CORREIO BRAZILIENSE

Publicado em 09/05/2022 - 05:56

PCC e Comando Vermelho controlam crimes digitais

GOLPE DIGITAL

Facções criminosas de olho nos celulares

PCC e Comando Vermelho articulam roubos em busca de senhas e informações bancárias armazenadas nos aparelhos

» VICENTE NUNES
» FERNANDA STRICKLAND

Duas das maiores facções criminosas do país, o Primeiro Comando da Capital (PCC) e o Comando Vermelho, entraram com tudo no mundo digital e estão roubando o que podem de brasileiros. Com a vida financeira da população concentrada nos celulares, esses aparelhos se transformaram nos principais alvos de bandidos, diz Rafael Cordeiro, diretor de Vendas da Tempest, uma das maiores empresas de cybersegurança do mundo, com base em relatos da polícia Em muitos casos, as vítimas são sequestradas para que todas as informações bancárias sejam repassadas. De posse dos dados, os criminosos abrem contas especialmente em bancos virtuais em nome dos raptados, que são transformados em laranjas deles próprios.

"Hoje, tudo está nos celulares: documentos, dados bancários, informações de cartões de crédito", afirma Cordeiro. "Por isso, os roubos de aparelhos estão batendo recordes, sobretudo nas grandes cidades", acrescenta. O executivo lembra que, diante dos altos volumes de recursos roubados, o PCC e o Comando Vermelho estão arregimentando um grupo cada vez maior de criminosos. "Eles atuam em todas as frentes. Não só roubando celulares, mas enviando mensagens maliciosas, os phishing. E muita gente cai como peixe na rede", detalha. Os golpes se estendem às empresas, que estão tendo os dados sequestrados, muitas vezes, por falhas nos sistemas de segurança.

O diretor da Tempest ressalta que, por temerem o roubo de dados, muitas pessoas estão optando por ter dois celulares. Um, com as informações financeiras, fica em casa. O outro, com dados básicos, vai para as ruas. Se furtado, não causa tantos transtornos. Ele acrescenta, ainda, que, muita gente não se preocupa em usar mecanismos de proteção nos celulares, o que torna as pessoas mais vulneráveis às ações dos bandidos. "De posse de informações confidenciais, os criminosos conseguem descobrir o padrão de consumo das vítimas, que ficam mais expostas à violência", complementa. Portanto, diz ele, todo cuidado é pouco.

Dados mais recentes de crimes cibernéticos mostram que o Brasil aparece no ranking dos cinco países com mais fraudes digitais. O levantamento está Fraud & Abuse Report, da Arkose Labs, empresa norte-americana especializada em segurança da informação. A lista inclui Estados Unidos, Rússia, Indonésia, Filipinas e Reino Unido. No Brasil, 89% dos crimes são no mundo virtual e 11%, ações manuais. Em 2017, o país registrava uma tentativa de fraude a cada 16 segundos, conforme relatório do Serasa Experian. Já entre 2019 e 2020, houve um aumento recorde de 308,2% no volume de phishing — como especialistas chamam o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito —, de acordo com dados da Axur.

Riscos do wi-fi público

O especialista em segurança pública e privada Leonardo Sant'Anna destaca que os brasileiros não têm muita cultura de cibersegurança. "O Brasil é um dos países em que mais se baixa aplicativos, além de aparecer entre os cinco que mais sofrem com golpes cibernéticos. Mas, quando a pessoa está baixando um aplicativo, esquce que, nele, vão todos os seus dados, todas as suas informações", alerta. Ele acrescenta que, pelo gosto dos brasileiros pela tecnologia, o país é um mais afetados na internet em todos os aspectos. "O primeiro motivo para isso é a questão populacional, nós somos quase 220 milhões de habitantes, então, essa questão interfere muito", explica. "Outro ponto, que é um problema grande, é a infraestrutura tecnológica precária. Isso prejudica, sobretudo, as pessoas mais carentes, que enfrentam dificuldades em coisas relativamente básicas, como o dinheiro que recebem do governo", emenda.

Na visão de Sant'Anna, cientes das fragilidades na segurança da tecnologia e de como é lucrativo o roubo no mundo virtual, os grupos criminosos resolveram investir em informática. "Os golpes virtuais são um celeiro maravilhoso para que consigam coletar todo tipo de informação pessoal, bancária e quaisquer outras que sejam do interesse deles", comenta. Os criminosos, acrescenta Rafael Cordeiro, da Tempest, também se aproveitam das redes públicas de wi-fi. Sem segurança adequada, essas redes permitem que dados importantes sejam interceptados. Isso vale, inclusive, para redes oferecidas por hotéis e restaurantes. "Muita gente, quando está viajando, faz transações bancárias usando essas redes. Não é recomendável."

Esse alerta referente às redes públicas de wi-fi vale tanto para celulares quanto para computadores, que, no entender do diretor da Tempest, são ainda mais vulneráveis a ataques. "A recomendação é de não usá-las. Mas, se for inevitável, que tanto os celulares quanto os computadores tenham antivírus, pois conseguem bloquear muita coisa", afirma Cordeiro. No caso das empresas, os sistemas de proteção devem ser ainda mais fortes, uma vez que, depois de invadidos, os sistemas dificilmente serão recuperados. Será melhor construir um novo. "Não existe uma solução única. Não existe uma bala de prata. Nenhuma rede é 100% segura. Mas é possível ter bons mecanismos de proteção", frisa.

Ameaças de morte

A confeiteira Suelen Santos dos Santos, 35 anos, conta que, há algumas semanas, vem procurando um empréstimo de forma on-line, pois está precisando muito de dinheiro. "Durante a pesquisa, um rapaz muito educado se apresentou pelo aplicativo WhatsApp, dizendo que o crédito tinha sido aprovado. O que achei estranho foi que ele pediu uma foto da minha identidade com o comprovante de residência, além de um PIX de R$ 300 com a desculpa de que o valor seria devolvido, que era para fazer uma procuração no cartório", relata. Mas ela não se sentiu segura com a conversa e preferiu terminar o contato naquele momento.

"Na hora, me toquei de que era um golpe e falei isso para o rapaz, bloqueei o contato e não dei mais assunto", diz. "No dia seguinte, outro número de celular me mandou mensagem pelo WhatsApp me ameaçando de morte. Mandaram fotos da cabeça cortada de uma pessoa, fotos de armas." Não foi só. Suelen também recebeu vários áudios, e o golpista afirmou ser do PCC. "Fala para a polícia que aqui é o Primeiro Comando da Capital, e que nós somos o inimigo número um dela." Para apagar os dados de Suelen, o criminoso exigiu que ela pagasse R$ 500. A confeiteira fez um Boletim de Ocorrência (BO), e aguarda que a justiça seja feita.

Muitos se esquecem que as redes sociais também podem ser um vilão quando os dados pessoais estão em questão. Orquídea Oliveira, 30, professora de inglês, foi alvo de um golpe no Instagram. Ela destaca que anunciava as aulas particulares na rede social para fazer um extra. "Mas nunca tomei cuidado com a minha senha. Sou muito esquecida, então, sempre colocava datas que fossem importantes para lembrar", diz. Ela lembra que postou uma foto do seu aniversário, cuja data era a senha. "Um dia depois, não conseguia mais acessar a minha rede, estava bloqueada. Como liguei o Instagram ao celular, também perdi o acesso ao WhatsApp". Foi nesse momento que o terror começou. Os golpistas começaram a entrar em contato com seus clientes e pedir um adiantamento da aula. "Até recuperar o acesso ao meu número, eles embolsaram cerca de R$ 5 mil", diz. Orquídea afirma que, por vergonha de ter caído nesse golpe, apagou sua conta na rede social.

Bancos

A Federação Brasileira de Bancos (Febraban) afirma, em nota, que acompanha permanentemente todos os temas relacionados à segurança, ainda que não tenham origem no sistema financeiro, e está atenta aos problemas de segurança pública e seus reflexos nas transações bancárias e na segurança de seus clientes, especialmente com o uso do Pix. A entidade reforça que os aplicativos de bancos são seguros, e os dados de uso não ficam armazenados nos aparelhos. "No caso de o cliente ter seu celular roubado, deve notificar imediatamente seu banco para que medidas adicionais de segurança sejam adotadas, como bloqueio do app e senha de acesso", informa. "Os bancos também atuam em parceria com forças policiais para auxiliar na identificação e punição de criminosos", explica.

A Febraban também alerta que os bancos têm funcionalidades em seus aplicativos que permitem que o cliente ajuste os limites transacionais no celular para valores de sua conveniência, seguindo à risca as instruções normativas do Banco Central, que tratam sobre o tema. "Incentivamos que os clientes utilizem esta funcionalidade em seus aplicativos para ajustar os limites de acordo com suas necessidades e segurança", complementa.

» Risco baixo, retorno alto

Uma teoria chamada economia do crime, diz que qualquer agente que comete um ato ilícito faz uma análise de qual é o maior e o menor benefício a ser adquirido. Segundo o especialista em segurança pública e privada Leonardo Sant'Anna, o criminoso avalia o risco que vai correr no momento em que pretende tirar o dinheiro de alguém. "As organizações criminosas já sabem que o meio digital é extremamente frutífero para que se consiga muito dinheiro com baixo risco", diz. E acrescenta: "Quando o criminoso vai roubar um carro, uma bolsa, ele não vai querer ficar perdendo tempo com o objeto, mas, sim, buscar informações que vão trazer mais lucros. Hoje, quando rouba um celular de R$ 5 mil, conseguirá apenas R$ 300 nele. Mas, se conseguirem os dados contidos no aparelho, o valor sobe para R$ 2 mil", exemplifica.

Veículo: Impresso -> Jornal -> Jornal Correio Braziliense - Brasília/DF

Seção: Economia **Pagina:** 7