Grupo de Resposta a Incidentes de Segurança – GRIS

Departamento de Ciência da Computação

Universidade Federal do Rio de Janeiro

Phishing Scam

A fraude do Século 21

Por: Diego de Oliveira Martins

Rio de Janeiro - Brasil

2008

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

Título

GRIS-2008-A-002

Diego de Oliveira Martins

V. 1.0

A versão mais recente deste documento pode ser obtida na página oficial do GRIS

Índice

1 – Introdução:

1.1 - Crimes Virtuais: Uma breve panorâmica

Dentre as muitas tendências do mundo contemporâneo, podemos ressaltar como uma das mais notáveis a virtualização da vida. Ações como ir ao banco, fazer compras e conhecer novas pessoas, outrora exclusivamente realizadas por presença física vem sendo gradualmente substituídas por suas equivalentes virtuais.

A possibilidade de realizar tarefas no conforto do lar acaba por trazer a uma grande massa de internautas a ilusória sensação de segurança. Diz-se ser ilusória pois, uma vez que a internet é uma tendência globalizada, não menos do que esperada é a presença de criminosos.

A presença de indivíduos de má índole na rede é fortalecida por uma vasta gama de fatores. Primeiramente, o alto nível de ocultação a que se pode chegar na internet. Em segundo lugar, a ausência de uma legislação específica sobre crimes virtuais em muitos países acaba por encorajar a prática dos mesmos. Pode-se citar ainda o fato de que, na internet, o instinto natural de defesa humano torna-se um tanto quanto defasado, reduzindo as chances de discernir conteúdo genuíno e fraudes.

Para compreender a afirmação acima apresentada, vamos nos basear apenas em um fato: O instinto primário do ser humano não está relacionado à proteção de seus bens, mas sim à proteção de sua integridade física. No mundo real, uma vez que estamos suscetíveis à violência, ficamos mais atentos e preocupados quanto aos locais pelos quais caminhamos. Contudo, no mundo virtual, uma vez que não existe a hipótese de agressão física, o instinto defasa-se razoavelmente, e em se tratando de mecanismo de defesa principal, dá lugar ao grau de instrução. Aqueles que conhecem pouco a internet ficam, invariavelmente, mais vulneráveis que aqueles que conhecem seus perigos, e pode-se dizer que o primeiro grupo é certamente maior que o último.

Aproveitando-se de tanto, indivíduos maliciosos desenvolvem e põem à prática métodos cada vez mais sofisticados para cometer ações ilícitas. Alguns destes métodos, contudo, se destacam por sua eficácia e rendimento, e dentre estes, podemos citar, certamente, o ataque de Phishing Scam.

1.2 – O que é Phishing Scam?

Phishing scam é o termo utilizado para denominar o ataque que utiliza como via mensagens em geral, no qual pratica-se a assimilação da identidade de um indivíduo ou organização autêntica de modo a convencer o alvo a disponibilizar informações sensíveis, e configura-se como um dos mais difundidos da atualidade. Este termo origina-se da palavra *fishing* – pescar – fazendo alusão à pescaria de senhas. É um ataque bastante flexível, podendo empregar e-mails, sites ou mensagens de voz fraudulentas para tentar induzir o usuário a divulgar ao atacante informações sensíveis.

Ataques de Phishing vêm se tornando cada vez mais sofisticados, e estão em constante crescimento. O que começou apenas como um hobby malicioso, hoje configura-se como um tipo de infra-estrutura econômica, um ataque praticado por criminosos profissionais. Os danos causados por um ataque de Phishing podem ser devastadores, como perda de dados sensíveis e danos financeiros diretos.

Os Phishers adotam diversos vetores para distribuir seus ataques, indo do massivo envio de mensagens conhecido como Spam, até ataques altamente focalizados, conhecidos como Spear Phishing. De qualquer modo, os ataques têm nível razoavelmente alto de sucesso, ultrapassando os 5%, de acordo com o Anti-Phishing Working Group.

1.3 – Histórico do Ataque

O termo "Phishing" é relativamente novo, e sua criação data de meados de 1996, por hackers que praticavam roubo de contas da America Online (AOL), fraudando senhas de usuários. Sua primeira menção pública ocorreu no grupo hacker alt.2600, em 28 de Janeiro do mesmo ano de sua criação, feita pelo usuário mk590, que dizia:

"O que acontece é que antigamente, podia-se fazer uma conta falsa na AOL, uma vez que se tivesse um gerador de cartões de crédito. Porém, a AOL foi esperta. Agora, após digitar-se os dados do cartão, é feita uma verificação com o respectivo banco. Alguém mais conhece outra maneira de adquirir uma conta que não seja através de Phishing?"

Apenas um ano depois, em 1997, o termo foi citado na mídia. Neste mesmo ano, os phishs (contas hackeadas) já eram utilizados como moeda no mundo hacker, e podia-se facilmente trocar 10 phishs da AOL por uma parte de um software malicioso.

O Phishing, outrora utilizado para roubar contas de usuários da America Online, hoje tem aplicações muito maiores e obscuras, como por exemplo, o roubo de dinheiro de contas bancárias.

2 – Aprofundando-se

2.1 – O ataque de Phishing e a Engenharia Social

Uma vez que soluções de segurança da informação como antivírus e firewalls, e a, ainda que leve, desconfiança em relação a arquivos muito suspeitos, tornam a vida de indivíduos maliciosos mais difícil, estes últimos precisam buscar maneiras de burlar estes obstáculos. Pensando nisto, o conceito de Engenharia Social foi trazido para a área de Segurança da Informação.

Engenharia Social traduz-se como um conjunto de práticas a serem utilizadas na tentativa de persuadir indivíduos a realizar ações que favoreçam o atacante. Por se tratar de um ataque que é conduzido a nível psicológico, não há aplicativos que possam impedi-lo.

O ataque de Phishing Scam baseia-se largamente em Engenharia Social, utilizando-se da confiabilidade de organizações ou indivíduos genuínos para convencer o usuário a disponibilizar informações sensíveis ou efetuar a instalação de malwares, acreditando estar obtendo vantagens com tais ações, quando, na verdade, estará sendo "pescado" em uma fraude.

2.2 – Vertentes do Phishing

Desenvolvidas utilizando a mesma base, ou seja, a persuasão através da apropriação de identidade alheia confiável, são muitas as vertentes do ataque. A seguir, discorrer-se-á sobre as principais.

2.2.1 – Spear Phishing

Spear Phishing traduz-se como um ataque de Phishing altamente focalizado. É um tipo de ataque que exige toda uma etapa de minuciosa pesquisa por parte dos atacantes, além de muita paciência. Correlacionando ao nome "Phishing", sua denominação pode ser entendida como algo semelhante à "pesca com arpão".

Neste tipo de ataque, o atacante estabelece seu alvo (geralmente uma empresa/departamento desta, podendo incluir ainda universidades, instituições governamentais, dentre outras). Logo em seguida, inicia a etapa na qual o phisher sonda informações básicas de diferentes funcionários. Aqui, explora-se uma grande falha humana: A incapacidade de avaliar corretamente a sensibilidade de uma informação. Enquanto sozinha, esta informação pode não significar muito, mas em conjunto, se inteligentemente utilizada pelo atacante, pode garantir-lhe conhecimento suficiente para assimilar a identidade de alguém com mais poder na empresa.

Nesta primeira fase, enquanto o phisher assimila os jargões internos à empresa e entende o funcionamento de alguns procedimentos, moldam-se diferentes personagens, de posição cada vez mais elevada, até que se consiga atingir informações suficientes para chegar à fase principal do ataque: a investida final.

