GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Curso Superior de Tecnologia em Segurança da Informação (SI) e GTI

Prof. Nasser Arabi
Com adaptações
Prof. Clenio Emidio

Brasileiros são principais alvos de ataques de phishing no mundo

Relatório da Kaspersky mostra que um em cada cinco internautas no País sofreu ao menos uma tentativa de ataque de phishing em 2020.

Renato Rodrigues

2 mar 2021

Ataques disfarçados de apps de ensino crescem 60%

De acordo com novo relatório da Kaspersky, a isca mais popular foi o Zoom, seguida por Moodle e Google Meets

Renato Rodrigues

10 fev 2021

Roubo de contas foi o principal crime financeiro de 2020

Crimes de account takeover (roubo de contas digitais) aumentaram 20 pontos percentuais no último ano; saiba como os golpes funcionam

Kaspersky Team

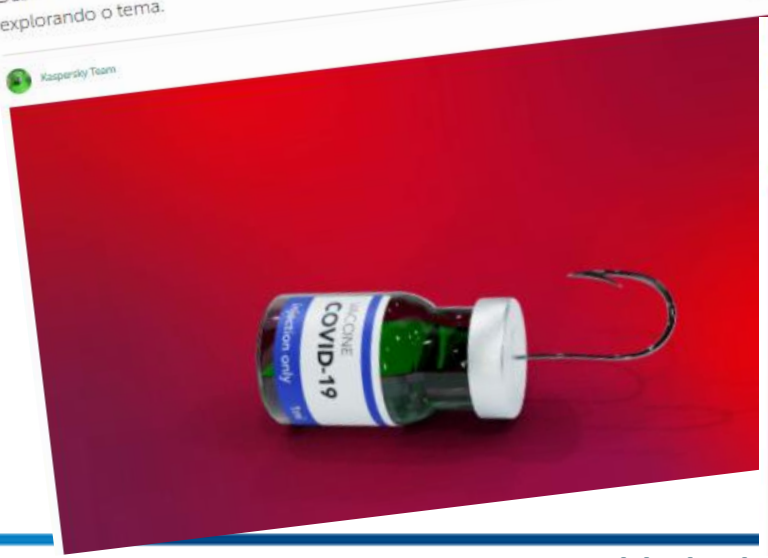
25 fev 2021

Covid-19: sites simulam cadastro para roubar dados pessoais

Desde o início da semana, especialistas da Kaspersky encontraram domínios de phishing explorando o tema.

Kaspersky Team

22 jan 2021

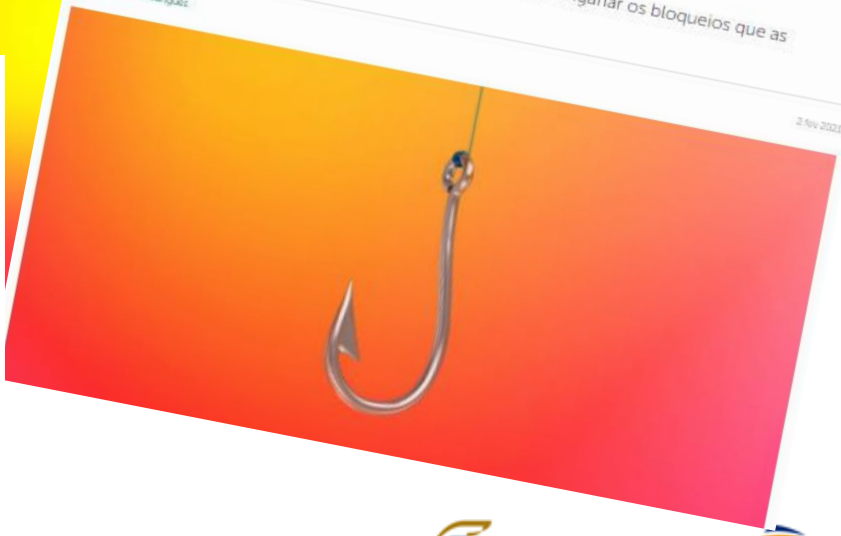


Criminosos criam nova técnica para enviar phishing por SMS

Recurso consiste em pequenas mudanças na escrita para enganar os bloqueios que as operadoras de telefonia realizam.

Renato Rodrigues

2 fev 2021



Brasileiros são alvo de quase metade dos ataques de ransomware na AL

Segundo dados da Kaspersky, região registra 5 mil ataques de ransomware por dia e empresas são o principal alvo em nível mundial

Renato Rodrigues

17 nov 2020

Ameaças

Fatores que colocam em risco a segurança da informação — ou seja, podem comprometer a integridade, a confidencialidade e a disponibilidade dos dados.

"Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.“ (RFC 2828, Internet security glossary)

https://www.hscbrasil.com.br/

Estas são as informações que mais chamam a atenção...

Os **ataques de phishing aumentaram 226%** em comparação com o último semestre de 2021

Os ataques de ransomware passaram a ser cada vez mais direcionados e as empresas **não estão devidamente preparadas** para enfrentar este tipo de ameaça

O país da América Latina mais afetado por ameaças focadas no **Android** é o Brasil

Ransomwares, trojans bancários e RATs são as ameaças mais utilizadas por cibercrimosos para afetar aos **dispositivos móveis.**

As vulnerabilidades mais detectadas, além do fato de serem vulnerabilidades relacionadas a **produtos Microsoft**, estão relacionadas com falhas descobertas há mais de cinco anos atrás.

Ameaças

Naturais

Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc.

Involuntárias

Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidente, erros, falta de energia, etc.

Voluntárias

Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computadores, incendiários.

Ameaças cibernéticas

- Ataques direcionados – diferentemente dos ataques em massa e automatizados, os ataques direcionados utilizam informações específicas de uma organização para executar um ataque.
- Ataques persistentes avançados - APT (Advanced Persistent Threats), ataque direcionado focado em espionagem via internet. São descritas desta forma, pois na maioria das vezes são invasores contratados para atacar uma empresa específica.
- Ataques a dispositivos IoT - podem copiar ou comprometer os dados transmitidos por eles, possibilitando a espionagem industrial ou mesmo a danificação do sistema como um todo.
- Malwares - software malicioso que tem como objetivo danificar dados ou agir no sistema da vítima sem sua autorização. E-mails de desconhecidos, acesso a sites impróprios e downloads ilegais são os principais causadores da entrada de malwares.

Ameaças cibernéticas

- Business E-mail Compromise – é um ataque em que o criminoso envia uma mensagem se passando por um profissional de alto cargo, como o presidente da empresa.
- Trojan – "Cavalo de Troia", é um software que se passa por um programa legítimo.
- Camubot - é um tipo de Trojan que se passa por módulo de segurança de um banco, utilizando identidade visual fraudada para ganhar a confiança do usuário. Os criminosos induzem a vítima a instalar um novo módulo de segurança, que obviamente é um software malicioso.
- Documentos maliciosos - explora vulnerabilidades de documentos do padrão Office. O Hacker insere um código malicioso com um link que leva a um programa que roda automaticamente e fecha uma VPN "Reverse Shell" com a máquina do atacante. Isso permite o controle remoto da estação ou servidor.

Ameaças cibernéticas

- Engenharia social – o criminoso se passa por alguém confiável e a própria vítima passa seus dados pessoais de livre e espontânea vontade.
- Adwares - malware criado para apresentar anúncios não solicitados na tela dos usuários via navegador web, podendo abrir nova abas, alterar a página inicial ou redirecionar para sites não seguros ou impróprios.
- Man-in-the-Middle - ataque virtual em que um hacker intermedia a comunicação entre um usuário e um terceiro, interceptando mensagens enviadas e se passando por uma das partes envolvidas.
- Phising - prática que visa roubar dados cadastrais de clientes por meio de mensagens iscas, geralmente por e-mail.
- Vhising - variante do phishing e seu nome vem da junção dos termos Voice + Phishing. sistema de autoatendimento que simula a experiência de atendimento real.

Ameaças cibernéticas

- Pharming – o usuário acessa um site legítimo, mas é inadvertidamente redirecionado para um site falso com aparência autêntica.
- Ransomware - criptografa todos os dados do HD, impedindo o acesso aos arquivos. Para liberar a chave, os criminosos pedem um pagamento em criptomoedas (em geral, Bitcoins).
- Smishing - tipo de phishing e a origem de seu nome vem da junção de “SMS” + “Phishing”.
- Spyware - geralmente atua abrindo caminho no sistema operacional sem o consentimento da vítima, pegando informações sobre sites acessados, histórico de navegação e pode ter acesso a câmera de um dispositivo.
- DDoS-for-hire - alguns cibercriminosos vende seus serviços botnets que fazem o serviço de ataques DDoS (ataque de negação de serviço).

Mapeamento de ameaças
(algumas...)

https://smartdefender.cloud/search

https://cybermap.kaspersky.com/stats

https://www.netsol.com.br/mapa-de-ataques-ao-vivo/

Tipos de “atacantes”

1. *White Hats:* conhecidos como *hackers* éticos; pesquisadores e operadores de segurança para rastrear e monitorar ameaças de forma ativa. Quando descobertas, notificam as empresas sem levá-las ao público.

