

www.clubedohacker.com.br

# “Roubar dados de um computador é tão fácil como sair à noite com um belo carro e voltar acompanhado...”

Entrevista: Carlos Saraiva

**Adonel Bezerra é um dos maiores especialistas brasileiros em segurança digital. Fundador e gestor de um dos maiores portais de segurança de sistema do país, Bezerra tem dado contribuições relevantes para o mercado de segurança da informação, principalmente no meio académico.**

Em entrevista a “o Crime”, o perito e investigador fala dos principais perigos que espreitam os nossos computadores e a forma de os evitar... quando isso é possível. **‘o Crime’ - Quais são os perigos emergentes para a segurança digital, numa altura em que quase tudo o que nos rodeia, do lançamento de mísseis à lista de compras domésticas está dependente dos computadores?**

cala e tenta responder na medida de suas limitações.

**As sociedades estão hoje mais vulneráveis, precisamente devido à sua dependência dos sistemas informáticos?**

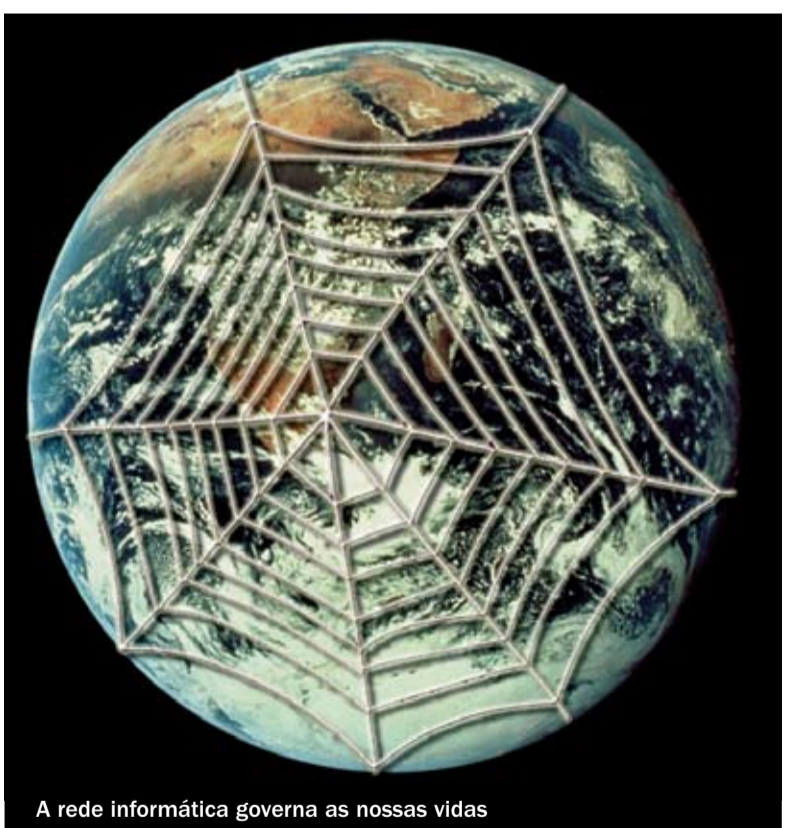
Está ocorrendo no mundo moderno algo que ninguém percebe, mas não é tão bom quanto parece: As redes sociais nos permitem encontrar pessoas no mundo inteiro, nos relacionar, fazer amizades virtuais e até sexo. Recentemente, estava vendo uns produtos específicos para isso, onde, remotamente um casal poderia fazer sexo ligando um pênis na porta usb do computador e passando o controlo remotamente para o parceiro remoto.

Temos feito vários testes de engenharia social aqui no Brasil e em mais de 80% dos casos temos êxito, porque as pessoas, quanto mais participam das redes sociais, mais solitárias ficam. O ser humano tem necessidades que só podem ser preenchidas com o calor dos corpos, ‘olho no olho’.

Temos tido bastante êxito com essas pessoas, elas se apaixonam, trocam confidências, já fiz isso até com pessoas do meu prédio e nunca imaginaram que estava contando segredos do casal para seu vizinho pensando que estavam falando com alguém de outro país.

**Em Portugal, tem crescido um tipo de burla ou crime associado a fraudes bancárias via Internet. Considera que esta criminalidade tem tendência a desenvolver-se (no Brasil este fenómeno é igualmente preocupante)?**

Esse crime deve continuar crescendo à medida que aumenta o acesso à internet e a nossa dependência aos bancos. Hoje, temos acesso a



A rede informática governa as nossas vidas

crédito fácil, pagamos nossas taxas etc.... Somos dependentes de um sistema capitalista mundial, onde todo o dinheiro está concentrado em bancos. Antigamente, tínhamos que tomar cuidado ao sair à rua com dinheiro porque poderíamos ser assaltados por alguém que tivesse nos seguindo. Nos tempos que correm, temos que tomar cuida com as 65.536 portas do nosso computador.

Por uma delas podem estar sendo enviadas informações confidenciais de meu computador, onde faço minhas transações bancárias.