Em posse de tanto, o atacante assume o papel do indivíduo de maior poder que consegue, como por exemplo, o presidente de uma empresa. Elabora um e-mail de estrutura similar a dos genuínos, utilizando os jargões para parecer o mais autêntico possível, e, aproveitando-se da confiança ou autoridade que inspira dentro da instituição a identidade assimilada, solicita nomes de usuário e senhas, ou o download e instalação de um software (que oculta, na verdade, um malware).

Uma vez que atinja seu objetivo, o atacante passa a ter a rede da instituição nas mãos, com acesso a informações sigilosas e com poder para realizar, por exemplo, transferências (no caso de um banco).

2.2.2 – Fraude 419

Criada em meados de 1980, quando a economia petrolífera da Nigéria estava em crise, por estudantes universitários, para manipular indivíduos interessados no petróleo nigeriano. Eram inicialmente distribuídos por cartas ou fax, mas com a popularização do e-mail, este passou a ser o meio utilizado. Na verdade, há registros de que a fraude já existia previamente, datando de antes de 1588, quando redigiam-se cartas supostamente provenientes de prisioneiros de castelos espanhóis, que prometiam compartilhar um tesouro com aquele que os enviasse dinheiro para subornar os guardas.

Seu nome vem da seção 419 do código penal nigeriano, que tipifica atividades fraudulentas. O e-mail é proveniente de indivíduos que dizem ser do Banco Central da Nigéria ou do Governo deste mesmo país. Porém a fraude 419 não se resume a meramente um único e-mail. Muito além disso, é um verdadeiro jogo, no qual o risco e as regras dependem das capacidades de persuasão do atacante. Vale frisar que neste caso, "atacante" pode ser lido como uma verdadeira equipe de criminosos profissionais, que articula minuciosamente seus planos.

O atacante, neste tipo de ataque, para tornar-se aparentemente confiável, assume a identidade de um funcionário corrupto de alto escalão do Banco Central Nigeriano, do Governo Nigeriano ou de representante de alguma grande empresa. Mas não é exatamente com sua suposta posição social que o atacante conquista a confiança de suas vítimas.

Vamos a um exemplo traduzido de fraude 419.

Remetente: mbulu_tutu2@ananzi.co.za
Assunto da mensagem: Transferência de US$ 6.000.000,00 (Seis milhões de dólares)

Prezado senhor,

Nós desejamos efetuar uma transferência no valor de US$ 6.000.000,00 do Banco Central Nigeriano, e eu gostaria de pedir um grande favor a você: Gostaria que alguém confiável e honesto, como o senhor, pudesse disponibilizar uma conta bancária em seu país para receber este dinheiro, e confio e peço a Deus que eu não esteja enganado quanto a sua índole, pois meu cargo e minha vida estão em jogo.

Eu sou o Sr. Mbulu Tutu, auditor-chefe do banco, e durante uma auditoria descobri fundos sobressalentes em contas abertas em 1990 e não mais operadas desde 1993. Após pesquisar um pouco mais, descobri que o dono desta conta, o Sr. Hermann Radnitz, um industrial alemão, dono da Diamond Safari, morreu sem que ninguém soubesse desta, além da mesma não ter beneficiários. E se você me entende, me dói ver tanto dinheiro sendo desperdiçado.

Meus planos são de transferir inicialmente 4 milhões de dólares, e se tudo correr bem, o resto, logo em seguida. Estou te contactando, um estrangeiro, pois não conseguiria aprovação para transferir tal montante para um nigeriano, mas como o dono anterior era um estrangeiro, para tais é possível, mediante passaportes internacionais válidos, ou licença de motorista.

De qualquer modo, assinaremos um contrato antes da transferência do dinheiro para qualquer conta que você disponibilize. Estou te revelando isto acreditando, por Deus, que você nunca vai me abandonar neste negócio, me sabotando. Você é a primeira e única pessoa que estou contactando para negócios, então, por favor, responda o mais rápido possível e eu o informarei dos próximos passos. Envie também seu telefone privado e fax, incluindo os detalhes da conta a ser utilizada para o depósito.

Preciso realmente de sua total cooperação para que tudo corra bem, pois está tudo pronto para a aprovação do pagamento a um estrangeiro que possua uma conta bancária verdadeira, que é a que espero que seja disponibilizada por você.

Com a minha influência e a alta posição de um parceiro de negócios no banco, podemos transferir o dinheiro para qualquer conta estrangeira disponível, e garantir que o dinheiro se manterá intacto. Meu parceiro destruirá todos os documentos relativos a transação assim que o dinheiro for recebido, sem deixar pistas. Para criar um laço maior de confiança entre nós, você poderia vir imediatamente para discutirmos ao vivo, e aguardar a transferência do dinheiro. Assim que tudo estiver acertado, voaremos os três para o seu país para retirar o dinheiro.

Não se preocupe com o visto para entrar no país, vou usar minha posição e influência para obter junto aos ministérios e departamentos competentes as aprovações necessárias para sua chegada, estadia e volta.

Ao concluirmos o negócio, você receberá 35% do montante, 60% serão meus, enquanto 5%

serão para dispesas que qualquer uma das partes possa ter tido durante a transferência, como passagens, subornos, etc. Te enviarei meus números de telefone e fax assim que você indicar ter interesse nos negócios.

Espero, com urgência, por sua resposta, no meu e-mail pessoal.

Sinceramente,

Mbulu Tutu

Tudo começa com um e-mail como este, que solicita à vítima a permissão para utilizar sua conta bancária para fazer grandes transferências, da ordem de milhões de dólares, de modo discreto, para evitar taxas "desnecessárias" ou para desviar dinheiro da maneira mais sub-reptícia possível. Uma vez que a vítima é fisgada no golpe, o limite fica a cargo da criatividade e crueldade do atacante.

A motivação inicial para uma vítima que cai na fraude 419 é a mesma compartilhada por jogadores compulsivos: a ganância. A possibilidade de receber somas astronômicas de dinheiro de maneira fácil as ludibria. Em segundo lugar, são criados laços falsos de cumplicidade e toda uma situação que faça parecer que a vítima tem, em relação ao atacante, poder superior sobre a situação. No caso de nosso e-mail, podemos citar, por exemplo, as frases apelativas do remetente, como *"Estou te revelando isto acreditando, por Deus, que você nunca vai me abandonar neste negócio, me sabotando"*. Além de tudo, o atacante faz com que a situação pareça mais segura, falando sobre seus contatos e poderes para eliminar as pistas.

E o jogo não para neste primeiro e-mail. Após uma resposta positiva da vítima, demonstrando interesse em participar dos "negócios", o phisher procura estabelecer laços mais fortes. Para fazer-se mais confiável, envia à vítima diversos documentos aparentemente legítimos, além de conversas ao telefone, troca de fotografias, dados pessoais, dentre outros.

Uma vez que se consegue envolver a vítima por completo no golpe, o atacante sugere a existência de alguns obstáculos, graves mas muito "simples" de se resolver, bastando a antecipação de uma determinada quantia para despesas imediatas, como subornos, taxas, dentre outros. Embaladas pela confiança e pelo medo do negócio fracassar, as vítimas acabam fazendo-o o mais rápido possível, sem pensar. A depender do grau de envolvimento da mesma, o phisher pode solicitar ainda outros pagamentos, com sucesso, até que a "fonte" seja drenada ao máximo e o jogo

acabe em um grande prejuízo.

Em alguns casos, a vítima pode ser convidada a viajar para a Nigéria, e o atacante convence-a de que não deve se preocupar em solicitar o visto no passaporte. A justificativa é fazer algo mais discreto, e o phisher tranqüiliza a vítima alegando que amigos estarão a sua espera no aeroporto para resolver qualquer possível problema com as autoridades da imigração. Contudo, uma vez que não possui visto no passaporte, a vítima cai na ilegalidade, tornando-se um alvo mais vulnerável.

