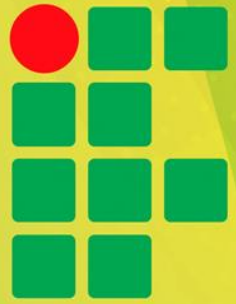
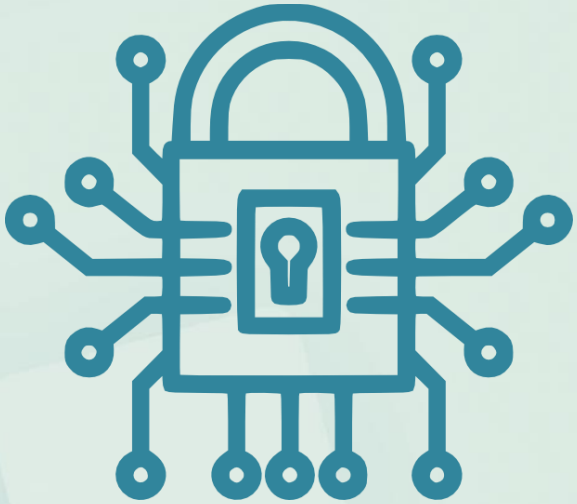


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Principais ameaças virtuais

Da atualidade

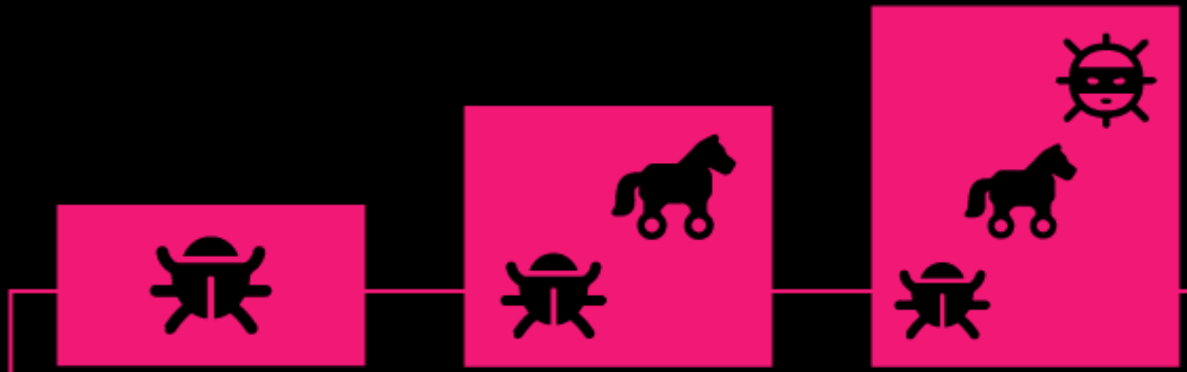
Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

1. Introdução

1. Introdução

- A transformação digital fez da informação uma poderosa ferramenta de geração de valor para as organizações. Consequentemente, a cibersegurança ganhou ainda mais importância.
- Vamos conhecer agora os principais tipos de ameaças à segurança da informação na atualidade.



A EVOLUÇÃO

dos Ataques por E-mail

2. Ataques direcionados

- Diferentemente dos ataques em massa e automatizados, os ataques direcionados utilizam informações específicas de uma organização para executar um ataque.

2.1. Como eram os ataques antes?

- Historicamente, a maioria dos ataques virtuais se deu a partir da exploração de falhas em softwares.

2.2. O que muda com a evolução dos ataques?

- A evolução tecnológica e a maior difusão do conhecimento em desenvolvimento de software permitiu criar ataques automatizados para sequestrar dados sensíveis e roubar informações pessoais, como número de cartão de crédito. Neste momento o cyber crime se profissionalizou!

2.2. O que muda com a evolução dos ataques?

- Hoje, **o principal alvo é o usuário** e não a vulnerabilidade nos sistemas.
- Dentro dos ataques automatizados o e-mail se tornou o principal meio de propagação.

2.2. O que muda com a evolução dos ataques?

57mi
brasileiros acessaram links maliciosos em 2018

55%
de todos os e-mails são SPAM

90%
dos ciberataques usam e-mail de phishing

AMEAÇAS

PERSISTENTES AVANÇADAS

3.1. O que são ameaças persistentes avançadas?

- O termo ameaças persistentes avançadas (APT – Advanced Persistent Threats) é utilizado para descrever um determinado tipo de ameaça cibernética, especialmente focado em **espionagem via internet.**


Por que PERSISTENTES?

3.1. O que são ameaças persistentes avançadas?

- São descritos como persistentes, pois na maioria das vezes são **invasores contratados para atacar determinada organização** e as tentativas de invasão só irão cessar após o objetivo final ser atingido, o que **pode às vezes demorar meses**.

3.2. Características do APT

- Ameaças Persistentes Avançadas passam facilmente despercebidas, pois **seu foco de infecção não é uma rede inteira, mas sim um computador específico**. Geralmente focam no dispositivo de um funcionário comum, mas que compartilha a rede com máquinas importantes.

3.3. Estágios de um ataque APT

- Um ataque por ameaça persistente avançada é dividido em três estágios, sendo que para que haja sucesso na invasão não pode ocorrer a detecção da ameaça em nenhum dos estágios.

