Sistemas Distribuídos

Anhanguera


AVALIE
SUA PROFISSÃO
QUANDO APARECER EM SEU PORTAL UMA AVALIAÇÃO SOBRE SEU CURSO, RESPONDA:
NOTAS
9 OU 10
SIGNIFICA QUE VOCÊ INDICA
NOTAS
7 OU 8
SIGNIFICA QUE VOCÊ NÃO INDICA
Anhanguera

Anhanguera

Segurança em sistemas distribuídos

Anhanguera

Todo sistema distribuído implementado tem, como um dos principais e mais importantes, aspectos de projeto à segurança, conforme foi estudado anteriormente. Em um sistema distribuído temos uma série de componentes de hardware e software, físicos ou virtualizados, que se comunicam para a execução das aplicações distribuídas. Por conta disso vários tipos de ameaças podem afetar a segurança de nossos sistemas.

Uma das formas mais funcionais de prevenir nossos sistemas atualmente é utilizar uma estratégia de segurança multicamadas. Este tipo de estratégia protege com diferentes tecnologias de segurança os principais pontos de entrada de ameaças. A segurança multicamada aumenta consideravelmente o grau de dificuldade para uma invasão de um intruso, reduzindo drasticamente o risco de um hacker ter acesso indevido à rede e dados de empresas. Com a estratégia de segurança multicamadas, as ameaças encontram muito mais dificuldade em causar algum dano, pois caso ultrapassem alguma camada, deverão ser barradas pela camada seguinte. Quando implementada corretamente, uma estratégia em várias camadas oferecerá proteção contra vírus, spyware, malware, phishing, invasão de redes, spam e vazamento de dados.

Sempre devemos levar em consideração que tudo que é relacionado à segurança em um sistema computacional depende do fator tecnológico, que é composto pelos componentes de hardware e software, e também pelo fator humano que acaba sendo o ponto mais vulnerável do sistema. Por exemplo, quantas páginas falsas (fakes) se passando por lojas virtuais famosas ou até mesmo bancos não são encontradas na internet e afetam centenas de usuários diariamente com o roubo de informações sigilosas? Esse tipo de ameaça é chamado de Trojan Banking, e é muito frequente sua distribuição através de e-mails e sites infectados.

Podemos dividir a parte de segurança de sistemas distribuídos em duas: permissão de acessos a serviços e recursos disponíveis no sistema e comunicação entre máquinas que contém mais de um processo e usuários diferentes (GOODRICH e TAMASSIA, 2012).

Podemos relacionar a segurança de um sistema distribuído aos seguintes fatores:

1. Confidencialidade

A confidencialidade significa que a informação só estará disponível para os usuários ou máquinas autorizadas. Uma das formas de se garantir confidencialidade das mensagens é através do uso de autenticação baseada em chave privada.

2. Integridade

A integridade significa que a informação armazenada ou transferida é apresentada corretamente para quem precisa fazer a sua consulta. A integridade das mensagens pode ser alcançada através de assinaturas digitais e chaves de sessão.

3. Autenticidade

A autenticidade pode ser alcançada quando criamos permissões de autenticação para os principais usuários e máquinas do serviço, com isso nosso sistema só irá funcionar corretamente com os usuários e máquinas autenticados.

4. Disponibilidade

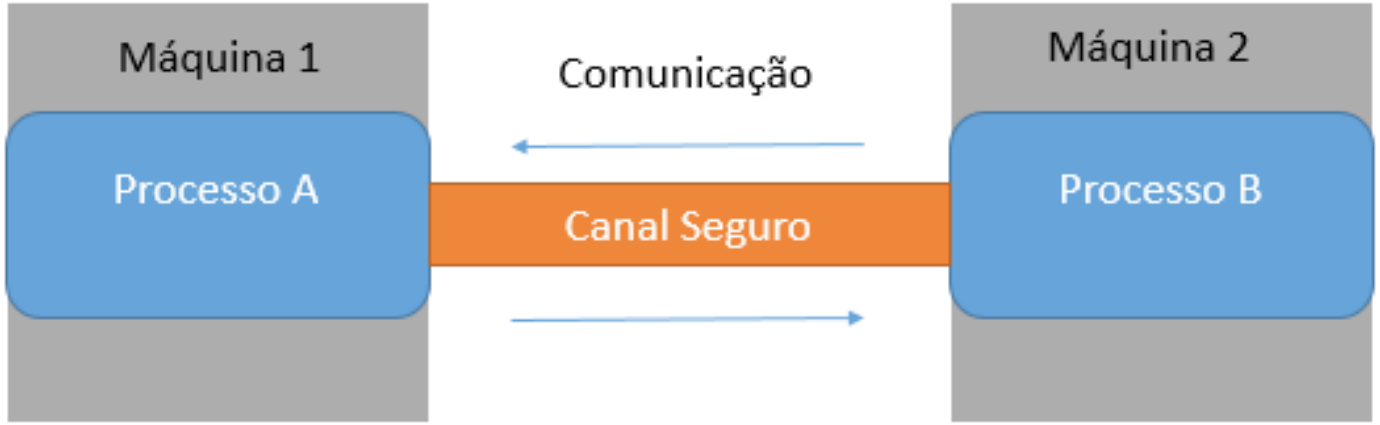
A disponibilidade significa garantir que a informação esteja sempre disponível para quem precisar dela. Podemos obter a disponibilidade do sistema utilizando as políticas de segurança corretamente em nosso sistema.

