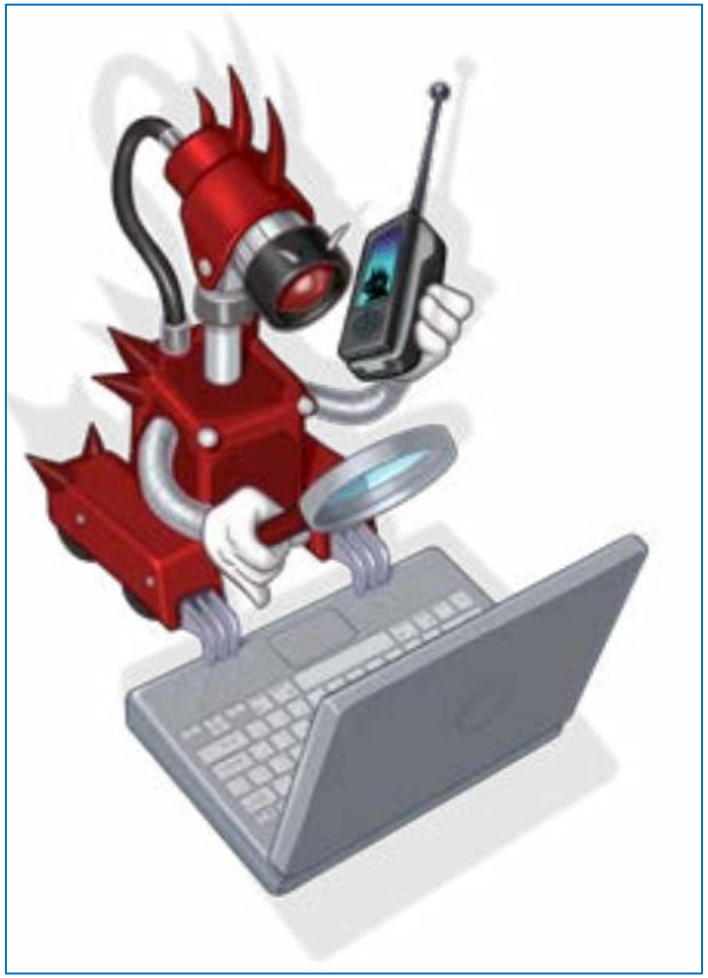
10 – SCAREWARE

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

57) 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.

58) 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.

59) Q3429243 Prova: FGV - SEAP - BA – Agente Penitenciário - 2024

Alguns jornais noticiaram recentemente um ataque cibernético que restringiu o acesso ao sistema carcerário da prisão de Bernalillo, nos Estados Unidos. As notícias descrevem um ataque cibernético de ransomware, um tipo de malware, que desativou as portas automáticas e as câmeras de segurança do sistema prisional do centro de detenção de Bernalillo, nos Estados Unidos.A forma de ataque característica de um ransomware é a de

A) codificar os dados do usuário, exigindo pagamento para liberação da chave de acesso.

B) direcionar a um site falso, que reproduz um serviço legítimo, com o objetivo de obter dados sigilosos.

C) gerar um grande volume de dados, com o objetivo de produzir formas de ataque de negação de serviço (DoS – Denial of Service).

D) produzir uma grande quantidade de e-mails para endereços encontrados no computador atacado.

E) produzir ataques a outras máquinas a partir da máquina infectada pelo malware.

60) Q3339088 Prova: Instituto AOCP - Polícia Penal do Paraná - Policial Penal - 2024

Quanto aos softwares maliciosos, assinale a alternativa que apresenta uma característica de um malware do tipo bomba lógica.

A) É capaz de infectar outros sistemas, enviando cópia de si mesmo para outros computadores da rede.

B) Exibe propagandas indesejadas na tela durante o uso do computador.

C) Permite o retorno do invasor a um sistema previamente infectado.

D) Captura as teclas digitadas no teclado físico do computador.

E) Entra em atividade quando uma determinada condição ocorre no sistema.

61) 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

62) Q3192267 Prova: CESPE/CEBRASPE - APEX Brasil - Analista - Área: Aquisições e Jurídico - 2024

Determinado software malicioso é conhecido por se propagar automaticamente pela rede de computadores, explorando vulnerabilidades dos sistemas e aplicativos instalados, sendo, inclusive, responsável por consumir muitos recursos, chegando até a afetar o desempenho da rede. Esse é um software do tipo

A) ransomware.

B) vírus.

C) botnet.

D) worm.

63) 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.

