Tutorial sobre Phishing

Data: 2006-08-15

O que é o Phishing?

Phishing é um tipo de fraude electrónica que tem se desenvolvido muito nos últimos anos, visto que a Internet a cada dia que passa tem mais utilizadores e mais serviços, bem como cada vez mais pessoas tratam dos seus assuntos financeiros pela Internet. Este tipo de fraude electrónica é projectada de forma a tentar enganar pessoas de formar a "roubar" informações a quem é vítima dele. É uma das principais preocupações ao nível da segurança informática e baseia-se no envio de um e-mail fraudulento com o objectivo de obter códigos de acesso (nomes de utilizador e senhas) e dados financeiros.

No início desta prática um ataque de phishing consistia em um indivíduo, com intenções menos correctas, enviava um e-mail que parecia vir de um banco, ou de serviços on-line como o eBay ou o Amazon, utilizando pretextos falsos mas muito convincentes onde até o design é "igual" ao da empresa pela qual está a fazer-se passar. Normalmente este e-mail diz que precisa confirmar alguns detalhes sobre o utilizador e muitas vezes ameaça o fecho da mesma caso a vitima não responda à solicitação que lhe é feita no e-mail. O e-mail contém um caminho (link) para a suposta página do banco ou serviço em questão onde lhe é pedida determinada informação nomeadamente o nome de utilizador e palavra chave no caso dos serviços on-line, e no caso de serviços financeiros informações relativas ao cartão de crédito.

Porém isto foi só o inicio do phishing pois nos últimos tempos têm surgido cada vez formas mais apuradas, melhoradas e sofisticadas de phishing sendo que as situações mais recentes envolvam o envio de um e-mail que ao invés de conter links que direccionam para um formulário onde é requerida informação confidencial, os links direccionam para páginas que contêm programas maliciosos, que se auto - - instalam no computador da vitima. Estes programas pertencem muitas vezes à classe dos keyloggers e podem registar a sequência de teclas pressionadas, actividades realizadas com o rato ou até mesmo imagens do écran. Estes programas, depois de recolhida a informação, enviam-na pela Internet, quando disponível para um site controlado pelo autor da fraude, que pode fazer uso dessas informações confidenciais que não lhe dizem respeito.

A história do Phishing

A palavra "Phishing" deriva da analogia da palavra "Phish" (em inglês) pois esta técnica consiste na "pesca" de informações, por parte de pessoas mal intencionadas, num "mar" de utilizadores da Internet, ou seja em muitos utilizadores da Internet alguns são apanhados nestes esquemas tal e qual como no mar os peixes são apanhados. O nome foi utilizado pela primeira vez em 1996 quando hackers roubaram informações de contas do AOL. Em 1996, contas hackeadas começaram a

ser chamadas de "phish", devido às contas serem como peixe pois delas eram feitas pescas de informações. E em 1997 a palavra "phish" começou a ser usada entre a comunidade informática como uma forma de fraude electrónica. A palavra "phish" também já foi atribuída a "crackins" de aplicações e jogos. A primeira referência a esta palavra nos meios de comunicação data de 16 de Março de 1997 pela vice presidente de uma companhia de integridade dos dados pessoais online na Florida. A palavra nos tempos correntes não só engloba a obtenção de detalhes de contas, como também inclui o acesso a todo e qualquer acesso a informações pessoais e financeiras. Uma técnica que inicialmente consistia em "truques" para fazer com que os utilizadores respondessem a um e-mail para obter dados de acesso a contas de utilizador e dados de contas bancários. Hoje em dia expandiu-se para websites que podem conter Cavalos de Tróia (trojan), keylogger's, capturadores de ecrã, spyware's, entre outros. Para complementar os "phisher's" criaram outros serviços atractivos como sites muito similares, aos sites dos quais pretendem receber a informação do utilizador, com uma formatação, imagem, conteúdo, estilos, e texto quase idênticas à do site original, ou serviços de trabalho fácil em que supostamente será muito bem remunerado.

Como prevenir?

