PROTEÇÃO CONTRA ATAQUES DE PHISHING NO EXÉRCITO BRASILEIRO

Daniel Moura Félix Cardoso[1], Daniel Bomfim Nunes[2]

Pós-graduado em Operações Militares[1], Técnico em Eletrônica, Especialista em Manutenção de Comunicações[2]

Resumo: Este trabalho apresenta um estudo acerca do mais comum ataque sofrido diariamente por pessoas, em esferas do poder público e na iniciativa privada, o Ataque de Engenharia Social, Phishing. Foram estudadas algumas formas que são utilizadas normalmente nesse tipo de ataque, quais ativos de rede normalmente podem ser infectados e quais os alvos mais compensadores. Foi identificado também o ataque de Spear Phishing como ferramenta direcionada de ataque e apresentadas medidas de proteção contra esse tipo de ataque. A intenção desse artigo foi a de conscientizar o público militar da ameaça existente no Ambiente Cibernético e que qualquer um pode estar suscetível a sofrer esse ataque.

Palavras-chave: Engenharia Social. *Phishing*. Ataque. Ambiente Cibernético. Exército Brasileiro

INTRODUÇÃO

Com o crescimento exponencial da utilização de dispositivos informacionais por militares do Exército Brasileiro (EB), sejam ativos particulares ou material da própria Unidade Militar, pôde-se observar o aumento do número de casos de tentativas de invasão das redes militares pelos mais diversos tipos de ataque. Dessa forma, os diversos Centros de Telemática (CT) que se encarregam de prover e manutenir a rede lógica do Exército garantem uma certa segurança efetiva desses links com a Internet e Intranet do EB.

Partindo do princípio que praticamente todos os militares utilizam da conexão com a Internet para trabalhar, pesquisar, ensinar e nas horas vagas para o lazer, coube incrementar mais ainda essa segurança ofertada pelos CT nas próprias Unidades, pelo estabelecimento de Políticas de Segurança da Informação e Comunicações (POSIC), segregação de rede corporativa das utilizadas para interesses particulares (geralmente dispositivos particulares não acessam a rede corporativa), implementação de dispositivos como Firewall, IPS/IDP, estabelecimento de Proxy, monitoramento da Rede e outros procedimentos.

Podemos fazer um paralelo de uma rede lógica com uma corrente. Esta é formada por diversos elos. Esses elos são forjados individualmente e possuem em sua liga metálica diferentes composições (até mesmo pela mistura metálica e temperatura de forja do metal). A corrente é tão forte quanto o elo mais fraco de sua corrente. Da mesma forma, qualquer ativo da rede pode ser entendido como um elo. Cada um deles é responsável pela manutenção do acesso à rede.

Mas se mesmo com todas essas formas de segurança pudesse ser elencada uma forma de invasão mais simples? E se no final de tudo, mesmo com todo esse nível de segurança implementado pelos melhores gerentes de rede e gerentes de segurança das respectivas Unidades, o mais simples dos ataques fosse realmente efetivo? Onde pode-se encontrar esse tal de “elo mais fraco”? Historicamente a maioria dos programadores, gerentes de rede e de segurança, e outros conhecedores da área de Tecnologia da Informação (TI) apontam o mesmo como sendo elo o mais fraco: o usuário.

O usuário é a razão de ser de qualquer rede informacional pautada em dispositivos lógicos. Também conhecido como “Cliente”, usufrui dos dispositivos, visando um produto final nem sempre ligado à Computação propriamente dita. Até mesmo porque a TI normalmente é uma atividade “meio” para toda a máquina empresarial ou particular.

O grande problema é que o usuário nem sempre tem o devido conhecimento (ou paciência de estudar e aprender) sobre segurança da informação. Normalmente quer apenas comprar ou receber a máquina e usar sem aprender sobre as ferramentas que ela tem ou sobre suas capacidades. Aí que está o problema. O usuário sempre prefere ter mais usabilidade que é a facilidade com a qual um equipamento ou programa pode ser usado, em detrimento da segurança do seu ativo, muitas das vezes permitindo que atualizações de segurança deixem de ser instaladas nos seus computadores.

Como exemplo disso, segundo Cossetti (2017), o ransomware Wannacry, que explorou uma vulnerabilidade nos Sistemas Operacionais (SO) Windows 7, Windows 8, Windows Server 2008 e outras versões da empresa Microsoft, já tinha sido corrigida 2 meses antes, mas muitos usuários simplesmente deixaram as atualizações do seu SO no modo manual e não as fizeram antes do ataque.

Com o crescente número de reportagens veiculadas na mídia (inclusive mídias sociais) tratando sobre quebras de segurança, mais usuários estão começando a aceitar opiniões de especialistas da área de Segurança da Informação para implementar medidas de segurança ativas e passivas nos seus dispositivos e melhoria nos seus procedimentos diários de utilização de computadores, tablets e smartphones.

Esses ataques orientados aos usuários e que nem sempre utilizam diretamente dispositivos informacionais são conhecidos como Engenharia Social. Nesse nicho, existem diversas formas de ataque que podem ser empregados. Será analisado neste artigo o ataque de Phishing, quais danos ele pode trazer à rede corporativa e quais as formas de combater a ocorrência desse ataque no Exército Brasileiro.

1 DESENVOLVIMENTO

Segundo a Cartilha de Segurança para Internet Cert.Br (2020), os ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. As motivações que levam *Hackers Black Hat, Crackers* ou Engenheiros Sociais a realizarem ataques são os mais variados, sendo os abaixo relacionados como mais importantes já elencados pela comunidade internacional da área de Segurança da Informação (SI):

a. Demonstração de poder: mostrar a um órgão público, corporação ou empresa que pode ser invadido ou ter serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente;

b. Prestígio: vangloriar-se, perante outros atacantes ou sobre a própria comunidade da Internet, por ter invadido computadores, tornar serviços inacessíveis ou desfigurar sites visados (*Defacement*); disputar com outros atacantes para verificar quem realiza o maior número de ataques ou ser o primeiro a conseguir atingir um alvo específico;

c. Motivações financeiras: coletar e

utilizar informações confidenciais de usuários para aplicar golpes;

d. Motivações ideológicas: tornar inacessível ou invadir sites para negar o seu serviço ou mudar ideias que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia; e

e. Motivações comerciais: inviabilizar o acesso ou invadir sites e dispositivos de empresas concorrentes, buscando impedir o acesso dos clientes ou comprometer as suas reputações.

Pode-se imaginar que estes ataques nem sempre consigam atingir objetivos por completo pela forma como são desferidos e o seu dano causado aos alvos, mas os realizados com maior probabilidade de êxito são aqueles que envolvem diversas técnicas de ataque e normalmente se iniciam com técnicas de Engenharia Social.

Alguns autores quando discorrem sobre os alvos, apontam que existe uma escala de estados de percepção do alvo em relação ao ataque/exploração. Parece curioso e até um pouco absurdo tentar elencar uma “escala de estados de percepção do alvo”, mas observando com profundidade, o estado em que se encontra o atacado pode influir diretamente no êxito do ataque e da sua própria continuidade.

Pode-se elencar como estado inicial aquele em que o alvo sabe que está sendo atacado/explorado e sabe quem é o autor. Essa é a situação mais favorável para o alvo, pois irá aumentar o máximo possível o seu nível de segurança direcionando para a forma de ataque que sabe ou acredita que será empregada contra ele (ou pelo menos de quem está vindo o ataque). No segundo estado, o alvo sabe que está sendo atacado/explorado mas não sabe quem é o autor. Dessa forma, o alvo precisa buscar incrementar ao máximo a sua segurança em todas as frentes.

Um terceiro estado é aquele que o alvo não sabe que está sendo atacado/explorado e não sabe quem é o autor. Dessa forma, tudo ocorre normalmente na vida do alvo e o atacante permanece explorando a vulnerabilidade enquanto esta não for eliminada. O estado mais favorável ao atacante é aquele em que o alvo não sabe que está sendo atacado/explorado, porém garante que não está sendo alvo de ataques e explorações. Essa atitude tomada por um gerente de segurança em sua rede é muito nociva pois pode tranquilizar os usuários acerca de uma situação inverídica e pode causar danos irreversíveis ao seu órgão ou empresa.

1.1 ENGENHARIA SOCIAL

Ao pensar no fator segurança da informação/cibernética é necessário elencar primeiramente todos os aspectos tecnológicos possíveis, sejam eles dispositivos, aplicações ou sistemas que venham a prover a segurança planejada. Desta feita, todo o projeto de segurança física e lógica é elaborado e aperfeiçoado continuamente a fim de mitigar as ameaças existentes no cenário cibernético. No entanto, um fator primordial, muitas vezes esquecido, é o sujeito que opera, controla, acessa, manipula e realiza as mais variadas tarefas através dos equipamentos e sistemas aos quais possuem acesso.

E por que o fator humano é tão vulnerável? Isto ocorre devido à individualidade reservada a cada um, ou seja, para cada indivíduo há interesses pessoais diferentes, os quais culminam em rotinas de trabalho diferenciadas e conceitos diversificados sobre o que é seguro ou não. Esta falta de informação, capacitação ou mesmo interesse quanto ao que convém para garantir a segurança de dados é o que torna os recursos humanos tão susceptíveis a quebras ou falhas de segurança, quer sejam intencionais ou não. Dessa forma o fator humano torna-se um alvo de grande valia para os Engenheiros Sociais.

A Engenharia Social é uma técnica (ou conjunto de técnicas) por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. É considerada uma

prática de má-fé, usada por fraudadores para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de angariar ganhos financeiros, aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza Engenharia Social (CERT.BR, 2020).

