Simulado

Criado em: 06/04/2021 às 12:10:29

1. [Q1067757] Um Assistente de TI identificou o malware que atacou o seu computador como sendo do tipo ransomware, pois apresentava como principal característica

a) o pedido de resgate para liberar o acesso aos arquivos.

b) mostrar propagandas continuamente abrindo janelas do navegador web.

c) o controle do computador de forma remota.

d) a modificação dos arquivos do sistema operacional para anular o seu uso.

e) o uso de muitos recursos deixando o computador lento.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2019 / Secretaria Municipal de Finanças, Tecnologia da Informação e Controle Interno do Amazonas SEMEF Manaus - AM / Assistente Técnico de Tecnologia da Informação da Fazenda Municipal - Área Suporte / Questão: 56

2. [Q1044352] Vírus e worms são dois tipos de malware que podem ser obtidos por e-mail, em sites da internet, no compartilhamento de arquivos, em redes sociais e mensagens instantâneas, entre outros. Diferentemente dos vírus, os worms

a) propagam-se enviando cópia de si próprio automaticamente pelas redes.

b) propagam-se por meio da inserção de cópia de si mesmo em outros arquivos.

c) normalmente alteram e/ou removem arquivos do computador.

d) são instalados no computador quando se executa um arquivo infectado.

e) normalmente enviam spam e phishing automaticamente a partir do computador.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2019 / Prefeitura de Recife - PE / Assistente de Gestão Pública / Questão: 68

3. [Q972794] Considere o texto abaixo:

Um grupo de especialistas em segurança encontrou um novo tipo de malware, que está se espalhando massivamente por meio do Facebook Messenger.

Trata-se do Digmine, um malware que usa sistemas infectados para extrair a criptomoeda Monero. Esse malware é enviado às vítimas como um link para um arquivo de vídeo, quando na verdade é um script executável que afeta as versões desktop e web do Facebook Messenger, usando o navegador Google Chrome para minerar a moeda Monero no computador.

(Adaptado de: **https://guiadobitcoin.com.br/**)

Esse tipo de malware, que parece ser uma coisa (vídeo), mas na realidade é outra (script de mineração), é categorizado como

a) trojan.

b) backdoor.

c) adware.

d) rootkit.

e) ransomware.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2018 / Tribunal Regional do Trabalho da 6ª Região TRT 6 - BR / Analista Judiciário - Área Administrativa / Questão: 22

4. [Q972732] Uma ação que NÃO potencializa o risco de golpes (scam) na Internet e de infecção de computador por malware é

a) baixar atualizações ou softwares em sites de acesso mais rápido que o do fabricante.

b) entrar em sites para baixar uma faixa musical, álbum ou filmes sem pagar.

c) utilizar a mesma senha complexa em todos os sites que possui cadastro.

d) utilizar Virtual Private Network confiável para acessar a Internet em locais públicos.

e) abrir arquivos anexos no webmail, quando o assunto indicar alta prioridade.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2018 / Assembléia Legislativa de Sergipe ALE - SE / Técnico Legislativo - Área Apoio Técnico-Administrativo - Administração / Questão: 30

Acerca de malwares, julgue os itens subsecutivos.

5. [Q968543] Ransomware é um tipo de malware que cifra os arquivos armazenados no computador da vítima e solicita um resgate para decifrá-los.

c) Certo

e) Errado

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: CESPE/Cebraspe - Centro de Seleção e de Promoção de Eventos da UnB 2018 / Superior Tribunal de Justiça STJ - BR / Técnico Judiciário - Área Apoio Especializado - Especialidade: Suporte Técnico / Questão: 97

6. [Q968544] 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.

c) Certo

e) Errado

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: CESPE/Cebraspe - Centro de Seleção e de Promoção de Eventos da UnB 2018 / Superior Tribunal de Justiça STJ - BR / Técnico Judiciário - Área Apoio Especializado - Especialidade: Suporte Técnico / Questão: 98

7. [Q967920]

Não importa se um usuário utiliza Microsoft, MacOS, Android ou outro tipo de sistema operacional, pois ao se conectar na internet com um deles, já fica vulnerável a uma infinidade de ataques digitais e pode sofrer com um tipo de malware *cuja invasão é realizada com o intuito de causar algum dano ou roubar informações.*

(Adaptado de: **http://tecnologia.ig.com.br/2017-04-04/malware-cimes-ciberneticos.html**)

O malware referenciado no texto é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções maliciosas sem o conhecimento do usuário. Ataca através de programas que necessitam ser explicitamente executados para que sejam instalados, mas também pode ser instalado por atacantes que, após invadirem o computador, alteram programas já existentes para que também executem ações maliciosas. Este malware é denominado

a) worn.

b) rootkit.

c) trojan.

d) wanna cry.

e) ransomware.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2018 / Agência Estadual de Defesa Agropecuária do Maranhão AGED - MA / Técnico de Fiscalização Agropecuário / Questão: 19

Nas questões que avaliam os conhecimentos de noções de informática, a menos que seja explicitamente informado o contrário, considere que todos os programas mencionados estão em configuração padrão, em português, que o mouse está configurado para pessoas destras, que expressões como clicar, clique simples e clique duplo referem-se a cliques com o botão esquerdo do mouse e que teclar corresponde à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Considere também que não há restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.

