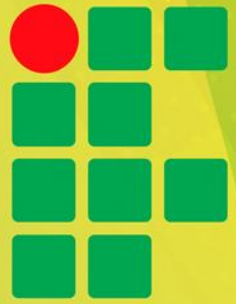
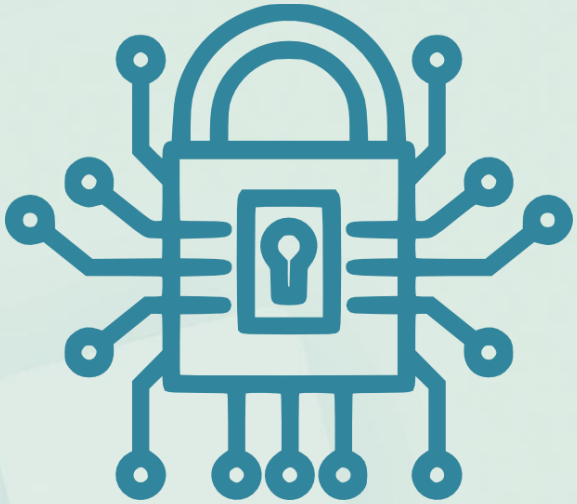


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Principais ameaças virtuais

Da atualidade

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

1

O que é PHARMING?

E COMO SE PROTEGER

1.1. O que é o Pharming?

- O pharming é um ataque que utiliza a técnica de DNS Cache Poisoning, ou **envenenamento de cache DNS**.

1.1. O que é o Pharming?

- Consiste no **corrompimento do DNS** em uma rede de computadores para que **a URL de um site aponte para um servidor diferente do original**.

1.1. O que é o Pharming?

- Durante um ataque de pharming, um usuário que está tentando entrar em um site legítimo é inadvertidamente redirecionado pelo software malicioso para um **site falso, mas com aparência autêntica**.

1.2. Como funciona?

- O comprometimento do DNS local ocorre por meio da introdução de dados não oriundos de servidores DNS de hierarquia superior, no banco de dados de cache.
- Esse banco de dados de cache é usado para que o IP do servidor destino seja resolvido mais rapidamente. Ou seja, tem a finalidade de aumentar o desempenho Web.

1.2. Como funciona?

- Quando o usuário digita suas informações pessoais, **os fraudadores podem acessar essas informações**.
- Os atacantes podem usar essas informações para várias atividades, como **compras online e acessar as contas**.

1.3. Qual é a diferença entre Pharming e Phishing?

- O **Phishing** envolve fazer com que um usuário insira informações pessoais por meio de **um site falso**.
- O **Pharming** envolve a **modificação de entradas de DNS**, o que faz com que os usuários sejam **direcionados para o site errado** quando visitam um determinado endereço da Web

1.4. Quais os tipos existentes?

- No primeiro tipo, um fraudador **entrará em contato por e-mail**, fingindo ser uma organização bem conhecida, e pedirá que a vítima clique em um link malicioso. **Se o link for clicado, ele instalará um vírus no computador que fará o desvio para o site falso.**

1.4. Quais os tipos existentes?

- O segundo tipo funciona usando um **site legítimo com um vírus**. Quando alguém insere o endereço desse site na barra de pesquisa, o vírus remete para o site falso.

1.5. Quais são os alvos?

- Mas não são apenas as grandes empresas as mais vulneráveis. **Os hackers podem até mesmo alterar a configuração de DNS no roteador doméstico inseguro de um cliente**, permitindo o redirecionamento para sites fraudulentos.

1.6. Como se proteger do Pharming?

- O que torna o Pharming assustador é que você pode ter um computador completo sem infecção e ainda ser redirecionado para um site ruim por causa de um **servidor DNS contaminado**.

1.6. Como se proteger do Pharming?

- **Inserir manualmente o URL do site que você deseja visitar também não ajudará**, o redirecionamento acontecerá no nível de tráfego da Internet, não no seu computador.

1.6. Como se proteger do Pharming?

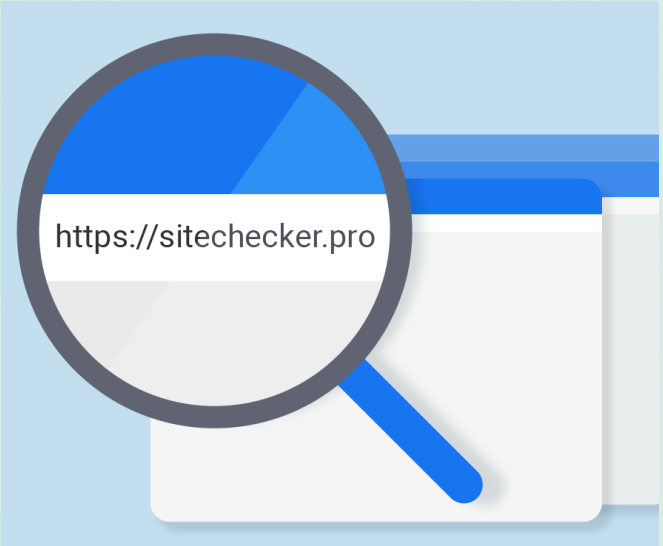
- A melhor maneira de permanecer seguro é **ficar de olho em todos os sites que solicitam credenciais** e **evitar clicar em links em e-mails** ou outros lugares para acessá-los.

