



McAfee Phishing/Pharming

# Phishing e Pharming

Entendendo o Phishing e o Pharming

**Índice**

<b>Introdução – Entendendo o Phishing e o Pharming</b>	<b>3</b>
<b>O que são Phishing e Pharming?</b>	<b>4</b>
<b>Figura 1 – Tendência de ataques exclusivos de Phishing em 2003-2004</b>	<b>4</b>
<b>Primeiras tentativas</b>	<b>4</b>
<b>Ataques sistemáticos</b>	<b>5</b>
<b>Figura 2 - Sites de Phishing ativos 2004-2005</b>	<b>5</b>
<b>Ficando mais atentos</b>	<b>5</b>
<b>Impacto financeiro, Pharming – nasce uma nova ameaça</b>	<b>6</b>
<b>Redução de Phishing e Pharming com a McAfee</b>	<b>7</b>
<b>Filtragem anti-spam – proteção contra Phishing</b>	<b>7</b>
<b>Tecnologia de varredura de vírus da McAfee, E quanto à proteção de desktops?</b>	<b>7</b>
<b>Proteção contra invasões de hosts e redes, O Phishing - evolução</b>	<b>7</b>
<b>Conclusão</b>	<b>8</b>

## Introdução

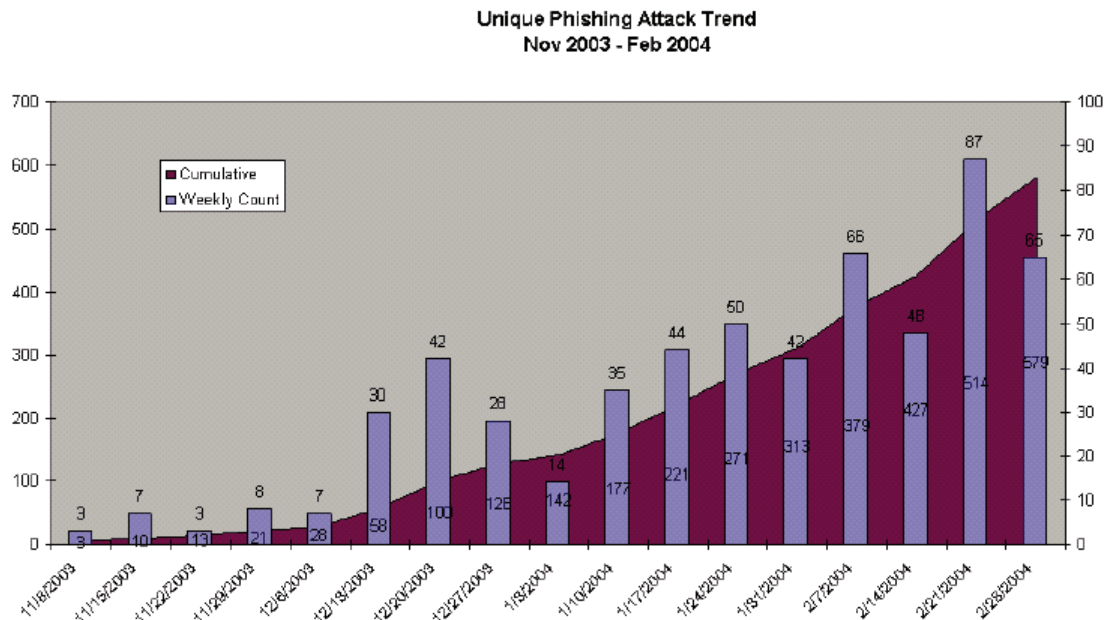
### Entendendo o Phishing e o Pharming

Para proteger corretamente os seus principais recursos de negócios contra os ataques de “Phishing” de hoje, primeiramente você precisa entender a história dessa ameaça, os tipos de técnicas de Phishing usados no submundo da segurança atual e as maneiras pelas quais a McAfee pode ajudar você a detectar e se defender contra esses ataques. Além disso, é preciso saber qual é a mais nova tendência em ataques à segurança, conhecida como “Pharming”, a atual evolução do “Phishing”, em que ela é diferente, o que pode ser feito para se defender contra ela e quais são as melhores técnicas de resolução para ambos os tipos de ataques.