8. [Q950863] Considere o texto a seguir.“Este malware criptografa os arquivos da vítima de forma que somente a chave criptográfica em poder dos criminosos virtuais pode descriptografá-los. Basicamente os criminosos “sequestram” os dados da máquina infectada pedindo dinheiro em moeda virtual bitcoin para liberarem os dados.” Trata-se de um:

a) vírus chamado Jerusalém.

b) ransomware chamado Stuxnet.

c) worm chamado Chernobyl.

d) ransomware chamado WannaCry.

e) vírus chamado Morris.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: Instituto Quadrix 2018 / Conselho Regional de Farmácia de Alagoas CRF - AL / Farmacêutico Fiscal / Questão: 13

9. [Q951904] Ransomware é uma categoria de malware que atacou recentemente muitos computadores pelo mundo. Os ataques mais perigosos foram causados pelos ransomwares

WannaCry, Petya, Cerber, Cryptolocker e Locky. O WannaCry:

a) formata o computador do usuário, apagando todos os seus arquivos e softwares instalados.

b) envia e-mails a partir do computador do usuário com uma imagem de uma mulher chorando. Ao clicar na imagem, o computador da pessoa que recebeu o e-mail é infectado e novos e-mails partem deste computador, reiniciando o ciclo.

c) faz com que todos os arquivos do computador sejam visualizados como pastas. Ao tentar abri-los, esses arquivos são apagados e a memória é infectada.

d) criptografa arquivos do computador e impede que o usuário os acesse, a menos que pague um determinado valor em bitcoins.

e) ataca os sites de instituições financeiras, convertendo os valores da moeda local em bitcoin e enviando-os para as carteiras de bitcoin dos criminosos.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: Instituto Quadrix 2017 / Conselho Regional de Enfermagem de Santa Catarina COREN - SC / Agente Fiscal / Questão: 14

10. [Q921989] Numa reunião sobre Segurança da Informação um especialista mencionou as seguintes definições: ( ) Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. ( ) Keylogger é um recurso técnico que permite auditar tudo que o usuário digitou para identificar erros graves de segurança nas entradas do sistema. ( ) O Cavalo de Troia é um malware que é também conhecido na área de segurança pelo termo técnico em inglês Trojan. Identifique o que foi mencionado pelo especialista com valores de Verdadeiro (V) ou Falso (F) e assinale a alternativa que apresenta a sequência correta (de cima para baixo):

a) V - V - V

b) V - V - F

c) V - F - V

d) F - F - V

e) F - F - F

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: IBFC - Instituto Brasileiro de Formação e Capacitação 2017 / Tribunal de Justiça de Pernambuco TJ PE - PE / Técnico Judiciário - Área Suporte Técnico / Questão: 28

11. [Q914484] Considere o texto abaixo publicado pela Microsoft.

É um tipo especial de malware, *porque você não sabe o que ele está fazendo e é muito difícil de ser detectado e removido. Seu objetivo é esconder a si mesmo e de outros* softwares *para não ser visto, buscando evitar que um usuário identifique e remova o software atacado. O* malware *pode se esconder em quase todos os* softwares, *incluindo servidores de arquivos, permitindo, assim, que um atacante armazene diversos arquivos infectados, invisivelmente, em seu computador.*

Eles não infectam os computadores como os vírus ou worms *fazem. Em vez disso, um atacante identifica uma vulnerabilidade existente no sistema de destino. As vulnerabilidades podem incluir uma porta de rede aberta, um sistema não protegido ou um sistema com senha fraca do administrador. Após obter acesso ao sistema vulnerável, o atacante pode instalar manualmente, como administrador, o* malware. *Esse tipo de ataque secreto direcionado não ativa controles automáticos de segurança da rede, como os sistemas de detecção a intrusos.*

Identificá-los pode ser difícil, mas há diversos pacotes de software *que os detectam. Esses pacotes dividem-se em duas categorias: detectores baseados em assinatura, que procuram arquivos binários específicos, e em comportamento, que procuram elementos ocultos.*

(Adaptado de: **https://technet.microsoft.com/pt-br/library/dd459016.aspx**)

O texto refere-se ao malware

a) Cavalo de Troia.

b) Spyware.

c) Adware.

d) Rootkit.

e) Ramsonware.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2017 / Defensoria Pública do Rio Grande do Sul DPE - RS / Técnico - Área: Informática / Questão: 43

12. [Q912080] Considere a notícia abaixo.

