Universidade Federal do Rio de Janeiro
Instituto de Matemática
Departamento de Ciência da Computação
Grupo de Resposta a Incidentes de Segurança

Rio de Janeiro, RJ - Brasil

Técnicas de Engenharia Social

GRIS – 2011 – A – 002

Pedro Henrique da Costa Braga

A versão mais recente deste documento pode ser obtida na pagina oficial do GRIS: http://www.gris.dcc.ufrj.br

GRIS - Grupo de Resposta a Incidentes de Segurança
Av. Brigadeiro Trompowski, s/n°
CCMN - Bloco F1 - Decania
Cidade Universitária - Rio de Janeiro/RJ
CEP: 21949-900
Telefone: +55 (21) 2598-9491

Última atualização em 15 de Fevereiro de 2011

Agradecimentos:

Gostaria de agradecer a toda a equipe do GRIS, em especial a Luís Fernando Magalhães Novaes , Manoel Fernando de Sousa Domingues Junior, Guilherme Iria D'Abbadia Fontes Pereira e Vinícius de Sousa Pontes que me auxiliaram em minha pesquisa e na organização desse trabalho e a Pedro de Souza Asad que me ajudou durante a revisão do texto.

Sumário

1 Introdução:

1.1 O que é a Engenharia Social?

Paradoxalmente, o nome Engenharia Social apesar de pouco conhecido classifica uma categoria extremamente comum de ataques à Segurança da Informação. Apesar desse paradoxo o nome não poderia descrevê-la melhor:

Engenharia - Estudo da habilidade de criar, inventar e manipular algo a partir da técnica.

Social - Tudo aquilo que é relativo à forças externas ao indivíduo, provenientes do meio que este vive, que determinam grande parte do seu comportamento.

Uma ótima descrição da Engenharia Social foi dada pelo hacker Kevin Mitnick em seu livro "*A Arte de Enganar*" ("*The Art of Deception*" no original em inglês") . Abaixo se encontra uma livre tradução do original em inglês:

A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

Da definição acima dois pontos chaves devem ser destacados. O primeiro é que a Engenharia Social não é um ataque exclusivo do meio digital, sendo passível de ocorrência mesmo sem o auxílio da tecnologia, apesar de ataques assim não serem o foco deste artigo. O outro ponto do qual o primeiro é uma consequência direta é que o foco de um ataque de Engenharia social é o fator humano, daí a sua eficácia.

1.2 Definindo o fator humano e explicando o seu uso:

Quando pensamos na prevenção de um ataque à Segurança da Informação em geral pensamos logo na correção de falhas computacionais que podem levar ao sucesso destes ataques. Cercamos nossos sistemas por *firewalls*, instalamos antivírus e *anti-spywares* para detectar e remover programas maliciosos, atualizamos sempre todos os programas na esperança corrigir as suas falhas. Por mais criteriosas que sejam as políticas de segurança de um sistema, ele ainda pode ser comprometido por fruto de um deslize do seu operador.

Existe então uma segunda rota de invasão para o sistema: o erro humano. Definimos por erro humano todo comportamento inseguro, seja ele um ato contínuo ou fruto de um momento de distração, que pode ser usado por um atacante para que este consiga comprometer um sistema. O grande problema com o erro humano é que ele não pode ser completamente corrigido, apenas mitigado (como veremos no final desse artigo), afinal nenhuma pessoa é perfeita e nenhum treinamento pode mudar isso. Podemos concluir que o fator humano é o elo mais fraco da Segurança da Informação. Veremos a seguir como o atacante explora essa fraqueza.

1.3 Ferramentas usadas pelos atacantes:

- **Disfarces:** Parte fundamental de qualquer ataque de Engenharia Social é a capacidade do atacante de esconder a sua identidade e de assumir a identidade de alguém que possui acesso a informação que o ataque tem como alvo.