Para prevenir ser vítima desta fraude existem várias medidas em que deve apostar. Vamos de seguida fazer uma breve referência a algumas das medidas cruciais para se manter seguro.

1) Instale Software para se proteger - É necessário ter sempre um Antivírus e uma boa Firewall no nosso computador para fazer "frente" às "pragas" informáticas que o nosso computador fica em risco de receber caso esteja ligado a outros computadores.

2) Mantenha-se actualizado - Descarregue regularmente actualizações de segurança e patches para o seu sistema operativo e para os seus softwares de segurança. Pois as empresas de segurança publicam actualizações e patches para eliminar as vulnerabilidades descobertas no seu software. Muitas vezes são descobertos os chamados bugs nos programas que permitem a pessoas mal intencionadas, às quais a nossa sociedade chama de hacker, ataquem o computador que tem essa vulnerabilidade. Antes que ocorra a maioria desses ataques, as empresas e vendedores de software criam patches gratuitos para os seus programas que publicam nas respectivas páginas na Internet, para que o utilizador do software da empresa possa descarregar.

3) Pense sempre antes de executar - Mesmo os utilizadores da Internet mais experientes podem ser facilmente enganados se não tiverem atenção ao que fazem no seu computador e ás informações que fornecem. Se receber um e-mail aparentemente amigável de um estranho, ou de uma empresa a pedir-lhe que actualize os seus dados pessoais, apague-o de imediato! Os alvos mais frequentes do Phishing são os utilizadores de PayPal, eBay, Amazon, e os clientes de bancos. No entanto que fique saliente que ninguém está livre de ser um alvo de Phishing.

4) Informações confidenciais - Nunca dê informações financeiras ou outras informações pessoais que o identifiquem ou outro tipo de dados como a idade que tem (aqui também se incluem os sites que perguntam se é maior ou menor do que uma certa idade) para aceder ou assinar páginas que não lhe sejam familiares ou de empresas com boa reputação.

5) Passos a tomar antes de enviar qualquer informação - Estranhar toda a comunicação vinda de entidades que lhe peçam informação sensível e pessoal como por exemplo bancos. - Estranhar qualquer e-mail ou site que lhe peça informação pessoal. - Verificar o código fonte da mensagem, analisar o remetente, os endereços IP, o código que está por trás das ligações. - Antes de enviar qualquer informação sua faça questão de confirmar com a instituição via telefone, fax ou pessoalmente a veracidade da comunicação.

6) Verifique sempre se os sites usam criptografia - Existem diferentes maneiras de saber se um site é seguro. Primeiro, antes de inserir qualquer informação pessoal, verifique se o site usa criptografia para transmitir informações pessoais. No Internet Explorer bem como no Mozilla Firefox pode fazer isso se verificar se existe o ícone amarelo de cadeado amarelo na barra de status situada na parte inferior do navegador. Esse símbolo significa que o site usa criptografia para proteger as informações pessoais importantes inseridas. Clique duas vezes no ícone de cadeado para exibir o certificado de segurança do site. O nome após Issued to deve corresponder ao nome do site em que pensa estar. Se o nome for diferente, poderá estar num site falsificado. No entanto caso não tenha certeza de que um certificado é legítimo, não insira informações pessoais e saia do site.

Cuidados a ter quando recebe um e-mail

1) Verifique o remetente - Desconfie de e-mail's que não tenham um remetente conhecido e não acredite em ofertas milagrosas.
2) Não baixe nem execute arquivos não solicitados - Cavalos de Tróia e Keyloggers são \"não solicitados\". Se alguém conhecido enviar um arquivo que você não pediu, verifique com a pessoa se ela realmente enviou o arquivo, e pergunte qual o conteúdo desse. Evite ao máximo executar programas que lhe sejam enviados por e-mail que contenham extensões como estas: .exe, .cmd, .com,.bat, .dll, entre outras.