Ao chegar na Nigéria, inicia-se a fase cruel. A vítima é levada para um cativeiro, e forçada a entregar até o último centavo que puder aos atacantes, e seu destino fica nas mãos dos atacantes. Há inúmeros relatos de vítimas que foram para a Nigéria e nunca mais foram vistas, ou foram encontradas mortas tempos depois.

Famílias arruinadas, financeira e/ou socialmente. A fraude 419 é um golpe que pode ir muito além do simples contato virtual. É uma fraude muito bem elaborada, na qual os atacantes estão prontos para ir até as últimas conseqüências, ainda que isto envolva matar.

2.2.3 - iPhishing

Com a popularização da internet, hoje diversos aparelhos eletrônicos, de celulares a refrigeradores, passando ainda por video-games, trazem a si assimilados navegadores web. Com toda esta onda de modernidade, toma-se como preocupação principal o design, em detrimento dos aspectos da segurança.

Devido as limitações de espaço físico, principalmente no que diz respeito ao tamanho de tela e dispositivo de entrada (teclado, por exemplo), alguns aparelhos podem ocultar a URL do website ou permitir que este último o faça, além de encorajar a navegação por links, que sujeitam o usuário à maior propensão de cair em um ataque de phishing.

Além de tudo, acrescenta-se ainda o fato de que aplicar atualizações de segurança fundamentais à boa manutenção do sistema é uma tarefa não tão fácil de se realizar quanto em desktops, o que desencoraja a muitos a aplicá-las.

iPhishing é a vertente que visa explorar vulnerabilidades conseqüentes do avanço excessivamente rápido da tecnologia, que acaba por deixar aspectos de segurança em segundo plano, dando lugar à funcionalidade e ao design. O ataque pode ocorrer de algumas maneiras, mas podemos citar o envenenamento de DNS para exemplificar.

Um servidor DNS, ou Domain Name System (Sistema de Nomes e Domínios) tem como função traduzir nomes para IP's e IP's para nomes. Um envenenamento de DNS faz com que usuários sejam redirecionados para sites diferentes daqueles que desejavam alcançar. Devido a limitação de espaço na tela de portáteis como o iPhone, os usuários podem não conseguir ver toda a URL das páginas que visitam, tornando-se assim muito mais vulneráveis.

Há ainda outras vulnerabilidades, como por exemplo, o uso do método scrollto(), do Javascript, na elaboração da página. Com este método, enquanto a página se carrega, salta para outra área da mesma onde não se possa ver a URL. Ao tentar ir ao topo e vê-la, o usuário pode ainda deparar-se com um método que faça com que, a cada vez que se aproxime do topo, onde localiza-se a URL, seja lançado para outro ponto da página.

Sabendo-se tal, os hackers encontram uma nova “mina de ouro”: As fraudes em eletrônicos com acesso a internet, que por serem tão novos, carregam consigo grandes vulnerabilidades.

2.2.4 - Vishing Scam: Phishing por telefone

Como bem se sabe, o advento de novas tecnologias geralmente traz consigo a possibilidade de ser explorada pela natureza humana para ser utilizada maleficamente. A VoIP (Voice over IP), tecnologia desenvolvida para possibilitar comunicação telefônica através da rede baseando-se no Protocolo de Internet (IP), não se tornou uma exceção a regra.

Uma vez que apresenta diversas vantagens sobre a telefonia convencional, como o fato de ser uma tecnologia de baixo custo, e, acrescentando-se ainda a possibilidade de mascarar o número de telefone que será identificado pelo receptor, a VoIP configura-se como uma excelente "oportunidade" para indivíduos maliciosos, que, percebendo-a, criaram uma nova vertente baseada no Phishing Scam tradicional: O Vishing Scam.

Ataques de Vishing Scam são geralmente propagados através de mensagens de texto (SMS), e-mails ou até mesmo mensagens de voz, e seu procedimento assemelha-se em muito ao do Phishing Scam tradicional.

Na execução do ataque, o atacante envia as mensagens para o celular da vítima, ou até mesmo e-mails, e, utilizando-se de engenharia social, tenta conduzir a mesma a discar para um número fornecido na mensagem. As justificativas dadas para se efetuar a ligação variam, mas dentre as mais comuns delas podemos citar, por exemplo, "a ocorrência de possíveis atividades fraudulentas na conta bancária que levaram à suspensão da mesma" .

Uma vez dada a justificativa, a mensagem solicita que a vítima disque para o tal número fornecido, de modo a reativar sua conta ou qualquer coisa que o valha. Caso o receptor acredite no conteúdo da mensagem e atenda à solicitação, é atendido por um sistema eletrônico de voz, criada para ser similar a de alguns grandes bancos, que pedem a inserção de dados da conta bancária no teclado do aparelho, como sua conta bancária e senha de acesso. A mesma voz então declara que a conta foi reativada, porém o que na verdade está acontecendo é um ataque de Vishing Scam. Com base nestas informações, o atacante poderá então criar cartões de crédito clonados (de alto valor no mercado negro) ou até mesmo efetuar transações bancárias.

De modo a se tornar mais convincente, algumas mensagens podem até mesmo trazer o nome do cliente e o número de seu cartão de crédito. Porém, o que muitos não sabem é que este tipo de

informação, bem como número de telefone e muitas outras, podem ser obtidos através de sites e-commerce, através do mercado negro ou outros meios. Ataques de phishing scam podem ter como único objetivo apenas completar as informações assim obtidas.

Há formas bastante agressivas de se realizar ataques de Vishing Scam. Atacantes utilizam-se de scripts para iniciar chamadas VoIP para todos os telefones contidos numa determinada faixa de números. Pode-se até mesmo mascarar o número de origem, fazendo-o parecer o número genuíno de uma dada instituição. Quando em uma ligação, cai-se na caixa de mensagens de voz, deixa-se uma solicitando (e "justificando"), bem como na explicação já feita acima, que o cliente ligue para um dado número, este, obviamente falso. Aliás, sabendo-se que atualmente mensagens de voz indesejadas são distribuídas massivamente, criou-se um novo termo para denominar as mesmas: SPIT – Spam over Internet Telephony.

Vale ressaltar que, já que o Vishing Scam deriva-se do Phishing Scam tradicional, traz consigo conceitos como o de Spear Vishing, ou seja, ataques de Vishing altamente focalizados.

Ataques de Vishing Scam crescem continuamente em quantidade e sofisticação. Atualmente, este tipo de ataque não é largamente posto em prática no Brasil, já que a tecnologia VoIP não é muito popular, mas invariavelmente nos atingirá em um futuro breve.

2.2.5 – Phishing em Mensageiros Instantâneos

Como uma das principais formas de comunicação no mundo atual, os mensageiros instantâneos estão longe de estarem isentos dos perigos do Phishing. Na verdade, pode-se dizer que é um dos terrenos mais férteis para a proliferação deste ataque, devido a alguns fatores, a serem aqui citados.

O primeiro destes fatores é o tipo de comunicação que geralmente se estabelece em mensageiros instantâneos. É uma comunicação mais informal, entre indivíduos que geralmente se conhecem ou são até mesmo grandes amigos. Todo este ambiente "familiar" traz uma maior sensação de segurança, fazendo com que os cuidados sejam reduzidos, até porque em muitas vezes o remetente da mensagem é um amigo de confiança que foi, contudo, infectado por um malware que está distribuindo a mensagem através de sua rede de contatos.

Em segundo lugar, podemos citar a velocidade (em tempo real) e grande quantidade de conversas estabelecidas simultaneamente. Estando o usuário perdido em tantas conversas, nas quais a troca de URL's é comum e constante, uma URL maliciosa tem maiores chances de passar desapercebida.