- **Informações descartadas incorretamente**: O descarte de informação na forma impressa ou o ato de esvaziar a lixeira de um *desktop* não são seguros o suficiente quando tratamos com dados sigilosos, já que basta uma inspeção mais cautelosa para que um atacante chegue até eles.[1] Devemos sempre garantir o descarte seguro da informação, usando meio adequados para isso (a queima no caso da informação em papel ou o uso de *softwares* seguros para apagar dados sigilosos do computador).

- **Redes de contato:** Amigos e conhecidos são uma fonte de informação valiosa, se bem explorada. Por isso, um engenheiro social experiente se aproximará destas pessoas a fim de extrair informações e conseguir favores.

- **Apelo sentimental:** Emoções são a maneira mais fácil de se manipular alguém. Uma história convincente que leve a vítima a achar que está fazendo o bem, ou que ganhará algo no final pode ser determinante para o sucesso de um ataque de Engenharia Social.

- **Programação Neurolinguística:** Consiste no uso de jargões e maneirismos artificiais por parte do engenheiro social para que a vítima acredite na sua história e no seu disfarce. Além disso também cria um elo de confiança entre a vítima e o atacante, sendo assim uma peça central de um ataque de Engenharia Social.

- **Pesquisas na Internet:** Qualquer concurso público feito por uma pessoa, seu CPF, a faculdade que cursou, a escola na qual se formou, entre outros dados, podem ser facilmente encontrados com uma busca na Internet. Além disso, redes sociais permitem que um indivíduo mal-intencionado descubra diversas informações pessoais sobre seus usuários. Pode-se se afirmar que as informações na Internet são uma das maiores armas do engenheiro social.

2 Ataques comuns de Engenharia Social

2.1 *Phishing*:

Tipo de ataque de engenharia social extremamente comum. Consiste do envio de mensagens falsas para a vítima, buscando obter, sem o conhecimento desta, informações sigilosas. Seu funcionamento baseia-se na exploração de um vínculo de confiança entre a vítima e por quem o atacante está se passando.

Nesse ataque ocorre com frequência a cópia do *layout* do site pelo qual o atacante tenta se passar, seja esse *layout* usado na mensagem enviada para a vítima ou em um site falso. Nesse

1 Quando um arquivo é removido da lixeira de um computador ele não é realmente apagado, apenas se torna oculto para o usuário, Eventualmente o sistema operacional irá escrever alguma nova informação no espaço no disco onde se encontra, mas até que isso ocorra o arquivo pode ser recuperado com o uso de aplicações apropriadas.

segundo caso, também e necessário por parte do atacante mascarar a URL do site. Uma forma muito comum de fazer isso é usando encurtadores de endereços web, como o migre.me e o bit.ly, mas as vezes nem isso é necessário, como no exemplo a seguir:

http://www.paypal.com/
http://www.paypaI.com/

A forna em caixa-alta da letra 'i' se confunde facilmente com a letra 'l' em caixa-baixa, em algumas fontes isso se torna até imperceptível. Esse exemplo simples ilustra claramente a facilidade pela qual uma vítima desatenta pode cair em um ataque de *phishing*.

Um caso recente de *phishing* ocorreu em Maio de 2009, quando atacantes enviaram dezenas de e-mails para usuários do Facebook, rede social que informa seus usuários desta maneira com frequência. Os links contidos nessas mensagens levavam a páginas falsas, deliberadamente projetadas para parecer com as páginas legítimas do Facebook. Elas continham campos para que os usuários digitassem os dados de suas contas. O porta-voz do Facebook, Barry Schnitt, afirmou na ocasião que a equipe de segurança do Facebook acredita que os atacantes pretendiam coletar um grande número de credenciais para, mais tarde, usar essas contas para enviar spam a outros usuários do Facebook. A empresa não revela os números exatos de contas invadidas.

Preocupantemente, o CERT.br, o Centro de Estudos, Resposta e Tratamentos a Incidentes de Segurança no Brasil, registrou um aumento de 61% nos casos de *phishing* no primeiro trimestre de 2010 em relação ao mesmo período em 2009. Isto mostra que esta é uma ameaça cada vez mais comum no cenário nacional.

Em escala global, os sites que mais registraram esse tipo de ataque em 2010 foram: PayPal (52,5% dos ataques registrados), eBay (13,3%), HSBC (7,8%), Facebook (5,7%), Google (3,1%), IRS (2,2%), Rapishare (1,8%), Bank of America (1,7%), UBI (1,6%), Bradesco (1,2%). Os demais sites somaram (9,2%) das ocorrências, mas individualmente representam menos de 1%.

2.2 Anexos Maliciosos:

Um dos mais antigos e conhecidos ataques de Engenharia Social. Consiste no envio de mensagens contendo algum tipo de *malware* em anexo. O atacante busca atiçar a curiosidade da vítima para que esta execute o anexo, contaminando o seu sistema no processo.

Outro fator importante é a necessidade de se esconder a natureza do anexo, para isso emprega-se técnicas de esteganografia[2] e aproveita-se de uma falha computacional, como ocorreu no caso do *worm* ILOVEYOU.

Nesse famoso caso, que teve inicio no dia 4 de Maio de 2000, diversas mensagens foram enviadas via e-mail e canais de IRC contendo em anexo o arquivo “LOVE-LETTER-FOR-YOU.TXT.VBS”, naquela época diversos clientes de e-mail e IRC só mostravam até a primeira extensão do anexo, ocultando o “.VBS”, dessa forma o *worm* se passava por um arquivo de texto comum que aparentemente continha uma mensagem de amor. Uma vez executado ele se instalava no computador da vítima e substituía diversos arquivos por cópias de si mesmo, incluindo a extensão “.VBS” escondida. Após isso o *malware* se espalhava usando o livro de contatos do cliente de e-mail Microsoft Outlook. A propagação do vírus foi impressionante: nove dias depois, de seu surgimento, 50 milhões de infecções já tinham sido reportadas no mundo todo. Apesar da falha que o *worm* explorava ter sido corrigida, ele ilustra muito bem o perigo desse tipo de ataque.

2**. Esteganografia:** Do grego "escrita escondida", é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra. No contexto dos ataques de anexos maliciosos, se refere ao ato de esconder código malicioso dentro de um arquivo aparentemente inofensivo. Para mais informações, o GRIS possui em seu acervo uma apresentação sobre esteganografia escrita por Luís Fernando Magalhães Novaes.
http://www.gris.dcc.ufrj.br/documentos/apresentacoes/esteganografia

2.3 Falso Antivírus (*Rogueware*):

Um tipo de ataque que surgiu recentemente é a criação de *malwares* disfarçados de programas antivírus. A eficiência dessa técnica reside no uso pelo atacante do medo do usuário de ter seu sistema comprometido. Seu funcionamento é simples: o usuário é levado por um *pop-up* ou por uma busca na Internet para uma página contendo links para o download de um suposto *software* antivírus. É muito comum que nessas páginas exista uma enganosa busca on-line por *malwares* no computador da vítima, que alerta para a presença de programas maliciosos e sugere o download do *software* indicado na página. Ao instalar o programa uma nova falsa busca é realizada mas o computador é desta vez dado como livre de ameaças. Assim o atacante consegue não só comprometer o computador da vítima como também, convencê-la de que seu computador não possui nenhum software mal-intencionado.

Apesar do surgimento recente, esse tipo de ataque já chamou a atenção de gigantes da tecnologia, como o Google, que exibiu em 29 de 2010 uma pesquisa, realizada entre janeiro de 2009 e fevereiro de 2010, mostrando que os programas antivírus falsos já representam 15% de todos os softwares maliciosos para computadores . A pesquisa também afirmava que mais de 11 mil domínios registrados na Internet estão relacionados à distribuição de antivírus falsos .

