Ferramentas de espionagem e invasÃ£o crescem na Internet

HÃ¡ mais ou menos dois anos o principal executivo da Sun Microsystems, Scott McNealy proferiu sua solene – e sombria – assertiva de que a privacidade na Internet Ã© igual a zero e que isto jamais iria mudar. Desencadeou grande resistÃªncia no mercado infonauta mas se pararmos para analisar, de lÃ¡ para cÃ¡ nunca assistimos a tantos casos de *hacking*, *cracking*, invasÃ£o de sistemas, novos e cada vez mais sofisticados vÃrus inundando a Grande Rede e a clonagem de cartÃµes de crÃ©dito se tornando uma praga mundial.

Agora temos notÃcia atÃ© da primeira gangue virtual, aparentemente sediada em algum paÃs da Ã•frica; se autodenominam*Cyberstalkers* ou assaltantes cibernÃ©ticos. Para se ter uma idÃ©ia da gravidade da questÃ£o de seguranÃ§a na Internet, recentemente a Microsoft reconheceu publicamente que todas as versÃµes do Windows 2000, inclusive as primeiras cÃ³pias *beta* do sistema operacional XP que ainda nem foram lanÃ§adas, contÃªm sÃ©rias vulnerabilidades que permitem que *hackers* assumam o controle das mÃ¡quinas invadidas.

A empresa alertou a todos os que compraram o programa e prometeu ajustar tudo atÃ© a data do novo lanÃ§amento. Os usuÃ¡rios da Internet atualmente tÃªm alguma noÃ§Ã£o de que estÃ£o abrindo mÃ£o de sua privacidade quando acessam os seus *modems*, mas a situaÃ§Ã£o ainda estÃ¡ longe de representar uma unanimidade mundial.

A maior preocupaÃ§Ã£o hoje Ã© a coleta de grande quantidade de dados pessoais dos usuÃ¡rios sem sua autorizaÃ§Ã£o e na grande maioria das vezes sem seu conhecimento, atravÃ©s dos famigerados cookies. Hoje jÃ¡ podemos listar oito formas diferentes de burlar a seguranÃ§a na rede Internet:

Sua identidade pode ser furtada na Internet

A polÃcia de Nova Iorque prendeu um sujeito chamado Abraham Abdallah, empregado como contÃnuo de uma empresa, que havia adquirido um exemplar da revista *Forbes*, listando as 400 pessoas mais ricas do mundo, alÃ©m dos seus nÃºmeros de Seguro Social (o equivalente melhorado do nosso INSS), de seus cartÃµes de crÃ©dito e informaÃ§Ãµes bancÃ¡rias, alÃ©m dos nomes completos de sua filiaÃ§Ã£o, tudo com o objetivo de perpetrar um golpe milionÃ¡rio contra personalidades como o cineasta Steven Spielberg e a apresentadora de televisÃ£o Oprah Winfrey, entre outros. Abdallah utilizou *sites, e-mails e mÃ©todos off-line* para conseguir as identidades dessas pessoas e furtÃ¡-las em milhÃµes de dÃ³lares.

Quando foi preso, Abdallah, atravÃ©s de seu advogado, negou tudo e atÃ© agora ainda nÃ£o foi indiciado pelas autoridades americanas, ciosas de que estÃ£o diante de um caso novÃssimo e que requer estudo detalhado para nÃ£o ferir alguma emenda constitucional americana de liberdade ou direitos civis, coisa que Ã© realmente levada a sÃ©rio por lÃ¡. Esse Ã© apenas um dos casos recentes – e o mais rumoroso – a chamar a atenÃ§Ã£o para o chamado *furto de identidade*, que, segundo o FBI, a polÃcia federal americana, Ã© o crime de colarinho branco que mais cresce nos EUA.

Em torno de 500.000 americanos tÃªm suas identidades usurpadas a cada ano. Sinal dos tempos: pelo

menos quatro companhias de seguro americanas jÃ¡ oferecem apÃ³lices para cobrir o furto de identidade, o chamado ID-theft e os prejuÃzos considerÃ¡veis que causam Ã s suas vÃtimas. Segundo estudo recente conduzido pela empresa *The Privacy Rights Clearinghouse*, que trabalha para recuperar a imagem das vÃtimas, leva-se em torno de dois anos para limpar completamente o nome e o crÃ©dito de uma vÃtima de furto de identidade.

Um dos cenÃ¡rios mais mirabolantes que vem crescendo exponencialmente, Ã© quando criminosos utilizam as identidades furtadas ao serem presos, deixando suas vÃtimas com registros criminais muito difÃceis de serem esclarecidos e limpos. AtÃ© sites oferecendo identidades falsas jÃ¡ estÃ£o proliferando na Internet imperturbados.

Todos nÃ³s estamos constantemente revelando informaÃ§Ãµes pessoais e privadas enquanto navegamos pelo ciberespaÃ§o

“Surfar” na Internet transmite uma sensaÃ§Ã£o de anonimato, como se estivÃ©ssemos pesquisando as pÃ¡ginas de um livro numa biblioteca, mas todos os *sites* que visitamos estÃ£o “olhando” de volta para nÃ³s. A maioria deles usa os *cookies* para coletar dados sobre sua passagem. O seu *browser* tambÃ©m pode estar oferecendo informaÃ§Ãµes de sua “viagem” pelo mundo virtual. A maioria de nÃ³s nÃ£o sabe mas os nossos navegadores podem incluir nossos nomes, endereÃ§os eletrÃ´nicos e outros dados relevantes que podem ser capturados e arquivados pelos *sites* que visitamos na Grande Rede. AtÃ© mesmo o TCP/IP pode estar nos “dedurando”.

Cada computador na Internet tem um endereÃ§o de IP, ou *Internet Protocol*, o equivalente *online* aos endereÃ§os de ruas, que permite o recebimento de informaÃ§Ãµes. As conexÃµes de *dial-up*, por exemplo, normalmente lhe conferem um novo endereÃ§o de IP a cada vez que vocÃª conecta. Mas no caso de conexÃµes fixas o endereÃ§o Ã© permanente e permite que todos os *sites* visitados arquivem os seus dados pessoais. Ã?s vezes o vilÃ£o da histÃ³ria Ã© um “ET”, que, uma vez instalado dentro de seu PC, “telefona pra casa”, para seu *master site*, identificando seu endereÃ§o eletrÃ´nico definitivamente.

As informaÃ§Ãµes pessoais que na maioria das vezes fornecemos a determinados *sites* de nosso interesse, podem ser facilmente vendidas ou furtadas

Isso Ã© real principalmente em sÃtios de *e-commerce*, que coletam grande quantidade de dados dos usuÃ¡rios. A compra de um livro ou um CD numa loja do mundo real com pagamento em espÃ©cie nÃ£o resultarÃ¡ em qualquer registro *linkando* vocÃª Ã operaÃ§Ã£o, mas a mesma operaÃ§Ã£o realizada *online* fica diretamente vinculada ao seu nome.

Lojistas virtuais vÃªm coletando enorme quantidade de informaÃ§Ãµes de compradores, quem estÃ¡ comprando o quÃª e para qual finalidade e jÃ¡ se tornou prÃ¡tica comum na Internet esses lojistas passarem adiante esses dados. A Amazon jÃ¡ incluiu nos seus contratos de adesÃ£o *online* aexpressÃ£o “asset” (patrimÃ´nio), para definir os dados de seus clientes que possui armazenados, com oobjetivo de vender ou transferi-los no futuro.

Os defensores da privacidade estÃ£o lutando nos Estados Unidos para aprovar legislaÃ§Ã£o federal que obrigue os sÃtios a permitir que navegantes exerÃ§am o direito de exclusÃ£o dos seus dados destas transaÃ§Ãµes, mas ainda estamos longe de um denominador comum nesse sentido que possa representar uma iniciativa global na rede. Os *hackers* tambÃ©m nÃ£o descansam na tentativa de furtar dados, informaÃ§Ãµes e nÃºmeros de cartÃµes de crÃ©dito.

O *Universe*, um sÃtio de mÃºsica, teve cerca de 300.000 nÃºmeros de cartÃµes de crÃ©dito roubados recentemente; o *Bibliofind*, uma subsidiÃ¡ria da *Amazon* teve todos os nomes, endereÃ§os e nÃºmeros de cartÃµes de 98.000 clientes furtados. O que alivia um pouco no caso dos cartÃµes Ã© que na praxe as administradoras e os bancos costumam pagar a maioria das contas nÃ£o reconhecidas pelos clientes.

Ponto para o vaticÃnio de Steve MacNealy sobre a privacidade na *Web*. Ainda falta muito para a tecnologia alcanÃ§ar controle completo sobre as informaÃ§Ãµes quecirculam diariamente na Internet de forma a oferecer seguranÃ§a total aos usuÃ¡rios e navegantes, por isso todo cuidado Ã© pouco ao preencher formulÃ¡rios virtuais ou ceder seus dados pessoais na Grande Rede, pois as dores de cabeÃ§a podem ser substanciais.

O sÃtio no qual vocÃª acaba de digitar o nÃºmero de seu cartÃ£o de crÃ©dito pode ser falso

O FBI estourou uma rede russa de fraude e conspiraÃ§Ã£o. Os *hackers* estavam envolvidos no que jÃ¡ foi cunhado como “*website spoofing*“, que significa mimicar um determinado sÃtio na Internet e se beneficiar dos serviÃ§os e dos usuÃ¡rios que inadvertidamente navegam ali. Ã? relativamente fÃ¡cil conseguir nomes de domÃnio praticamente iguais a outros jÃ¡ existentes para perpetrar esses atos de esperteza *online* e lesar milhares de pessoas.

Bancos tambÃ©m tÃªm sido alvo freqÃ¼ente dos *spoofers*, como no caso do Bank of America, um dos maiores dos Estados Unidos, que teve seu nome de domÃnio imitado com a simples supressÃ£o do [ponto] apÃ³s o www (*wwwbankofamerica.com*) iludindo milhares de clientes que informaram seus dados financeiros pessoais.

Empresas com fins lucrativos e pessoas que nÃ£o gostam de vocÃª podem estar transmitindo seus dados pessoais privados na Rede

O assassinato de uma assistente de consultÃ³rio dentÃ¡rio de 20 anos em New Hampshire/EUA por um admirador obcecado em 1999 chamou a atenÃ§Ã£o para outro aspecto perigoso da cibereconomia: os corretores de informaÃ§Ã£o *online*. O assassino da moÃ§a pagou US$ 45.00 a um *site* da FlÃ³rida chamado *Docusearch.com*, para obter o nÃºmero de Seguro Social dela, descobriu o endereÃ§o de seu trabalho, assediou a jovem e a matou.

Os tais corretores de informaÃ§Ã£o insistem que fazem um trabalho necessÃ¡rio, fornecendo informaÃ§Ã£o sensÃvel para empregadores, credores e outras pessoas que precisam dos dados. Mas muitos vendem nÃºmeros de Seguro Social (o equivalente ao nosso INSS) e informaÃ§Ã£o financeira privativa para qualquer um que quiser pagar.

SÃ£o uma porta aberta para ladrÃµes de identidade e falsÃ¡rios. E o mais curioso Ã© que a fonte mais importante desses corretores de informaÃ§Ã£o Ã© o prÃ³prio governo. A Internet torna mais fÃ¡cil para as pessoas negociarem informaÃ§Ãµes sobre outras pessoas de que nÃ£o gostam. HÃ¡ uma batalha em marcha nos EUA entre os defensores da liberdade absoluta de expressÃ£o e troca de informaÃ§Ãµes e aqueles que defendem um maior controle sobre as informaÃ§Ãµes sensÃveis que circulam na Grande Rede.

Sua empresa ou seu companheiro (a) pode estar usando a Internet para espionar vocÃª.

Empresas tÃªm o direito legal de monitorar os e-mails dos seus empregados, ICQ e outras formas de *instant messaging*, para evitar abusos e desvios de conduta. A maioria delas faz isso, embora devessem sempre informar aos funcionÃ¡rios sobre esse controle. A Universidade do estado do Tennessee, nos EUA, divulgou mais de 900 mensagens eletrÃ´nicas de amor entre uma administradora e um diretor da instituiÃ§Ã£o, nas quais ela conta como recorreu ao Ã¡lcool e Ã s drogas para lidar com a frustraÃ§Ã£o resultante da rejeiÃ§Ã£o. VÃ¡rias empresas, entre elas o New York Times e a Dow Chemical, demitiram funcionÃ¡rios por envio de e-mails considerados inadequados.

Mas a Ã¡rea que mais cresce na bisbilhotagem *online* sÃ£o as residÃªncias. A SpectorSoft, uma fabricante de equipamentos de espionagem, comeÃ§ou vendendo seus produtos para pais e patrÃµes. Mas as vendas explodiram mesmo foi quando a empresa mudou seu *target* para cÃ´njuges e parceiros romÃ¢nticos. “Em apenas um dia rodando o programa Spector no meu PC fui capaz de descobrir a verdadeira personalidade do meu noivo. Descobri diversas das suas outras namoradas”, revela uma usuÃ¡ria do *software* em questÃ£o.

O Spector 2.2, uma vez instalado no seu computador, irÃ¡ secretamente “fotografar” todos os sites, *chat groups e e-mails* que vocÃª visitar ou enviar e salvÃ¡-los em um arquivo secreto que possibilitarÃ¡ Ã pessoa que estÃ¡ bisbilhotando examinÃ¡-los mais tarde. Um outro produto da mesma empresa ainda envia, de 30 em 30min, relatÃ³rios completos sobre sua navegaÃ§Ã£o para o espiÃ£o. Esses programas funcionam no chamado *stealth mode*, isto Ã©, em modo camuflado, de forma que vocÃª jamais terÃ¡ conhecimento de que estÃ£o na sua mÃ¡quina. A empresa jÃ¡ vendeu mais de 40.000 cÃ³pias desses programas e prevÃª que isso Ã© apenas o comeÃ§o de um mercado exponencial.

Estranhos podem estar usando seu PC para espionar vocÃª.

Os *hackers* podem penetrar no seu computador e olhar tudo o que vocÃª tem se as suas salvaguardas estiverem desativadas. MÃ¡quinas ligadas na Internet atravÃ©s de conexÃµes a cabo ou DSL, que estÃ£o permanentemente ligadas, sÃ£o mais vulnerÃ¡veis do que aquelas via serviÃ§o *dial-up*. Um *firewall* domÃ©stico Ã© a melhor proteÃ§Ã£o para esses ataques disfarÃ§ados.

Outro mÃ©todo muito utilizado para usar o seu PC contra vocÃª mesmo Ã© enganÃ¡-lo a baixar programas de bisbilhotagem como os que jÃ¡ descrevemos aqui. DaÃ advÃ©m o nome Cavalo de TrÃ³ia (*Trojan Horse*). Esse programa se encontra escondido dentro de outro, aparentemente inofensivo. Ã? por isso que tantos vÃrus como aquele “I Love You”, que rodou o mundo, e outros prometendo fotos de belas mulheres famosas, vÃªm “embrulhados” como presentes.

A maioria dos vÃrus Ã© criada para danificar computadores mas alguns sÃ£o desenhados para furtar informaÃ§Ã£o. Os vÃrus podem navegar atravÃ©s dos arquivos do seu disco rÃgido. O VBS.Noped.A@mm invade as mÃ¡quinas e procura pornografia infantil. Se encontra arquivos de imagem com nomes suspeitos, o programa imediatamente notifica a polÃcia e envia a eles alguns arquivos, alÃ©m de mandÃ¡-los tambÃ©m a vÃ¡rios endereÃ§os eletrÃ´nicos dos seus contatos. *Back Orifice*, um famoso programa criado hÃ¡ alguns anos por um grupo de *hackers* chamado *Cult of the Dead Cow* (Culto da Vaca Morta), invade e domina completamente o seu computador e espiona, entre outras coisas, suas senhas e cada tecla premida em sua mÃ¡quina.

O programa estÃ¡ disponÃvel de graÃ§a na Internet, juntamente com outras ferramentas para *hackers* como o *Sub-Seven*. Existem sÃtios como hack.co.za e *astalavista.box.sk* que auxiliam a planejar um ataque a outros computadores.

Nas palavras de um *hacker* anÃ´nimo: “Hoje em dia, qualquer idiota que saiba premir teclas Ã© capaz de assaltar seu computador.” Tudo isso prova que a Internet Ã© realmente incontrolÃ¡vel. Se por um lado a tecnologia dos programas legais avanÃ§a constantemente, o mesmo acontece com as ferramentas de espionagem, bisbilhotagem e invasÃ£o. Todo cuidado Ã© pouco nestes tempos digitais, em que a informaÃ§Ã£o se transformou no bem mais precioso da humanidade.

Autores: RedaÃ§Ã£o Conjur