Phishing

POR QUE AINDA CAÍMOS NESSE GOLPE?

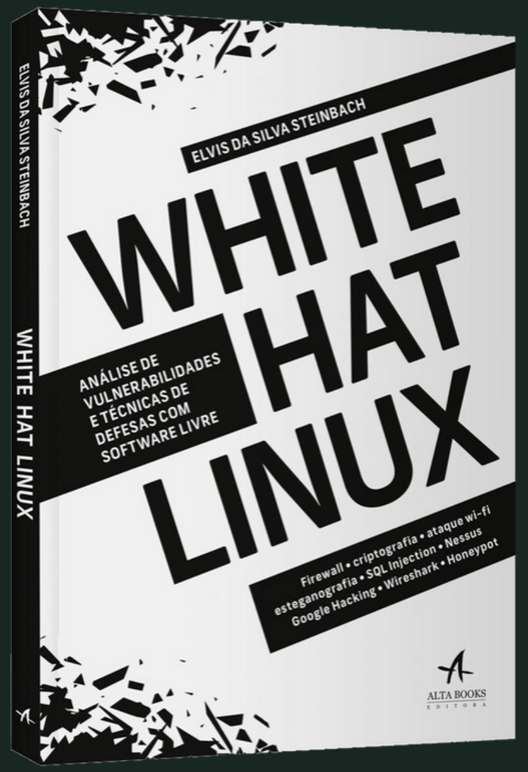
12 de Dez 2019

Quem sou?

FORMAÇÃO

Formado Técnico de Informática
Graduado em Análise e Desenvolvimento de sistemas
Pós-graduado em Segurança da Informação

Autor do livro: white Hat Linux
Adm do grupo F3 Security



O que é Phishing?

TERMO

É uma mistura de **pheaker** com **fishing**.

CONCEITO

Técnica usada para roubar informações (pescar ou fisgar) através de informação falsa.

Spear Phishing

ATAQUE DIRECIONADO

Quando falamos em spear phishing estamos falando de um ataque cuja missão é um alvo específico como: uma pessoa em particular ou empresa.

Como se origina o ataque?

ENGENHARIA SOCIAL

Através de persuação e ou aproveitando-se da inocência da vítima.

E-MAIL FALSOS

E-mails enviados como se fossem de um empresa legítima que rouba suas credenciais.