A segurança cibernética se baseia em quatro pilares, os quais são confidencialidade, disponibilidade, integridade e autenticidade da informação. Segundo Jeremy *et al* (2015):

> A Engenharia Social, no contexto da Segurança da Informação é a manipulação de pessoas para levá-las inconscientemente a executar ações que causam danos à confidencialidade, integridade e disponibilidade de recursos da organização, incluindo a informação, os sistemas de informação e os sistemas financeiros (*apud* MAULAIS, 2016, p. 23).

Um engenheiro social em alguns casos, costuma estudar as preferências, acessos, páginas visitadas, ambiente social, amizades, objetos pessoais, opiniões políticas e tudo aquilo que possa ajudar a traçar um perfil do alvo desejado. Com menos riqueza de detalhes, há também, o estudo de grupos com características comuns, por exemplo "pessoas com dívidas" e "pessoas que precisam de emprego".

Com o estudo mais pormenorizado é comum o atacante coletar informações nas redes sociais. Isso ocorre porque, sem uma consciência de segurança da informação, as pessoas acabam publicando, registrando, arquivando na rede e compartilhando informações pessoais e, em alguns casos, até mesmo confidenciais. Então, o engenheiro social analisará os dados que lhe forem convenientes e, a partir daí, formulará uma "porta de entrada" para acessar a informação que o alvo estudado pode fornecer. O ideal, para o atacante, é que a obtenção do que deseja ocorra de modo que a vítima não perceba e para isso há diversas formas.

O Engenheiro Social pode se aproximar de maneira mais rápida, como uma falsa entrevista de emprego, onde retirará o máximo de informações aproveitando a vulnerabilidade de um sujeito que deseja trocar de emprego, por exemplo. Mas também pode ser um processo mais demorado onde espera que a vítima se sinta confortável o suficiente para compartilhar informações sem perceber sua importância. Uma ameaça em troca de informação pode ocorrer quando inocentemente publicamos ou registramos em redes sociais conteúdos como composição familiar, horários da rotina pessoal, local e função em que determinada pessoa trabalha.

No caso em que grupos com características comuns são tidos como alvo, o método de ataque é mais abrangente. Uma ligação com a intenção de oferecer um empréstimo mediante um cadastro e que pergunta sobre dados pessoais é um caso corriqueiro onde o objetivo é apenas coletar documentos pessoais e financeiros. Todas essas informações são passadas pela própria vítima por confiar em quem está do outro lado da linha.

Com a diária utilização de dispositivos que acessam a Internet, as pessoas costumam trocar informações ou realizar cadastros através de seus e-mail pessoais e, no caso de algumas organizações, dos e-mails funcionais (e-mails corporativos utilizados normalmente para assuntos que dizem respeito ao trabalho).

No caso do Exército Brasileiro, por exemplo, uma ligação ou e-mail contendo diretrizes ou solicitando dados e que se caracterize como uma autoridade tem maiores chances de ser seguido. Isso ocorre pois o Engenheiro Social sabe que os militares seguem o princípio da hierarquia e no caso do público menos experiente a tendência é não agir com a mentalidade da segurança da informação.

As mensagens de e-mail podem conter links que direcionam a vítima para um site falso que coleta informações ou mesmo que realiza o download de alguma ferramenta com um malware (software malicioso) escondido. Além disso, há a possibilidade de ameaças

via e-mail. Todas essas modalidades se enquadram numa forma de ataque denominada *Phishing*.

1.2 *PHISHING*

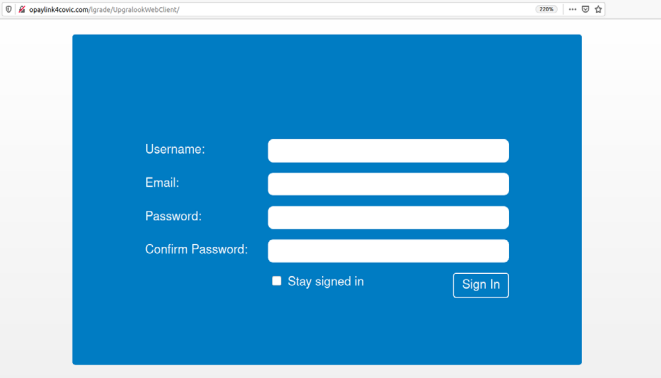
O *Phishing-Scam, Phishing/Scam* ou simplesmente *Phishing* é o tipo de golpe por meio do qual um atacante tenta obter dados pessoais e financeiros de um usuário, de maneira fraudulenta, pela utilização combinada de meios técnicos e Engenharia Social (CERT.BR, 2020). Dentro daquela ideia de que o usuário é o elo mais fraco da corrente por necessitar do serviço e desconhecer muito da Computação, é mais exitoso tentar ludibriá-lo com técnicas nem sempre “ortodoxas”.

