RELATÓRIO 9 – ENGENHARIA SOCIAL

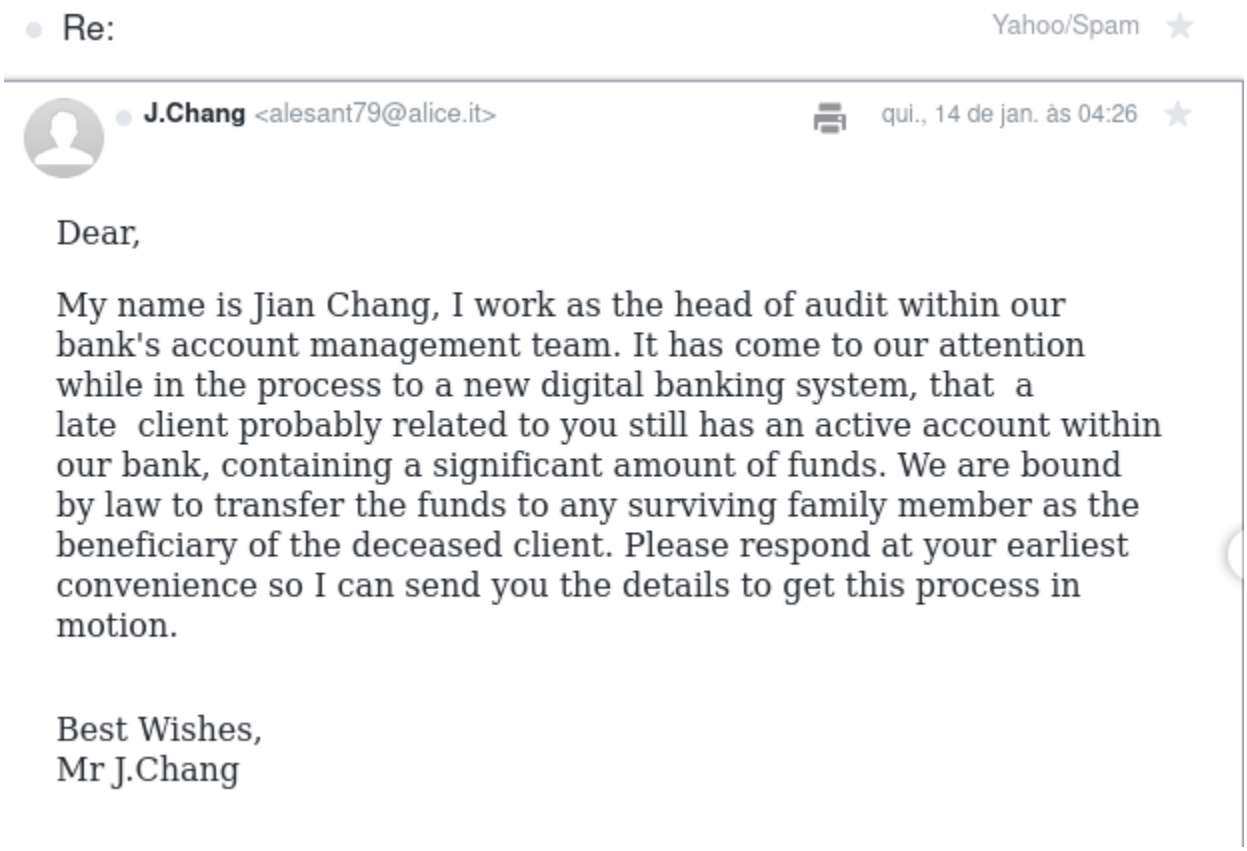
Lucas Loscheider Reis Muniz – lucaslc01@hotmail.com

TERMOS IMPORTANTES

- **Phishing**: É uma tentativa de obter informações confidenciais por meio de disfarce de uma entidade confiável em uma comunicação eletrônica. Essa técnica de engenharia social pode ser feita usando um email, mensagens via whatsapp ou sms, por exemplo, com um título importante, como dívida de um banco ou sorteio de um prêmio, obtendo assim informações como cpf, senhas, nomes, cartões de crédito.
- **Servidor Proxy:** Também chamado de apenas proxy, é um servidor que se apresenta a um grupo de máquinas de usuários, ou seja, se apresenta a frente do cliente para chegar a algum servidor. Quando os usuários solicitam o site ou um serviço da internet, o servidor proxy intercepta a solicitação e se comunica com os servidores da internet a pedido dos clientes. Esse serviço é usado para contornar restrições, impostas por governos e firewalls de certos locais, de acesso a sites. Também são usados para bloquear acesso a certos sites em uma rede de escola, por exemplo. Por fim, para proteger a identidade online ao dificultar o rastreamento do endereço IP.
- **Proxy Reverso**: Ao contrário do servidor proxy, o proxy reverso se apresenta a frente do servidor, ou seja, quando um cliente deseja solicitar um site, ele é direcionado a um servidor do meio que responde ao servidor alvo original. Não necessariamente é algo malicioso, pois pode garantir maior segurança, performance e confiabilidade.