Os problemas de Phishing

1) Factores de engenharia social

Ataques de Phishing consistem na sua totalidade em conhecimentos técnicos e na engenharia social. Na maioria dos casos o "Phisher" tenta persuadir a vitima a executar uma serie de acções que lhe vai permitir a ter acesso a informações confidenciais da vitima. As técnicas que obtêm mais sucesso são iniciados por e-mail pois convencem a vitima a fornecer dados confidenciais.

2) Envio de Mensagens
2.1 E-mail e Spam

Os ataques mais comuns são iniciados com um e-mail e consistem no envio de um e-mail falso utilizando a identidade de entidades de prestígio consideradas confiáveis, tais como sites de entretenimento, empresas financeiras, lojas, órgãos governamentais, entre outros. Estes e-mail estão muito bem camuflados pois apresentam-se configurados similarmente aos e-mail enviados oficialmente pelas instituições, com formatação iguais, imagens iguais, tipo de serviços os mesmos, e links idênticos.

Geralmente, as mensagens são enviadas para milhões de endereços de e-mail que

foram previamente recolhidos na Internet ou então foram compradas listas com milhões de e-mails activos, e com conhecimentos de SMTP estas técnicas são comuns aos Spammers. A entrega do e-mail normalmente é feita por computadores que estão sob o controle de pessoas mal intencionadas nos quais são incluídos servidores mal configurados e computadores com uma conexão de banda larga infectados com Cavalos de Tróia, mais conhecidos por trojan, que foram desenvolvidos para permitir o envio de e-mail em enormes quantidade, o chamado Spam. No entanto todos os outros tipos de máquinas ligadas à Internet não estão livres de serem usados.

Uma técnica popular é o roubo de identidade via e-mail. Pessoas mal intencionadas enviam e-mail tentando persuadir os receptores a fornecer dados pessoais, tais como nome completo, morada e código postal, nome de familiares, número do bilhete de identidade, números de contas bancárias, entre outros. Quando obtidos esses dados podem ser utilizados para qualquer fim. A identidade usada nessas mensagens geralmente é a mesma referida acima. No corpo da mensagem normalmente existem links que apontam para sites falsos, normalmente muito parecidos com os sites verdadeiros, onde existem formulários que a vítima é quase forcada a preencher com as informações solicitadas. O conteúdo preenchido no formulário é enviado para quem está a desenvolver esse projecto.

A maneira de persuadir a vitima é semelhante à do roubo de identidade, no entanto o e-mail contém links que apontam para sites que contém programas que, se instalados, podem permitir a captura de informações. A instalação é, na maior parte dos casos, feita pela vítima. Pode existir uma possibilidade, ainda que pequena, da instalação automática desses programas apenas pela leitura da mensagem, mas isso depende de uma combinação de muitos factores e de um grau um pouco mais elevado de programação que não vamos abordar aqui. O Phishing via e-mail não vem apenas com a identidade de entidades prestigiadas. Pois são também usados diversos tipos de assuntos de forma a criar curiosidade fazendo desta maneira com que o receptor da mensagem entre no local onde não deve. Um detalhe ao qual o utilizador deve prestar a máxima atenção são aos erros de gramática e de ortografia que essas mensagens geralmente apresentam.

Técnicas usadas nos e-mails:
• Visual similar à correspondência oficial;
• Os links utilizados são muito parecidos com os links oficiais, com poucas alterações;
• A base do HTML é usada para fazer com que os links sejam camuflados;
• Anexos que contém programas maliciosos;

2.2 Envio de mensagem baseado na Internet

Um método também muito popular é através de Web sites com código malicioso. Sites estes que são na maior parte das vezes administrados pelo "Phisher" ou então têm conteúdo que lhe pertencem.

Técnicas baseadas na Internet incluem:
• Links camuflados tal como no envio de e-mail;
• Banners ou outro tipo de conteúdo que levam para o site do "Phisher"
• O uso de erros no sistema do utilizador para poderem aceder ao seu computador, instalar software malicioso ou prepara-lo para receber outros ataques;
• O uso de pop-us ou frames para mostrar a mensagem do "Phisher" camuflando seu

código.

Este artigo foi enviado por ***Skin***, ao qual agradecemos o trabalho realizado.