5. Não repúdio

O não repúdio ou princípio do não repúdio, como é conhecido, garante a autenticidade de uma informação utilizada por sistemas distribuídos. Ele é uma grande medida de segurança, já que pode ser aplicada a e-mails, imagens, formulários web, arquivos eletrônicos transferidos entre empresas (EDI), entre outros itens. Uma das principais maneiras de se aplicar essa exigência de segurança é através de assinatura digital e certificados digitais.

Aplicando esses fatores temos o objetivo de proteger o canal de comunicação de nossas aplicações, tornando assim canais seguros em nossos sistemas distribuídos. O grande objetivo de nossa aplicação distribuída é que ela possa se comunicar, ou seja, trocar dados, com confiabilidade, integridade e autenticidade. Portanto, uma das principais formas de proteção é deixar a comunicação permitida apenas em máquinas e por usuários autenticados em nosso sistema e com as permissões necessárias.

Podemos observar na Figura 4.1 a comunicação entre processos e máquinas de um sistema distribuído através de um canal seguro. Para que isso ocorra temos que ter as máquinas 1 e 2 autenticadas dentro do nosso sistema. Com isso, caso o sistema sofra um ataque, o atacante não será capaz de ler, copiar, alterar, reenviar, reordenar ou enviar novas mensagens. Dessa forma nosso sistema estará protegido.


Máquina 1
Comunicação
Máquina 2
Processo A
Canal Seguro
Processo B

Para produzir um sistema que seja seguro contra diversas ameaças, precisamos aprender a classificar essas ameaças e entender seus métodos de ataque. As ameaças aos sistemas distribuídos podem ser divididas nas seguintes classes (COULOURIS et al., 2013):

- Leakage (vazamento): acesso à informação por agentes não autorizados.
- Tampering (falsificação): modificação não autorizada de uma informação.
- Vandalism (vandalismo): interferência no funcionamento de um sistema sem ganhos para o criminoso.

Para que o invasor consiga violar um sistema através de algumas das estratégias apresentadas anteriormente, é necessário acessá-lo. Geralmente, todas as máquinas que compõem um sistema distribuído têm canais de comunicação para acesso autorizado às suas facilidades, e através desses canais de comunicação que o acesso não autorizado pode ocorrer.

As estratégias de violações de segurança em sistemas distribuídos dependem da obtenção de acesso aos canais de comunicação de nosso sistema, ou do estabelecimento de canais que escondem conexões, com a autoridade desejada. Fazem parte destas estratégias:

• Eavesdropping: acesso a cópias de mensagem sem autorização. Geralmente essa estratégia funciona através da captura de mensagens da rede. Por exemplo, usando a internet um computador pode se passar por outro, quando configurado com o endereço de rede de outro, desta forma ele pode receber as mensagens endereçadas a outro destinatário.

• Masquerading (disfarce): a máquina do invasor faz envio ou recebimento de mensagens utilizando a identidade de outra máquina autorizada pela aplicação.

• Message tampering (falsificação de mensagem): a máquina do invasor faz a captura e alteração do conteúdo das mensagens e após isso faz a transferência ao destinatário. Uma das maneiras mais fáceis de se defender a esse tipo de ataque é utilizando broadcast para o envio das mensagens, como ocorre nas redes Ethernet.

• Replaying: quando o invasor consegue fazer a captura e armazenamento das mensagens por um período de tempo, utilizando para isso o envio atrasado das mensagens aos seus destinatários.

Para os invasores conseguirem acesso ao sistema é utilizado um método simples de infiltração que pode ser o uso de programas de quebra de senhas para obter as chaves de acesso de algum usuário do sistema. Além desta forma simples e não muito eficaz de invasão, existem outras maneiras mais sutis, que estão se tornando bem conhecidas:

• Vírus: um programa anexado a um hospedeiro legítimo, que se instala sozinho no ambiente alvo, sempre que o programa hospedeiro é executado. Uma vez instalado, ele realiza suas ações criminosas. A notícia do Portal BBC traz um ataque cibernético que paralisou um hospital e foi causado por um vírus. Disponível em: https://www.bbc.com/portuguese/brasil-40870377. Acesso em: 18 dez. 2018.

• Worm: um programa que varre um sistema, ou uma rede, replicando-se e buscando bloquear todos os recursos disponíveis, até torná-lo inoperante. Ao contrário do vírus, um worm normalmente não destrói dados.

• Cavalo de Troia (Trojan Horse): um programa oferecido aos usuários através de um sistema que mostra ser capaz de utilizar uma função útil, mas que tem uma segunda intenção que vem oculta através de uma função. O exemplo mais comum é o spoof login, um programa que apresenta aos usuários um diálogo idêntico ao diálogo normal de obtenção de login (nome do usuário) e password (senha), mas que na realidade armazena as informações fornecidas pelos usuários em
um arquivo, com o objetivo de uso posterior ilícito.

• Spyware: são programas espiões utilizados para roubar informações sobre os costumes dos usuários na internet, com o propósito de fornecer uma propaganda preparada de acordo com as pesquisas daquele usuário.

• Keyloggers: são programas de computador capazes de monitorar, armazenar e enviar todas as teclas digitadas pela vítima para um invasor. Atualmente, os keyloggers são incorporados em outros códigos como trojans, utilizados principalmente para roubo desenhas ou dados bancários.

• Backdoor (Porta dos Fundos): é um recurso utilizado por diversos malwares para conseguir acesso remoto a uma rede ou sistema infectado.

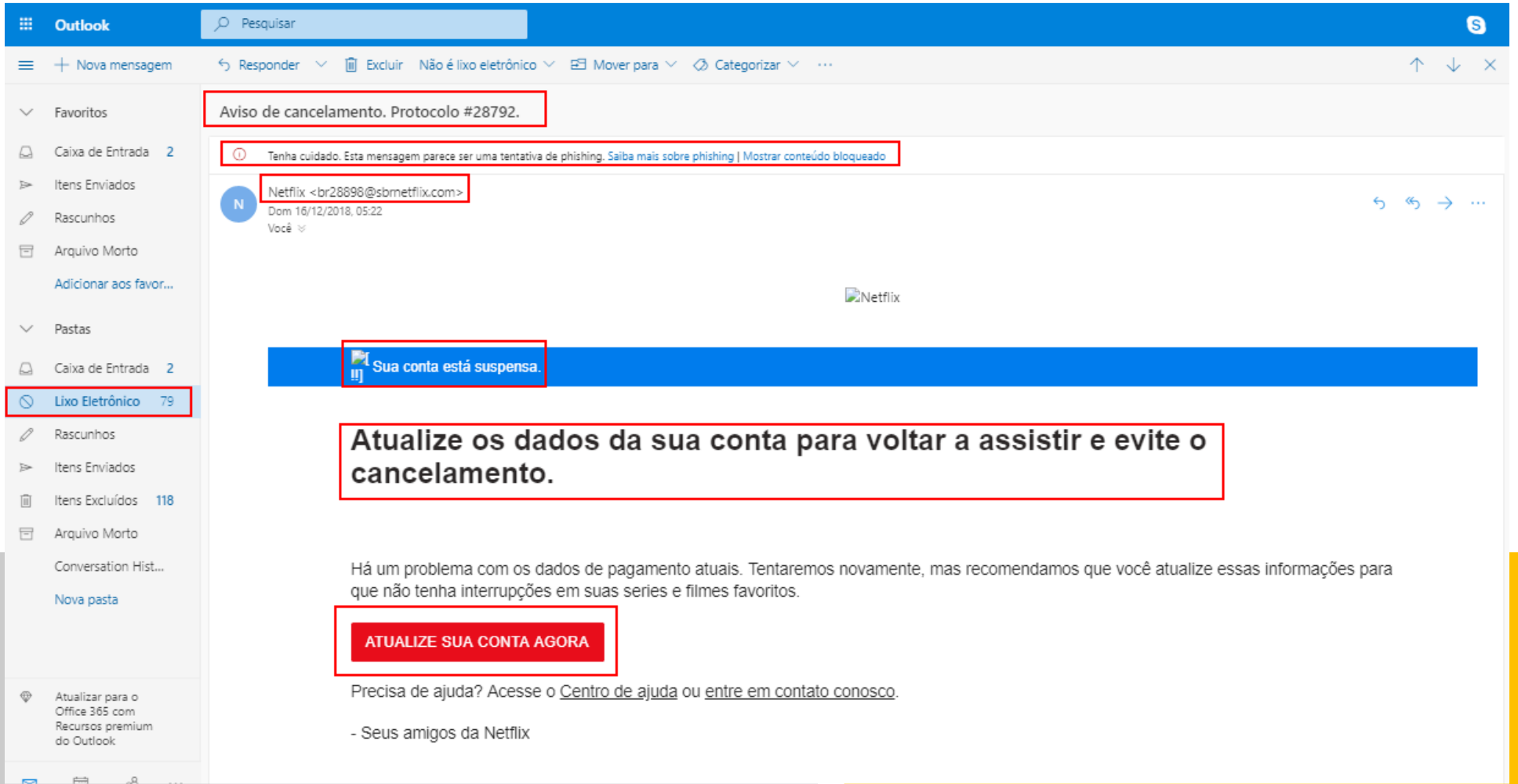
• Spam: são e-mails indesejáveis, que muitas vezes têm o intuito de conseguir dados do usuário.

• Adware: são programas que exibem uma grande quantidade de anúncios sem a autorização do usuário.

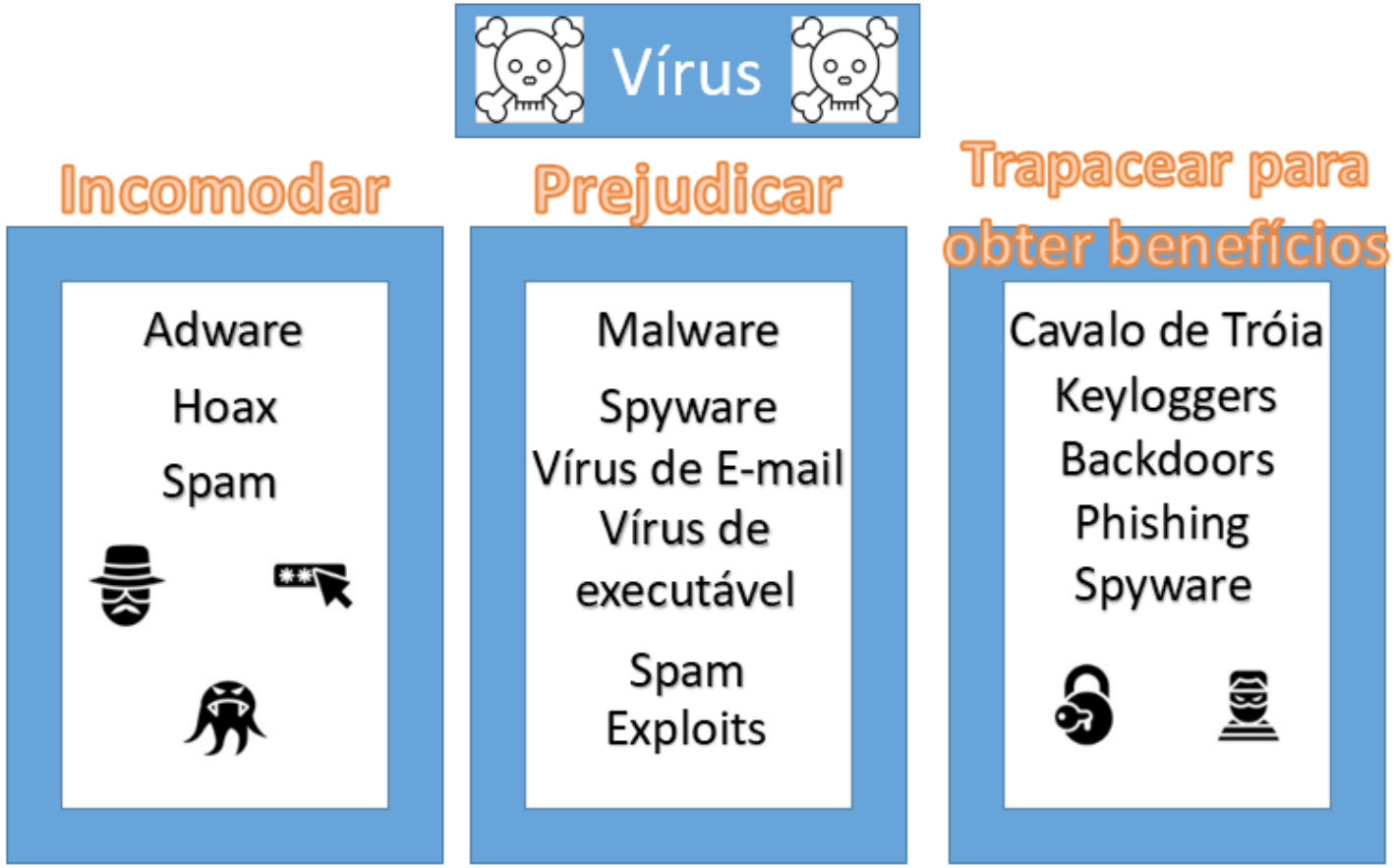
• Exploits: programas com conteúdo malicioso, que tendem a utilizar vulnerabilidades do sistema e outros programas.

• Hoax: são falsas mensagens que alertam o usuário sobre um determinado tipo de vírus disponível em sua máquina.

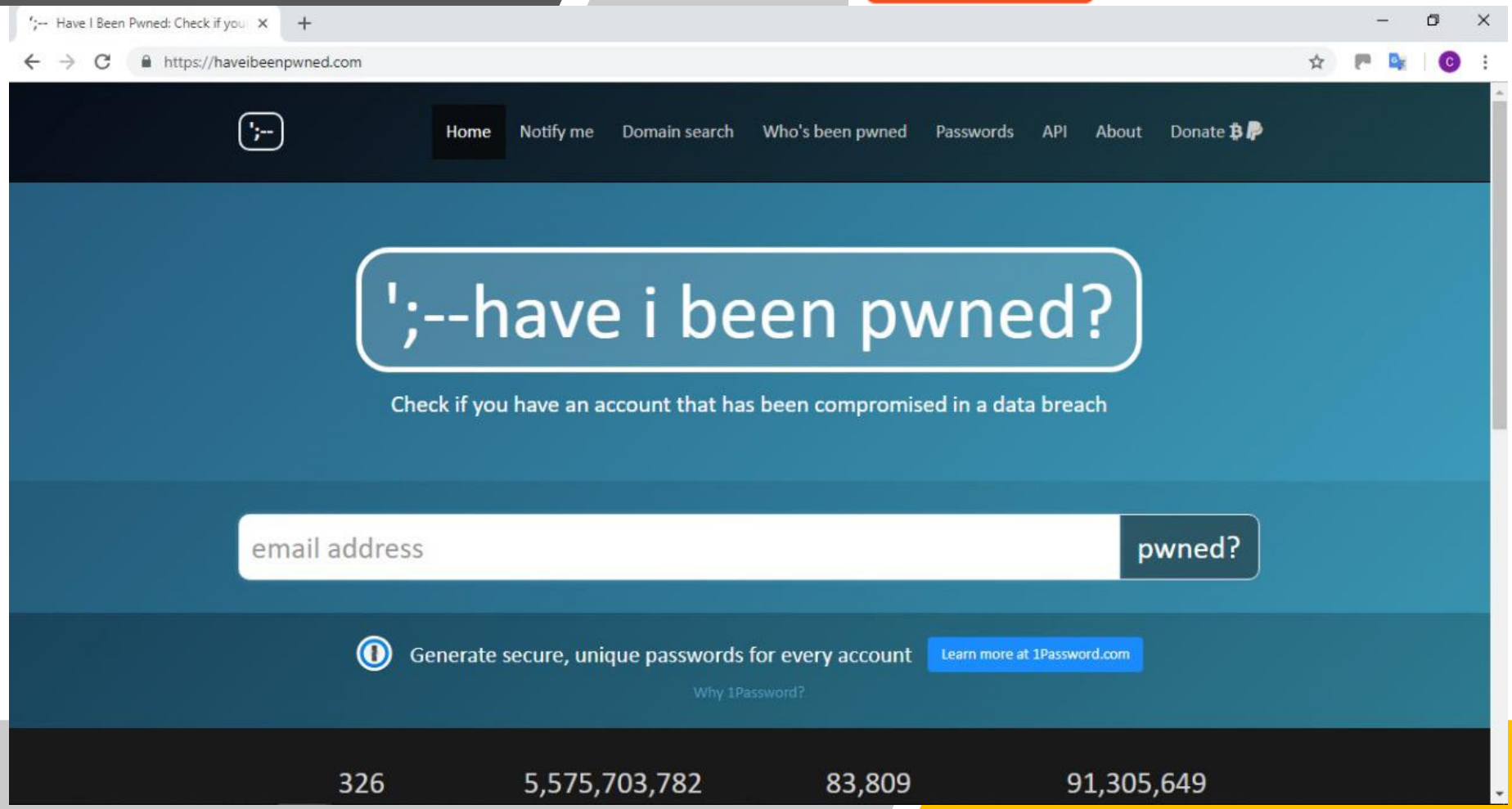
- Phishing: são programas com o objetivo de adquirir informações sigilosas de um usuário, podem se disfarçar de mensagens, softwares e outras formas de aplicações amigáveis.