Com informações sobre as ameaças de Phishing e Pharming (veja as definições), este documento ajuda a identificar o que é um ataque de Phishing, como ele se apresenta em uma rede e como ele pode ser atenuado. Além disso, mostramos com o que se parecem os ataques de Pharming, de acordo com diferentes situações de ataque, e como atenuar os efeitos sobre os seus recursos de negócios. Também descreveremos em linhas gerais como esses dois tipos de ataques se transformaram na sofisticada “dupla fatal” dos dias atuais voltada para empresas, usuários domésticos e órgãos públicos.

## O que são Phishing e Pharming?

Os ataques de Phishing utilizam engenharia social e subterfúgios técnicos para roubar dados pessoais e credenciais de contas bancárias dos usuários. Os esquemas de engenharia social utilizam e-mails falsificados para levar os usuários a sites falsos criados para induzir os destinatários a divulgar dados financeiros, como números de cartão de crédito, nomes de usuários de contas, senhas e números de documentos. Apropriando-se indevidamente de marcas de bancos, lojas virtuais e administradoras de cartões de crédito, os Phishers conseguem convencer os destinatários a responder. Os esquemas de subterfúgio técnico plantam programas criminosos nos PCs para roubar credenciais diretamente, muitas vezes utilizando cavalos de Tróia, programas de captura de digitação e spywares. Os programas criminosos de Pharming levam os usuários a sites ou servidores de proxy fraudulentos, normalmente por meio de seqüestro ou envenenamento de DNS.



**Figura 1 - Tendência de ataques exclusivos de Phishing em 2003-2004**

### Primeiras tentativas

Os primeiros ataques de roubo de informações (cartão de crédito, entre outros) eram menos sofisticados. O e-mail continha um link para um site que parecia legítimo (naturalmente não era). Muito freqüentemente, o endereço do site não era um domínio, mas simplesmente um endereço IP como 162.122.19.2 e os e-mails, muitas vezes, eram muito mal escritos, com erros de gramática e ortografia

e a pouca atenção aos detalhes denunciavam o que eles realmente eram: um golpe barato.

Os novos ataques de Phishing evoluíram rapidamente. E-mails mais sofisticados, mais bem escritos, com melhor ortografia e mais convincentes, dificultando o reconhecimento. Rapidamente, os Phishers ficaram mais eficientes, muitas vezes utilizando o HTML com imagens e gráficos dos verdadeiros bancos ou instituições financeiras; os links representados nesses e-mails levavam a sites

que realmente pareciam os sites das instituições representadas, levando a vítima a crer que o remetente era a verdadeira instituição.

Isso é muito simples de ser feito, pois o HTML em que o link aparece pode ter qualquer nome ou descrição, e o verdadeiro destino pode ficar oculto.

## Ataques sistemáticos

Desse modo, perto do final de 2003, o Phishing assumiu um aspecto mais sinistro: os dados bancários e as informações de cartão de crédito das pessoas começaram a ser roubadas, sendo posteriormente usadas para obter dinheiro ou adquirir mercadorias.

No ano passado, o número de ataques de phishing aumentou em uma velocidade alarmante, como mostra a Fig. 2.