Além disso, a maior percentagem de usuários deste tipo de software engloba leigos em geral, crianças e adolescentes, que muitas vezes não possuem a capacidade de discernir entre mensagens autênticas e maliciosas, acabando por acessar portais maliciosos e/ou efetuar o download de malwares sem ter notícia de tal. Este fato agrava-se caso o computador seja compartilhado com outros que possam vir a efetuar possíveis transações bancárias (ou ações de importância equivalente) nesta mesma máquina, uma vez que pode estar infectada por keyloggers.

Fatores humanos somam-se a periculosidade do ataque de Phishing Scam, tornando este vetor possivelmente mais ameaçador que e-mails.

2.2.6 – Phishing em Sites de Relacionamento

Assim como no caso dos mensageiros instantâneos, os sites de relacionamento são, por assim dizer, ambientes virtuais mais descontraídos que, por exemplo, uma caixa de e-mails, e novamente tem-se uma redução na cautela. Não assemelha-se apenas neste ponto: Além disto, na maior parte das vezes o remetente da mensagem é algum amigo de confiança, possivelmente infectado por um malware.

Por se tratar de uma rede onde circulam fotografias, informações da vida alheia, e onde estabelecem-se paralelos com o mundo real, são estes os pontos que os phishers exploram. As possibilidades são inesgotáveis: os atacantes indicam a existência de uma foto da vítima circulando pela rede, de uma comunidade difamando-a, ou de um vídeo que deveria ser assistido, dentre outros.

Os recados podem conter dois tipos de links:

- Links que têm pequenas diferenças em relação aos domínios originais, que tentam se aproveitar de momentos de desatenção do usuário, como www.yultube.com (youtube), ou www.0rkut.com (orkut).

- Links cuja escrita é igual ao de links originais, mas que apontam para outro domínio que não o sugerido, através da inserção de código HTML, utilizando-se um “href”. Por exemplo: www.ufrj.br. Neste caso, aparecerá escrito no recado www.ufrj.br, mas na verdade, o endereço apontado é www.gris.dcc.ufrj.br.

O website para o qual o usuário é redirecionado assemelha-se ao original, e tem como finalidade roubar senhas e/ou induzi-lo a instalar malwares, aproveitando-se de qualquer lapso de atenção.

Os sites de relacionamento são um terreno fértil para phishings, pois nas páginas de recados, além da disseminação de links ser normal, são de acesso público (se não forem definidos como privados), e há a possibilidade de fisgar outros usuários que naveguem pela rede. Devido à desenfreada inclusão digital, temos nestes, ainda, muitos usuários leigos, completamente vulneráveis, passíveis de serem facilmente fraudados.

2.3 – A condução de um ataque tradicional

Embora se tenha apresentado passos seguidos por phishers na seção anterior, esta seção visa evidenciar a estruturação padrão de um ataque de Phishing Scam, constituído de diversas fases. São elas:

1) Fase de planejamento (Fase inicial):

Nesta fase, o atacante escolhe seu alvo, define o objetivo do ataque, de que artimanhas vai se valer e o método a utilizar.

2) Fase de preparação:

Nesta fase, elabora-se todo o material a ser utilizado, como e-mails, websites falsos, dentre outros. Obtém-se informações sobre o alvo, prepara toda a parte eletrônica a ser utilizada no ataque e, no caso de atacantes mais experientes, eleva seu nível de ocultação.

3) Fase de ataque:

Na fase de ataque, o atacante utiliza a via pela qual optou na fase de planejamento. O ataque pode ocorrer:

- Via e-mail;
- Via website;
- Via mensageiros instantâneos;
- Via VoIP;
- Via malware;

4) Fase de coleta:

Nesta fase, ocorre a coleta dos dados obtidos com o ataque. Dados inseridos em páginas web previamente preparadas para o ataque, em respostas das mensagens disparadas ou capturadas por malwares.

5) Fase da fraude:

Fase onde ocorre a fraude propriamente dita. Nesta fase, há o roubo de dinheiro, de informações sensíveis, apropriação da identidade alheia para cometer outros delitos, vendê-las a quem interesse ou utilizar em um segundo ataque em busca do objetivo definido na fase inicial.

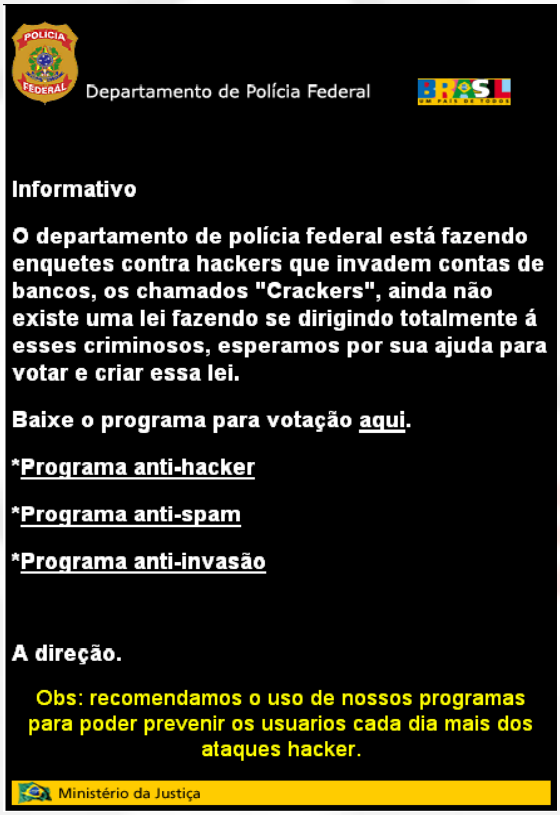
6) Fase pós-ataque:

Nesta fase ocorre o desligamento das máquinas utilizadas, e a destruição das evidências. Há ainda a avaliação da efetividade e possivelmente lavagem do dinheiro adquirido (no caso de tê-lo sido).

2.4 – Reconhecendo Phishing Scam

A cada dia que se passa, a comunicação humana converte-se mais para o meio eletrônico, seja ele internet, telefone, ou o que quer que seja. A partir disto, pode-se facilmente perceber que se há algo fundamental para a utilização segura das tecnologias de comunicação é a habilidade de reconhecer tentativas de Phishing Scam. Nesta seção, trataremos justamente deste aspecto.

Ataques de Phishing Scam, como qualquer outra tentativa de cópia, sempre possuem falhas que permitem sua identificação. Uns mais, outros menos:



Os logos são autênticos, e algumas vezes constam até mesmo alguns dados pessoais Porém, como identificá-los como Phishings? Estas mensagens sempre possuem pontos críticos, a saber:

1) O endereço do remetente:

É o primeiro ponto a se observar. Na maioria das vezes, este endereço não corresponde ao e-mail de uma instituição autêntica. Por exemplo, um e-mail que sugere ser proveniente do orkut, vindo de um endereço como suporte@0rkuty.com. Contudo, há técnicas de e-mail spoofing, ou seja, técnicas para forjar o cabeçalho de uma mensagem, como no caso da mensagem número 2. Portanto, este cuidado não é suficiente.

2) Formatação da mensagem:

A maioria das tentativas de Phishing possui graves falhas em sua formatação. Por muitas vezes, tornam-se facilmente identificáveis, devido à presença de erros gramaticais, como na mensagem 1. Esta, em particular, foi muito mal escrita, e encontram-se erros grotescos como "[...] ainda não existem leis fazendo se dirigindo [...]", a presença de acento agudo onde sequer deveria haver crase, a péssima pontuação, dentre outros.

A mensagem 2 possui menos erros, mas ainda assim peca. Pontuação estranha, como em "[...] o mais rápido possível, caso não seja esclarecido [...]", onde encontra-se vírgula onde deveria haver ponto. Além disso, a presença constante de "esclarecer", "esclareça", "esclarecido", demonstra um pouco de amadorismo na maneira como foi escrita. Apesar de tudo, esta mensagem é potencialmente perigosa, pois muitos não percebem tais falhas.