Podemos observar na Figura 4.3 uma divisão entre os tipos de vírus listados, onde separamos por vírus com o objetivo de incomodar usuários, prejudicar e trapacear para obter benefícios aos seus invasores.



Anhanguera


Have I Been Pwned: Check if you
https://haveibeenpwned.com
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?
326
5,575,703,782
83,809
91,305,649

Uma ameaça que é frequente em sistemas distribuídos voltados para internet (web) é a invasão dos servidores webs, que armazenam os arquivos e objetos que são parte do sistema. Este tipo de invasão ocorre através de portas acesso. O que acontece em muitas empresas, é que às vezes há algum servidor mais vulnerável, com suas portas de acesso liberadas para alguns casos que acabam sendo alvo para invasões, através dessa porta de entrada todo o sistema web é contaminado. Já ocorreu em um ambiente coorporativo que trabalhei de uma máquina antiga com um serviço de Wordpress (blogs) quase esquecido, ser utilizada como porta de entrada para hackers acessarem boa parte dos arquivos web importantes da empresa. Uma das formas de se proteger contra essa grande ameaça é utilizar um serviço baseado no protocolo FTP (File Transfer Protocol) de transferência de arquivos, que utiliza autenticação para envios de novos arquivos. Esse protocolo é muito utilizado quando falamos em ambientes web. Outra forma de se proteger é implantando o protocolo SSH (Security Shell) de acesso seguro, como principal forma de proteção ao acesso dos servidores. Temos outras formas de aumentar a segurança de nossos sistemas distribuídos voltados para web, assim como também temos outros tipos de ameaças. Portanto, devemos nos atualizar frequentemente sobre novas proteções e novas ameaças para que possamos ter um sistema seguro da melhor maneira possível.

No contexto de segurança de sistemas em rede e, portanto, também em sistemas distribuídos, existem vários tipos de ameaças, como por exemplo, os Trojans, Malware, Vírus, Spams, Spywares e Cavalos de Troia; ameaças estas que têm características e objetivos diferentes, conforme discutido no texto-base desta Seção.

Independentemente do tipo de ameaça, elas podem ser categorizadas em 3 tipos.

Quais são esses tipos?

a) Vazamento, vandalismo e falsificação.

b) Danoso, doloso e sem ônus.

c) Falsificação, roubo e hackeamento.

d) Vírus, Malwares e Trojans.

e) Vazamento, falsificação e sequestro.

Sistemas distribuídos podem ser entendidos como máquinas em redes que possuem uma maior integração que sistemas puramente de redes. A razão dessa maior integração reside no fato de que as máquinas que fazem parte desse tipo de sistema fazem uso intensivo de comunicação de informações entre si, através dos canais de comunicação.

Sabendo que a falha na segurança de um sistema distribuído significa que o canal de comunicação foi comprometido e, considerando as afirmações abaixo, assinale a alternativa que apresenta boas práticas para proteção do canal de comunicação em termos de segurança.

I – Permitir acesso somente a usuários autenticados.

II – Permitir acesso somente a serviços autenticados.

III – Permitir acesso exclusivo a usuários anônimos.

IV – Permitir acesso somente a máquinas autenticadas.

V – Permitir uso do canal de comunicação exclusivamente por processos que sejam executados localmente.

a) Somente a afirmação I está correta.

b) Somente as afirmações I e II estão corretas.

c) Somente as afirmações I, II e IV estão corretas.

d) Somente as afirmações II, III e IV estão corretas.

e) Somente as afirmações I, II, IV e V estão corretas.