2. *Black Hats:* tem amplo conhecimento sobre como invadir, ignorar protocolos de segurança e escrever *malwares*. A principal motivação ao invadir empresas é ganho pessoal ou financeiro e espionagem cibernética.

3. *Gray Hats:* explora uma falha de segurança em um sistema ou produto para chamar a atenção da empresa; não tem intenção maliciosa e com o objetivo de melhorar a segurança, porém ao contrário do *White Hat*, divulga publicamente as brechas de segurança. Pode levar à exploração de criminosos.

Tipos de “atacantes”

4. ***Cracker:*** o termo *“cracker”* foi criado pelos próprios ***hackers*** para diferenciar as atividades exercidas por cada categoria. Um cracker tem muito conhecimento em informática e usa isso para quebrar (daí o termo *crack*) sistemas de segurança (e monetizar em cima disso) e de softwares (fomentando a pirataria).

5. Script Kiddies: geralmente utilizam programas escritos por outros ***hackers*** porque eles não têm habilidades para escrever os próprios códigos; foca seus ataques em sistemas e redes de computadores e sites de internet (as vezes chamados de “Lammer”).

6. Phreaker: especializado em telefonia, sistema de comunicação e outros.

7. Carder: especializado em falsificar, copiar cartões de crédito ou outro tipo.

Ameaças Passivas X Ativas

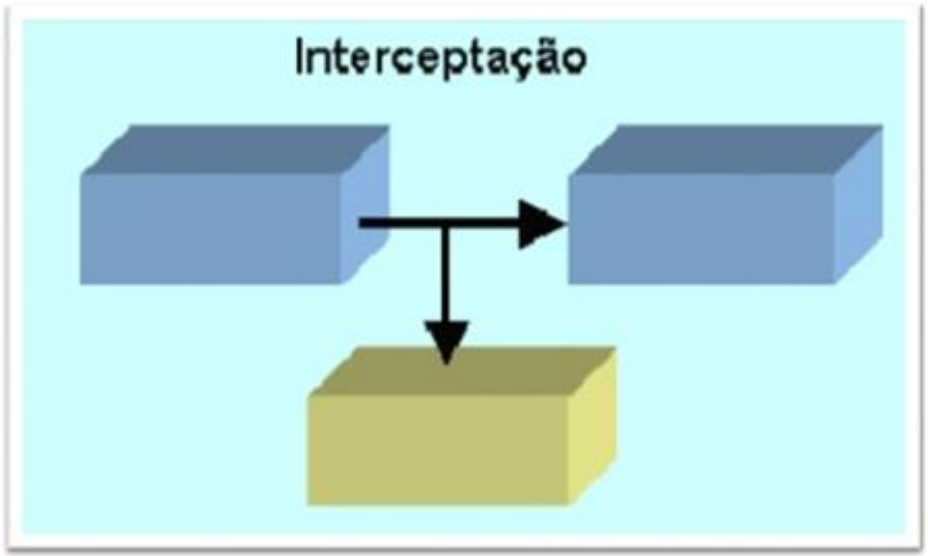
Ataques passivos são aqueles que não alteram a informação, nem o seu fluxo normal, no canal sob escuta.

Ataques ativos são os que intervêm no fluxo normal de informação, quer alterando o seu conteúdo, quer produzindo informação não fidedigna, normalmente com intuitos de atentar contra a segurança de um sistema.

Tipos de Ataques

Interceptação:

Considera-se interceptação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).

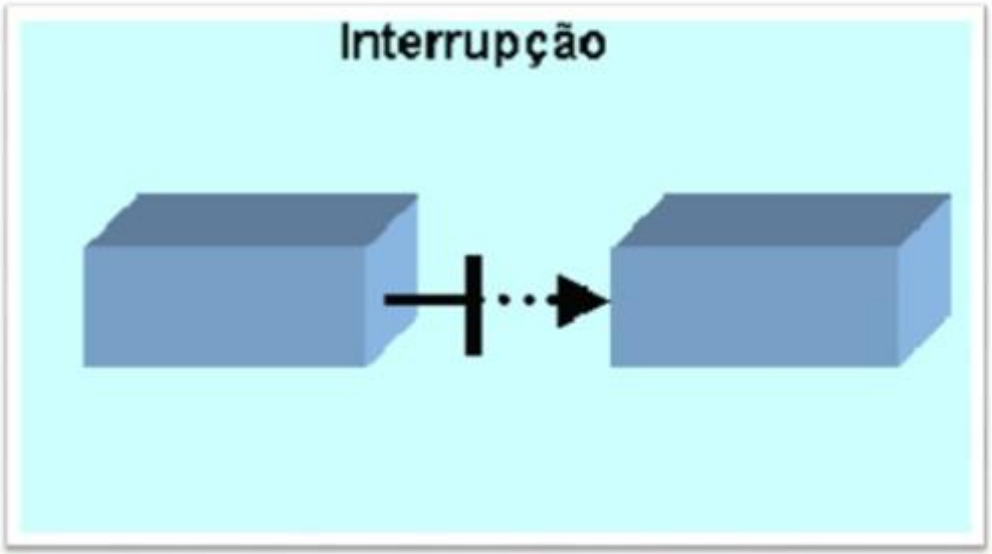


Fonte: estacio.br

Tipos de Ataques

Interrupção:

Pode ser definida como a interrupção do fluxo normal das mensagens ao destino.