O *Phishing* ocorre por meio de envio de mensagens eletrônicas (normalmente por e-mail) que tentam coagir, convencer ou enganar o alvo de algo que deva ser feito. No caso da coação, geralmente o alvo é colocado em uma situação que deva cumprir com tarefas para poder impedir um mal maior. Recentemente, um e-mail foi encaminhado para uma determinada Unidade Militar que requeria que fossem adquiridos cartões de crédito pré-pagos e enviadas fotos dos cartões para um específico e-mail, pois o dito Hacker informou que havia acessado à máquina e criptografaria o seu armazenamento inteiro. O mesmo atacante informou que tinha informações sigilosas de cunho pessoal e que iria expor o alvo se não fossem cumpridos os procedimentos.

Já a tentativa de convencimento é aquela que o alvo recebe informações que procuram atrair a sua atenção, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira. Pelo convencimento, o alvo pode fornecer informações, recursos financeiros ou dados pessoais ao atacante, clicando em algum link ou literalmente enviando informações para o atacante, por meio de e-mail ou de uma página de que receba os dados.

Enganar o alvo envolve tentar se passar por comunicação oficial de uma instituição conhecida, como um banco, empresa ou site popular. Basicamente esse tipo de ataque é mais efetivo com aquele tipo de usuário que realiza muitas transações financeiras pela Internet. Comumente, são utilizadas páginas falsas clonadas das reais; de instalação de códigos maliciosos de toda ordem, projetados para coletar informações sensíveis; ou de preenchimento de formulários contidos na mensagem ou em páginas Web. Em maio de 2020, foi veiculada nas contas do EBMail de vários militares do Exército uma mensagem dizendo que o militar deveria atualizar os dados de usuário, e-mail e senha para que não fosse desativada permanentemente sua conta de e-mail.

Figura 1 Tela de login falsificada



Fonte: O Autor (2020)

O que é muito claro nesses ataques de Phishing é a urgência em que o alvo é colocado, necessitando sempre fazer tudo de forma rápida para que “o pior não ocorra”. Essa urgência tem a finalidade de evitar que a vítima tenha tempo para raciocinar melhor e evitar o golpe. Alguns outros ataques são direcionados apontando uma solução aparentemente plausível para o problema apresentado, como por exemplo o ataque que diz que o antivírus da vítima não está atualizado mas um link apresentado em um e-mail pode resolver esse problema. Analisando friamente a situação, dificilmente um e-mail recebido estaria orientado exatamente ao antivírus de uma máquina específica.

Ainda assim, nos e-mails de *Phishing*, o atacante nem sempre dispõe de informações específicas para o seu alvo. As poucas infor-

mações apresentadas no ataque são genéricas, não direcionadas. Dessa forma, o *Phishing* pode ser distribuído para muitos alvos, visando atingir o máximo possível de pessoas para poder obter maior resultado, ou pelo menos um alvo para acessar a rede em que aquele usuário está participando.

Segundo o site *Intuit Online Security Center* (2020), as variantes do *Phishing* são o *Vishing, Smishing e Pharming*. Todas essas formas de ataque, baseado no *Phishing* possuem resultado semelhante. O *Vishing* nada mais é do que a mesma técnica de Engenharia Social empregando uma ligação Telefônica e o Smishing por mensagem de texto (SMS ou aplicativos de mensagens). Novamente, assim como o *Phishing*, a ligação telefônica *Vishing* e a mensagem de *Smishing* geralmente requisitam atenção imediata. Já o *Pharming* é um golpe em que o Engenheiro Social instala, utilizando normalmente um link compartilhado por ele, em que este código redireciona todos os cliques feitos em um site para outro site falso sem o consentimento do usuário. Essa tarefa é realizada pela corrupção de direcionamento do *Domain Name System* (DNS), que é responsável em linhas gerais por apontar o endereço lógico, traduzido do endereço escrito na barra dos navegadores. (Site Netspeed, 2019).

Existe ainda uma forma mais específica do *Phishing* chamado de *Spear Phishing.* Essa técnica de Engenharia Social será abordada no capítulo seguinte, visando identificar melhor a sua forma de atuação e porque acaba sendo mais efetiva do que um *Phishing* comum.

1.3 SPEAR PHISHING

O *Spear Phishing* é um tipo de técnica de Phishing que consiste em um ataque direcionado para um alvo específico. Este trabalho normalmente é muito bem feito para que possa cobrir todas as falhas de um ataque de *Phishing*. Na verdade, o *Spear Phishing* normalmente é uma das últimas fases do ataque propriamente dito. Existe uma gama de outras técnicas de coleta de informações que são necessárias a serem realizadas anteriormente para poder enfim aplicar o golpe.

Existem várias maneiras pelas quais um Engenheiro Social pode tentar obter informações confidenciais, tais como:

a. *Dumpster Diving*. Procurar informações nos lixos das empresas;

b. Monitoramento de Rede. Invadir a rede e monitorar o tráfego que ocorre nela ou o tráfego que sai da rede para a Internet;

c. *Open Source Inteligence*. Coletar informações em fontes abertas, como redes sociais ou buscadores da Internet;

d. *Shouder Surfing.* Coletar informações por “cima do ombro” de um alvo*;* e

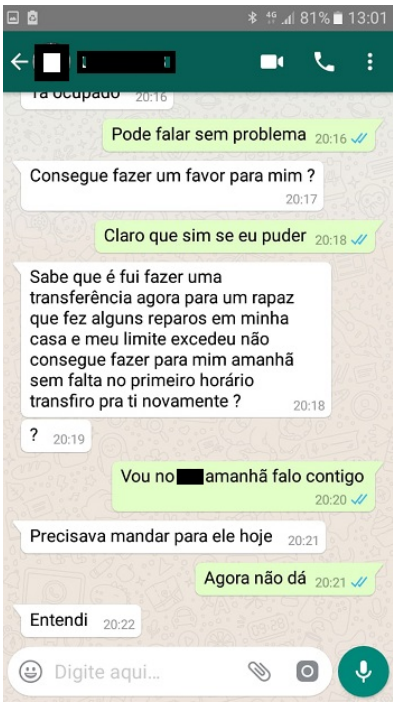
e. *Tailgating*. Acessar setores da empresa impedidos, simplesmente seguindo pessoas credenciadas.

Essas técnicas são apenas algumas das quais podem ser utilizadas para coletar inicialmente informações que subsidiam o ataque de *Spear Phishing* propriamente dito. No próximo passo do ataque, o alvo recebe um contato (e-mail, SMS, telefônico ou outro) em que dados particulares e de conhecimento exclusivo do alvo ou de um círculo de pessoas bastante restrito são apontados inicialmente. Nesse ponto, o Engenheiro Social apresenta o ataque conforme descrito anteriormente, tentando coagir, convencer ou enganar o alvo de que algo deva ser feito.

Na coação, normalmente uma informação ou dados do alvo são apresentados e o mesmo tem pouco tempo para realizar um pagamento ou tomar uma atitude em favor do atacante. Quando a forma é o convencimento ou enganação do alvo, normalmente as informações coletadas anteriormente são utilizadas para dar crédito ao atacante e se fazer passar como uma pessoa/empresa legítima. Acreditando no atacante, o alvo realiza transações financeiras ou a ação desejada em favor desse.

Na Internet, há vários casos de ataques direcionados, em que, após o roubo da conta do aplicativo WhatsApp de um usuário, o atacante realiza contato com um amigo ou parente do titular real do aplicativo (alvo) solicitando transferir dinheiro para uma conta ou pagar um boleto por exemplo.

Figura 2 Conversas Telefônicas

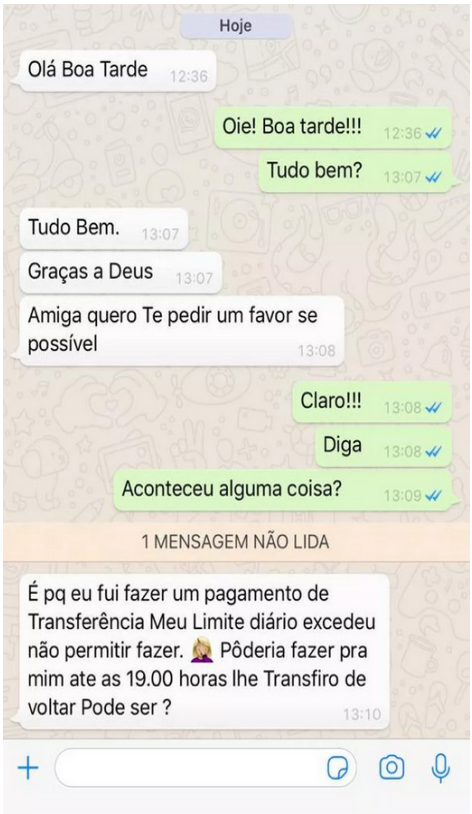


Fonte: Brasil Agora (2019)

Uma história no mínimo curiosa que aconteceu de *Spear Phishing* foi a da venda do jogador de futebol Leandro Paredes, transferido do time russo *Zenit* para o francês *Paris Saint-Germain* (PSG) pelo valor de 40 milhões de Euros.

> Quem ficou feliz com a notícia foi o argentino Boca Juniors: como clube formador do atleta, segundo regras da FIFA, ele tinha direito de receber cerca de 3,5% da venda. (...)
>
> O valor total que o Boca Juniors deveria receber é de € 1,3 milhão. Como o valor é alto, o PSG combinou que pagaria em três parcelas, sendo que a primeira a ser paga cairia dia 6 de março de 2019 no valor de € 519.750,99. (...)
>
> Após checar recibos de comprovação de transferência e algumas semanas passadas, o clube argentino notou que algo deveria ter dado errado. Durante investigação nos documentos e mensagens trocadas entre os times, o Boca descobriu que o dinheiro do PSG foi transferido primeiro para uma conta bancária de uma empresa mexicana, Vector Casa de Bolsa, e depois para um banco em New York, antes de retornar ao México, para uma conta da empresa OM IT Solutions S.A. de C.V. Uma movimentação atípica.
>
> O que aconteceu: cibercriminosos fizeram um esquema de *Phishing* para enganar o PSG. Eles enviaram emails de endereços falsos, parecidos com o domínio real do Boca, com instruções de depósito dos € 520 mil. A diferença entre o email real e o falso estava em apenas 1 caractere. (Site Terra, 2019)