3 Evitando ataques de Engenharia Social

3.1 Segurança da conexão e criptografia:

Um comportamento simples, mas eficiente no combate à Engenharia Social é a atenção a segurança da conexão e o não envio de dados sigilosos em uma conexão insegura. Uma conexão criptografada impede que um terceiro obtenha dados de uma vítima e use-os contra ela em um posterior ataque de Engenharia Social. Para auxiliar o usuário a maioria dos navegadores atuais mostra se a conexão é criptografada e, caso positivo, o tipo da criptografia empregado. Também é recomendado o uso de protocolos seguros no referente ao acesso remoto, como por exemplo o uso do SSH em detrimento do TELNET, uma vez que esse último não garante por padrão a segurança da conexão.

3.2 Sites e certificados digitais:

Entidades certificadoras são instituições responsáveis pela emissão de certificados digitais que identificam sites na Internet e seus respectivos proprietários. Ao assinar digitalmente os certificados que emite, a entidade certificadora relaciona a identidade do portador do certificado, e portanto da chave privada, à chave pública existente no certificado. A maioria dos navegadores exibem se a página visitada possui um certificado digital válido, caso não possua, o site provavelmente é uma fraude.

3.3 Bom senso e atenção aos detalhes:

Em grande parte dos ataques de Engenharia Social ocorrem erros de escrita. Isto é devido ao emprego de tradutores para passar a mensagem de sua língua original para outras. Além disso outros detalhes podem expor um ataque: o domínio de um site, dados conflitantes na mensagem, entre outros. Conferindo as informações recebidas e não acreditando em tudo a primeira vista, o usuário consegue escapar de diversos ataques de Engenharia Social.

3.4 Uso de senhas fortes:

Jamais use senhas constituídas de informações pessoais que possam ser descobertas por um engenheiro social. Números de CPF ou RG, datas de aniversário, nomes de amigos ou familiares, endereços, o nome de um time de futebol e o próprio *login* são exemplos de senhas que um atacante descobrirá rapidamente. Prefira senhas extensas, com letras em caixa-alta e baixa, números e caracteres especiais.[3]

4. Conclusão:

Talvez o maior problema que surge ao combater a Engenharia Social é o fato de não existir solução imediata, algo que para a sociedade atual parece impensável. Apenas com a a conscientização e o treinamento dos operadores e usuários dos sistemas de informação que obtém-se resultados, processo este que é lento e custoso, porém indispensável.

Apesar de parecer algo tolo e que apenas afeta o usuário leigo, a Engenharia Social é uma das maiores ameaças à segurança da informação e a sua aparente simplicidade esconde uma perigosa forma de invadir até os sistemas mais bem protegidos. Como é possível que o elemento chave da Engenharia Social, o fator humano, jamais seja removido dos sistemas computacionais, talvez sempre exista a ameaça de um ataque deste tipo. Este fato jamais deve ser ignorado por todos que prezam pela segurança da informação, uma vez que a Engenharia Social se torna ainda mais perigosa quando a vítima a descarta como uma ameaça séria.

3 Para mais informações sobre a escolha de senhas fortes consulte o artigo escrito por Breno Guimarães de Oliveira, antigo membro do GRIS.

http://gris.dcc.ufrj.br/documentos/artigos/GRIS2005A002.pdf

Fontes:[4]

http://www.symantec.com/security_response/writeup.jsp?docid=2000-121815-2258-99

http://en.wikipedia.org/wiki/ILOVEYOU

http://g1.globo.com/Noticias/Tecnologia/0,,MUL1127249-6174,00-HACKERS+LANCAM+ATAQUE+A+USUARIOS+DO+FACEBOOK.html

http://www.kaspersky.com/news?id=207576083

http://googleonlinesecurity.blogspot.com/2010/03/phishing-phree.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleOnlineSecurityBlog+%28Google+Online+Security+Blog%29

http://googleonlinesecurity.blogspot.com/2010/04/rise-of-fake-anti-virus.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleOnlineSecurityBlog+%28Google+Online+Security+Blog%29

Kevin Mitnick - "*The Art of Deception*" , 2002, John Wiley & Sons

4 Todas os endereços *web* listados nas referências bibliográficas eram válidos no dia 15 de Fevereiro de 2011.