ANÁLISE DE UMA TENTATIVA DE PHISHING VIA EMAIL

No email a seguir, analisaremos uma suposta tentativa de phishing:



Re: Yahoo/Spam

J.Chang <alesant79@alice.it> qui., 14 de jan. às 04:26

Dear,

My name is Jian Chang, I work as the head of audit within our bank's account management team. It has come to our attention while in the process to a new digital banking system, that a late client probably related to you still has an active account within our bank, containing a significant amount of funds. We are bound by law to transfer the funds to any surviving family member as the beneficiary of the deceased client. Please respond at your earliest convenience so I can send you the details to get this process in motion.

Best Wishes,
Mr J.Chang

1. Inicialmente, este email foi recebido na minha caixa de spam, o que já levanta suspeitas. É possível que alguns emails phishing consigam entrar direto na caixa principal.
2. O domínio deste email "**alesant79@alice.it**", o que levanta outra suspeita já que uma pesquisa sobre esse domínio não revela nenhuma informação sobre o mesmo. Também o assunto do email sobre minha suposta conta no banco, não parece se relacionar com o domínio do email. Vale ressaltar que algumas tentativas de phishin, são mais difíceis de identificar porque usam domínios de email bastante convincentes, contendo diferenças sutis para um email verdadeiro de uma empresa ou até mesmo nenhum diferença aos olhos da vítima. Por isso, teremos que analisar outras características do email para ajudar a identificar a veracidade.
3. No início do email, o suposto Jian Chang auditor principal da equipe de gerenciamento de contas do meu banco, inicia o e-mail me cumprimentando com "**Dear**" sem ao menos citar o meu nome. Serviços importantes como o de um banco sempre sabem os nomes dos seus clientes, pois possuem um banco de dados com informações pessoais de cadastros.
4. Estranhamente, este email nao menciona o nome ou imagens de identificação do banco ou instituição financeira responsável pelo contato.
5. O idioma do email revela que é uma pessoa for a do Brasil, o que não faz sentido já que não tenho contas exteriores de um banco
6. Analisando o assunto do email, eu nao me recordo de membro nenhum familiar o qual tenha morrido recentemente e muito menos que eu deva receber esse dinheiro da conta da pessoa. Quando algum familiar próximo falece e eu tenha o direito de resgatar seus bens, incluindo

qualquer quantia guardada em um banco, o banco nunca manda email, pois eu teria que solicitar e avisar ao banco e preencher muitos papéis burocráticos para isso.
7. O banco ou outras instituições importantes as quais um usuário tenha cadastro, nunca pedem dados pessoais via email.
8. Ao final do email, não há nenhum endereço do local ou banco.

Observamos que essa tentativa de phishing contém vários deslizes e consequentemente é fácil de identificar que é falso. Porém existem alguns muito bem elaborados, que passam confiança. Para facilitar a identificação temos que: 1. Empresas legítimas não solicitam suas informações confidenciais por e-mail, 2. Empresas legítimas geralmente chamam você pelo seu nome, 3. Empresas legítimas têm e-mails de domínio específicos, 4. Empresas legítimas não digitam palavras ou frases com erros de escrita, 5. Empresas legítimas não enviam anexos não solicitados, 6. Os links legítimos da empresa correspondem a URLs legítimos (só de colocar o ponteiro do mouse em cima somos capazes de ler o link).

PROXY REVERSO PARA CAPTURAR CREDENCIAIS

Um proxy reverso é um servidor que toma dianteira, em relação a um ou mais servidores web, para receber pedidos de clientes. Quando um cliente faz requisição de um servidor web esses pedidos são interceptados pelo proxy reverso. Com isso o proxy reverso manda recebe requisições e manda para o servidor web destino.
O objetivo dessa prática será criar um proxy reverso para capturar credenciais de um usuário qualquer.

Para realizar a prática, foi utilizado uma máquina virtual com o ubuntu server 20.10 instalado. Com isso foi instalado também nesse servidor a ferramenta nginx para realizar o proxy reverso. Depois disso é usado o comando "*sudo nano /etc/nginx/nginx.conf*" para configurar onde será redirecionado o tráfego e a porta a ser escutada, escrevendo os seguintes parâmetros dentro das chaves de http{}:

```
server{
        listen 80;
        location / {
                proxy_pass http://testphp.vulnweb.com;
        }
}
```

e com isso usado os comandos "*sudo service nginx configtest*" e "*sudo service nginx restart*" paratestar as configurações modificadas e reiniciar o servidor para o proxy reverso. Por fim acesso o browser da máquina sem com o OS utilizado kali linux e digito "127.0.0.1.80". Porém em minha máquina o proxy reverso não foi funcionou, já que o endereço anterior dava erro de conexão o tempo todo. Tentei modificações no número de porta do server mas mesmo assim não funcionou, e depois de dias de tentativas não consegui encontrar uma solução, o que me fez desistir pelo esgotamento mental. Julgando as discussões que tive com outras pessoas que tentaram, acredito que o motivo mais próximo desse problema seja ou o SO que utilizo ou o servidor ubunto simulado na virtual machine, mas isso é um achismo, já que não soube identificar o erro.