IA012 - Tarefa 6

Rodrigo Seiji Piubeli Hirao (186837)

16 de dezembro de 2021

01)

- **cavalo de tróia** - programa que faz algo indesejado se passando por outro
- **vírus** - programa que faz cópia de se mesmo em outros programas
- **bactéria** - programa que duplica sua execução ou seu código exponencialmente
- **verme** - programas que usam da rede para se propagar e, depois, funcionar como um dos outros acima explicados

02) O ransomware criptografa os dados do computador infectado e exige um resgate em troca da chave privada.

Não há muito que se fazer caso seus dados tenham sido criptografados, a melhor solução seria ter um backup anterior ao acidente. O processo também pode ter sido parado no meio caso o comportamento estranho tenha sido percebido.

03) Os invasores se comunicam muito mais facilmente e frequentemente que os administradores do sistema. Além dos invasores precisarem encontrar apenas um ponto de falha, enquanto os administradores precisam proteger todos. Desse ponto pode ser visto que os administradores estão cercados pelos invasores desde o início.

04) Um sistema de autencicação que faz com que todas suas ações sejam auditadas com seu usuário, bem como uma limitação e controle de seu acesso aos recursos.

05)

- Pode ser possível detectar uma atividade maliciosa antes da ação
- É possível encontrar falhas no sistema
- Invasões recebem um contra-incentivo

06) Uma análise estatística é a comparação de comportamentos potencialmente maliciosos com o de comportamentos previamente estudados de atividades comuns, assim, se o comportamento estiver muito longe do esperado ele deve ser questionado pois pode ser uma ação maliciosa.

O problema de análises estatísticas é que ainda podem existir ataques que não se distoam o suficiente de atividades comuns para serem consideradas estranhas.

07) Os registros de autoria especificam qual usuário fez qual ação e em qual momento, o que pode ser usado para analisar comportamentos estranhos afim de encontrar atividades maliciosas. Além de descobrir o autor do crime, assim sendo um contra-incentivo contra invasões futuras.

08)

- **Bomba-relógio** - O primeiro uso foi em uma linguagem de marcação chamada Scribe, que teria seu código desativado em 90 dias se não fosse comprado um código para desabilitar a bomba da empresa.
- **Trapdoor** - O verme mydoom que se espalhava por emails, criava uma trapdoor no sistema para poder enviar mais emails pela internet, para assim se multiplicar globalmente.
- **Cavalo de Tróia** - A FBI e a AFP distribuíram um cavalo de tróia no foramto de um app para celular chamado ANOM, que se passava por um aplicativo de chat, mas na verdade tinha suas mensagens interceptadas pelas agências criadoras do app.

09) O programa mencionado é um malware pois este se comporta contra as necessidades do usuário, se espalhando pela rede.

10) Hoje em dia surgiram muitas técnicas eficientes do virus se misturar com um programa sem alterar seu tamanho, ofuscando seu próprio código e entrando no meio do programa sem que o tamanho total seja alterado.