A criminalidade evoluiu e evoluirá cada vez mais. Acontece que as polícias não estão evoluindo na mesma proporção. Na maioria das Capitais aqui no Brasil, nem delegacia de crimes digitais existe, e quando existe é só no papel, eles colocam policiais

que não entendem nada da infra-estrutura de internet, limitam-se a colher depoimentos. Salvo as delegacias especializadas da policia federal ou algumas capitais que já tem esses peritos especializados em crimes digitais nas policias civil.

**É fácil invadir um computador e roubar dados pessoais?**

Sim, e tão fácil como sair à noite com um belo carro e um pouco de dinheiro e voltar muito bem acompanhado (a). As pessoas são vulneráveis na essência. É fácil explorar as vulnerabilidades humanas utilizando-se de engenharia social, detectar o que as pessoas gostaria de ouvir, de ler naquele momento, se suas emoções são satisfeitas, elas estão aptas a fornecer informações de retorno, sentem-se na obrigação de retribuir porque as suas emoções foram satisfeitas naquele momento. Sem contar com as vulnerabilidades dos sistemas operacionais. Hoje em dia, o usuário final é quem realmente testa os softwares que são lançados cheios de falhas e vão corrigindo à medida que alguém reclama ou publica um novo problema. Ou mesmo os softwares piratas que nem sempre estão íntegros e na maioria das vezes já foram modificados para executar determinadas ações sem que o utilizador final tome conhecimento.

Não estou aqui criticando quem utiliza softwares piratas, esse é um problema dos governos e de pessoas que arrecadam dividendos com



“Nessa guerra não há vencedor nem vencido, se ganha uma aqui, perde-se outra ali. Um dia, acha que ganhou!”

“As pessoas, quanto mais participam das redes sociais, mais solitárias ficam.”

“As polícias não estão evoluindo na mesma proporção do crime digital.”

“Alguém sempre esquece alguma coisa por alguns segundos, mas, na maioria das vezes, o invasor cai em armadilhas deixadas pelos especialistas, os chamados ‘honeypots’ (potes de mel)”

isso, estou citando problemas do dia-a-dia, é com o utilizador final que me preocupo, já que, normalmente, este não tem como saber se as coisas estão bem ou não.

**Quer descrever algumas técnicas usadas pelo potencial invasor?**

Normalmente utiliza-se contra o usuário final os ‘keyloggers’ e ‘trojans’, bem como alguns programas espíes enviados por e-mail ou scrips como ‘exploits’ para explorar falhas do sistema operacional e aplicativos. No caso de redes corporativas os ‘exploits’ são predominantes. Depois de ganhar acesso a uma das máquinas na rede, o que vai vale é o conhecimento que o invasor tem de redes.

**E de que forma as pessoas, as empresas e os Estados podem defender-se?**

Em primeiro lugar, as pessoas devem manter seus sistemas actualizados, um firewall pessoal, um bom antivírus actualizado diariamente e bem configurado, configuração correcta do navegador Web. Os Estados e as grandes empresas já mantêm os seus sistemas de defesa porque podem pagar os melhores especialistas e eles sabem o que fazer.

**E em relação a computadores da defesa ou das grandes empresas, também são vulneráveis nessa medida (um inglês está actualmente a lutar para não ser extraditado para os EUA por ter invadido os computadores do Pentágono e da NASA)?**

Sim, alguém sempre esquece alguma coisa por alguns segundos, mas, na maioria das vezes, o invasor cai em armadilhas deixadas pelos especialistas, os chamados ‘honeypots’ (potes de mel) com o objectivo de pegar alguém para servir de exemplo e mostrar que estão atentos. E as autoridades jamais ficam a saber se foi ‘isco’ ou não.

**A invasão dos sistemas informáticos a este nível não é alimentada pelos próprios países, a nível governamental (embora nunca o assumam) para espionagem, seja ela militar ou industrial?**

Espionagem industrial sempre existiu e vai continuar existindo.

Quanto ao nível governamental, não entrarei nessa questão.

**Têm ocorrido casos semelhantes no Brasil?**

Sim **Acha que, no futuro próximo, corremos o risco de alguém invadir os computadores militares e disparar um míssil? Ou é uma hipótese absurda?**

Creio ser absurda, mesmo tratando do ser humano, onde sempre haverá interesses que nem sempre são bons para a colectividade. Será diferente em relação a uma empresa de serviços públicos. Nesse caso, o interesse seria simplesmente mexer numa conta para baixo ou para cima ou mesmo isolar uma conta de energia para um módulo especial do banco de dados e parar de pagar as contas, pois sabem que enquanto estiver naquele módulo, nunca haverá ordem de corte para aquela unidade.

**É frequente, as grandes empresas, e também os serviços secretos, contratarem “hackers”. Pode descrever o perfil característico de um hacker? É um tipo metódico ou pode ser desorganizado, tem que ter uma inteligência acima da média ou isso não é relevante?**

Normalmente baseia-se no conhecimento. São pessoas com excelentes conhecimentos de redes, sistemas operacionais e programação, além de um talento nato para curiosidade (alguém que não acredita que algo está correcto até ele mesmo testar e provar que tem falha).

**O que é um ataque de DOS**

(denial of service)?

É um ataque de negação de serviço. Imagine uma estrada que só suporta a passagem de 4 carros por vez e você tente passar 10 para ver o que acontece! No caso dos sistemas de informática, considere que um site só tenha banda para atender 1000 usuários por vez. Se alguém fizer 1000 conexões simultâneas a esse site, não sobrá banda para atender os outros usuários porque apenas uma pessoas ordenou 1000 conexões simultânea de origem diferente normalmente utilizando-se de máquinas ‘zombies’...

**Quais podem ser, na sua opinião, os ataques mais destrutivos, em termos de causar o máximo de danos?**

Em minha opinião, o dano é sempre de acordo com quem o sofre. Imagine um aposentado que ganha salário mínimo e desse dinheiro depende para compra de alimentação e remédio para manter-se vivendo e tem seu cartão clonado, quando chega ao banco para pegar seu dinheiro descobre que alguém já sacou tudo. Imagine, agora, uma grande empresa de telecomunicações que sofreu um ataque em seu roteador de borda que atendia outras corporações também de grande porte. Juntando tudo, essas empresas terão um prejuizo de milhões de dólares.

**De quem será o dano maior?**

Em minha opinião o dano maior é do aposentado, até porque essas empresas, quando perdem dinheiro, até os governos correm a socorrê-las.

**Como é que um utilizador normal de um computador pode evitar os vírus, na maioria dos casos enviados com mensagens ou nomes (Michael Jackson, Gripe A, etc...) pensados para levar as pessoas a cometer o erro de os acolher no seu computador?**

Em primeiro lugar, deve ter cuidado com a emoção, configurar correctamente e manter seus sistemas actualizados.

**Há aplicações informáticas que permitem copiar as informações de computadores, a partir do Messenger ou do Skype? Avale, por favor, esta descrição: “A aliciente de conhecer novas pessoas é a base desta nova armadilha. Ao utilizar um destes programas (mIRC, Msn Messenger ou Skype), o utilizador é confrontado com um novo ‘amigo’. Este inicia**

uma conversa com um cordial ‘olá, tudo bem’, fazendo em seguida o resto da apresentação. O auge da conversa é atingido com a pergunta: ‘és homem ou mulher?’. Consoante a resposta, o programa activa uma série de 10 respostas fixas pré-programadas (para eles e para elas), pensadas para estimular a curiosidade. Por fim, a última frase é ‘vou-te mandar uma foto, clica para me veres’. Nessa altura, a vítima já está ligada, abre a foto mas nada aparece. A partir desse momento, a tal aplicação informática criminosa está activada e programada para fazer um scan constante do conteúdo do computador da vítima, incluindo o email, os dados bancários (senhas, contas), documentos pessoais, etc...”

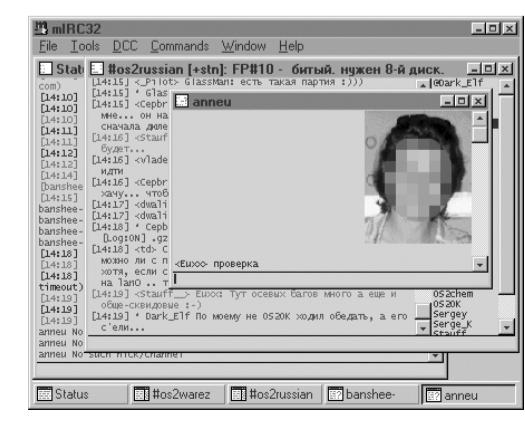
Isso é possível e ocorre todos os dias, na maioria das vezes é feito em processo automatizado, em outras, mesmo em conversas. Se você troca um arquivo remotamente com outro computador, pode conhecer o IP que a máquina remota esta utilizando. Nesse caso, é enviada uma foto ou um vírus, ou mesmo um programa espião, ou mesmo varrer a máquina remota em busca de vulnerabilidades que possa permitir uma invasão e instalação de programas.

**Ou seja, é possível aos piratas conhecer os códigos de utilização dos clientes do “e-banking”. De que forma operam?**

Sim, existem técnicas para sequestro de dados, principalmente através de páginas falsas para roubo de dados ou programas espíes que enviam os dados do computador da vítima. Para o banco, quem detém as informações do cliente é o próprio cliente.

**Falando de ciberterrorismo. Hoje é possível sabotar as sociedades por via de ataques a serviços essenciais, por exemplo causar o desnrte no transporte aéreo, na electricidade, no simples controlo do trânsito ou até sabotando a circulação de comboios para causar acidentes. Na sua opinião, será o ciberterrorismo a substituir acções como o 11 de Setembro?**

É possível ocorrerem factos isolados, mas não coisa de grande monta. A não ser que os desenvolvedores e especialistas em segurança que cuidam disso durmam mais de 10 horas por dia...



Programas de conversação são uma das plataformas mais utilizadas para cometer crimes