3) Proposta ou requisição:

Há coisas das quais se deve sempre suspeitar. Solicitações que possuam contradições, ofertas excessivamente tentadoras, como aquelas vistas no golpe 419, solicitações repentinas com curto prazo, que sugerem o cancelamento de uma conta, ou até mesmo abertura de inquérito, mensagens que solicitam dados pessoais e outras que disponibilizam links em seu corpo são algumas das quais se pode citar.

Este é, juntamente a verificação do endereço para o qual o link contido na mensagem remete, o ponto mais importante na análise e reconhecimento de uma tentativa de Phishing.

Conforme já dito anteriormente, este ataque toma como base a Engenharia Social, e portanto age, em boa parte, a nível psicológico. Para alcançar o objetivo de convencer o usuário, busca-se afetá-lo de modo tal que este pense o mínimo possível. Daí a tática de assustar e apressar, com ameaças, ou de ludibriá-lo com a possibilidade de dinheiro fácil.

Analisando-se as duas mensagens, notamos na primeira solicitações contraditórias, sem nexo. Primeiramente, o e-mail sugere que há uma simples enquete. Só por si, isto já torna a mensagem estranha, pois logo vem à mente a pergunta: qual a necessidade de questionar o público quanto a criação de uma lei contra criminosos? De algum modo, poderiam os fraudantes vencer a enquete, tendo a maioria dos votos convertidos para "Desaprovo a criação desta lei. Não tenho dúvidas de que o roubo de contas bancárias jamais deve ser punido, devendo ser, na verdade, incentivado."?

Além disso, qual a necessidade de se baixar um programa para votação em enquetes, uma vez que é extremamente simples adicioná-la à uma página web? Podemos ainda notar que a Polícia Federal não vota leis, quanto mais solicitando apoio público. Para dar continuidade ao espetáculo, o e-mail disponibiliza um programa "anti-spam", "anti-invasão" e, por fim, "anti-hacker". Que sorte não? Um programa milagroso. Pura fraude. E para fechar com chave de ouro, assina-se "A direção", o que seria comum, talvez, no caso de e-mails empresariais. Porém, soa bastante estranho no caso da Polícia Federal.

Já no segundo caso, tem-se uma mensagem melhor elaborada, mas ainda assim, suspeita. O e-mail busca explorar uma ou mais, dentre três falhas humanas em potencial

1. Medo: A primeira falha em potencial. Temer por ter feito qualquer acesso que possa ser considerado ilegal. E uma vez que a mensagem é intimidadora, o usuário pode considerar até mesmo que ter acessado um perfil em um site de relacionamentos possa ter sido seu acesso indevido.
2. Suspeita: A segunda falha em potencial. Ocorre quando se compartilha um computador. Ao receber um e-mail deste tipo, um pai pode julgar que seus filhos podem estar envolvidos em atividades suspeitas, ou uma esposa pode julgar que seu marido está realizando acessos ilegais. Pode ainda ocorrer a suspeita de um possível malware no computador, que esteja fazendo acessos indevidos.
3. Curiosidade: A terceira falha em potencial. O que existe para auxiliar-nos na construção de conhecimentos é também um dos mais graves defeitos humanos. Pode ocorrer de o

indivíduo ter certeza de que não realizou o acesso, mas insistir em abrir o arquivo, para saber do que se trata. Acaba, assim, infectado.

Há ainda um prazo de 24 horas, para apressar a vítima a acessar o link. Porém, há traços bastante suspeitos. Por que a Polícia Federal enviaria um e-mail contendo um inquérito? Primeiramente, o usuário não necessariamente acessa sua caixa de e-mails diariamente, ou sequer a visita. Em segundo lugar, é uma maneira informal demais para se tratar de assuntos desta grandeza. Além disso, a ausência do nome do destinatário na mensagem comprova que sequer houve uma investigação para tal acusação.

4) O endereço para o qual o link remete:

Deve-se, após analisar os pontos acima sem chegar a uma conclusão, observar o endereço para o qual remete o link contido no corpo da mensagem. Frequentemente, é uma solicitação de download, geralmente de extensão .exe (arquivo executável do Microsoft Windows) ou .src (arquivo de proteção de tela do mesmo sistema operacional). É algo no mínimo suspeito um arquivo chamado "inquérito.src" (contido na segunda mensagem, por exemplo), que sugere ser um documento de texto, ou um arquivo denominado "foto.exe", que sugere ser um arquivo de imagem.

Pode-se ainda verificar que o link aponta para uma página web, onde ocorrerá o ataque propriamente dito. Nesta página, o usuário será induzido a realizar o download de um malware ou inserir dados pessoais e/ou sensíveis, ao crer inocentemente na autenticidade da página. Se o e-mail sugere ser, por exemplo, do Google (www.google.com), deve-se manter a atenção para links como "www.g00g1e.com".

É estritamente fundamental verificar cuidadosamente este endereço, que muitas vezes, pode parecer o original, mas não é. Pode estar disfarçado sob um hipertexto como "www.gris.dcc.ufrj.br", e, ainda assim, apontar para o endereço "www.meroube.com". O endereço apontado é geralmente exibido no canto esquerdo inferior do navegador.

Dicas rápidas - Parte 1:

- Sites que possuem hífen em seu endereço tem grandes chances de serem fraudes!

- Não confie em URL's contendo IP's!

- Conheçam o game http://cups.cs.cmu.edu/antiphishing_phil/new/index.html

2.5 – <u>Alguns casos de Phishing</u>

Esta seção visa uma melhor fixação da análise para reconhecimento de Phishings, e uma visualização do aspecto prático do ataque, citando-se casos bastante comuns. São eles:

1) Receita Federal:

Embora não tenha sido citado, o endereço remetente é, aparentemente, autêntico. Aliás, desconsideraremos este fato nessa análise mais profunda, por se tratar de um aspecto não-confiável (o fato de uma mensagem possuir um endereço de remetente aparentemente genuíno não indica sua autenticidade).

A ortografia do e-mail, do vocabulário à acentuação, é bastante convincente, e busca ainda eliminar quaisquer suspeitas relativas à fluência da escrita, ao citar "Certidão gerada automaticamente [...]". Há pequenos traços que podem ser notados por indivíduos mais observadores, como a presença de excessiva de palavras iniciadas por maiúsculas, em "O que Fazer Para Regularizar [...]", mas nada realmente gritante. Peca ainda na formatação: Um texto centralizado, um pouco estranho de se ler.

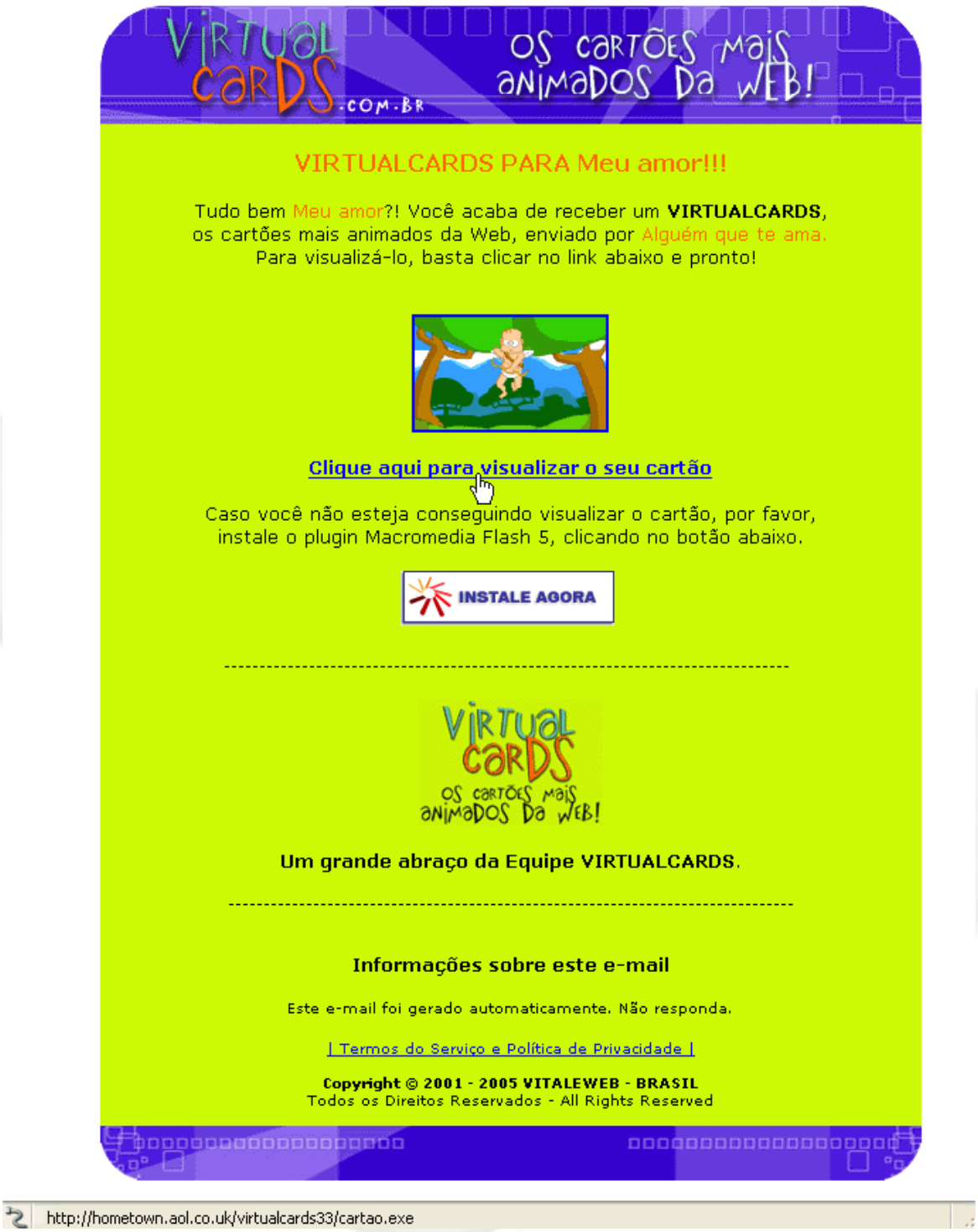
Analisando-se o corpo, a justificativa e as solicitações da mensagem, pode-se perceber ainda outras pequenas falhas, como o fato de sequer ter-se citado o nome do indivíduo irregular na mensagem, o que, apesar de tudo, ainda não garantiria a autenticidade da mensagem. É, no mínimo, passível de desconfiança que a Receita Federal tenha identificado o e-mail correspondente ao CPF irregular mas não tenha incluído sequer o número do mesmo ou o nome do proprietário.

Além disso, a Receita Federal não enviaria tal solicitação. Caso houvesse a extrema necessidade do envio de um e-mail, possivelmente seria algo mais próximo a um alerta, solicitando que o usuário entrasse em contato com a Receita Federal o mais urgentemente possível para resolver a situação.

Por fim, analisa-se o ponto final e decisivo: O endereço para o qual o usuário será remetido caso clique no link presente na mensagem é http://www.lyonworkspace.com/irpf/declaracao.exe, que não corresponde ao domínio autêntico da Receita Federal, o que já elimina a possibilidade desta mensagem ser autêntica. Além disso, o usuário é induzido a baixar um arquivo de extensão .exe, do qual sempre se deve duvidar, embora realmente exista um executável para auxiliar na confecção da declaração do imposto de renda. Neste caso, o arquivo não se afasta muito da realidade, como o faria um denominado "foto.exe".

A mensagem em questão está acima da média no que diz respeito a profissionalidade dos ataques de Phishing Scam. Um e-mail bem elaborado, com boa ortografia, bom layout e razoavelmente convincente. Sua sugestão (CPF suspenso ou pendente de regularização) é bem abrangente e ameaçadora, e o fato de a Receita Federal disponibilizar um aplicativo para auxílio na declaração do imposto de renda contribui no que diz respeito a induzir o usuário a baixar "declaração.exe". Certamente, alto nível de risco.

2) Cartão Virtual:



Configurando-se como um dos mais perigosos, o golpe do Cartão Virtual é exemplo da perfeita combinação entre simplicidade e eficácia. Dispensa a elaboração de uma proposta ou requisição mirabolante, e é de uma abrangência tal que supera qualquer outro tipo de mensagem.

Atinge única e exclusivamente o fragilíssimo lado humano da curiosidade, com um toque de empolgação (obviamente induzida): Afinal, quem não gosta de ser agraciado com um cartão? Não obstante, o phisher utiliza-se ainda do mistério, apresentando o remetente como secreto, não explicitado, de modo a envolver ainda mais a vítima em seu jogo, e desvia-la toda a atenção, ao fazê-la refletir, quase que imediatamente, sobre quem poderia ter-lhe enviado a mensagem.

Mas o ponto mais notável em toda a estratégia deste atacante é o fato de aproveitar-se da ludibriação que causa a possível existência de um amante secreto. É um ataque direto ao ego, que torna suscetíveis homens e mulheres, independentemente da idade. Até mesmo os melhores profissionais da segurança da informação inicialmente deixar-se-iam levar pelo enredo do cartão, até que identificassem a fraude.

Além disso, há de se explicitar a excelente confecção da mensagem. A ortografia está perfeita e o layout é impecável. O jogo de cores torna a mensagem ainda mais distrativa, onde temos as partes como “Meu amor” e “Alguem que te ama”, as mais importantes da mensagem, em laranja, cor conhecida por despertar entusiasmo.

A proposta do e-mail é mais do que válida: Um cartão virtual. Nada para se desconfiar. Geralmente, estas mensagens possuem o nome do destinatário, previamente inserido pelo remetente, mas sua ausência é justificável a partir do ponto em que estes campos podem ser preenchidos com qualquer coisa, como, no caso, “meu amor”.

É um Phishing bastante profissional, sem dúvida. A fraude só pode ser identificada ao verificar a solicitação do download de um arquivo “cartões.exe”, não-proveniente dos domínios virtuais da VirtualCards. Por isso o phisher buscou usar o maior número de artifícios possíveis para distrair a vítima. Este ataque, certamente, possui um alto índice de sucesso.

3) Notícias de grande repercussão:

Outra tática muito comumente adotada por phishers é aproveitar-se de notícias que estejam em grande evidência na atualidade para veicular ataques. Mais um ataque que visa atingir a curiosidade humana, porém pode, por algumas vezes, ir muito além. É o caso da mensagem exibida acima.

O caso da menina Isabela Nardoni, ocorrido em março de 2008, chocou o país. Ela teria sido jogada do sexto andar de seu prédio, após ser esganada, e as suspeitas recam sobre o próprio pai e a madrasta. A mídia nacional mobilizou-se quase que por completo para cobertura do caso.

Tendo isto em vista, phishers encontraram a oportunidade perfeita: Esquecendo totalmente os escrúpulos e comprovando seu perfil criminoso, criaram mensagens visando atacar não apenas a

curiosidade, conforme citado acima, como também o sentimento de pena e choque da população ante esta situação. Um ataque frio, mas eficaz.

