Análise socioeconômica dos registros de estelionato digital no Brasil (2018-2022)

Palavras-Chave: crime; estelionato; análise socioeconômica

Autora: Taís Lombardi da Costa, IFCH – UNICAMP

Prof(ª). Dr(ª). Susana Durão, IFCH - UNICAMP

INTRODUÇÃO:

O aumento de registros dos crimes de estelionato digital nos últimos anos levanta alarde exigindo respostas e possíveis soluções para uma realidade digital segura para todos. Porém, o mundo tecnológico não é estático e sofre mudanças a todo momento, como a massificação de novas tecnologias, por exemplo a Inteligência Artificial (IA), e também a criação e implementação de sistemas complexos e de grande escala como o PIX - sistema de pagamento online brasileiro. Portanto, para investigar o crescimento de crimes no ambiente digital se faz necessário também olhar para o avanço da tecnologia e suas respectivas formas de acesso pela população.

Diante do impacto causado pela pandemia da COVID-19, a tecnologia se transformou e se recriou para suprir as demandas causadas pelas políticas de distanciamento digital, revelando as consequências e efeitos, tanto positivos quanto negativos, que o seu uso intensivo pode causar. No que se refere à segurança pública, é notável que tanto o avanço como a relação com os meios tecnológicos impactaram o mundo do crime e a segurança social e privada.

Assim, para investigar os aspectos socioeconômicos de estelionato digital entendo como necessário não apenas a investigação do perfil dos criminosos e das vítimas, mas também as características do ambiente em que tal prática ocorre.

METODOLOGIA:

Para a realização da pesquisa foram utilizadas referências quantitativas e qualitativas.

Sobre as referências quantitativas, foram utilizados os dados do Anuário de Segurança Brasileira (Fórum Brasileiro de Segurança Pública) e os dados da PNAD (Pesquisa Nacional por Amostra de Domicílios). Os dados de ambas as pesquisas foram mesclados com a intenção de identificar possíveis padrões de vulnerabilidades. Usando como referência as UFs brasileiras, foram comparados os casos de registros de estelionato digital e dados socioeconômicos como características do acesso à internet, educação e demografia entre 2018 e 2022.

Sobre as referências qualitativas, foi feito um levantamento de textos acadêmicos a respeito da prática de estelionato digital, crimes em ambientes online e característica do uso e acesso a internet no Brasil e no cenário internacional. Também, foi feito um levantamento de notícias sobre estelionatos digitais entre 2018 e 2022 na plataforma de notícias G1. Além disso, documentários e vídeos sobre crimes online e estelionatos digitais também foram assistidos.

Houve também a observação em grupos online no Telegram e Reddit sobre golpes na internet e o acompanhamento de páginas no Instagram sobre o mesmo tema.

RESULTADOS E DISCUSSÃO:

Características sobre acesso a internet

A pesquisa apontou dois fatores principais para a execução do crime de estelionato digital:

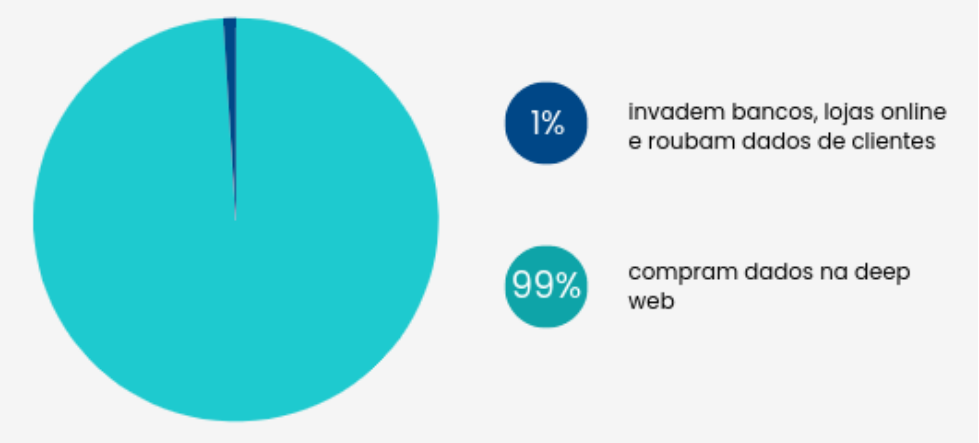
1. Conexão com a internet, tanto por parte da vítima como por parte do criminoso;
2. A manipulação sofrida parece estar associada ao tipo de dispositivo utilizado pela vítima

Essa conclusão se deu a partir da análise das estratégias dos crimes cometidos. No caso brasileiro, as formas mais frequentes desse tipo de crime são: criminoso(s) se passando por funcionário(s) de um banco ou instituição financeira e induzindo a vítima a perda monetária; sites de compras falsos; manipulação por mensagens de texto e áudio que induzem a vítima a ter perda financeira. Outro elemento constatado foi que na maior parte das vezes a vítima recebeu mensagens e/ou ligações pelo celular enquanto estava sob manipulação; estava navegando em sites ou redes sociais pelo celular e encontrou ofertas imperdíveis ou produtos de alto valor sendo anunciados a preços baixos. Nos casos em que o criminoso finge ser um parceiro amoroso é frequentemente mencionado que o criminoso e vítima se falavam por aplicativos de mensagem diariamente e em alguns casos quase o dia todo, há casos em que esse contato dura algumas semanas e outros que duram anos. Assim, foi entendido que a grande maioria dos estelionatos digitais praticados foram pensados para ser executados através de plataformas e aplicativos de celular. Sendo assim, foi possível especular que as potenciais vítimas desse tipo de crime são usuárias de smartphones com acesso a internet. No Brasil, os dados da PNAD de 2022 mostram que 94,3% dos brasileiros afirmaram utilizar a internet diariamente de forma habitual e que o celular era o principal equipamento de acesso (98,9% dos usos comparado aos outros dispositivos). Portanto, foi compreendido que a prática de estelionato digital também pode ser entendida como um reflexo da realidade digital brasileira. As estratégias dos crimes praticados parecem não ser apenas fruto de uma engenhosidade por parte dos criminosos, mas também, um reflexo das formas de uso da internet pelos brasileiros. Em outras palavras, os golpes parecem ocorrer com mais frequência através dos app mais utilizados pelo brasileiro não porque há uma preferência por parte dos criminosos em montar esquemas de golpes

para essas plataformas, mas sim, porque é lá onde os brasileiros estão na maior parte de seu tempo e é lá onde os criminosos procuram se infiltrar para localizar e manipular suas potenciais vítimas.

Perfil dos criminosos

Foi constatado que os criminosos que aplicam estelionato digital agem sozinhos ou em grupo. Devido a facilidade de entrada nesse tipo de prática (um investimento em torno de R$80,00 à R$300,00), diferentes tipos de pessoas iniciam no mundo do crime digital por diferentes motivos e visando diferentes metas. Mesmo com a grande variedade dos perfis é possível dividi-los em dois grupos:



O grupo que representa 1% é composto por pessoas que detém conhecimento especializado em tecnologia da informação e programação e o usam para roubar dados sensíveis. Enquanto os outros 99% é formado por uma massa heterogênea de pessoas que compram os dados roubados pelo primeiro grupo. Aqui se encontram pessoas que têm letramento digital em nível básico, outras com conhecimento especializado em tecnologia e algumas já pertencentes ao mundo do crime, mas todas com uma mesma intenção: aplicar golpes a partir dos dados roubados. A aplicação dos golpes juntamente com as técnicas de engenharia social podem ser aprendidos através de cursos vendidos em plataformas de ensino como Hotmart na surface web e demais fóruns na deep web.

Segundo as informações encontradas, os criminosos frequentemente apreendidos pertencem ao grupo dos 99%, em grande maioria do sexo masculino e com faixa etária predominante entre 20-30 anos, os que não estão dentro dessa faixa de idade comumente são jovens com menos de 18 anos.

Os principais motivos que atraem potenciais estelionatários são: pessoas sem perspectiva de carreira/emprego; vêem o êxito de outras pessoas e se sentem motivados a tentar também; baixo investimento para começar; começa fazendo poucas operações, obtém êxito e passa a realizar cada vez mais golpes (comum nesses casos convidar outras pessoas para poderem atuar em conjunto); como uma renda extra. Porém, independente do motivo, aquele que decide praticar tais atos entra para o mundo do crime, ameaçando a ordem digital e causando danos às vítimas.

Perfil das vítimas

Observando a partir das UFs brasileiras, segundo os dados da PNAD juntamente com os dados

de registros de estelionato digital no Anuário Brasileiro de Segurança, as desigualdades sociais não parece ser a única determinante que condiciona a vulnerabilidade da vítima, pois tal tipo de crime se utiliza mais da falta de atenção e da(s) técnicas utilizadas no momento da manipulação. Sendo esses dois fatores totalmente possíveis de serem modificados e manipulados para serem aplicados em qualquer tipo de golpe com qualquer perfil de vítima.

Devido aos avanços da Inteligência Artificial e da engenharia social, os crimes de estelionato digital tem se tornado cada vez mais convincentes e mais difíceis de serem detectados. A clonagem de voz e imagem tornou possível gerar conteúdos diversos com alta qualidade permitindo que criminosos alterem suas verdadeiras identidades sem levantarem suspeitas. Por outro lado, a engenharia social é um tipo de ataque que explora a confiança e o comportamento humano. Juntando tais possibilidades que a tecnologia oferece juntamente com os princípios da engenharia social, nota-se o aprimoramento de algumas técnicas, como por exemplo a captação de dados e informações relevantes sobre a vítima; o acompanhamento online e muitas vezes em tempo real de atividades e/ou localizações em que a vítima executou ou esteve; contato com a vítima, por troca de mensagens, emails, áudios e/ou vídeos, possibilitando a comunicação a distância. Aqui retomo o ponto discutido anteriormente sobre smartphones, no Brasil mais de 90% da população têm celular e o utilizam como meio principal para acessar a internet, além disso o brasileiro passa aproximadamente nove horas diárias usando o aparelho, esses dados demonstram que a comunicação constante a distância por meio online tem alta probabilidade de acontecer, lembrando que a comunicação verbal ou não é o elemento constituinte da manipulação.

Porém, para além da tecnologia, há também as desigualdades sociais. As baixas condições financeiras e nível de escolaridade tornam determinados grupos mais vulneráveis a diferentes tipos de violência, defendo que uma dessas violência é o estelionato digital. Mas, ao olhar para o perfil das vítimas (obtido através das notícias selecionadas), nota-se que as pessoas de classe alta e com ensino superior são vítimas tão frequentes quanto as de perfil mais inferior. Também, que pessoas com letramento digital são tão vulneráveis quanto aquelas que são leigas. O triunfo do golpe se deve a boa aplicação da engenharia social, com um levantamento detalhado das características da vítima seus pontos fortes e fracos são identificados, a partir deles uma estratégia é montada explorando suas fragilidades na intenção de encontrar um possível ponto de vulnerabilidade.

Sendo assim, segmentei os dados da vítima de acordo com a faixa etária. Através da observação nos grupos do Telegram e Reddit, descobri que em muitos casos ali narrados, para buscar por possíveis vítimas os criminosos procuram por perfis em redes sociais que contenham um grande número de informações sobre suas vidas pessoais. Ao buscar por tais perfis, utilizam majoritariamente os campos de buscas oferecidos pelas redes sociais: sexo, localização e idade. Como já tinha realizado certas inferências com a localização a partir das UFs, tentei fazer o mesmo com as outras categorias utilizadas pelos criminosos em suas buscas. Percebi que apenas segmentar as vítimas por

sexo não oferecia nenhum dado relevante, mas quando fiz o mesmo com a categoria idade descobri um padrão: certos tipos de golpes acontecem mais com um grupo de idade do que com outros, ou seja, determinados grupos etários estão mais propensos a serem vítimas de um determinado tipo de golpe do que por outros. Isso mostra que, sendo o êxito do estelionato digital marcado pela falta de atenção da vítima, focar nos padrões de comportamento de cada grupo de idade que geram possíveis vulnerabilidades pode ser um caminho possível para mitigar sua eficiência.

CONCLUSÕES:

Diante do aumento de registros de crime de estelionato digital e visando contribuir para a problemática, a presente pesquisa analisa os dados do Anuário Brasileiro de Segurança Pública (Fórum Brasileiro de Segurança Pública), os dados da PNAD (Pesquisa Nacional por Amostra de Domicílios) e os dados de vítimas de estelionato digital publicados em notícias do site G1, para compreender qual o perfil de vítima predominante desse tipo de crime. Os resultados mostram que o perfil socioeconômico da vítima não é a único determinante de vulnerabilidade para tal tipo de delito, pois graças aos avanços tecnológicos, os golpes e manipulações podem ser alterados e implementados para qualquer perfil de vítima. Porém, a pesquisa revela que segmentar as vítimas por idade torna possível identificar padrões de vulnerabilidades. Segundo dados levantados, determinado grupo etário está mais propenso a ser fisgado por certos tipos de golpes do que por outros. Como por exemplo, adolescentes e jovens são mais propensos a cair em golpes de extorsão virtual diante de ameaça, enquanto adultos e idosos são vítimas mais frequentes de golpes de falsos vendedores. Também foi identificado que características sociais do uso e acesso a internet também são fundamentais para o êxito do crime. Usuários de smartphones com acesso a internet e uso frequente de redes sociais são os principais alvos. Sendo assim, a presente pesquisa defende que a compreensão das características sociais do estelionato digital é crucial para a prevenção e combate desse tipo de crime.

BIBLIOGRAFIA

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2024.

Pesquisa Nacional por Amostra de Domicílios (PNAD) 2018-2023. Disponível em: <http://www.ibge.gov.br