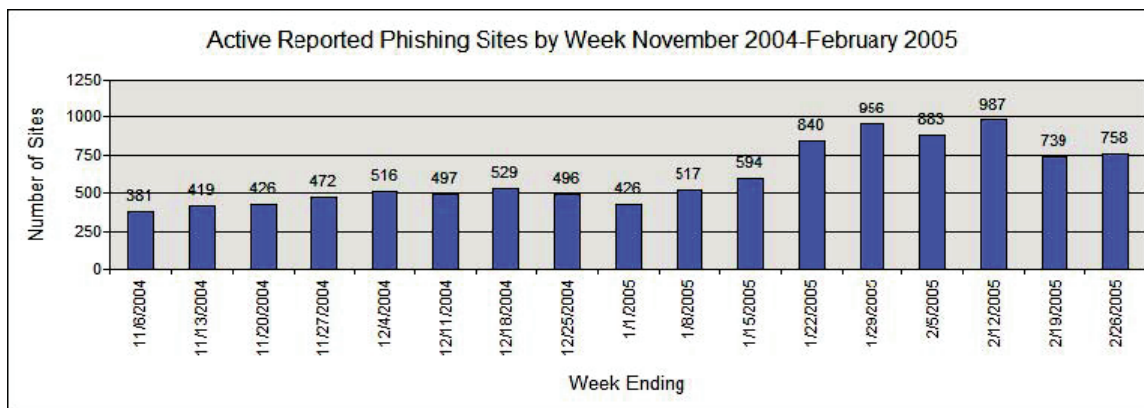


Figura 2 – Número de sites de phishing ativos denunciados de novembro de 2004 a fevereiro de 2005 (dados do Grupo de Trabalho Anti-Phishing)

## Ficando mais atentos

Para o olho treinado, ainda era relativamente fácil identificar os sites de phishing. Os usuários foram instruídos a verificar se o site que estavam visitando continha a URL correta e o cadeado amarelo garantindo a segurança do site.

Os Phishers estavam, novamente, um passo à frente. Uma falha na tecnologia do Internet Explorer da Microsoft permitia que scripts ocultassem a barra de URL, ocultando o endereço do site com o verdadeiro endereço do banco. A mesma técnica permitia que

A isca desses ataques de phishing é, normalmente, enviada por e-mail. Uma mensagem de e-mail contendo um link para um site é enviada para um grande número de pessoas. Normalmente, o e-mail solicita que o usuário atualize suas informações, com o pretexto de 'reforçar os sistemas de segurança' ou de um possível vazamento de informações. Uma ampla variedade de técnicas de engenharia social é utilizada.

Quando o usuário clica no link, ele é enviado a uma página que se parece muito com a da verdadeira instituição, mas, na verdade, é uma falsificação. Quando o usuário insere suas informações pessoais, elas são armazenadas, permitindo que o hacker as acesse posteriormente.

eles exibissem um cadeado falso na barra de status.

Com o consumidor cada vez mais atento, mais uma vez, os Phishers reagiram. Em vez de enviar e-mails para persuadir os consumidores a visitarem sites, cavalos de Tróia de captura de digitação começaram a ser distribuídos. Assim que o usuário entra no site do seu banco, todas as teclas digitadas são armazenadas e transmitidas, fornecendo ao hacker o número da conta, as senhas e outros dados importantes.

Os bancos e as instituições financeiras tentaram reagir à ameaça solicitando apenas senhas parciais, mas ainda assim, com o tempo, os insistentes Phishers poderão obter a senha completa.

A batalha continua: os bancos introduzindo listas suspensas para seleção de senhas e teclados virtuais, e

## O impacto financeiro

As estimativas de quanto dinheiro é perdido devido aos ataques de phishing variam muito. A associação australiana de bancos registrou prejuízos de A\$ 10 milhões devido a fraudes pela Internet no ano passado. Estima-se que o custo do phishing para os bancos e emissores de cartões de crédito dos EUA tenha atingido US\$ 1,2 bilhão em indenizações em 2003 (InternetNews.com) e a Association of Payment Clearing Services (Associação de Serviços de Compensação de Pagamentos) do Reino Unido relatou que os prejuízos diretos causados por golpes de phishing custaram £12 milhões em 2004.

Independentemente do número real, os Phishers ganham muito dinheiro e acredita-se que eles pertençam a grupos de crime organizado e, até mesmo, terroristas. As complexas redes de contas bancárias e "laranjas" (pessoas recrutadas para processar o dinheiro em valores menores, muitas vezes sem saber) dificultam cada vez mais o seu rastreamento pelas autoridades.

Mais recentemente, os ataques de Phishing foram responsáveis pelo comprometimento de dezenas de milhares de registros bancários e de cartões de crédito de consumidores de empresas que são pagas para fornecer essas informações a entidades legítimas. Os ataques de Phishing realizados pelo crime organizado aumentaram de 6.597 em outubro de 2004 para 14.411 em abril de 2005, um aumento de aproximadamente 45% nos últimos 7 meses.

## Pharming – nasce uma nova ameaça

Uma nova tendência na batalha pela fraude de identidades na Internet é uma técnica chamada 'Pharming'. Há dois tipos de técnica: o primeiro envolve o uso de um vírus ou um cavalo de Tróia para modificar o arquivo de 'Hosts' do usuário. Esse arquivo é um remanescente dos primórdios da Internet, sendo usado para relacionar um endereço da Web (URL) ao endereço específico de uma máquina (endereço IP). Trata-se de um arquivo de texto simples. A técnica de Pharming modifica esse arquivo, incluindo nele o endereço na Web de bancos e instituições financeiras conhecidos com o

os Phishers respondendo com programas de captura de mouse e de tela para obter as informações. Técnicas cada vez mais sofisticadas estão sendo empregadas tanto pelos Phishers quanto pelas empresas, pois há muita coisa em jogo.

endereço IP do site de phishing. Assim, quando o usuário abre o navegador e digita o endereço do seu banco, ele é enviado ao site de phishing. Ele não precisa clicar em links de e-mails ou realizar qualquer outra ação.

A segunda técnica é igualmente sinistra e, novamente, depende de uma função obsoleta, desta vez implementada no DNS. O DNS substitui o arquivo local de hosts, como o mecanismo de conversão de endereços da Web em endereços IP específicos. Quando o usuário digita um endereço, ele é consultado no servidor DNS. Se o servidor não reconhecer o endereço IP, ele consultará o endereço em outros servidores DNS e, então obterá o resultado. O problema é que uma parte do protocolo permite a transmissão de outras informações também. Assim, o Phisher envia um e-mail contendo um link para um site. Quando a consulta desse endereço no DNS for realizada, essa informação extra será incluída na URL do banco, mas será dirigida para um site de phishing. Este exemplo descreve melhor o ataque:

1. O Phisher envia um spam para 'www.phishsite.com'
2. Uma consulta sobre 'www.phishsite.com' é feita no DNS
3. O servidor DNS 'www.phishsite.com' também envia dados para 'www.thebank.com', que fica armazenado no DNS.
4. Quando uma pessoa, utilizando o mesmo provedor de Internet, tenta visitar 'www.thebank.com', ela é redirecionada para o site de phishing.

Esse tipo de ataque pode ser facilmente evitado pela configuração do servidor DNS para que ele não aceite esses registros extras. Porém, as vulnerabilidades são grandes, pois esse é um ataque relativamente novo e exclusivo, e a maioria dos gerentes de TI não o conhece.

## Redução do Phishing e Pharming com a McAfee

### Filtragem anti-spam – proteção contra Phishing

A família de produtos McAfee SpamKiller possui regras e filtros específicos para detectar ataques de phishing. Utilizando várias técnicas heurísticas para identificar as características comuns de e-mails de phishing, os ataques podem ser detectados e bloqueados, mesmo que um ataque específico não tenha sido tentado antes (“ataque imediato”). Testes Independentes realizados em dados enviados ao APWG (Anti-Phishing Working Group, Grupo de Trabalho Anti-Phishing) e dados coletados pelas capturas de spam da McAfee demonstram taxas de detecção sempre acima de 97% para e-mails de phishing conhecidos e desconhecidos.

O McAfee SpamKiller pode ser instalado de várias maneiras, dependendo das suas necessidades e aplicações específicas. É uma solução física que pode ser instalada diretamente nos seus servidores de e-mail (Microsoft Exchange ou Lotus Domino), no seu firewall (Microsoft ISA Server) e, finalmente, como um serviço gerenciado hospedado pela McAfee (para os clientes que desejam uma solução de serviços terceirizados).

### Tecnologia de varredura de vírus da McAfee

O engine de varredura antivírus de todos os produtos para e-mail da McAfee também detecta os alvos mais comuns de phishing, identificando características específicas e classificando-as como Phish- bankfraud.eml.

Além disso, muitos sites de phishing utilizam vulnerabilidades conhecidas do Internet Explorer (como descrito acima) para tentar ocultar a verdadeira localização e, muitas vezes, utilizam cavalos de Tróia, backdoors e programas de captura de digitação. A McAfee já possui amplos bloqueios implementados contra esses tipos de ataques.

### E quanto à proteção de desktops?

O McAfee VirusScan Enterprise 8.0i, com a sua tecnologia integrada de proteção contra invasões e de firewall, é um mecanismo eficiente de proteção contra as ameaças de Phishing em constante mudança. Com a simples inclusão de uma regra, as tentativas de roubo do arquivo de host local dos usuários podem ser evitadas. A tecnologia de firewall impede que cavalos de Tróia ou backdoors enviem os dados coletados para o Phisher, além de evitar que a máquina seja recrutada para uma ‘bot-net’ para distribuir e-mails de spam. Tudo isso, além da detecção de altíssima qualidade do engine de varredura antivírus e da organização de pesquisas AVERT da McAfee.

### Proteção contra invasões de host e rede

Muitas vezes, o alvo dos Phishers são máquinas mal protegidas, seja para hospedar o seu site de Phishing, comprometendo o servidor de Web legítimo, ou para distribuir e-mails de Phishing posteriormente, coletando os dados para a exploração.

As soluções Intercept, Desktop Firewall e IntruShield da McAfee ajudam a impedir que os recursos das empresas sejam utilizados inadvertidamente para fins ilegais voltados para fora da sua infra-estrutura, bem como ajudam a proteger os seus usuários e clientes contra ataques de Phishing.

### O Phishing – evolução

‘Phishing’ é a prática de tentar obter informações confidenciais, como números de cartões de crédito, informações bancárias, informações de contas, etc., de usuários inocentes, tendo sido criada como um meio de obter credenciais de login da AOL. O hacker simplesmente enviava um e-mail fingindo ser da AOL pedindo o nome de login e a senha de um usuário, normalmente sob o pretexto de alguma falha na segurança. Usuários inocentes enviavam os dados solicitados, fornecendo ao Phisher as informações pessoais necessárias de que ele precisava para ter acesso a informações confidenciais da sua conta.

## Conclusão

O Phishing e o Pharming, com os roubos de identidade associados a eles, continuam crescendo a uma velocidade alarmante, causando grandes danos à economia mundial e à situação financeira de indivíduos. Como esses golpes são de difícil detecção, e como as organizações criminosas estão ganhando muito dinheiro com dessas atividades, a complexidade e a frequência dos ataques continuarão crescendo, pois há muito mais dinheiro a ganhar.

A comprovada proteção de sistemas da McAfee ajuda a evitar o seqüestro dos computadores pelos Phishers, impede que eles enviem spam, bloqueia o recebimento de spam, detecta cavalos de Tróia e programas de captura de digitação, protege contra técnicas de Pharming e bloqueia os sites de phishing. A ampla variedade de produtos de segurança comprovada e proativa da McAfee oferece vários níveis de proteção contra essa crescente ameaça.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766

A McAfee e/ou outras marcas mencionadas neste documento são marcas comerciais, registradas ou não, da McAfee, Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. A cor vermelha usada em relação à segurança é marca distintiva dos produtos que levam a marca McAfee. Todas as outras marcas comerciais, registradas ou não, mencionadas neste documento pertencem exclusivamente aos seus respectivos titulares. © 2005 McAfee, Inc. Todos os direitos reservados.

Phishing & Pharming WP V.002– (Arquivo: Phishing Pharming WP 08-17-05.pdf)