INTERNET/REDES DE COMPUTADORES II

MALWARE

1. SPYWARE

2. VÍRUS

Ele precisa ser executado e depende da ação humana, ou seja, é necessário que a pessoa clique no arquivo contaminado para que a infecção tenha início. Além disso, necessita de um arquivo hospedeiro, utilizando outro arquivo para isso. Após ser executado, o vírus cria cópias de si mesmo.

2.1. VÍRUS DE BOOT

Boot é o processo de inicialização do computador, quando ele é ligado e o sistema operacional, como Windows ou Linux, é carregado. Embora o Linux também possa ser infectado por vírus, ele é muito mais resistente. O vírus de boot infecta a área do disco rígido responsável pela inicialização e costuma ser carregado antes mesmo do sistema operacional, o que dificulta sua detecção, já que, normalmente, não há antivírus em funcionamento nesse momento – são raros os que conseguem atuar nessa fase.

2.2. VÍRUS DE MACRO

A macro é um miniprograma que permite automatizar tarefas no Word, PowerPoint e Excel. Esse tipo de vírus contamina arquivos que utilizam macros. Quando a pessoa abre um arquivo que contém uma macro, o sistema emite um aviso.

2.3. VÍRUS DE POLIMÓRFICO

Altera a assinatura, mas mantém sua funcionalidade, o que dificulta a detecção do vírus.

2.3. VÍRUS DE METAMÓRFICO

Altera tanto a assinatura quanto a funcionalidade, o que torna sua detecção muito mais difícil.

3. WORM

Não precisa ser executado manualmente, pois é um programa autônomo que se propaga automaticamente. Ele explora vulnerabilidades e falhas de segurança nos computadores para realizar a infecção.

4. BACKDOOR

5m

Ele permite que um invasor retorne a uma máquina previamente comprometida. Abre portas no computador, facilitando a infecção por outras ameaças.

5. TROJAN HORSE

Trata-se de um programa aparentemente inofensivo, mas, ao ser aberto, infecta o sistema com um vírus.

6. BOT

Eles não precisam ser executados, não utilizam arquivos hospedeiros e se propagam pelas redes, explorando vulnerabilidades. O bot, ao contrário do worm, pode ser controlado remotamente. Existem vários tipos de ataques, como os DDOS, que são ataques de negação de serviço distribuído.

6.1. BOTNET

Com uma rede infectada por bots, forma-se uma botnet. Um computador infectado por um bot é denominado computador zumbi, pois realiza ações sem o controle de seu proprietário.

7. RANSOMWARE

Ele sequestra os dados, criptografando-os. Para recuperar os dados, a pessoa precisa efetuar um pagamento, geralmente em moedas virtuais (criptomoedas).

- Ransomware locker
  - Bloqueia acesso ao computador.
- Ransomware crypto
  - Bloqueia acesso aos dados.

8. ROOTKIT

É um conjunto de técnicas e programas usados para invadir um computador e mantê-lo sob controle do invasor.

9. RAT (REMOTE ACCESS TROJAN)

É a combinação de um Trojan com um backdoor.

10. SCAREWARE

É um software que gera alarmes, propagando uma mensagem assustadora. Ao clicar no link da mensagem, a pessoa infecta seu computador.

10m

11. STALKERWARE

É quando um stalker começa a monitorar a vida de uma pessoa.

DIRETO DO CONCURSO

57. (BANCO/OBJETIVA CONCURSOS/FEAES) Em relação aos diversos tipos de vírus de computadores e suas definições, numere a 2ª coluna de acordo com a 1ª e, após, assinale a alternativa que apresenta a sequência CORRETA:

(1) Vírus de boot.

(2) Vírus de macro.

(3) Vírus stealth.

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

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

III. ( ) 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.

I. Ele não necessariamente impedirá sua inicialização correta, mas essa é uma possibilidade.

---

58. (2024/FUNDAÇÃO CARLOS CHAGAS/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. (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.

a. O pagamento do resgate não garante a liberação da chave de acesso.

c. O DoS (Denial of Service) é um ataque de negação de serviço, no qual uma máquina é utilizada para derrubar outra.

e. Essa característica é da botnet.

15m

60. (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.

a. Essa é definição de vírus.

b. Essa é a definição de adware.

c. Essa é definição de backdoor.

d. Essa é a definição de keylogger.

---

61. (INSTITUTO AOCP/POLÍCIA PENAL DO PARANÁ/POLICIAL PENAL/2024) 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.

62. (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. (2024/FUNDAÇÃO CARLOS CHAGAS/FCC/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) stalkerware.
b) scareware.
c) worm.
d) zumbi.
e) rat.

b. É o vírus que exibe uma mensagem assustadora.

c. O worm não precisa ser executado.

d. É quando o computador é infectado por um bot.

e. O Rat é o Remote Access Trojan.

---

64. (CESPE/CEBRASPE/MPE TO/TÉCNICO MINISTERIAL/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.

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

O hijacker é o sequestrador de navegador, que bloqueia a página inicial do navegador e impede o acesso a determinados sites.

ATAQUES

1. Exploração de vulnerabilidades;
   - Procura falhas de segurança no computador.
2. Varredura em redes (SCAN);
   - Apesar de ser usada como ataque, ela também pode ser empregada de forma legítima.
3. Falsificação de e-mail (e-mail spoofing);
   - É quando se explora uma falha no e-mail e altera seu cabeçalho.
4. Interceptação de tráfego (sniffing) sniffers;
   - Ele monitora todo o tráfego da rede, capturando-o.
5. Força bruta (BRUTE FORCE);

20m

- São softwares utilizados para tentar, por meio de tentativa e erro, fazer o login de uma pessoa em um site.

6. Desfiguração de página (DEFACEMENT);
   - Alguém invade um site e o desconfigura.
7. Negação de serviço (DOS E DDOS).
   - O DoS é negação de serviço, enquanto o DDoS é Distributed Denial of Service, ou seja, negação de serviço distribuído. No DoS, é utilizada uma única máquina para atacar, enquanto no DDoS várias máquinas são usadas para atacar uma única máquina.

65. (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 desse usuário.

25m

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.

a. Esse seria um ataque de negação do serviço.

b. Esse é um golpe do tipo fishing.

e. Esse ato é feito pelo backdoor.

GABARITO

57. b
58. c
59. a
60. e
61. C
62. d
63. a
64. E
65. d

Este material foi elaborado pela equipe pedagógica do Gran Concursos, de acordo com a aula preparada e ministrada pelo professor Jeferson Bogo.
A presente degravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.