"Um tipo sofisticado de ..... (programa automático de computador projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros) vem infectando sigilosamente centenas de computadores de governos por toda a Europa e nos Estados Unidos, em um dos mais complexos programas de espionagem cibernética descobertos até hoje. Vários pesquisadores em segurança e funcionários da área de inteligência ocidentais dizem acreditar que o malware, *conhecido como 'Turla', é um programa espião que está sendo vinculado a uma enorme operação previamente conhecida de espionagem cibernética mundial, apelidada de Outubro Vermelho, e cujo alvo eram redes de pesquisa nuclear, diplomática e militar. Essas constatações se baseiam na análise das táticas empregadas pelos* hackers, *bem como nos indicadores técnicos e em relatos das vítimas que eram seu alvo."*

(Adaptado de: **http://g1.globo.com/tecnologia/noticia/2014/03/**)

Com base nas características descritas do malware, a lacuna do texto é corretamente preenchida por:

a) ransomware.

b) trojan DoS.

c) spyware.

d) addware.

e) bootnetspy.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2017 / Tribunal Regional Eleitoral do Paraná TRE PR - BR / Técnico Judiciário - Área Apoio Especializado - Especialidade: Enfermagem / Questão: 13

Julgue os itens que se seguem acerca de vírus, worms, pragas virtuais, aplicativos para segurança da

informação e procedimentos de backup.

13. [Q880638] O Cavalo de Troia é um malware que, entre outras ações que desencadeia no computador, acessa os arquivos em drives locais e compartilhados e até mesmo age como um servidor.

e) Errado

c) Certo

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: Instituto Quadrix 2017 / Conselho Federal de Odontologia CFO - DF / Agente Operacional / Questão: 37

14. [Q849981] Segundo a Cartilha de Segurança para Internet (http://cartilha.cert.br/malware/), códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Sobre códigos maliciosos, é correto afirmar que:

a) spyware é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim;

b) backdoor é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo, de computador para computador;

c) bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente;

d) rootkit é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

e) worm 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.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FGV - Fundação Getúlio Vargas 2017 / Assembléia Legislativa do Rio de Janeiro ALE - RJ / Especialista Legislativo - Área Registro de Debates / Questão: 63

15. [Q848362] Considere que um usuário, embora tenha procurado seguir regras de proteção e segurança da informação, teve seu computador infectado por um malware. Dentre as razões abaixo, a que pode ter contribuído para este fato é o

a) programa antimalware ter sido atualizado, incluindo o arquivo de assinaturas.

b) computador ter um firewall pessoal instalado e ativo.

c) programa leitor de e-mails ter a auto-execução de arquivos anexados a mensagens habilitadas.

d) sistema operacional do computador ter como configuração padrão não ocultar a extensão de tipos de arquivos.

e) computador estar configurado para solicitar senha na tela inicial.

Disciplinas/Assuntos vinculados: Informática > Hacker.

Fonte: FCC - Fundação Carlos Chagas 2017 / Tribunal Regional do Trabalho da 11ª Região TRT 11 - BR / Técnico Judiciário - Área

Enfermagem / Questão: 24

16. [Q841300] Considere, abaixo, as características de um tipo de malware. − Capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. − 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. − Responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, pode afetar o desempenho de redes e a utilização de computadores. − Processo de propagação e infecção que ocorre da seguinte maneira: − Identificação dos computadores alvos: após infectar um computador, tenta se propagar e continuar o processo de infecção. − Envio das cópias: efetua as cópias de si mesmo após identificar os alvos. − Ativação das cópias: após realizado o envio da cópia, necessita ser executado para que a infecção ocorra. − Reinício do processo: após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de então, o computador que antes era o alvo passa a ser também o computador originador dos ataques. Com base em tais características, um Técnico identifica este malware, corretamente, como

a) front-end.

b) worm.

c) backdoor.

d) vírus.

e) warm-trojan.

Disciplinas/Assuntos vinculados: Informática > Hacker, Malwares (ameaças e pragas virtuais).

Fonte: FCC - Fundação Carlos Chagas 2017 / Tribunal Regional Eleitoral de São Paulo TRE SP - BR / Técnico Judiciário - Área Operação de Computadores / Questão: 53

Gabarito

Criado em: 06/04/2021 às 12:10:29

(1 = a) (2 = a) (3 = a) (4 = d) (5 = c) (6 = e) (7 = c) (8 = d) (9 = d) (10 = c) (11 = d) (12 = c) (13 = c) (14 = c) (15 = c) (16 = b)