Assimilando a identidade da globo.com, veiculam a mensagem exposta acima. A mensagem possui alguns erros de ortografia bastante perceptíveis, como “vejá”, e algumas falhas de pontuação. Outro ponto que podemos notar é o layout do e-mail, que torna-se um tanto quanto amador ao inserir-se um gritante “Última hora [...]” em vermelho, e com alinhamento estranho em relação ao resto da mensagem.

A proposta é mais do que válida para o objetivo final: fraudar. Disponibilizar uma suposta confissão de um suspeito de um crime nacionalmente famoso é um ataque eficaz, e não levanta muitas suspeitas. Não há subterfúgio para desviar a atenção ou ameaçar de alguma forma o usuário: O sentimento de pena e a repercussão do caso são o suficiente.

Porém, ao verificar o endereço para qual o link de download do vídeo remete, desmascara-se a fraude: um vídeo de formato .exe. Além disso, encontra-se fora dos domínios virtuais da globo.com.

2.6 – Como proteger-se

Após tanto, pode-se perceber claramente a necessidade da criação de métodos para proteger-se. Este capítulo tem exatamente este objetivo.

2.6.1 – Software e Informação: O Escudo e a Muralha

Conforme citado diversas vezes nas seções anteriores, o ataque de Phishing utiliza-se largamente de engenharia social, um ataque realizado a nível psicológico. Tendo isto em mente, logo percebe-se a insuficiência do uso exclusivo de softwares. Daí a alusão feita no título desta seção.

Hackers de má índole possuem grande engenhosidade, especialmente no que diz respeito à esfera computacional, que pode ser utilizada para burlar facilmente aplicativos de proteção. Porém, enganar um indivíduo, com um conhecimento mesmo que básico e capacidade de raciocínio é uma arte para pouquíssimos. Engenhosidade combate-se com conhecimento. Se softwares fossem, por si só, capazes de resolver todos os problemas de segurança existentes no mundo digital, não haveria a necessidade de tantos profissionais na área de Segurança da Informação.

Um indivíduo com conhecimentos básicos em Phishing Scam estará muito mais protegido do que aquele que estiver equipado com diversos aplicativos anti-phishing. Isto porque a maioria trabalha sobre um banco de dados de mensagens fraudulentas previamente reportadas, identificando-as caso venham a ser recebidas novamente, e alertando o usuário. Tem-se aí três pontos a discorrer.

O primeiro é que caso a mensagem não esteja inclusa no banco de dados (não houver sido reportada previamente), não será filtrada. Há a possibilidade de, no melhor dos casos, o aplicativo anti-phishing possuir um sistema “inteligente” (que, ainda assim, pode ser burlado) fazer um alerta de suspeita, como no download de executáveis, dentre outros.

Em segundo lugar, fica a cargo do usuário se deseja ou não ver a mensagem, visitar o endereço ou efetuar o download. Caso a mensagem o tenha convencido de sua autenticidade, e este não tenha conhecimento dos possíveis riscos, ele o fará.

Em terceiro lugar, mecanismos de proteção não estão sempre disponíveis em todos os

pontos suscetíveis a um ataque de Phishing Scam. Em um ataque de vishing, por exemplo, não haverá um aplicativo alertando ao usuário: “Senhor, esta é uma tentativa de Phishing. Não forneça informações e desligue o telefone imediatamente”. Porém, caso o usuário tenha a capacidade de discernir entre o real e a farsa, poderá defender-se com muito mais eficácia.

Um soldado com um escudo pode proteger-se de um, dois ou até três adversários. Porém, um que esteja atrás de uma muralha estará protegido de um exército, se necessário. E é basicamente esta a filosofia: Aplicativos podem proteger-te de, talvez, 60% das fraudes, mas não hão de proteger-te de todas.

Obviamente, contudo, qualquer segurança extra é bem-vinda. Embora o ideal para tornar o ambiente virtual mais seguro seja a proliferação de conhecimentos preventivos dentro de qualquer grupo, organização, instituição e demais, o uso de anti-phishers é ainda de grande valia, principalmente em computadores compartilhados, onde, apesar de todos os cuidados, há sempre um elo mais fraco.

Soluções de segurança anti-phishing estão geralmente acopladas a outros aplicativos, como é o caso de extensões de navegadores web e clientes de e-mail. O Mozilla Firefox, desenvolvido pela Mozilla Foundation, é um dos exemplos que se pode citar. Ao visitar-se um site identificado como fraudulento, o navegador exibe uma mensagem de alerta, sugerindo a retirada do usuário.

Há ainda pela rede outros que atuam de maneira independente. Porém, vale lembrar que nenhum aplicativo pode substituir a cautela ou atenção do usuário.

Dicas rápidas – Parte 2:

- Para saber um pouco mais sobre softwares anti-phishing, visite:

http://en.wikipedia.org/wiki/Anti-phishing_software.

Obs.: O GRIS e o autor não se responsabilizam pelo conteúdo de sites externos.

2.6.2 – Scam Baiting: Divertindo-se com o inimigo

"O maior prazer de um Homem inteligente é fazer-se de idiota frente a um idiota que se faz de inteligente."

Phishers são indivíduos maliciosos, que utilizam-se de toda sua engenhosidade para enganar usuários muitas vezes inocentes, criando até mesmo uma espécie de jogo com a vítima. Mas o que acontece quando a vítima também sabe jogar?

Scam baiting é o termo utilizado para designar uma espécie de contra-ataque sobre os phishers. Não possui uma tradução exata na língua portuguesa, mas pode-se dizer que corresponde a algo como "apresentar uma isca ao atacante". Configura-se como a prática de, sendo razoavelmente habilidoso na arte da engenharia social e conhecendo a anatomia do ataque, entrar no jogo do atacante, passando-se por uma vítima em potencial.

É particularmente utilizado no caso de fraudes 419, pois estas envolvem um longo jogo de e-mails. Enquanto o objetivo do atacante é fazer de tudo para enganar-te, o seu é, basicamente, se divertir, induzindo o atacante a gastar seus recursos e a expor-se ao ridículo, o máximo possível. Deste modo, além da diversão, você estará fazendo com que o phisher perca tempo, de maneira inútil, tempo este que poderia estar sendo utilizado para fraudar usuários inocentes.

Como todo jogo, há regras a se seguir. A mais básica delas é **nunca, em momento algum, exponha quaisquer dados pessoais reais, ou permita-se ir a um encontro ao vivo.** Lembre-se, você está lidando com bandidos, e nunca se sabe o que esperar deste tipo de indivíduo. Crie uma conta de e-mail com dados fictícios, e utilize-a para tal finalidade.

São muitas as possibilidades, e grupos como o 419 eater (www.419eater.com) dispõem de informações e dicas bastante úteis para aqueles que querem iniciar-se nesta prática.

2.6.3 – <u>Recomendações diversas</u>

Nesta seção, explicitar-se-á os mais fundamentais cuidados, alguns previamente citados, porém, frisados aqui.

São as recomendações:

Suspeite!

Não se trata de viver em paranóia, mas cautela nunca é demais. A cada mensagem recebida, ainda que proveniente de amigos, fazendo solicitações de dados sensíveis ou de downloads, aplique a análise demonstrada na seção anteriormente apresentada neste mesmo artigo: "Reconhecendo Phishing Scam"

Em caso de dúvida, confirme!

Ao deparar-se com uma solicitação suspeita, ainda que urgente, busque entrar em contato diretamente com o possível remetente para confirmar sua identidade e os motivos, além de como proceder. Nunca use o sistema de "rediscagem" ou utilize o número contido na própria mensagem para confirmá-la por telefone. Pesquise em fonte confiável o número e só então disque para o encontrado.

Use o Google!

O Google é uma ferramenta bastante poderosa, e, caso haja suspeita se um domínio realmente corresponde a uma empresa, basta realizar uma busca. Raramente se há de encontrar um domínio phisher antes de um domínio original.

Verifique atentamente a extensão do arquivo!

Arquivos cuja extensão seja .exe, .bat, .cmd ou .src são os mais passíveis de conter um malware. Verifique ainda o que o arquivo sugere ser, e se sua extensão confere-lhe nexo. Por exemplo: Arquivos de imagem terminados em .exe, vídeos em .src, dentre outros, não estabelecem nexo entre proposta e extensão.

Se possui conhecimentos, pratique Scam Baiting

Une o útil ao agradável: É divertido e colabora na luta contra o crime cibernético, ao consumir tempo e recursos de um phisher que poderiam estar sendo voltados a fraudar usuários inocentes. Contudo, lembre-se de seguir as regras de proteção.

Treine seu grupo

Conforme previamente citado, a instrução é a melhor defesa contra ataques de Phishing Scam. Para proteger a si, à sua empresa, organização ou instituição, reserve tempo em seu programa de treinamento para discorrer sobre cuidados a serem tomados ao receber-se um e-mail, mensagem ou telefonema, cuja proposta seja suspeita e/ou possa causar perda de dados sensíveis. Diga aos treinandos que jamais confiem cegamente em qualquer mensagem, e que nunca dêem informações sigilosas através de telefones ou mensagens.

Utilize filtros anti-phishing!

Embora não substituam a instrução, são aplicativos (ou extensões) úteis, e uma vez que contribuem com a segurança do ambiente virtual, sua utilização, além de muito válida, é bem-vinda.

Utilize antivírus, firewall e anti-spyware!

Estes aplicativos não protegem contra ataques de Phishing, mas podem protegê-lo contra possíveis malwares que venham a ser adquiridos caso, acidentalmente, você ou indivíduos que compartilham do mesmo computador tenham sido fisgados no ataque.

Leve a informação adiante

No mundo virtual, a arma necessária para a auto-defesa e defesa alheia é a informação. Divulgue recomendações de segurança de seu conhecimento a toda sua rede de conhecidos.

Reporte!

Saiba como na seção a seguir.

2.6.4 – Reportando

Reportar incidentes é de grande valia para a comunidade de segurança da informação e, conseqüentemente, para todos aqueles que dela se beneficiam. Ataques de phishing scam não fogem à regra e devem ser reportados.

Ao receber uma mensagem de phishing, reporte-a o mais rápido possível a reportphishing@antiphishing.org. O AWPG (Anti-Phishing Working Group) faz um excelente trabalho no que diz respeito a reporta-lo a outras entidades, além de contribuir com o desativamento de domínios utilizados para Phishing.

Deve-se reportar ainda às entidades cujos nomes estão sendo utilizados na fraude, para que possam tomar as medidas cabíveis, como alertar a seus clientes e à população.

No caso de um ataque recebido em uma empresa ou instituição, deve-se reportar ao seu CSIRT, caso exista. Este grupo ficará responsável por tomar todas as medidas necessárias.

2.7 – Quando já é tarde

Agora é tarde. Você foi pego em um golpe de Phishing, e já não há o que fazer.

Errado! Caso o usuário perceba que acaba de morder a isca de um phisher, ficar estático e lamentar não é a postura correta a se assumir.

Primeiramente, deve-se reportar o incidente:

- À sua companhia de cartões de crédito, caso tenham sido fornecidas informações acerca do mesmo. Quanto mais cedo esta ação for tomada, maior será a efetividade das medidas adotadas para sua proteção.
- À companhia que você julga ter sido forjada, para que a mesma possa advertir seus clientes da iminência de phishing scam sob sua logomarca.
- Opcionalmente, porém recomendável, reportar o caso ao Anti-Phishing Working Group, no site http://www.antiphishing.org/report_phishing.html.

Deve-se ainda alterar todos as senhas de suas contas online, começando por aquelas que têm relação com instituições financeiras. Opte por utilizar senhas fortes (contendo caracteres maiúsculos e minúsculos, números, caracteres especiais como '!', '@', etc.).

Mantenha as próximas faturas de seus cartões de crédito e o extrato de sua conta sob observação, de modo a perceber alterações ou transações que você não realizou.

E, por fim, proteja-se: Informe-se e mantenha-se atento, alertando e instruindo ainda ao máximo de indivíduos possível.

3 – Conclusão:

Após tanto, pode-se claramente perceber a periculosidade do ataque de Phishing Scam. Este ataque torna-se particularmente eficaz devido ao seu embasamento em engenharia social, fato que reduz em muito a eficiência de proteções a nível de aplicativos, fazendo com que o grau de instrução em relação a fraudes virtuais, fator relativamente pouco difundido atualmente, seja a principal forma de defesa e, muitas vezes, a única.

Tudo isto, aliado a "virtualização da vida", faz com que o Phishing Scam configure-se progressivamente mais como a fraude do século 21. Portanto, é necessário saber defender-se, além de difundir conhecimento, de modo que possamos, ao menos, reduzir o avanço da criminalidade no mundo virtual.

4 – Agradecimentos:

Gostaria de agradecer primeiramente a Deus, cujos motivos sequer necessitam ser explicitados. Agradeço também à minha família, que sempre me apoiou durante toda a vida pessoal e acadêmica, contribuindo com a minha ascensão até hoje e, certamente, pela eternidade.

Aproveito para agradecer aos membros do GRIS, primeiramente pela oportunidade de fazer parte desta família e, além disso, pela ajuda em alguns pontos deste artigo.

Agradeço ao Google, sem o qual elaborar este artigo seria uma tarefa herculana.

E, finalmente, agradeço a todos os leitores deste artigo, despedindo-me na esperança de que lhes possa ter sido útil. Quaisquer dúvidas, críticas e sugestões podem ser enviadas para diego@gris.dcc.ufrj.br.

Para saber mais sobre o grupo, visite: http://www.gris.dcc.ufrj.br

Obs.: Você verificou se este é o endereço autêntico?
Brincadeira!

Sinceramente,

Diego de O. Martins
Pesquisa e Desenvolvimento
GRIS – DCC – IM - UFRJ

5 – Bibliografia:

- **Nigerian Spam:**
  http://www.nigerianspam.com/
- **419 Eater:**
  http://www.419eater.com/
- **419 Fun**:
  http://www.419fun.com
- **Márcio D'Ávila Web Site – Exemplos de Phishing.**
  http://www.mhavila.com.br/topicos/seguranca/scam.html
- **Microsoft – Protect yourself against phishing**
  http://www.microsoft.com/protect/yourself/phishing/remedy.mspx
- **Brian Wizard**
  http://www.brianwizard.com/
- **Quatloos – Nigerian 419 Scam**
  http://www.quatloos.com/scams/nigerian.htm
- **iPhish: Phishing Vulnerabilities on Comsumer Eletronics – Niu, Hsu, Chen**
  http://www.usenix.org/events/upsec08/tech/full_papers/niu/niu_html/
- **On Guard Online – Phishing**
  http://onguardonline.gov/phishing.html
- **Phone Phishing: The role of VoIP in Phishing Attacks**
  http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294527,00.html
- **Millersmiles.co.uk**
  http://www.millersmiles.co.uk/
- **Behind Phishing: An examination of Phisher Modi Operandi - McGrath, Gupta**
  http://www.usenix.org/events/leet08/tech/full_papers/mcgrath/mcgrath_html/
- **Wikipedia (English) – Phishing**
  http://en.wikipedia.org/wiki/Phishing
- **Technical Info – The Phishing Guide**
  http://www.technicalinfo.net/papers/Phishing.html
- **WordSpy – Phishing**
  http://www.wordspy.com/words/phishing.asp
- **First Monday – The Economy of Phishing**
  http://www.firstmonday.org/issues/issue10_9/abad/