Editor: José Carlos Vieira (Cidades)
josecarlos.df@dabr.com.br e
Tels. : 3214-1119/3214-1113
Atendimento ao leitor: 3342-1000
cidades.df@dabr.com.br

INVESTIGAÇÃO

Golpistas cibernéticos na mira da polícia

PCDF desarticula quadrilha de estelionatários que agiam on-line em todo o país. Cerca de R$ 1 milhão foi bloqueado para ressarcimento das vítimas. Delegados e especialistas alertam que o registro da ocorrência reforça o combate ao crime organizado

» DARCIANNE DIOGO

Espalhados pelo país e escondidos atrás de telas, criminosos cibernéticos seguem na busca voraz por potenciais vítimas para faturar alto com os golpes virtuais. No Distrito Federal, uma megaoperação da Polícia Civil (PCDF) que resultou no bloqueio de mais de R$ 1 milhão em contas bancárias para ressarcimento às vítimas, expõe a ousadia dos criminosos e coloca em evidência a importância do registro da ocorrência.

A operação de ontem foi desencadeada pela 9ª Delegacia de Polícia (Lago Norte) e cumpriu quatro mandados de busca e apreensão contra a organização criminosa. De forma articulada e discreta, a quadrilha montou uma central no estado de São Paulo como pontapé para o começo da empreitada criminosa. Segundo a investigação, somente no Distrito Federal, ao menos 12 vítimas registraram ocorrências relacionadas ao grupo. "Na maioria das vezes, as vítimas são sempre idosos com pouca familiaridade com informática", destacou o delegado Erick Sallum.

De São Paulo, os estelionatários ligavam para pessoas de todo o Brasil e se passavam por representantes de centrais de segurança de bancos e induziam as vítimas a acessarem sites clonados — que imitavam as páginas oficiais das instituições — e baixarem um falso antivírus. O programa, na verdade, instalava um malware chamado GhostRat, que permitia acesso remoto total aos celulares das vítimas, possibilitando até saques e transações financeiras.

Durante o cumprimento dos mandados de busca, a polícia encontrou cerca de R$ 556 mil e US$ 4 mil em uma das residências. Os criminosos foram indiciados por fraude eletrônica, associação criminosa e lavagem de dinheiro. De acordo com o delegado, os valores apreendidos são depositados em conta judicial e, após a condenação, o dinheiro vai para ressarcir as vítimas. "Nossa preocupação é sempre ressarcir as vítimas. Prender apenas não adianta. Os bancos não restituem os valores nesses golpes. Imagina você, aposentado, tendo que pagar uma dívida de R$ 200 mil com juros?", argumentou Sallum.

Migração on-line

Dados do *Anuário de Segurança Pública* de 2023 mostram que a cada hora, 208 brasileiros são enganados por criminosos on-line. No total, foram 1.819.409 estelionatos, um aumento de 326,3% desde 2018.

A tecnologia permitiu que a migração dos criminosos para os golpes ficasse mais acelerada. Entre os fatores está um risco menor de prisão e confronto direto com as vítimas, maior lucratividade, facilidade com os mecanismos da internet e a sensação de impunidade. Welliton Caixeta, pesquisador vinculado ao Grupo Candango de Criminologia (GCCrim/FD), explica que, em casos de golpes, geralmente, os criminosos são golpistas de oportunidades, que migram para a internet com a ideia de que não serão rastreados, localizados e detidos, e, por isso ficarão impunes.

"Quanto ao perfil, podemos observar que, na maioria dos casos, são jovens com familiaridade e experiência prática com tecnologia, computador ou outro dispositivo conectado à internet. Dependendo do tipo de crime — por exemplo: pedofilia, calúnia, difamação e injúria — agem como 'lobos solitários'. Já no caso de outros crimes cibernéticos — como compras falsas on-line, fraude de identidades, furto de dados financeiros ou de pagamento com cartão, furto e venda de dados corporativos, ciber extorsão etc. — os criminosos podem agir em grupo, em organização criminosa", exemplifica.

O delegado Henry Galdino, chefe da Divisão de Proteção ao Consumidor da Coordenação de Repressão aos Crimes Contra o Consumidor, a Propriedade Imaterial e a Fraudes (Corf/DPCon), explica que não há um perfil específico desse tipo de criminoso, tendo em vista que eles descobriram a facilidade e a rentabilidade dos golpes eletrônicos. "Todavia, os cabeças das organizações criminosas geralmente são pessoas que conhecem de tecnologia ou pagam para pessoas que conhecem."

Conseguir dados pessoais das vítimas, como telefones, CPF, RG e nome completo não é dificuldade para os estelionatários. "Eles (os criminosos) conseguem em fontes abertas e em plataformas clandestinas de bancos de dados, e, ainda, com colaboradores de instituições financeiras envolvidos nas fraudes", frisa o delegado.

Faça o boletim

Os dados mais recentes da Polícia Civil sobre o total de registros de crimes praticados pela internet são de agosto deste ano, contabilizando 2.197 ocorrências no mês — no número, inclui estelionatos, falsa identidade, ameaça, injúria, furto mediante fraude, difamação, extorsão, calúnia e outros. O crime de estelionato cometido pela internet ocupa o topo do ranking, com 26.253 registros entre janeiro de 2023 e agosto de 2024. Desse total, 10.899 ocorreram somente nos primeiros oito meses deste ano.

A Secretaria de Segurança Pública (SSP/DF) só dispõe de dados de 2022 e 2023. A pasta informou que houve uma queda de 7% nos crimes de estelionato na capital, com 46.548 ocorrências em 2023 contra 50.071 casos de 2022. Mas esse número pode ser bem maior, já que nem todas as vítimas declaram oficialmente o golpe. Levantamento divulgado em agosto deste ano sobre o cenário de golpes e fraudes virtuais, feito pela Koin, fintech especializada em prevenção de crimes em e-commerce, aponta que 62,4% dos brasileiros já sofreram alguma tentativa de golpe virtual — 92,3% delas, por meio de dispositivos móveis, principalmente celulares. E um aspecto relevante é que 64,3% das pessoas não registraram boletim de ocorrência após sofrerem a ameaça, indicando uma possível falta de confiança na resolução do problema ou desconhecimento sobre a importância desse registro.

Em nota, a SSP/DF ressalta que os levantamentos das ocorrências são utilizados na elaboração de estratégias para o policiamento ostensivo da Polícia Militar (PMDF), bem como para a identificação e a desarticulação de possíveis grupos especializados por parte da PCDF. O boletim de ocorrência pode ser feito em delegacias localizadas nas regiões administrativas e também por meio da Delegacia Eletrônica, disponível em *https://www.pcdf.df.gov.br/servicos/delegacia-eletronica*.

Saiba quais são os principais golpes

O **Correio** listou, com base na Federação de Bancos (Febraban), os 12 principais golpes virtuais aplicados por criminosos

Valdo Virgo/CB/D.A Press

Golpe do Pix errado

O golpista envia um Pix para a conta da vítima. Depois, manda uma mensagem ou liga dizendo que o dinheiro foi enviado por engano e solicita à vítima que ela devolva o valor. No entanto, ao invés de dar a chave Pix da transferência original, o golpista fornece uma chave de uma terceira conta. Quando a vítima devolve o dinheiro para essa terceira conta, o bandido aciona o MED (Mecanismo Especial de Devolução) para tentar obter de volta o Pix originalmente enviado à vítima. Se tiver êxito, além de receber o dinheiro enviado pela vítima, o bandido recebe também o valor pelo MED e a vítima fica no prejuízo.

Golpe da falsa central de atendimento

O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual ela tem um relacionamento ativo. Com a desculpa de que a conta do cliente foi invadida ou clonada, o golpista pede os dados pessoais e financeiros da vítima. E até mesmo pede para que ela ligue na central do banco, no número que aparece atrás do cartão, mas o fraudador continua na linha para simular o atendimento da central e pedir os dados da sua conta, dos seus cartões e, principalmente, a senha, quando digitar.

Golpe do falso motoboy

O cliente recebe uma ligação do golpista, que se passa por funcionário do banco, dizendo que o cartão foi fraudado. O falso funcionário solicita a senha e pede que o cartão seja cortado, mas que o chip não seja danificado. Em seguida, diz que o cartão será retirado na casa do cliente e, para isso, um motoboy (outro golpista) aparece onde a vítima está e retira o cartão para fazer transações e roubar o dinheiro.

Golpe da troca de cartão

Golpistas que trabalham como vendedores prestam atenção quando você digita sua senha na máquina de compra e, depois, trocam o cartão na hora de devolvê-lo. Com seu cartão e senha, fazem compras. O mesmo pode acontecer com desconhecidos oferecendo ajuda no caixa eletrônico. Eles se aproveitam de alguma dificuldade no terminal eletrônico para pegar rapidamente o cartão e depois devolver um que não é seu, ao mesmo tempo que espiam a senha.

Golpe da maquininha quebrada

O golpe começa quando a pessoa faz um pedido por aplicativo e, no momento da entrega, é apresentada uma maquininha com o visor danificado ou o golpista se posiciona de uma forma que a vítima não veja o preço cobrado na tela. O valor inserido é bem superior ao pedido e a vítima só percebe que fez um pagamento maior depois de um tempo. Pode ocorrer também quando a pessoa efetua o pagamento pelo app, mas é convencida de que ocorreu um problema e é cobrada novamente ou cobrado algum frete adicional.

Golpe do Whatsapp

Os golpistas descobrem o número do celular e o nome da vítima de quem pretendem clonar a conta de WhatsApp. Com essas informações em mãos, eles tentam cadastrar o WhatsApp da vítima nos aparelhos deles. Para concluir a operação, é preciso inserir o código de segurança que o aplicativo envia por SMS, sempre que é instalado em um novo dispositivo. Os fraudadores enviam uma mensagem pelo WhatsApp fingindo ser do Serviço de Atendimento ao Cliente do site de vendas ou da empresa em que a vítima tem cadastro. Eles solicitam o código de segurança, que já foi enviado por SMS pelo aplicativo, afirmando se tratar de uma atualização, manutenção ou confirmação de cadastro. Com o código, os bandidos conseguem replicar a conta de WhatsApp em outro celular, têm acesso a todo o histórico de conversas e contatos. A partir daí, os criminosos enviam mensagens para os contatos, passando-se pela pessoa, pedindo dinheiro emprestado.

Golpe do falso leilão

Golpistas criam sites falsos de leilão, anunciando todo tipo de produto por preços bem abaixo do mercado. Depois, pedem transferências, depósitos e até dinheiro via Pix para assegurar a compra. Geralmente eles apelam para a urgência em fechar o negócio, dizendo que a vítima pode perder os descontos, mas nunca entregam as mercadorias pagas. Além disso, os fraudadores podem se aproveitar para roubar informações importantes, como CPF e número de conta das vítimas.

Golpe do link falso

O phishing, ou pescaria digital, é uma fraude eletrônica cometida pelos fraudadores (engenheiros sociais) que visa obter as senhas e dados pessoais do usuário. A forma mais comum de um ataque de phishing são as mensagens em e-mails, SMS, aplicativos de mensagens como WhatsApp, redes sociais que induzem o usuário a clicar em links maliciosos. Também existem páginas falsas na internet que induzem a pessoa a revelar as senhas e dados pessoais.

Golpe do acesso remoto ou mão fantasma

O fraudador entra em contato se passando por um falso funcionário do banco e informa que há movimentações suspeitas na conta da vítima. Avisa que ela foi invadida, clonada, entre outras artimanhas. Ele diz que, para solucionar o problema, é necessária a instalação de um aplicativo. Mas, se o cliente instalar o aplicativo, o criminoso terá acesso a todos os dados que estão no celular.

Golpe do falso empréstimo

As quadrilhas se passam por falsas instituições financeiras e fazem anúncios oferecendo crédito com condições atrativas na internet. Quando o interessado preenche o cadastro nesses sites, os bandidos entram em contato e enviam um suposto contrato com diversas multas para evitar desistência. E, para que o falso empréstimo seja liberado, pedem um pagamento de taxas e impostos.

Golpe do falso investimento

Golpistas entram em contato com o usuário oferecendo uma série de investimentos com retornos super-rápidos, ou imediatos, e lucros vantajosos em um primeiro momento. À medida que os depósitos vão subindo e o valor é interessante para o golpista, ele some sem retornar o último investimento prometido.

Golpe da restituição do imposto de renda

Os golpistas se passam pela Receita Federal e criam um e-mail falso dizendo que a vítima pode sacar a restituição, mas, para isso, basta clicar no link e seguir o passo a passo. Assim que a vítima clica no link, as informações dela ficam disponíveis para os infratores.

Fonte: Febraban

Orientações aos correntistas

- Suspeite de ligações telefônicas que questionem compras realizadas com o cartão de crédito
- Não forneça por telefone dados pessoais tais como endereço e senha de cartão bancário
- Os bancos não dispõem de serviço delivery, ou seja, não enviam funcionários a residências de clientes para pegar documentos e cartões
- Fique atento às mensagens de solicitação de dinheiro por conhecidos.
- Se a conta bancária informada para depósito de valores estiver em nome de terceiro, a chance de ser fraude é ainda maior
- Desconfie se a fotografia do perfil do WhatsApp estiver vinculada a uma linha telefônica que não esteja cadastrada nos seus contatos.
- Sempre suspeitar de ofertas de investimentos com ganhos acima daqueles praticados pelo mercado bancário regular, ainda que apresentados por empresas com aparente credibilidade, ou por pessoas conhecidas e familiares, que podem estar na base do sistema e por isso receberam algum "rendimento", os fazendo crer na rentabilidade do negócio
- Verificar se existe autorização do Banco Central e fiscalização do Conselho de Valores Mobiliários
- Suspeite de contatos que oferecem voucher/cupom de descontos de restaurantes a serem utilizados em plataformas de delivery
- Não clique no link fornecido nessas conversas antes de confirmar diretamente com o restaurante a veracidade do desconto