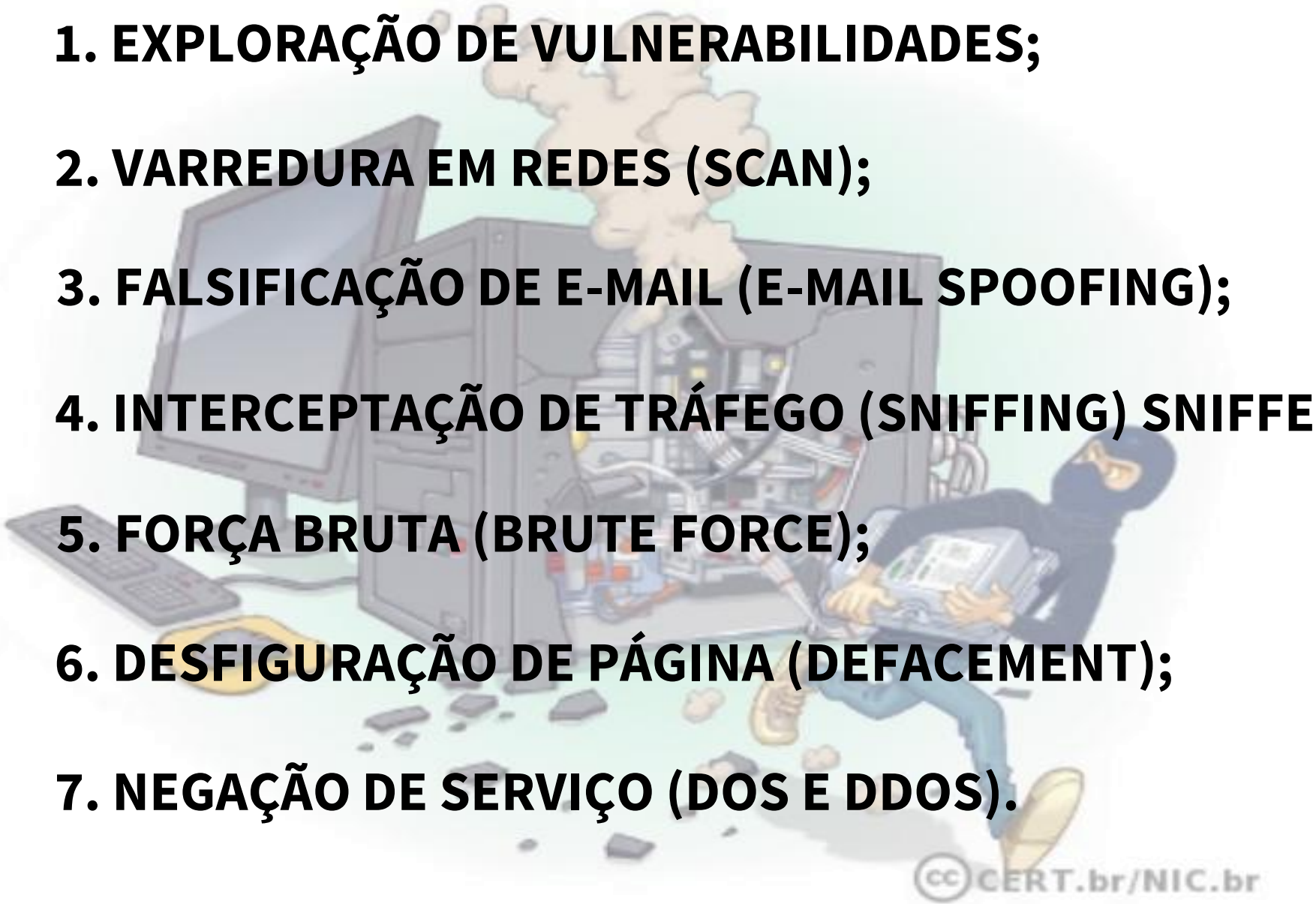
64) Q3194665 Prova: CESPE/CEBRASPE - MPE TO - Técnico Ministerial - Área: Técnico de Eletricidade - 2024

Hijacker é um tipo de malware que invade o computador e criptografa os dados de forma que o usuário perde o acesso aos próprios dados.

ERRADO

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).

65) Q3496022 Prova: SELECON - IAGRO - Fiscal Estadual Agropecuário - 2024

Um usuário de computador, ao investigar o conteúdo de sua máquina, constatou que nela existe um vírus do tipo Keylogger. Isso significa que:

A) um invasor externo vai poder sobrecarregar a máquina do usuário, fazendo-a travar ou ser impossível de operar por um tempo longo

B) o tráfego de acesso à internet por meio dessa máquina vai ser manipulado, de modo que o usuário irá a um site falso, que vai roubar seus dados

C) um invasor externo irá utilizar a camada 4 do TCP/IP para sobrecarregar o processador da máquina desse usuário, até a máquina ficar inutilizada e precisar ser trocada

D) tudo o que está sendo digitado na máquina desse usuário vai ser registrado em um arquivo, que será utilizado por uma pessoa maliciosa para ver senhas e textos importantes deste usuário

E) um hacker vai poder utilizar uma rota escondida, burlando o sistema de segurança do computador, de modo a invadir discretamente a máquina do usuário para roubar arquivos e dados