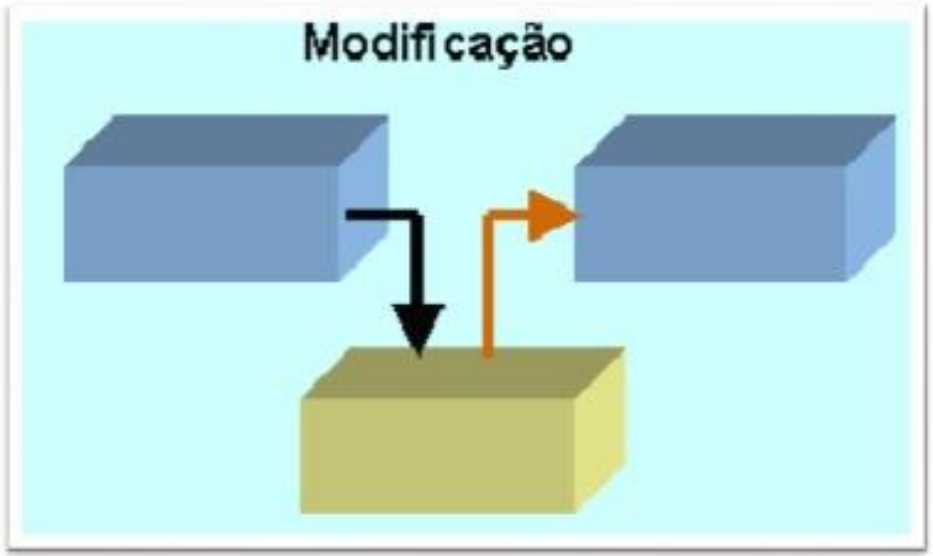


Fonte: estacio.br

Tipos de Ataques

Modificação:

Consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.

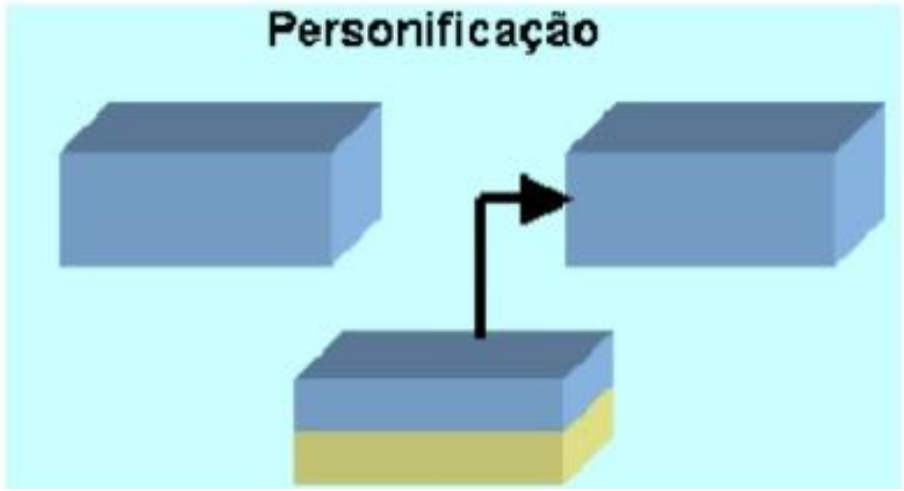


Fonte: estacio.br

Tipos de Ataques

Personificação:

Considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade.



Fonte: estacio.br

Retomando....

- Podemos ter confidencialidade sem privacidade ?
- Podemos ter integridade sem confiabilidade ?
- Podemos ter não-repúdio sem autenticidade ?
- Podemos ter auditoria sem integridade ?

Atividade no Moodle..

OBRIGADO!

https://www.eset.com/br/security-report/?utm_source=google&utm_medium=cpc&gad=1&gclid=CjwKCAjwloynBhBbEiwAGY25dJeP7vTKXv2aL3f3UaHoEVoSdOndescEdlcQPFs1gKoB_CBxcV9j7RoCBqgQAvD_BwE