Figura 3 Conversas Telefônicas



Fonte: G1 (2019)

Spear Phishing normalmente é direcionado a grandes empresas, na pessoa de *CEO* (Chefe Executivo), Vice-Presidentes ou Gerentes (principalmente os financeiros), visando anular terceiros que possam assessorar o chefe que se trata de um golpe. No caso apresentado anteriormente, o trabalho de levantamento de dados foi muito bem feito por parte

da equipe atacante, que sabia exatamente o valor, a data e as credenciais de e-mail que entraria em contato com o time PSG para a transação. Faltou por parte do time que depositou o dinheiro verificar exatamente se aquele contato realmente se tratava da parte da empresa que realmente deveria ser paga (Time Boca Juniors).

1.4 PROTEÇÃO CONTRA *PHISHING*

Ao se tratar de Segurança da Informação, é fundamental especificar as Políticas de Segurança da Informação e Comunicação. Estas devem conter, além das especificações técnicas (segurança física e lógica) de proteção, um programa que vise a defesa/proteção contra-ataques de Engenharia Social. Para tal, é essencial que sejam implementadas medidas que promovam uma cultura de segurança bem como a conscientização quanto à vulnerabilidade que todos os usuários podem trazer. Segundo LONG (2013), "A educação é naturalmente considerada um dos principais métodos para se defender contra *Phishing*" (*apud* MAULAIS, 2016, p. 52).

No âmbito de Exército Brasileiro o ideal é que ocorram palestras geridas pelos militares responsáveis pela área de Tecnologia da Informação e Comunicação e aqueles que gerenciam as Agências de Inteligência. As orientações devem ser conduzidas de modo a conscientizar cada usuário de que ele é alvo de ameaças e que possui a responsabilidade quanto à informação que é divulgada. Para tal, é necessário explicar o que é *Phishing*, suas variantes e dar exemplos práticos. Além das palestras, é recomendado que existam cartazes de conscientização e também que informem casos recentes de ataques, e as medidas adotadas para evitá-los. Orientações na páginas da Intranet das Organizações Militares (OM) também são um ótimo recurso para gerar a cultura de segurança.

A partir do momento que os usuários estejam familiarizados com as possibilidades de Phishing é ideal focar no reconhecimento e formas de evitá-lo. As principais recomendações são:

a. Verificar a origem (remetente) das mensagens recebidas;

b. Prender e identificar um documento oficial. Isto se dá observando a confiabilidade da fonte, procurando erros ortográficos, confirmando com outros integrantes da Organização a origem do documento, suspeitando de mensagens contendo links ou solicitando confirmação de dados pessoais;

c. Suspeitar de mensagens que contenham ameaças; e

d. Não fazer download de anexos que estejam em e-mails suspeitos.

O militar que identificar qualquer uma das possibilidades citadas deve imediatamente comunicar o fato ao chefe da Seção de Inteligência e à equipe de Segurança da Informação.

Os gestores da Segurança da Informação na OM que sofreu a tentativa de ataque devem realizar a análise da mensagem enviada bem como dos possíveis danos que ela possa ter ocasionado. Caso a mensagem tenha sido detectada antes de coletar dados, o primeiro passo é fazer a exclusão segura desta e em seguida veicular em todos os canais de comunicação o ocorrido para outros integrantes da rede. Dessa forma, é possível minimizar futuros danos do mesmo ataque. Para o caso em que dados já tenham sido coletados, será necessário fazer uma averiguação da rede e verificar o possível isolamento dos dispositivos e dados que tenham sido infectados ou exfiltrados. Além disso é fortemente recomendada a solicitação de apoio dos Centros de Telemática a fim de mitigar a propagação da ameaça.

CONCLUSÃO

Engenharia Social é uma das maiores armas de um hacker. Nem sempre é necessário ligar um computador para realizar um ataque cibernético. Um hacker de respeito é

aquele que consegue mesclar diversas técnicas de reconhecimento, exploração e ataque para conseguir lograr êxito em sua tarefa. O dever do gestor de Segurança da Informação é garantir que não somente seus servidores, bem como seus dispositivos finais e estrutura lógica, mas também (e muitas das vezes mais importante) os seus usuários estejam preparados para confrontar ataques cibernéticos, direcionados ou não.

Nas palavras do autor do Best Seller A Arte de Enganar e antigo Engenheiro Social Kevin Mitnick:

> Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: O hacker convencerá alguém a entrar no escritório e ligar aquele computador. Tudo é uma questão de tempo, paciência, personalidade e persistência. Kevin David Mitnick

Muitos presidentes de empresa, chefes de órgãos ou repartições públicas em todos os níveis acabam se atentando para a necessidade da segurança da sua estrutura lógica apenas quando é tarde demais. Um ataque cibernético pode atrasar em anos, talvez décadas de trabalhos realizados. Dificilmente alguma empresa utiliza um sistema que não seja pautado em dispositivos informacionais. Pelo menos não uma que queira trabalhar com velocidade na sua troca de Informação.

Portanto, treinar o Soldado do Exército Brasileiro em cibersegurança é fundamental para manter a segurança da informação da rede corporativa, dos seus ativos de rede, principalmente das informações sigilosas da Força Terrestre. A palavra-chave é conscientização!

Treinamentos periódicos de cibersegurança, alertas quanto aos ataques sofridos na Internet por outros órgãos públicos e empresas particulares, e vigilância contínua da rede são alguns dos procedimentos indicados para se manter uma relativa segurança à Rede. Isso porque não há firewall que impeça um ser humano de ser vítima de um golpe de Engenharia Social! Segundo o Site Proof (2020), essas são algumas medidas fundamentais:

a. Usar senhas fortes: que possuam letras maiúsculas e minúsculas, números, e caracteres especiais. Essas senhas demoram mais para serem quebradas por programas e algoritmos. O Site Kaspersky desenvolveu uma calculadora que apresenta em quanto tempo a sua senha pode ser quebrada. Essa calculadora é está disponível no site *Secure Password Check*, cujo endereço eletrônico é <https://password.kaspersky.com>.

b. Alterar as senhas com frequência;

c. Não usar a mesma senha para mais de um aplicativo, sistema ou website: para cada login, deve ser planejada uma senha distinta da outra, pois senhas variadas impedem a exposição de todas as suas contas se uma delas vazar (também não é muito indicado guardar as suas senhas na própria rede, pois se ela for invadida, todos os logins e senhas serão expostos);

d. Utilizar um gerenciador de senhas: para administrar senhas fortes e variadas sem precisar decorá-las, é interessante utilizar uma ferramenta dessas, de modo que o usuário possa gerar novas senhas aleatoriamente (que não possuam nenhum significado para o usuário e reduzam a possibilidade de serem adivinhadas por Engenharia Social); também pode ser utilizado para compartilhar informações de login com segurança e privacidade com outros usuários;

e. Não clicar em links suspeitos: analisar a URL disponível e no caso de hiperlink, ao passar o cursor do mouse em cima, esse estará disponível. URLs encurtadas (bit.ly), por exemplo, são amplamente utilizadas nas fraudes; e

f. Não abrir anexos não solicitados: podem possuir malwares ou documentação falsa, como um boleto fraudulento.

Quão seguro é a sua senha? A figura 4, produzida por Mike Halsey, do Site Ghacks.net (2012) que aponta quanto tempo leva apro-

ximadamente para serem quebradas as senhas em cada um dos casos de mescla ou não de números, letras maiúsculas e minúsculas e caracteres especiais.

Figura 4 Tempo de quebra das senhas

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Fonte: HALSEY, Mike. 2012.

Apesar do *Phishing* ser amplamente difundido por diversos meios de comunicação, tanto na vida particular quanto na profissional, muitas pessoas continuam sendo alvos exitosos de ataques de Engenharia Social, gerando grande prejuízo financeiro ou informacional. Isso mostra o despreparo que ainda reina entre os usuários que não permanecem alertas aos indícios do ataque tendo consequências desastrosas. Por isso é imperiosa a manutenção dos treinamentos, capacitações e conscientização de todos que participam das redes militares, nem que seja pelo menos por um instante.

PROTECTION AGAINST PHISHING ATTACKS IN THE BRAZILIAN ARMY

ABSTRACT. THIS PAPER PRESENTS A STUDY ABOUT THE MOST COMMON ATTACK SUFFERED DAILY BY PEOPLE, IN SPHERES OF PUBLIC POWER AND IN THE PRIVATE SECTOR, THE ATTACK OF SOCIAL ENGINEERING, PHISHING. SOME WAYS THAT ARE NORMALLY USED IN THIS TYPE OF ATTACK HAVE BEEN STUDIED, WHICH NETWORK ASSETS CAN USUALLY BE INFECTED AND WHICH ARE THE MOST REWARDING TARGETS. THE SPEAR PHISHING ATTACK WAS ALSO IDENTIFIED AS A TARGETED ATTACK TOOL AND PROTECTION MEASURES AGAINST THIS TYPE OF ATTACK WERE PRESENTED. THE INTENTION OF THIS ARTICLE WAS TO MAKE THE MILITARY PUBLIC AWARE OF THE THREAT THAT EXISTS IN THE CYBER ENVIRONMENT AND THAT ANYONE CAN BE SUSCEPTIBLE TO SUFFER THIS ATTACK.
KEYWORDS: SOCIAL ENGINEERING. PHISHING. ATTACK. CYBERNETIC ENVIRONMENT. BRAZILIAN ARMY

REFERÊNCIAS BIBLIOGRÁFICAS

ARIMURA, Mayumi. Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros. Disponível em: <https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros>. Acesso em: 22 maio 2020.