1.6. Como se proteger do Pharming?

- Se abrir um determinado site e parecer diferente do que você esperava, você pode ser um alvo do pharming. **Reinicie o computador para redefinir suas entradas DNS**, execute um programa antivírus e tente conectar-se ao site novamente.

1.6. Como se proteger do Pharming?

- **Dicas:**
  - **Verifique a URL:** A defesa tem sido sempre digitar a URL do site e, ao carregar o site, verificar se o endereço destino é o mesmo que foi digitado.



1.6. Como se proteger do Pharming?

- **Dicas:**
  - **Avalie a ortografia:** Na maioria dos casos, observa-se que o invasor obscurece o URL real sobrepondo um endereço com aparência legítima ou usando um URL similarmente escrito.

lfsertao-pe.edu.br | ifisertao-pe.edu.br

1.6. Como se proteger do Pharming?

- **Dicas:**
  - **Tenha um provedor confiável:** Use um provedor de serviços de Internet confiável e legítimo. A segurança rigorosa no nível do ISP é sua primeira linha de defesa contra o pharming.

1.6. Como se proteger do Pharming?

- **Dicas:**
  - **Confira o certificado do site:** Leva apenas alguns segundos para saber se um site em que você acessa é legítimo e verificar se o site possui um certificado seguro de seu legítimo proprietário.

1.6. Como se proteger do Pharming?

- **Dicas:**
  - **Instale um software de segurança:**

    Para não enlouquecer verificando cada URL digitada, é possível deixar esse trabalho para um software focado em garantir a segurança de navegação.

2

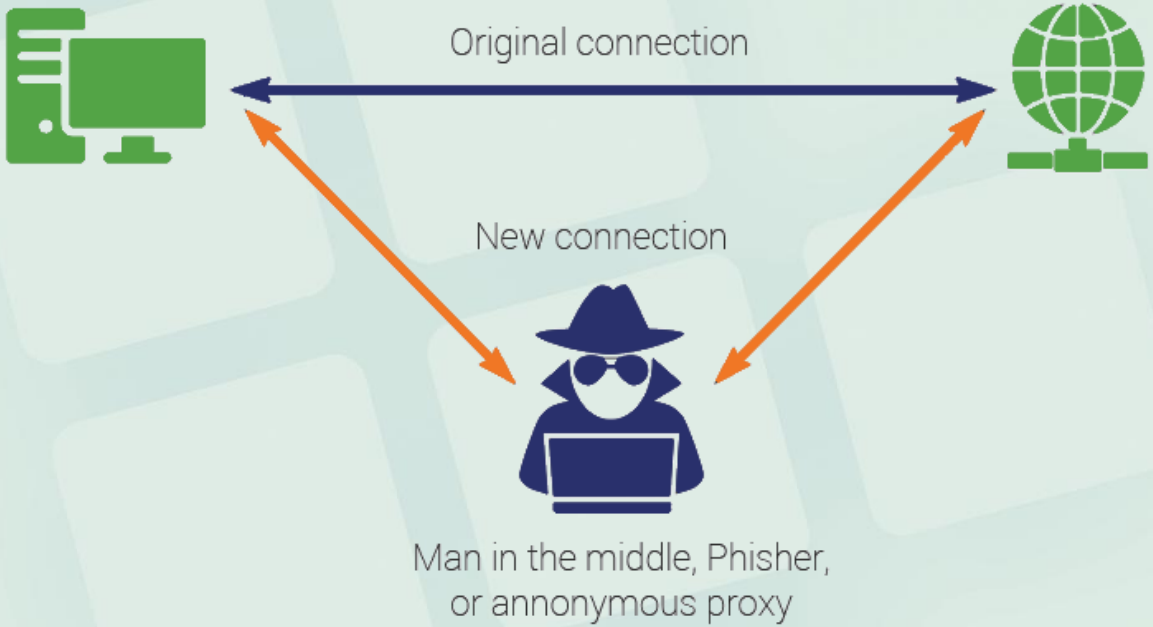
ATAQUE

de Man-in-the-Middle

2.1. Definição do Man-in-the-Middle

- O Man-in-the-Middle é um nome genérico para qualquer ataque virtual em que **um hacker intermedia a comunicação entre um usuário e uma outra parte envolvida**, como site de um banco, login e-mail ou redes sociais.

2.1. Definição do Man-in-the-Middle



2.1. Definição do Man-in-the-Middle

- Quando um invasor participa da comunicação entre os dois elementos, **ele pode adulterar ou bloquear a informação sem que as vítimas percebam**.

2.2. Ataque mais comum

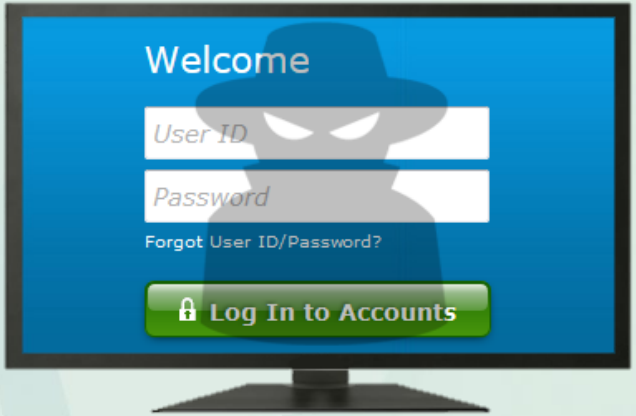
- Uma das formas mais comuns deste ataque é **utilizando um roteador wifi como mecanismo para interceptar conversas** das vítimas.

2.2. Ataque mais comum

- O atacante pode **configurar o notebook como ponto de acesso** e nomeia a rede com nome comum de redes públicas;

2.3. Man-in-the-Browser

- Uma das variantes do ataque é chamada de **man-in-the-browser**, em que o invasor implementa código malicioso no **browser** da vítima. Este ataque é realizado por meio da instalação de um malware.



2.4. Como se proteger do Man-in-the-Middle

- Evitar acessar redes de wifi públicas.
- Evite digitar qualquer informação em sites sem certificado digital (SSL).
- Utilize uma ferramenta anti-malware

3

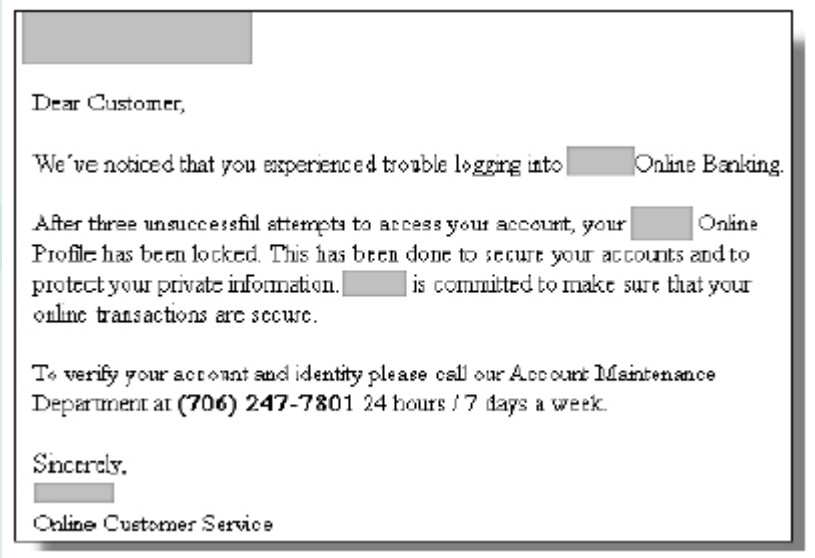
VISHING

3.1. O que é o Vishing?

- O Vishing é um novo tipo de phishing.
- A grande diferença do Vishing é que ele **utiliza a rede pública de telefonia como meio**, através da combinação entre mensagem de texto e Voip.

3.2. Funcionamento

- O atacante envia um e-mail ou SMS se passando por operadora de cartão de crédito com uma notificação de suspensão ou desativação de conta.



Dear Customer,

We've noticed that you experienced trouble logging into [redacted] Online Banking.

After three unsuccessful attempts to access your account, your [redacted] Online Profile has been locked. This has been done to secure your accounts and to protect your private information. [redacted] is committed to make sure that your online transactions are secure.

To verify your account and identity please call our Account Maintenance Department at **(706) 247-7801** 24 hours / 7 days a week.

Sincerely,

[redacted]

Online Customer Service

3.2. Funcionamento

- Para que o usuário faça a reativação é solicitado a realização de uma ligação para um número gratuito, que redireciona a chamada para um sistema de autoatendimento e pede **dados de cartão de crédito**.

3.3. Como evitar este ataque?

- Um dos métodos para evitar este tipo de ataque é **sempre ligar para os números oficiais do banco**, caso tenha dúvidas sobre algum procedimento ou receba alguma comunicação solicitando qualquer tipo de ação.

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano