

Marcelo Coradassi Eiras

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

“Engenharia Social e Estelionato Eletrônico”



[IBPI – ASIS D] / fevereiro de 2004

Marcelo Coradassi Eiras

“Engenharia Social e Estelionato Eletrônico”

*Trabalho de monografia do cursos de Graduação “Lato Sensu”
em Segurança de Informações na Internet.*

[IBPI] / fevereiro de 2004

ENGENHARIA SOCIAL.....	6
GLOSSÁRIO.....	7
CAVALO DE TROIA (Trojan Horse).....	7
CRACKERS.....	7
DoS ou DDoS.....	7
HACKERS	8
KEYLOGGER ou KEYKATCHER	8
Lamers (Lammers)	9
MAILBOMB.....	9
PASSWORD CRACKER	9
PHREAKING.....	10
SCANNERS DE PORTA	10
SCANNERS DE PORTA	10
SCAM.....	10
SCRIPTKIDDIE.....	10
SPAM.....	11
SPYWARE (Programa Espião).....	11
BACKDOOR (Porta dos fundos).....	11
ESTUDOS DE CASO	12
Caso Banco do Brasil 1.....	12
Caso Banco do Brasil 2.....	13
Caso Terra	14
Cartão Virtual “Genérico”.....	16
CASO CARTÃO BOL.....	17
CASO NET pay-per-view	18
CASO PROVEDOR DE INTERNET (Simplesmente pedindo)	18
O MAIOR ENGENHEIRO SOCIAL DE TODOS OS TEMPOS.....	19
Entrevista de Kevin Mitnick a Revista Época em 15.09.03 Autoria de LUCIANA VICÁRIA	19
ENGENHARIA SOCIAL E CRACKERISMO À LUZ DO DIREITO.....	26
Leis aplicáveis.....	26
Engenharia Social.....	26
Personificação ou Masquerade.....	26
Ataques Internos.....	27
O Problema da prova Informática no Direito Brasileiro.....	27
Conclusão: prevenção e treinamento	29
Glossário.....	32
Link para os programas citados	37
Link para os programas citados	37
FILMES RELACIONADOS	38
LINK DE PESQUISA E APOIO	39
BIBLIOGRAFIA:	40

Resumo

O presente trabalho procurará servir de introdução a uma das mais terríveis formas de invasão de sistema e de descoberta de dados sigilosos e fraudes. A Engenharia Social explora o elo mais fraco do sistema de segurança de informação, as pessoas.

Introdução

Este trabalho mostra que por mais poderosos e bem configurados firewalls, IDSs, passaportes biométricos e toda gama de tecnologias, tudo se mostra ineficaz a um ataque de engenharia social bem feito. Serão mostradas outras formas de engenharia social como o SPAM, SCAM, métodos persuasivos de todo tipo.

Por mais extraordinário que possa parecer, o método mais simples, mais usado e, infelizmente o mais eficiente de se descobrir uma senha é... adivinha? Perguntando!!! É sério... Basta alguém de boa lábia perguntar a um funcionário despreparado que ele solta a língua. Pode até não ser a senha, mas ele vai contar o tipo de sistema, o tipo de computador, e o que mais ele vir pela frente. Tudo vai depender de quão bom é o "Engenheiro Social" e quantos conhecimentos sobre a empresa ele possui.

Engenharia Social

Engenharia Social é o termo utilizado para a obtenção de informações importantes de uma organização, através de seus funcionários e colaboradores. Essas informações podem ser obtidas por ingenuidade ou confiança. Os ataques dessa natureza podem ser realizados através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e até mesmo pessoalmente.

Já foram identificados casos em que, alguém se passando por um analista de suporte técnico de um provedor de acesso Internet, telefonou para um usuário informando que a conexão estava com algum tipo de problema e que para consertar necessitava da sua senha.

O usuário, na sua ingenuidade, fornece a senha e depois vai verificar no extrato mensal do provedor que utilizou muito mais recursos do que realmente o tinha feito, além da utilização de sua conta, para propagação de spam, scam e de vírus.

Uma técnica bastante utilizada atualmente é a de se passar por grandes bancos ou provedores de Internet chamando os usuários para preencherem formulários on line.

Glossário

CAVALO DE TROIA (Trojan Horse)

Programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. Ele geralmente abre uma porta TCP para futuras invasões.

CRACKERS

Possuem as mesmas habilidades e conhecimentos do hacker, acrescentando alguns detalhes:

- Destroem e/ou roubam dados, podendo inclusive travar um sistema, como um provedor;
- Contribuem com a pirataria, uma vez que desenvolvem programas cracks;
- São desenvolvedores de vírus e trojan horses;

Em geral, um cracker também prefere atacar sistemas mais seguros a um simples usuário da internet, logo a chance de um internauta comum ter o computador invadido por um cracker também é muito pequena.

Por serem desenvolvedores de trojan horses, os crackers são os grandes responsáveis pelo surgimento de um outro tipo de internauta: O Lamer.

DoS ou DDoS

Ataque que consiste em sobrecarregar um servidor com quantidades excessivas de solicitações de serviço. Há muitas variantes, como os ataques distribuídos de negação de serviço (DDoS), que paralisam sites. O DDoS se utiliza geralmente de computadores zombies que foram infectados com um software zombie como o Tribal Flood Network ou o Trinoo, recebem a ordem de iniciar o ataque quando todos os micros simultaneamente bombardeiam o servidor tirando do ar.

HACKERS

Pessoas que se dedicam a explorar profundamente o potencial mais alto de sistemas computacionais. Por outro lado, a representação e imagem dos hackers passadas pela mídia atualmente (notícias e filmes) é em sua maior parte negativa (crackers). As principais características dos hackers são:

- Extremamente inteligente;
- Conhecedor profundo de Sistemas Operacionais, sistemas de rede e linguagens de programação;
- Jamais se identificam, entretanto podem se organizar em clãs;
- Desenvolvem suas próprias ferramentas de invasão;
- Em geral, quando invadem um sistema, não danificam e não roubam os dados;
- São muito raros, se comparados ao número de internautas existentes;
- Não suportam Lamers.

KEYLOGGER ou KEYKATCHER

Programa que captura dados digitados no teclado podendo retransmiti-lo para outro endereço. Existe também o keylogger físico que é conectado entre a porta ps/2 e o teclado.



Keylogger físico, também chamado de Key Katcher. Nele um microcontrolador interpreta os dados digitados e os armazena em memória não volátil. Custa cerca de US\$ 100

Lamers (Lammers)

São similares aos script kiddies, neste momento é possível que as portas de comunicação do seu computador estejam sendo rastreadas por um lamer, sem que você possa perceber. Aqui estão as principais características do lamer:

- Não passa de um usuário comum, na maioria das vezes sem conhecimentos de linguagem de programação. Em geral manipula bem o Windows;
- Gostam de aparecer, quase sempre se identificando como hacker
- Comuns em salas de chat, IRC e ICQ, gostam de fazer ameaças tipo "Sou um hacker e vou detonar o seu computador";
- Seus mecanismos de ataque são os Programas Clientes dos famosos trojans, os rastreadores de endereço IP e os escaneadores de portas. Os lamers, por não possuírem conhecimentos profundos, utilizam programas prontos, tipo "receita de bolo, confeccionados por crackers ou mesmo hackers";
- Quando atacam, são facilmente identificáveis através do endereço IP, desde que se estejam utilizando mecanismos de proteção adequados.

MAILBOMB

Técnica que usa um programa SMTP que manda um quantidade gigantesca de email para um determinado endereço com o objetivo de atormentar determinado usuário ou derrubar o servidor de correio eletrônico.

PASSWORD CRACKER

Programa usado para descobrir uma senha de um sistema ou programa protegido por senha. O método mais comum consiste em testar sucessivamente as palavras de um dicionário para encontrar a senha

PHREAKING

É o uso indevido de linhas telefônicas ou celulares para fins ilícitos como fazer chamadas sem identificação, não pagar a ligação entre outros. No passado os phreakers empregavam gravadores de fita cassete e outros dispositivos para produzir sinais de controle e enganar o sistema de telefonia. Conforme as companhias telefônicas foram reforçando sua segurança, as técnicas se tornaram mais complexas, que poucos dominam.

SCANNERS DE PORTA

São programas que buscam portas TCP ou UDP abertas por onde podem ser feitas invasões. Um dos scanners mais conhecidos é o NMAP

SCANNERS DE PORTA

São programas que buscam vulnerabilidades, portas abertas, bugs conhecidos para fazer um levantamento de vulnerabilidade de um sistema a ataques. Podem ser usado tanto para auditorias de seguranças como para planejamentos de ataques. Exemplos conhecidos são o Languard Netork Security Scanner e o Nessus.

SCAM:

É similar ao spam, mas tem como objetivo passar se por outra pessoa ou instituição a fim de levar o incauto internauta a preencher fichas e acabar liberando dados confidenciais, como senhas de bancos e cartão de credito.

SCRIPTKIDDIE

Pessoa com poucos conhecimentos técnicos que lança mão de scipties prontos ou ferramentas específicos para tentar invadir sistemas sem possuir conhecimentos técnicos para tal. Em suma, não sabem exatamente o que estão fazendo mas, algumas vezes conseguem sucesso.

SPAM

E-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês Unsolicited Commercial Email).

Os golpes são bem elaborados, porém basta um pouco de atenção para verificar uma série de incoerências. Em geral, as mensagens são similares às originais enviadas pelas empresas, e muitas delas têm links para sites que também são cópias dos verdadeiros. Mas, nos dois casos, é possível ver imagens quebradas, textos fora de formatação e erros de português - algo difícil de ocorrer com empresas que investem tanto em marketing para atrair clientes.

Outras mensagens pedem apenas que o usuário baixe um arquivo que na verdade, é um programa que envia os dados pessoais e financeiros por meio da Internet (spyware).

SPYWARE (Programa Espião)

É um programa que garimpa informações na máquina do usuário por meio de sua própria conexão a Internet. Posteriormente este programa envia essas informações em segundo plano de forma transparente para os usuários

BACKDOOR (Porta dos fundos)

Como o nome sugere são programas que criam uma “porta dos fundos”. Abre uma porta TCP ou UDP em determinado sistema para futuras invasões. Pode também ser uma forma não-documentada de acesso a um sistema, deixada por programadores.

Estudos de Caso

Caso Banco do Brasil 1

O truque é feito colocando-se, após o endereço do Banco do Brasil, o símbolo arroba, o que faz o navegador ignorar tudo o que consta antes disso no endereço (o site do BB) e chamar apenas a parte do endereço após essa arroba - uma sucessão de números que na verdade é o endereço IP.

<http://www.bb.com.br/appbb/portal/index.jsp@200.167.52.180/formulario.asp>

The screenshot shows the Banco do Brasil website interface. At the top, there is a yellow header with the BB logo and the text "BANCO DO BRASIL". Below this is a navigation bar with links for "você", "sua empresa ...", "governo ...", and "acesse sua conta". A secondary navigation bar lists various services: "Serviços", "Investimentos", "Empréstimos", "Cartões", "Seguros", "Previdência", and "Capitalização".

On the left side, there is a section titled "sob medida" with a dropdown menu "Do que você precisa?" and a "Momentos da vida" section with a dropdown menu "Para quem é cliente BB". Below this is a button "abra sua conta".

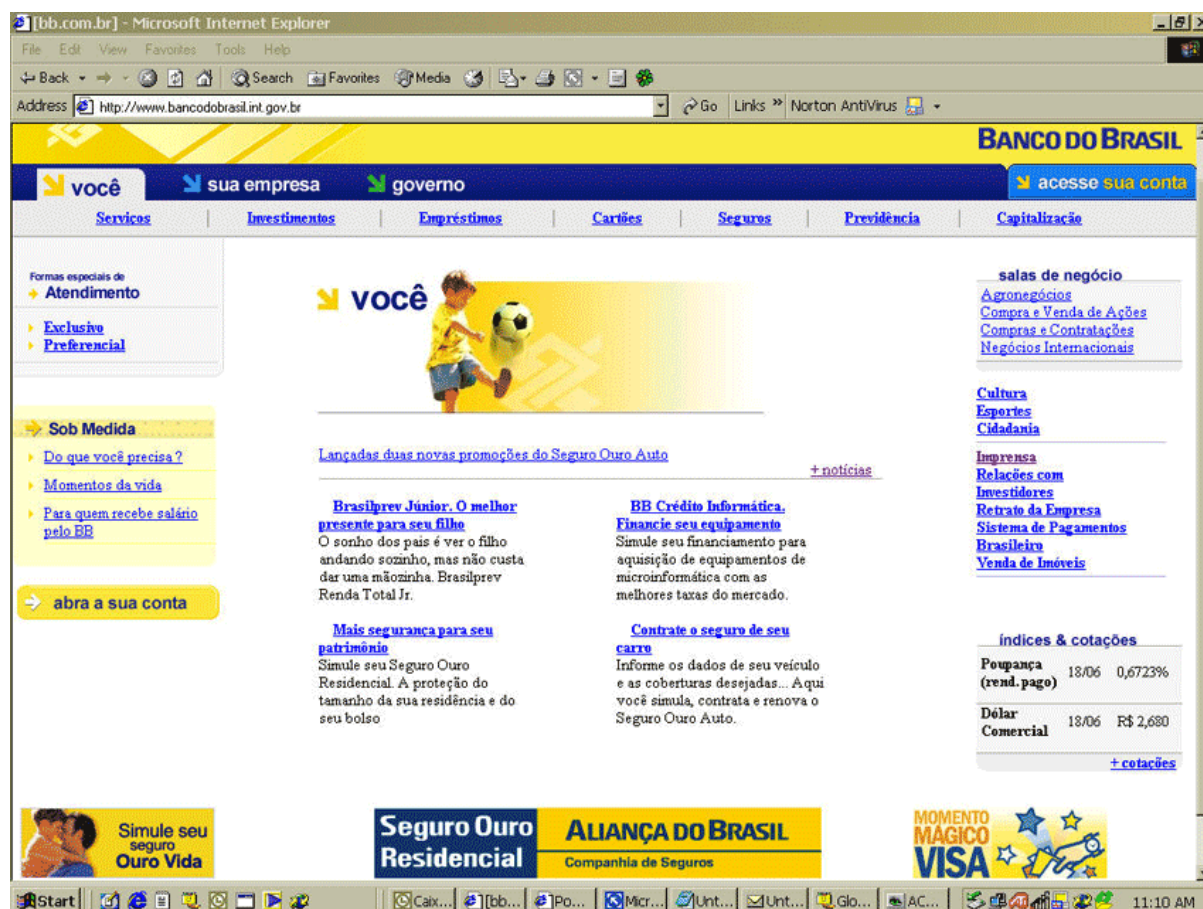
The main content area features a "você" section with a "Débito Automático" advertisement. Below the advertisement, there is a text box stating: "Participe do sorteio de prêmios de até R\$ 500.000,00. Para participar basta ser cliente do Banco do Brasil e preencher o formulário abaixo." This is followed by a "Titular" dropdown menu set to "1º Titular".

Below the "Titular" dropdown are input fields for "Agência", "Senha", "Conta", and "Letras de Acesso". There are "entrar" and "limpar" buttons at the bottom of the form. A link "Problemas com o campo senha, clique aqui" is provided below the "Senha" field.

On the right side, there is a "Promoções" section with a "Faça agora seu Seguro Ouro Auto e ganhe um brinde." button. Below this is a "Mantenha seus dados atualizados" section with a "verifique aqui" button. At the bottom right, there is a "Saiba o que o BB está fazendo pela inclusão social" section with a "FOME ZERO" logo.

The footer contains a yellow bar with links: "soluções de acesso à internet", "acesso e segurança", "política de privacidade", "patrocínios", "relações com investidores", "English", and "mapa do site".

Caso Banco do Brasil 2



O Banco do Brasil e outros bancos têm sido vítimas de vários ataques de SCAM

O que aumenta a credibilidade do e-mail é o fato de a página fraudulenta estar hospedada em um site do próprio governo brasileiro - mais precisamente, do Instituto Nacional de Tecnologia (<http://www.int.gov.br>),- dando a impressão de ser uma página verdadeira. Em contato com a Ombudsman do Instituto, Henriette M. Krutman, as 10h51 de segunda-feira, o relatório descobriu que o INT só voltaria a funcionar na quarta-feira, provavelmente, a razão para que os e-mails fossem distribuídos durante o carnaval. De qualquer forma, ela iria entrar em contato com a webmaster do INT, de nome Carolina, para tirar a página do ar, imediatamente.

Leia o conteúdo do e-mail fraudulento:

“Por determinação do Senhor Presidente da República, expressa através do Decreto-Lei 143.002/2002, o Banco do Brasil vem junto aos seus clientes informar que:

- 1) Em toda e qualquer movimentação IGUAL ou MAIOR que R\$ 5.000,00 (Cinco mil reais) deverá o Banco do Brasil notificar a Receita Federal.*
- 2) O Banco do Brasil verificará a veracidade de CADA endereço fornecido por seus clientes, a fim de verificar a autenticidade dos mesmos.*
- 3) Visando também a segurança de seus clientes, o Banco do Brasil informa que, contando 48h (Quarenta e oito horas) a partir do recebimento deste, seus clientes devem confirmar seus dados.*
- 4) Isso poderá ser feito imediatamente acessando sua conta através do endereço: <http://www.bancodobrasil.int.gov.br>*
- 5) Visando ainda aumentar a sua segurança, o novo endereço do Banco do Brasil é <http://www.bancodobrasil.int.gov.br> subordinado a sistemas de segurança internacionais e com rígidas contra-medidas anti-fraude.”*

Caso Terra

O Portal Terra está sendo usado como isca para um novo golpe que começou a circular por e-mail. Com o assunto (subject) "Parabéns Você Ganhou 50% de

Desconto na Mensalidade!!!!", a mensagem traz links para baixar um arquivo executável maléfico. Ao receber, você deve ignorar e apagar a mensagem.

O texto do golpe "parabeniza" o usuário por ter assinado o Kit Executivo, composto pelo Disco Virtual e pelo E-mail Protegido. Em seguida, sugere ao usuário clicar em dois links para ter acesso aos serviços. Os golpistas utilizaram como modelo a mensagem original, enviada aos usuários que assinaram os serviços. No código do e-mail, eles substituíram os endereços reais (www.terra.com.br/discovirtual e www.emailprotegido.terra.com.br) por outro falso. Os usuários não conseguem perceber isso já que a mensagem está no formato HTML.

Os links, na verdade, estão direcionados para o download de um arquivo executável que, provavelmente, permite aos fraudadores roubar informações como senhas ou ter acesso ao micro do usuário - Terra está analisando a função do arquivo. Tanto o E-mail Protegido como o Disco Virtual funcionam totalmente online, ou seja, não é necessário baixar nenhum arquivo.

Fraudes como esta já usaram como isca empresas, bancos e programas de TV conhecidos pelo público, entre os quais Banco do Brasil, Banco Itaú, Editora Abril, Big Brother Brasil e Show do Milhão. Para saber mais sobre os golpes em circulação na Web, clique aqui.

Veja, em tamanho reduzido, uma reprodução da mensagem fraudulenta:

Parabéns por ter escolhido o Kit Executivo !


Você Ganhou 50% de Desconto na sua mensalidade!!! Basta fazer download dos serviços abaixo. Com ele, você passa a contar com:

- **E-mail Protegido Terra**
O serviço protege você de mensagens com vírus ou que invadem seu e-mail sem sua autorização, conhecidas como SPAM. Tudo isso com a alta tecnologia HotMail.
- **50 Mb extra de Disco Virtual**
Seu novo arquivo pessoal. Guarda com segurança documentos, apresentações e tudo que você quiser, acessando de qualquer computador conectado à Internet. Conheça e use o seu Disco Virtual clicando em www.terra.com.br/discovirtual.

IMPORTANTE - Acesse o endereço www.emailprotegido.terra.com.br, siga as instruções do Passo-a-passo e aprenda a configurar o seu E-mail Protegido.

Ao escolher o Kit Executivo, você ganhou 30 dias GRÁTIS destes serviços. Após esse período, para sua conveniência e segurança o serviço continuará ativo por apenas R\$ 4,90 mensais, acrescidos à sua mensalidade Terra.

Kits de Serviços Terra. Mais mobilidade e segurança na Internet.
Terra Networks Brasil SA



Cartão Virtual “Genérico”

Cartão Virtual

Você acaba de receber um cartão virtual de "Segredinho".

Para visualizar seu cartão virtual faça o download do visualizador personalizado.

Assim que você baixar o visualizador digite o código do seu cartão virtual, e clique sobre o botão "Visualizar Meu Cartão Virtual".

De: Segredinho
Assunto: Amo Você
Código do Cartão: C62748926

Obs: Clique sobre o link abaixo e clique em SALVAR para baixar o visualizador personalizado.

Depois é só executar o arquivo "**visualizador.exe**", digitar o código do cartão e pronto

[DOWNLOAD DO VISUALIZADOR](#)

FreeCard's Gyn - Envie ja um cartão pra quem você ama.

No caso acima a pessoa recebe um cartão virtual que indica o usuário baixar um programa que na verdade é um cartão com um trojan. Neste caso geralmente são utilizados programas que agregam programas em outros como o conhecido SENNASPY.

CASO CARTÃO BOL

Seu amor lhe enviou um cartão do BOL.

Para vê-lo, clique no endereço abaixo:

<http://cts.bol.com.br/recebeu.html?id=1002C549CD02E9DECDCE00CC027091C502DE1DCD02B5B0CC028626C5021326C40136C6>

Este cartão ficará disponível por 15 dias.

Esta é uma mensagem automática. Por favor, não responda a este e-mail.

Para enviar um cartão do BOL para alguém, clique no endereço abaixo:

<http://cartoes.bol.com.br>

Quer ter seu próprio endereço na Internet?

Garanta já o seu e ainda ganhe cinco e-mails personalizados.

DomíniosBOL - <http://dominios.bol.com.br>

Acabe com aquelas janelinhas que pulam na sua tela.

AntiPop-up UOL - É grátis!

<http://antipopup.uol.com.br>

No email acima é enviada uma mensagem idêntica a de uma mensagem real do serviço de cartões do bol, a “trapaça” esta no link que redireciona para outro endereço, no caso para um endereço eletrônico onde existe um cartão em formato flash executável e que esta incluso um trojan.

CASO NET pay-per-view

André tinha 15 anos mas, estava querendo assinar o canal “Sexy Hot”. Ligou para a operadora NET local e pediu a inclusão do canal. André se fez passar por seu pai, Carlos apenas informando o CPF, identidade, data de nascimento e nome completo do mesmo. Isso mostra que o sistema de identificação de assinante da NET é bastante falho pois os dados pedidos são de fácil obtenção.

CASO PROVEDOR DE INTERNET (Simplesmente pedindo)

Mario liga para a vítima e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigi-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome.

O maior engenheiro social de todos os tempos.

Entrevista de Kevin Mitnick a Revista Época em 15.09.03
Autoria de LUCIANA VICÁRIA

KEVIN MITNICK, Hacker regenerado

KEVIN MITNICK

■ Dados pessoais

Nasceu em 6 de agosto de 1963, em Van Nuys, Califórnia. Solteiro, não chegou a terminar o ensino médio

■ Trajetória

Preso pelo FBI em 1995, ficou cinco anos no Instituto Corretivo Federal de Lompoc, na Califórnia. Escreveu *A Arte de Enganar* (2001) e abriu uma consultoria chamada Defensive Thinking

Divulgação



O mais famoso pirata digital saiu da prisão e agora ensina às empresas como se defender dos invasores cibernéticos

Cultuado na internet como o maior hacker de todos os tempos, o americano Kevin Mitnick, de 40 anos, tornou-se celebridade aos 17 ao invadir o sistema do Comando de Defesa Aérea dos Estados Unidos. Antes de completar 18 anos já estampava páginas de jornais e revistas com uma habilidade incomum e inédita para a época: destrinchar complexos programas de computador. A brincadeira tomou proporções perigosas quando desafiou gigantes da tecnologia como Motorola, Nokia, Novell e Sun Microsystem. Em 1993 ele foi caçado pela polícia e, dois anos depois, preso pelo FBI, acusado de causar prejuízos superiores a US\$ 80 milhões. Condenado, amargou cinco anos na prisão e ficou mais três em liberdade condicional, proibido de chegar perto de computadores. Nem assim perdeu a fama de fora-da-lei mais admirado da rede mundial. Pela primeira vez no Brasil, Mitnick será a estrela da IT Conference, encontro que reunirá mais de 800 profissionais de tecnologia entre os dias 17 e 19, em Salvador. Em entrevista exclusiva a *ÉPOCA*, ele descreve o prazer de voltar à web e explica como atuam os hackers do novo milênio.

ÉPOCA - *Você ainda sente vontade de invadir sistemas?*

Kevin Mitnick - Não. Estou mais velho e mais sábio, superei essa fase. Meu trabalho é até parecido com o que eu fazia, mas jogo no time adversário. Ajudo empresas, universidades e órgãos de governo a proteger seus sistemas. Se eu pudesse, voltaria atrás e daria outro curso a minha vida. Sempre quis ser reconhecido por minhas habilidades, mas não do jeito que aconteceu.

ÉPOCA - *Como você avalia a segurança na rede hoje em dia?*

Mitnick - A falta de segurança é um problema sério e, infelizmente, muitas universidades, empresas e muitos órgãos do governo não se exercitam, não se

atualizam. Eles deixam seus sistemas vulneráveis a ataques e não têm o mínimo de perspicácia para perceber falhas humanas, cada vez mais exploradas por hackers.

ÉPOCA - *Em sua passagem pelo Brasil você vai falar sobre 'engenharia social'. O que é isso?*

Mitnick- É uma técnica usada por hackers para manipular e persuadir os funcionários nas empresas. Em vez de ficar se descabelando para encontrar uma falha no sistema, o hacker pode, por exemplo, largar um disquete no chão do banheiro com o logotipo da empresa e uma etiqueta bem sugestiva: 'Informações Confidenciais. Histórico Salarial 2003'. É bem provável que quem o encontre o insira na máquina por curiosidade. O disquete pode ter sido preparado por um hacker para rodar na máquina da vítima e instalar um tipo de programa chamado Cavalo de Tróia, que dá acesso remoto à rede da empresa.

ÉPOCA - *Você pode citar outro método comum de persuasão?*

Mitnick - O velho e bom amigo telefone. Alguém liga para você dizendo que trabalha no departamento de tecnologia e que está verificando um problema na rede. Faz uma série de perguntas, pede para você digitar alguns comandos e cria um buraco na segurança. Parece tolice, mas 50% das invasões não se valem apenas da tecnologia, mas principalmente da fragilidade humana. A dica para os funcionários é checar a identidade de quem ligou e, para as empresas, adotar políticas de segurança e treinamento intensivo. O mais importante é demonstrar que todo mundo é vulnerável e pode ser manipulado, principalmente os que se julgam mais inteligentes. Eu já fui 'hackeado', achei engraçado na hora, mas depois parei para pensar e vi que tinha algo errado. Em meu livro, *A Arte de Enganar*, citei alguns exemplos, mas há sempre novas técnicas de persuasão.

'Em vez de ficar se descabelando para encontrar uma falha no sistema, o hacker pode largar no banheiro um disquete infectado, com o logotipo da empresa e uma etiqueta bem sugestiva: 'Informações Confidenciais. Histórico Salarial 2003'. É provável que alguém o encontre e insira na máquina'

ÉPOCA - *Como foi ficar sete anos sem acessar a internet?*

Mitnick - Foi terrível. Eu me senti excluído da sociedade e à margem de tudo o que acontecia no mundo. Eu vivi o nascimento da internet e vibrei com ele, e, de repente, aparece uma grande lacuna em minha vida. Em 1995, eu nem imaginava que em tão pouco tempo teríamos internet de alta velocidade. Ainda estou me readaptando aos avanços e tenho aproveitado bastante as novidades que se aplicam a meu trabalho. Mas não sou o mesmo expert de antes. Há uma infinidade de informações que ainda não pude utilizar.

ÉPOCA - *Como foi ser libertado, mas continuar proibido de usar computadores durante seu período de liberdade condicional?*

Mitnick - Não poderia haver castigo pior. Eu ficava sentado atrás de meus colegas tentando captar um pouco daquele mundo mágico que eu ainda não conhecia. E só senti o sabor da liberdade, de fato, quando sentei em frente a um computador e me conectei. Foi extraordinário.

ÉPOCA - *Como era 'hackear' um site em 1995?*

Mitnick - Nunca 'hackeei' um website nos modelos do que temos hoje (www), pois eles não existiam naquela época. A internet era algo muito novo em 1995 e só se tornou comercial depois que fui preso. Meu passatempo preferido era o Fun Freaking, que consistia basicamente em invadir sistemas telefônicos. Na infância,

eu adorava brinquedos que usavam tecnologia e, na adolescência, chegava a passar 16 horas na frente de um computador para descobrir uma senha.

ÉPOCA - *Qual era a sensação de invadir sistemas?*

Mitnick - Era melhor que vencer um jogo de computador ou tirar um 10 na escola. Eu me sentia poderoso, invencível. O mais excitante é que sempre havia algo mais complexo para me desafiar. Já cheguei a viajar para Londres só para invadir o sistema de um pesquisador de segurança. Ele ficava em casa e dificilmente se conectava com uma rede ou linha telefônica. Só seria possível se eu estivesse fisicamente na Inglaterra. Foi o que fiz. Viajei para lá e invadi. O único problema é que os sistemas operacionais são propriedade particular, e isso fez toda a diferença em minha vida (*risos*).

ÉPOCA - *Qual era sua motivação?*

Mitnick - O desafio intelectual, a busca pelo conhecimento e a aventura de estar num lugar onde não deveria estar. Comecei aos 17 anos e só parei quando fui preso. Mas eu não era o hacker temido como pintam por aí, um fora-da-lei que cria e espalha vírus. Eu era simplesmente um jovem curioso que buscava desafios em sistemas de segurança. Eu procurava brechas, e não informações. Jamais invadi um sistema para obter vantagens financeiras e até hoje não vi uma prova legal contra mim.

ÉPOCA - *Mas o roubo de senhas significou perdas milionárias para as empresas.*

Mitnick - Nem sempre. O valor do prejuízo foi bastante exagerado pelo governo federal. Quiseram me pregar a imagem de supercriminoso e colocaram em minhas costas valores bilionários. Veja só que loucura: para eles, o prejuízo que causei era proporcional ao dinheiro gasto com pesquisa e desenvolvimento de projetos, algo totalmente ridículo.

AP



'Eu era simplesmente um jovem curioso em busca de desafios. Sempre que invadia, eu me sentia poderoso, invencível. E o mais excitante é que sempre havia algo mais complexo para me desafiar. Fico feliz em saber que as gerações mais novas me admiram. Mas eu errei, faço questão de dizer isso a elas'

ÉPOCA - *A exposição negativa curiosamente surtiu efeito contrário. Hoje você é cultuado por milhares de jovens na internet.*

Mitnick - Fico feliz em saber que as gerações mais novas me admiram. Mas não encorajo ninguém a invadir computadores como fiz. Primeiro, porque não é algo socialmente aceitável, e segundo, porque vão ter sérios problemas com a Justiça. Eu errei, faço questão de dizer isso a elas.

ÉPOCA - *Você tem um ídolo?*

Mitnick - Na verdade não tenho um ídolo, apenas pessoas que admiro bastante, como Steve Jobs, um dos inventores do computador Apple. Ele é bem-sucedido nos negócios e ainda se preocupa com as pessoas mais pobres, o que valorizo

bastante. Compaixão pelo próximo é algo que não se adquire - ou você tem, ou não tem. No momento estou viajando muito pelo mundo, sem tempo para me dedicar à causa humanitária. Mas pretendo doar parte do que arrecado e investir em educação.

ÉPOCA - *Você está feliz com seu trabalho? Quais são seus planos?*

Mitnick - Estou curtindo. Além das dezenas de conferências pelo mundo, tenho me dedicado a meu segundo livro, que será publicado no ano que vem. Agora minha única preocupação é com a Defensive Thinking, minha empresa de consultoria. Quero torná-la líder no segmento de segurança da informação. Tenho paixão por tecnologia e sei que nunca vou conseguir me ver livre dela. Nem quero fazer isso. A intenção é desenvolver essa arte e criar propostas eficazes para proteger as empresas. Até agora vem dando tudo certo, não tenho do que me queixar. Só falta um pouco de tempo para relaxar.

Engenharia Social e Crackerismo à luz do Direito.

Leis aplicáveis.

Engenharia Social

A Engenharia social pode ser facilmente enquadrada no artigo 171 (estelionato) do Código Penal Brasileiro.

“Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento

Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.”

Personificação ou Masquerade

A masquerade é uma forma de ataque pela Internet na qual uma pessoa ou entidade passa-se por outra. Seria tipificado no nosso Código Penal Brasileiro, em seu artigo 299, que trata do crime de falsidade ideológica.

“Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa, se o documento é público, e reclusão de 1 (um) a 3 (três) anos, e multa, se o documento é particular.

Parágrafo único - *Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte.”*

Ataques Internos

Ocorrem ataques internos quando usuários legítimos comportam-se de modo não autorizado ou não esperado. Talvez o artigo 156 do Código Penal Brasileiro melhor representasse este delito.

“Art. 156 - Subtrair o condômino, co-herdeiro ou sócio, para si ou para outrem, a quem legitimamente a detém, a coisa comum:

Pena - detenção, de 6 (seis) meses a 2 (dois) anos, ou multa.”

O Problema da prova Informática no Direito Brasileiro

O nosso sistema de ordenamento jurídico mostra-se sobremaneira obsoleto para enfrentar criminosos virtuais. Isto porque muitos meios de prova que nos ajudariam a capturá-los, simplesmente não têm validade em nosso Direito. O fato é que crimes estão ocorrendo e criminosos estão sendo identificados, abrindo caminho para uma não-punição sem precedentes, fazendo com que, inclusive, o nosso ordenamento jurídico e soberania sofram com tudo isso. Neste ponto, é importante frisar dois artigos de grande relevância para o direito brasileiro:

Art 5º (CF/88). Todos são iguais perante a Lei, sem distinção de qualquer natureza, garantido-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...) LVI – São inadmissíveis, no processo, as provas obtidas por meios ilícitos;

Art. 323 (CPC) “ *Todos os meios legais, bem como moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa*”

Art. 155 (CPP) - *No juízo penal, somente quanto ao estado das pessoas, serão observadas as restrições à prova estabelecidas na lei civil.*

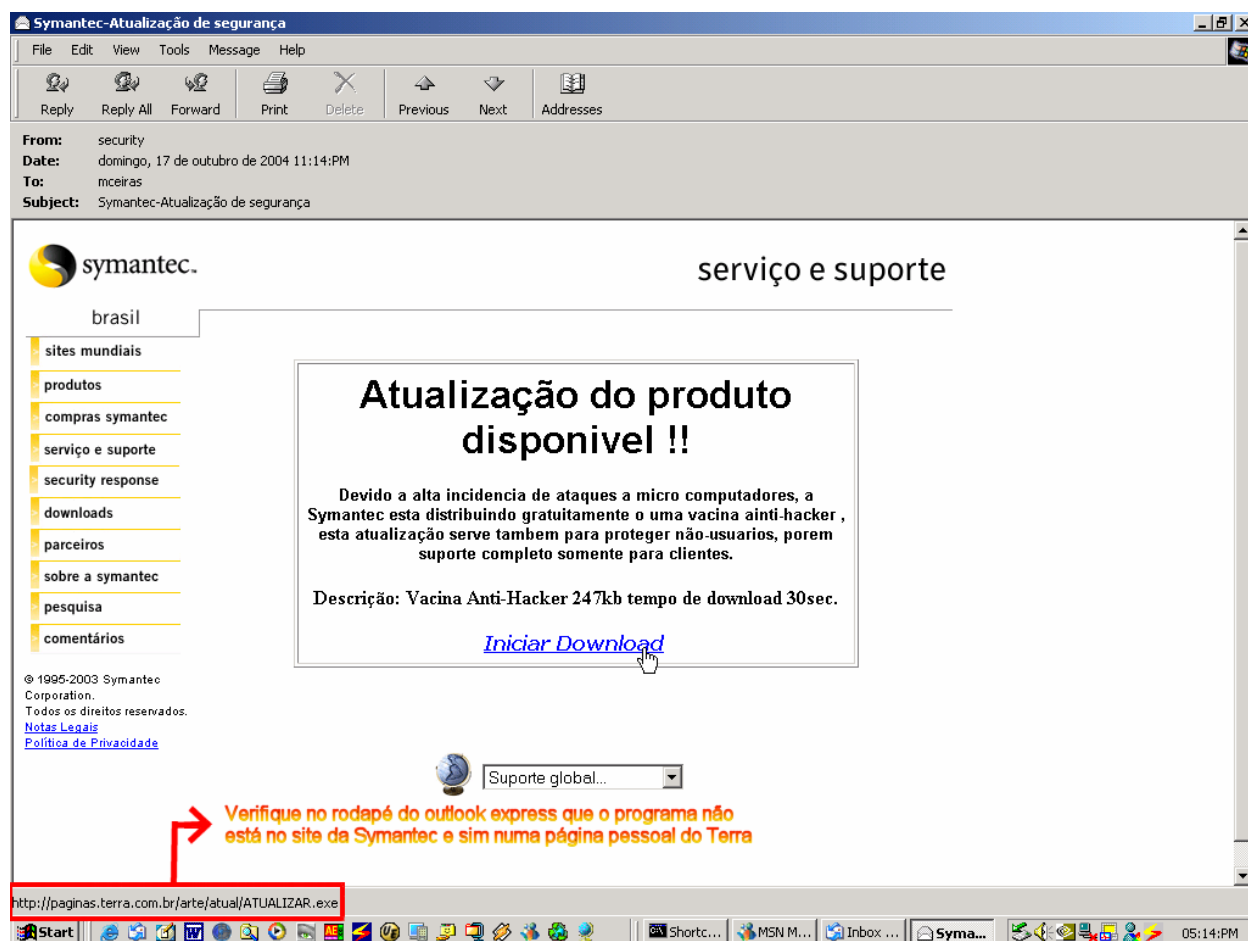
Conclusão: prevenção e treinamento

Como podemos observar os ataques de engenharia social, de SCAM (mensagens falsas com intuito de prejudicar uma ou mais pessoas normalmente com objetivos financeiros) ou Hoax (mensagem falsas, boatos ou mensagens com brincadeiras de fosto duvidoso).

Para evitar este tipo de problema em sua empresa a melhor forma é o treinamento e o esclarecimentos desses perigos ao funcionários, orinetando ao funcionários atualizarem o sistema ou criando sistemas de atualização automática, pelo menos nos patches críticos de segurança. Dar conselhos como para verificar a procedência dos email, divulgar os principais tipos de ataques, dizer que bancos e instituições financeiras em geral não pedem dados por email, nem cartões animados são enviados em formato .EXE. Também deve orientar os usuário com os arquivos .pif, que empresas de Antivírus não mandam vacinas pelo correio e que as atualizações são feitas pelos próprios programas de antivírus alem de outras técnicas usadas pelos meliantes e engraçadinhos.

Acima esta um exemplo claro de SCAN que deve ser apresentados aos funcionários (normalmentes os SCAN são parecidos). No exemplo abaixo o email se identifica como sendo da Symantec (conhecida desenvolvedora de soluções anti-virus) e que ela esta enviando o email com link para baixar a correção. Primeiro, uma empresa jamais manda este tipod e mensagem. E o mais chamativo neste caso é que quando clicado no link aparece na borda inferiro esquerda do Outlook o link completo que como pode ser visto é de uma pagina pessoal de clientes do provedor Terra, ou seja definitivamente deve ser um vírus, trojam ou spyware.

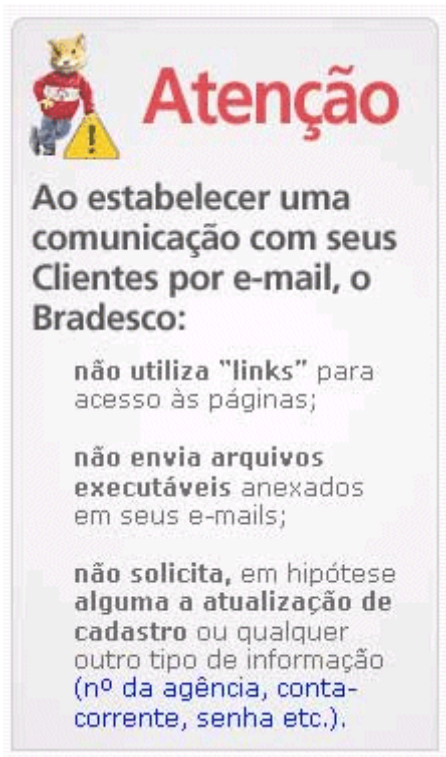
O treinamento intensivo e constante dos usuários é a maior arma contra a engenharia social. O engenheiro social age sempre confiando na boa fé da vitima, fazendo se passar por outra pessoa. Quebrando este elo de confiança atravez de treinamento não teremos mais promessas com engenharia social.



Para saber se um email é um boato (hoax) existem vários sites como o <http://www.museumofhoaxes.com> e HoaxBusters.ciac.org, onde podem-se encontrar listas contendo os boatos que estão circulando pela Internet e seus respectivos conteúdos.

Os administradores devem sempre verificar sempre os logs do firewall pessoal e de IDSs que estejam instalados no computador para verificar qualquer tipo de trafego estranho na rede.

Aviso anti-scam do Bradesco



Atenção

Ao estabelecer uma comunicação com seus Clientes por e-mail, o Bradesco:

- não utiliza "links" para acesso às páginas;
- não envia arquivos executáveis anexados em seus e-mails;
- não solicita, em hipótese alguma a atualização de cadastro ou qualquer outro tipo de informação (nº da agência, conta-corrente, senha etc.).

Isca: Banco do Brasil

Promessa: sorteios mensais de prêmios até R\$ 50 mil

Golpe: o e-mail oferece um serviço inventado pelos golpistas para convencer as pessoas a cadastrar seus dados em formulário falso. Para estimular os clientes, a mensagem promete sorteios mensais de prêmios até R\$ 50 mil.



Imagem de uma página web falsa do Banco do Brasil, intitulada "Sua Conta". A página contém campos para login (usuário e senha) e uma seção de "Atualizar dados pessoais". No topo, há uma barra amarela com o logo do Banco do Brasil e o texto "Banco do Brasil". À esquerda, há uma seção com o título "Atenção" e um ícone de alerta. À direita, há uma seção com o título "Sorteio de Prêmios" e um ícone de prêmio. No rodapé, há uma barra amarela com o texto "Banco do Brasil" e "© 2004 Banco do Brasil S.A. Todos os direitos reservados".

Cópia da página do Banco do Brasil utilizada na fraude.

Trecho da mensagem: "Atenção: O BB não envia e-mail sem a sua permissão. Porém, devido uma grande ocorrência de fraudes e o fato de levarmos algum tempo para atualizarmos nossos registros, estamos disponibilizando, via e-mail, um novo certificado de segurança, que garante maior conforto em suas transações".

Características: a texto da mensagem é convincente e deve ter sido escrito por um spammer profissional. No e-mail, vem um link para um falso site.

Glossário

802.11

Refere-se a um conjunto de especificações desenvolvidas pelo IEEE para tecnologias de redes sem fio.

ADSL

Do Inglês *Asymmetric Digital Subscriber Line*. Um sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um *modem* convencional.

Antivírus

Programa ou software especificamente desenvolvido para detectar, anular e eliminar vírus de computador.

AP

Do Inglês *Access Point*. Um dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Assinatura Digital

Um código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

Backdoor

Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Boatos

Veja *HOAX*.

Cable Modem

Um modem projetado para operar sobre linhas de TV a cabo.

Cavalo de Tróia

Programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Comércio eletrônico

Também chamado de *e-commerce*, é qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais, utilizadas para facilitar e executar transações comerciais de bens e serviços através da Internet.

Criptografia

Criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

Endereço IP

Este endereço é um número único para cada computador conectado à Internet, composto por uma sequência de 4 números que variam de 0 até 255 separados por ".". Por exemplo: 192.168.34.25.

Engenharia Social

Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Firewall

Dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores.

Firewall Pessoal

Um *software* ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet, e constitui um tipo específico de *firewall*.

HOAX

Mensagem recebida por *e-mail*, cujo conteúdo é alarmante e normalmente falso. Pode ser visto como um vírus social, pois utiliza a boa fé das pessoas para se reproduzir, sendo esse o seu principal objetivo.

HTML

Do Inglês "*HyperText Markup Language*". É uma linguagem universal utilizada na elaboração de páginas na Internet.

IDS

Do Inglês *Intrusion Detection System*. Um programa, ou um conjunto de programas, cuja função é detectar atividades incorretas, maliciosas ou anômalas.

IEEE

Acrônimo para *Institute of Electrical and Electronics Engineers*, uma organização composta por engenheiros, cientistas e estudantes, que desenvolvem padrões para a indústria de computadores e eletro-eletrônicos.

IP

Veja Endereço IP.

log

Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

Modem

Dispositivo que permite o envio e recebimento de dados através das linhas telefônicas.

Número IP

Veja Endereço IP.

Password

Veja Senha.

PGP

Do Inglês *Pretty Good Privacy*. Um programa de criptografia, de domínio público, que utiliza os conceitos de chave pública e chave privada.

Porta dos Fundos

Veja *Backdoor*.

Proxy

Um servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. *Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar Spam.

Senha

Conjuntos de caracteres, de conhecimento único do usuário, utilizados no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

Site

Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia

Spam

Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quanto o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial Email*).

Spammer

Pessoa que envia *Spam*.

SSID

Do Inglês *Service Set Identifier*. Um conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

Trojan Horse

Veja Cavalo de Tróia.

UCE

Do inglês *Unsolicited Commercial Email*. Termo usado para se referir aos *e-mails* comerciais não solicitados.

Vírus

Vírus é um programa capaz de infectar outros programas e arquivos de um computador. Para realizar a infecção, o vírus embute uma cópia de si mesmo em um programa ou arquivo, que quando executado também executa o vírus, dando continuidade ao processo de infecção.

VPN

Do Inglês *Virtual Private Network*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas, como a Internet, como infra-estrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para

garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

WEP

Do Inglês *Wired Equivalent Privacy*. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Este protocolo apresenta algumas falhas de segurança.

Wi-Fi

Do Inglês *Wireless Fidelity*. Termo usado para referir-se genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless

Tecnologia que permite a conexão entre computadores e redes através da transmissão e recepção de sinais de rádio.

WLAN

Do Inglês *Wireless Local-Area Network*. Um tipo de rede que utiliza ondas de rádio de alta frequência, ao invés de cabos, para a comunicação entre os computadores.

Link para os programas citados

NMAP

<http://www.insecure.org/nmap>

NESSUS

<http://www.nessus.org>

LANGUARD NETWORK SECURITY SCANNER

<http://www.gfi.com>

Filmes relacionados

CAÇADA VIRTUAL (TAKEDOWN)

Filme baseado no Livro de Tsutomu Shimomura e John Markoff

PIRATAS DO VALE DO SILICIO (Pirates of Silicon Valley)

Filme sobre a história da Apple, Microsoft e da microinformática

Link de Pesquisa e Apoio

Revista Época

<http://revistaepoca.globo.com>

Google

<http://www.google.com>

Módulo Security

<http://www.modulo.com.br>

Site da Defensive Thinking (empresa fundada por Kevin Mitinick)

<http://defensivethinking.com>

Proxies Públicos

<http://www.publicproxyservers.com>

Página do SANS

<http://www.sans.org>

Museum of Hoaxes

<http://www.museumofhoaxes.com/>

Wikipedia, the free encyclopedia

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

Bibliografia:

Estelionato Eletrônico – Segurança na Internet

Vicente Lentini Plantullo

Editora Juruá

A Arte de Enganar

Kevin D. Mitnick e Willian L. Simon

Editora Makron Books

Universidade H4CK3R

James Della Valle e Henrique Cesar Ulbrich

Editora Digerati Books

Revista Época 09/2003

Entrevista de Kevin Mitnick por Luciana Vicária