BRASIL AGORA. Golpe Whatsapp clonado pedindo dinheiro. Disponível em: <https://brasilagora.net.br/?p=1618>. Acesso em: 21 maio 2020.

CERT.BR. Golpes na Internet. Disponível em: <https://cartilha.cert.br/golpes/>. Acesso em 20 maio 2020.

COSSETTI, Melissa Cruz. WannaCry: tudo que você precisa saber sobre o ransomware. Disponível em: <https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ran somware-wannacrypt.ghtml>. Acesso em: 21 maio 2020.

FREEPIC. Cadeado fechado no fundo digital, segurança cibernética Vetor Premium. Disponível em: <https://br.freepik.com/vetores-premium/cadeado-fechado-no-fundo-digital-seguran ca-cibernetica_5159323.htm>. Acesso em 22 maio 2020.

HALSEY, Mike. How Secure is Your Password? Disponível em: <https://www.ghacks.net/2012/04/07/how-secure-is-your-password/>. Acesso em: 22 maio 2020.

INTUIT ONLINE SECURITY CENTER. Phishing, Pharming, Vishing, and Smishing. Disponível em: <https://security.intuit.com/index.php/protect-your-information/phishing-pharming-vishing-and-smishing>. Acesso em: 20 maio 2020.

KASPERSKY. Dicas para a prevenção de phishing . Disponível em: < https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips>. Acesso em: 23 maio 2020.

KASPERSKY. Secure Password Check. Disponível em: <https://password.kaspersky.com/br/?utm_

medium=rdr&utm_source=redirector&utm_campaign=old_url>. Acesso em 21 maio 2020.

LOPES Nathamy. SOUZA Liliane. Médica cai em golpe no WhatsApp e recebe 'conselho' de bandido: 'Tem que amadurecer'. Disponível em: <https://g1.globo.com/sp/santos-regiao/noticia/2019/06/07/medica-cai-em-golpe-no-whatsapp-e-recebe-conselho-de-bandido-amadureca.ghtml>. Acesso em 20 maio 2020.

MAULAIS, Claudio Nunes dos Santos. Engenharia Social: Técnicas e Estratégias de Defesa em Ambientes Virtuais Vulneráveis. 2016. Projeto de pesquisa (Mestrado em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, Belo Horizonte. Disponível em: <http://www.fumec.br/revistas/sigc/article/viewFile/3733/2031>. Acesso em: 22 maio 2020.

NETSPEED PORTAL EDUCAÇÃO. Qual a diferença entre phishing e pharming? Disponível em: <https://netspeed.com.br/mais/blog/empreendedorismo/empresarial/qual-a-diferenca-entre-phi shing-e-pharming-2/>. Acesso em 20 maio 2020.

PENSADOR. Kevin David Mitnick. Disponível em: <https://www.pensador.com/frase/ MTQ0MDcyNQ/>. Acesso em: 22 maio 2020.

PROOF. Como identificar um ataque de phishing em 9 passos. Disponível em: <https://www.proof.com.br/blog/politica-de-seguranca-da-informacao/>. Acesso em: 23 maio 2020.

PROOF. Spear Phishing: uma das ameaças mais efetivas. Disponível em: <https://www.proof.com.br/blog/spear-phishing/>. Acesso em: 21 maio 2020.

SILVA, Clayton S. et al. Engenharia Social: O Elo Mais Frágil da Segurança nas Empresas. Revista Eletrônica do Alto Vale do Itajaí. N° 02. Dezembro 2012. Disponível em: <http://www.revistas.udesc.br/index.php/reavi/article/view/2840/2172>. Acesso em: 23 maio 2020.

TERRA. Hackers desviam 520 mil euros do Boca Juniors. Disponível em: <https://www.terra.com.br/esportes/futebol/mercado-da-bola/hackers-desviam-520-mil-euros-do-boca-juniors-durante-transferencia-do-psg,467c82360a4db4f7b5fd74ce31821a52jgloipmc.html>. Acesso em 22 maio 2020.

Daniel Moura Felix Cardoso é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Infantaria do Exército Brasileiro, Pós-graduado em Guerra Cibernética pelo Centro de Instrução de Guerra Eletrônica. Atualmente, exerce a função de Instrutor na Escola de Comunicações e pode ser contactado pelo email: felix.daniel@eb.mil.br.

Daniel Bomfim Nunes é técnico em eletrônica pela Escola de Sargentos de Logística (EsSLog). Sargento de Manutenção de Comunicações, está cursando licenciatura em Física na Universidade de Brasília. Atualmente, exerce a função de Monitor na Escola de Comunicações e pode ser contatado pelo e-mail bomfim.daniel@eb.mil.br