Reportagem Especial

TIRE AS DÚVIDAS

Quais aplicativos são mais vulneráveis? Por quê?

A maioria dos ataques ocorre no sistema Android. Motivos: por ele ser o mais utilizado e pelo fato do sistema Android permitir que o usuário instale aplicativos de outras lojas virtuais que não seja a oficial. Assim acaba ficando mais vulnerável pelos aplicativos maliciosos que se instalam a partir dessas lojas piratas, segundo o especialista em crimes virtuais, Eduardo Pinheiro Monteiro.

O que os hackers gostam mais de roubar? Isso é fácil?

Normalmente eles buscam informações que tenham algum valor agregado, seja de cartões de crédito, contas bancárias ou qualquer outro tipo de informação que possam utilizar para extorquir a vítima e obter alguma vantagem financeira, destacou Eduardo Pinheiro Monteiro.

Mas o mestre em informática e professor da UVV Marcello Novaes acrescentou que geralmente roubar dados não é uma tarefa fácil de executar "manualmente", então são utilizados spywares (vírus) para capturar estes dados.

É perigoso receber e acessar arquivos desconhecidos?

Não se deve aceitar e baixar arquivos desconhecidos ou suspeitos, pois essa é a principal forma de atuação dos hackers. Eles sabem que muitas pessoas se deixam levar pela curiosidade e acabam por meio desses arquivos permitindo a instalação de códigos maliciosos que serão utilizados para coletar informações confidenciais da vítima, disse Eduardo Pinheiro Monteiro.

CRIME VIRTUAL

Piratas da internet vão atacar 22 milhões em 2015

O aumento no número de vírus e de usuários vai intensificar ataques a equipamentos para roubo de dados de cartões e senhas

Eliane Proscholdt
Giordany Bossato

Seguindo praticamente a mesma velocidade dos avanços tecnológicos, os piratas da internet pretendem aumentar ainda mais o número de ataques virtuais no ano de 2015. A previsão é de que, no ano que vem, ocorra mais de 22 milhões de invasões em todo o País.

Atento as investidas desses cibercriminosos — como são chamados os criminosos especialistas em informática e internet —, o estrategista em segurança digital da Symantec, André Carraretto, explicou que o motivo desse crescimento se dá pelo aumento do número de vírus e da grande quantidade de aparelhos em uso.

Seus alvos vão desde grandes empresas até simples usuários de redes sociais, por meio dos smartphones e computadores.

O foco é variado: senhas bancárias, número de cartões de crédito, fotos, vídeos ou qualquer outro tipo de informação que o criminoso virtual possa utilizar para extorquir a vítima e obter alguma vantagem financeira.

O especialista em crimes virtuais, Eduardo Pinheiro Monteiro, revelou que existem duas formas de ocorrer uma invasão: com o auxílio da vítima ou sem que a pessoa perceba.

"Sem o auxílio da vítima, o invasor terá que ter acesso físico ao aparelho. Geralmente, utilizam esse método de contaminação os namorados e os maridos. Já os hackers, por não terem acesso físico ao aparelho da vítima, geralmente agem enviando armadilhas virtuais, e os usuários menos avisados acabam 'mordendo a isca'."

Sobre o assunto, o gerente de serviços e de tecnologia da F-Secure, Ariel Torres, acrescentou que, até mesmo crianças, estão sendo vítimas desses bandidos, já que muitas usam os aparelhos dos pais para acessar jogos ou vídeos. O complicador é que esses pequenos ainda não têm a malícia para identificar um arquivo perigoso.

Mas o mestre em Informática e professor da UVV Marcello Novaes ponderou que existem maneiras de se blindar de ataques.

"Adotar boas práticas como senhas fortes (que não sejam óbvias, como data de aniversário), usar antivírus, estar sempre desconfiado e atento aos arquivos e programas a serem executados poderão auxiliar na proteção contra os ataques virtuais."

CELULAR INVADIDO

KADIDJA FERNANDES/AT

Diálogo monitorado por três dias

Por três dias, todos os diálogos do WhatsApp entre uma auxiliar administrativo, de 40 anos, e sua amiga foram monitorados por um hacker. Isso aconteceu há dois meses.

O espião se passava pela amiga e dava conselhos a auxiliar administrativo. "Suspeitei que algo estava estranho pela linguagem e ortografia usada. A pessoa, que se passava pela minha amiga, me dava conselhos ruins, referente a um problema amoroso. Liguei para minha amiga e perguntei se ela havia escrito aquela mensagem. Ela negou."

Preocupada, ela procurou um profissional de tecnologia da informação e ele resolveu o problema removendo o código malicioso do seu celular.

À reportagem, esse profissional, que pediu para não ser identificado, explicou que, sabendo o número do celular da auxiliar administrativo, o hacker enviou uma mensagem via WhatsApp com um arquivo em anexo. Supostamente um vídeo com vírus. A partir daí, instalou o software espião no aparelho dela.

Agora ela só usa o aplicativo para falar o básico. "É tudo muito vulnerável."

Há risco em receber arquivos de grupos do WhatsApp?

Grupos de mensagens coletivas do WhatsApp são um perigo, pois sempre tem aquele participante engraçadinho que poderá compartilhar o que está sendo publicado no grupo, podendo assim provocar transtorno a pessoas envolvidas na publicação.

Pessoas mal intencionadas e hackers utilizam esses grupos para lançarem suas armadilhas virtuais utilizando fotos e vídeos, e quando alguém baixa para visualizar o arquivo poderá instalar um código malicioso, alertou Eduardo Pinheiro Monteiro.

Links em redes sociais que direcionam o usuário para outros sites devem ser evitados?

Devem sim. Isso porque, segundo o gerente de serviços e de tecnologia da F-Secure Ariel Torres, os cibercriminosos aproveitam a confiança que os usuários têm nas redes sociais para criar links falsos de notícias populares ou de falsas promoções para espalhar vírus.

Nesses casos, a dica do especialista é sempre entrar no site oficial da empresa ao invés de clicar direto no link visto na internet. Pode ser um pouco mais demorado, mas muito mais seguro.

Qual o risco de acessar a internet por meio de wi-fi aberto?

Acessos à internet por meio de redes wi-fi abertas é arriscado, pois a senha é compartilhada e é grande a possibilidade de um hacker estar monitorando o tráfego e espionando a navegação dos usuários, segundo o especialista Eduardo Pinheiro Monteiro.

Mas Marcello Novaes (foto) destacou que, desde que se desabilite as funcionalidades de compartilhamento de arquivos, de pastas e compartilhamento familiar, não existe grande perigo em conectar-se em uma wi-fi aberta.