LINKS

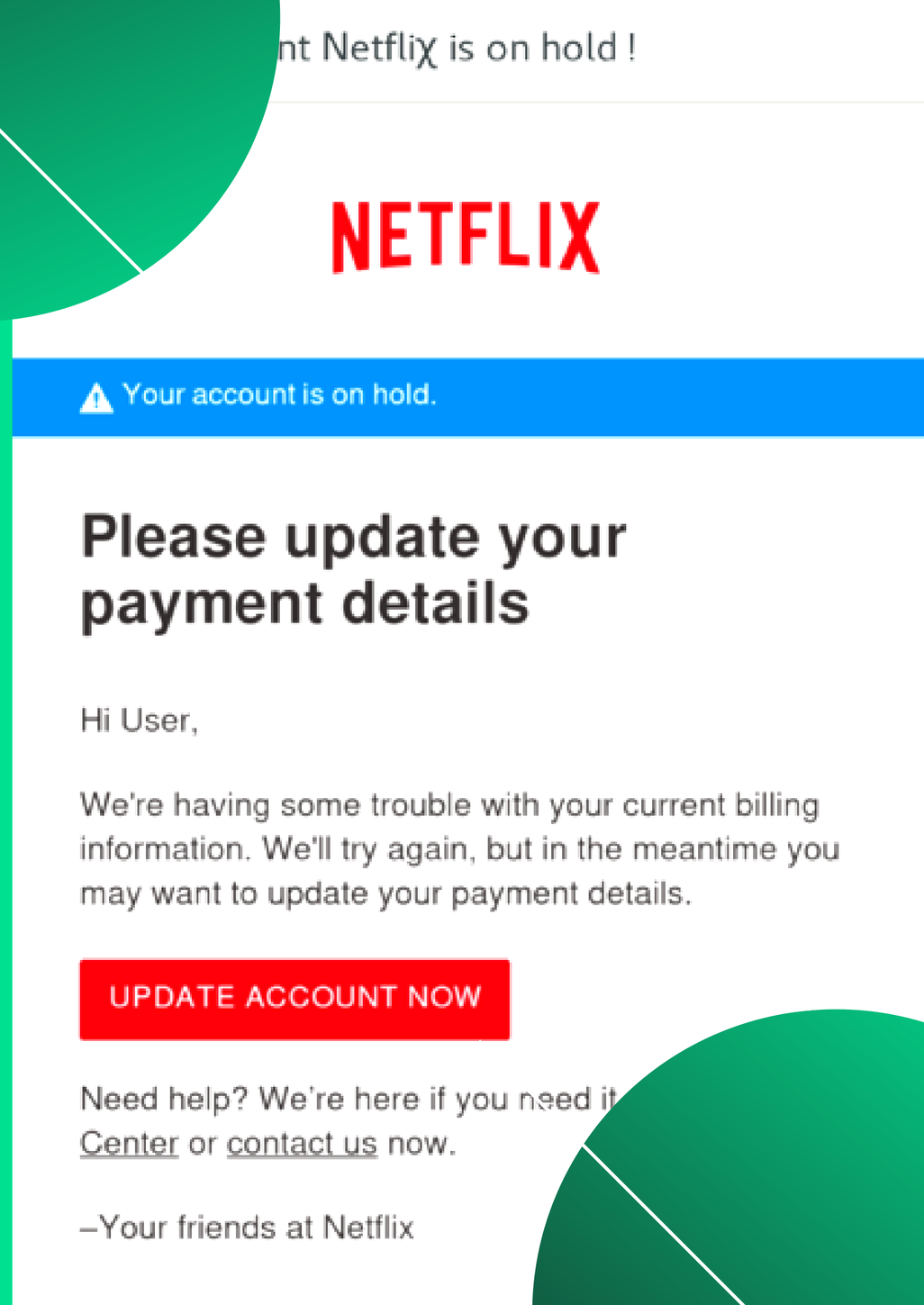
Links que inclusive podem ser incorporados em sites legítimos que também direcionam a vítima.

SITES FALSOS

Ataques de fake dns redirecionando a vítima para sites identicos aos legítimos.

Método mais comum

POR INCRÍVEL QUE PAREÇA AINDA É POR E-MAIL



Como funciona o ataque?

E-MAIL

Um e-mail é enviado para n alvos.

O E-MAIL É MUITO SIMILAR

O e-mail é muito convincente, inclusive contando com logo e tudo.

O QUE O E-MAIL PEDE?

O -email solcita atualizações de cadastro, atualizações de forma de pagamento, possui um link que redireciona para a página falsa de login da empresa. Este link geralmente é alguma promoção.

O que o cracker vai precisar?

SERVIDOR DE E-MAIL FALSO

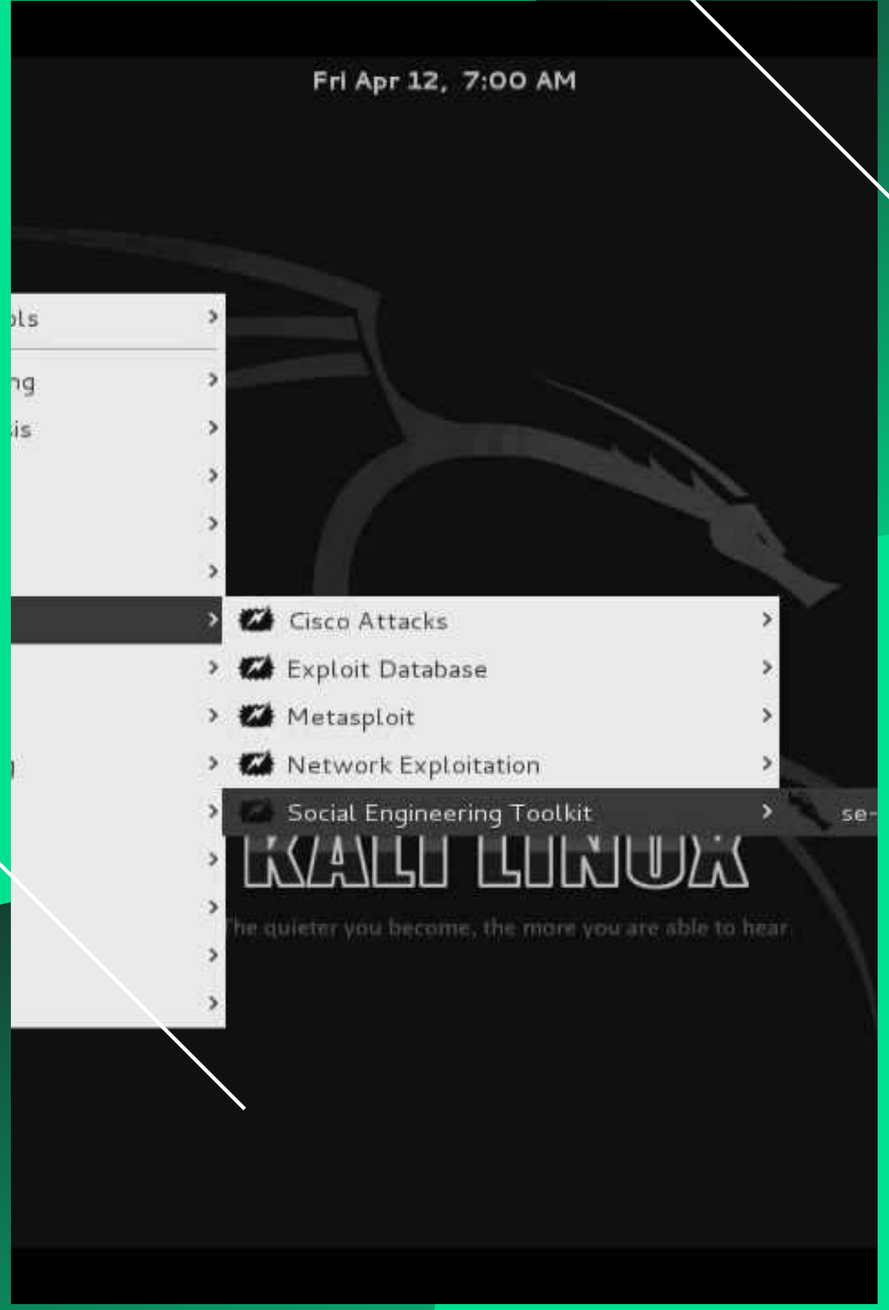
Existem diversos servidores tanto para envio como para recebimento de e-mails temporários

SERVIDOR WEB FALSO

Este servidor deve conter os serviços para que seja aprensetada a página falsa para a vítima.

ATAQUE VAI SER CURTO

Para que não seja pego o cracker vai atacar por períodos curtos e depois apagar seus lastros.



Ataques automatizados

EXISTEM INÍMERAS FERRAMENTAS PARA ATAQUES AUTOMATIZADOS QUE SÃO USADAS TANTO PARA O BEM NO CASO DE PENTESTERS, QUANTO PARA O MAL NO CASO DOS CRACKERS

ALGUMAS FERRAMENTAS

Setoolkit
SocialFish
BlackEye

Por que ainda caímos nesse golpe?

INOCÊNCIA

Acreditamos no que vemos, principalmente quando tem urgência.

DISPLICÊNCIA

Não prestamos atenção em detalhes e itens básicos que poderiam nos proteger.

DESCONHECIMENTO

Por não entendermos sobre segurança da informação.

FALHAS NO ATAQUE

ERROS DE ORTOGRAFIA

É normal as vezes vermos erros grosseiros em frases já dando indícios que é fake.

SEM ÍCONE DO CADEADO

O ícone do cadeado mostra que o site tem um certificado e indica que os dados navegam criptografados.

URL ESTRANHA

Geralmente a URL pode ser parecida e se nçao prestar atenção em detalhes pode ocnfundí-lo.

LINKS QUEBRADOS

É normal outros links da página fake não funcionarem e também ao fazer login, só verá página de erro.

Como as empresas podem se proteger?

TREINAMENTO

Deve ser feito treinamento com os colaboradores.

PENTEST

Deve ser feito testes para verificar falhas relacionadas.

FRASE DE PROTEÇÃO

Sites podem solicitar no cadastro, uma frase única que o cliente visualizará depois de logar.

INVESTIMENTO

As empresas deveriam levar a sério a segurança da informação e contratar equipes ou profisisonais específicos.

Como nós podemos nos proteger?

SEM INFORMAÇÕES

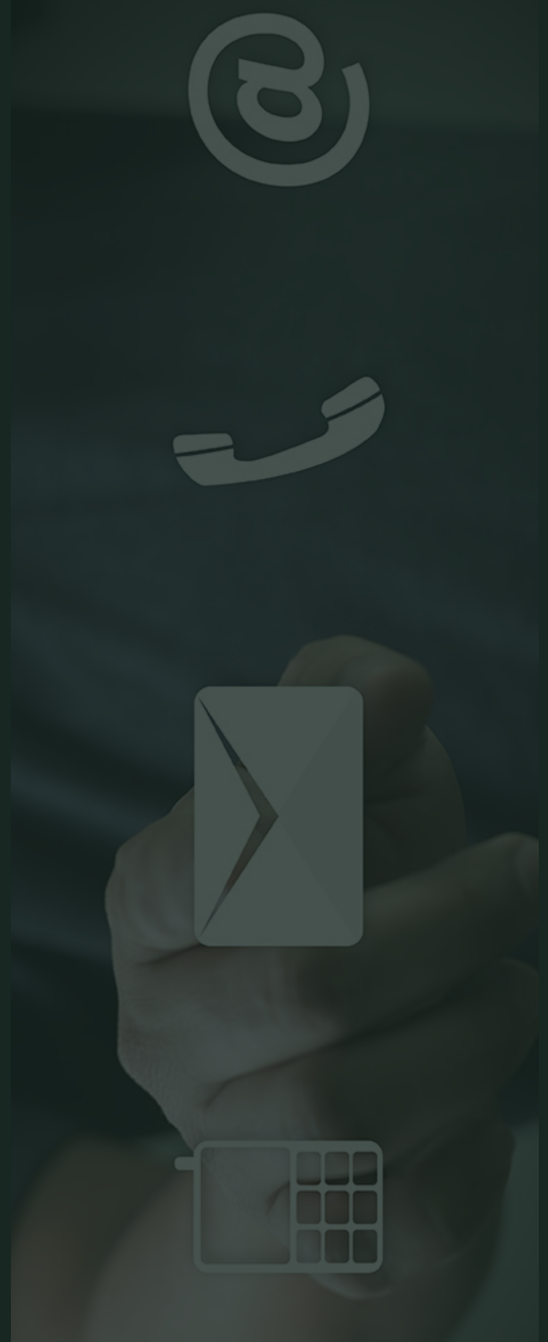
Nenhuma instituição que se preze pede por e-mail dados confidenciais.

PRESTE ATENÇÃO

Observe o cadeado, olhe a url do site e desconfie de qualquer coisa que identifique como errada.

UTILIZE ANTIVÍRUS

Os antivírus atuais checam links suspeitos de modo a criar uma camada de proteção extra.



Muito obrigado

E-MAIL

elvissteinbach@gmail.com

SITE

https://whitehatlinux.com

GRUPO

f3 security