3.3. Estágios de um ataque APT

- **1) Infiltração:** Os hackers entram na rede Comprometendo segmentos como ativos web, recursos da rede ou usuários com privilégio de acesso. Após a infiltração na rede os agentes instalam um backdoor, que pode ser em forma de trojans disfarçados de trechos de software legítimos. Evitando assim a detecção por ferramentas de segurança.

3.3. Estágios de um ataque APT

- **2) Expansão:** Já instalados na rede, os cibercriminosos podem acessar informações sensíveis, como dados sobre lançamentos de produtos. Esses dados podem vir a ser vendidos a concorrentes, vindo a prejudicar a empresa.

3.3. Estágios de um ataque APT

- **2) Extração:** Os dados extraídos ficam geralmente salvos em locais seguros dentro da própria rede da vítima. Quando os hackers obtêm o máximo de dados possível eles os exportam sem que sejam detectados

3.4. Como se prevenir de um ataque APT

- A proteção contra ameaças persistentes avançadas, deve ser focada em duas frentes: **boas práticas de uso corporativo da internet e do e-mail** e investimento em **tecnologia para automatizar essa proteção**.

ATAQUES

a dispositivos

IoT

4.1. Ataques a dispositivos IoT

- Os ataques aos dispositivos com IoT podem copiar ou comprometer os dados transmitidos por eles, possibilitando a espionagem industrial ou mesmo a danificação do sistema como um todo. Alguns hackers já utilizam **malwares para, por meio de dispositivos IoT, invadir computadores e controlá-los remotamente**.

4.2. Por que os dispositivos de IoT são um alvo atraente para os hackers?

- Os dispositivos de IoT, independentemente de seu uso, complexidade ou grau são um alvo atraente para os cibercriminosos, já que coletam informações privadas sobre o comportamento do usuário em certas áreas: financeira, saúde e educação.

ADWARE


FREE
DOWNLOAD!
NSFW
WARNING:
OUR COMPUTER IS INFECTED
LOSE
WEIGHT
QUICK

5.1. O que é um adware?

- Adware é um software malicioso projetado para jogar anúncios na sua tela, na sua maioria dentro do navegador web. Normalmente ele se disfarça como legítimo, sobrepondo outro programa para ludibriá-lo a instalá-lo em seu computador, tablet ou dispositivo móvel.

5.1. O que é um adware?

- Seu objetivo não é roubar dados, como é na maioria dos malwares, mas sim fazer com que você clique na maior quantidade de banner possíveis. Assim, gera receita para o desenvolvedor do software malicioso.

BUSINESS E-MAIL COMPROMISE

6.1. O que é Business E-mail Compromise (BEC)?

- Também conhecido como fraude do CEO, o Business E-mail Compromise (BEC) é um ataque novo e que utiliza de engenharia social como forma de enganar os colaboradores da empresa.

6.1. O que é Business E-mail Compromise (BEC)?

- Neste caso, o golpista estuda a empresa que será vítima do ataque, identificando no organograma da empresa as pessoas certas para aplicar a fraude. Ou seja, identifica um executivo de alto cargo e um profissional do setor financeiro responsável pelos pagamentos e tarefas administrativas.

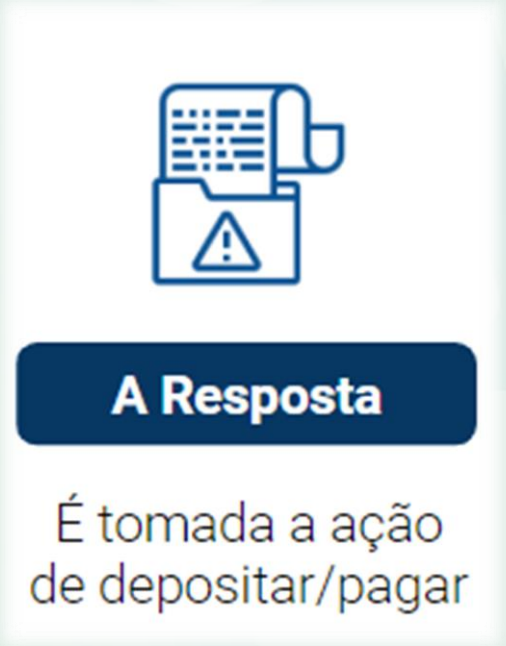
6.2. Como funciona o ataque?

- Um criminoso envia uma mensagem para uma empresa fraudando o e-mail de um profissional com alto cargo dentro desta organização, como um diretor ou presidente.

6.2. Como funciona o ataque?

- Na correria do dia a dia o profissional que recebe esta solicitação, geralmente com um cargo administrativo ou financeiro.

6.2. Como funciona o ataque?



- O funcionário faz o pagamento imediatamente e não chega a desconfiar de um possível golpe.

6.2. Como funciona o ataque?

6.3. Como se proteger do BEC?

- A primeira etapa indicada para qualquer processo de prevenção de ataques é o **treinamento da equipe**.
- A segunda etapa é investindo em tecnologia específica para **automatizar a prevenção**.

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano