COORDENAÇÃO

HIGOR VINICIUS NOGUEIRA JORGE
GAETANO VERGINE

RELATOS SOBRE A INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

2022

EDITORA JusPODIVM
www.editorajuspodivm.com.br

3

FRAUDES BANCÁRIAS PRATICADAS POR MEIOS ELETRÔNICOS – IMPORTÂNCIA DA ANÁLISE DE VÍNCULO NA COGNIÇÃO INVESTIGATIVA

NAYARA CAETANO BORLINA DUQUE

3.1. CONSIDERAÇÕES INICIAIS

Hodiernamente estamos vivendo um momento histórico de desenvolvimento tecnológico onde as mudanças profundas ocorrem em um curto espaço de tempo, e, por reflexo, grande parte das relações interpessoais, sociais e comerciais migraram para os meios eletrônicos.

A título de exemplo, podemos citar os aumentos das reuniões virtuais de trabalho, congressos, palestras e aulas on line; o volume de trabalhadores no regime *home office*; a suspensão das atividades de entretenimento impulsionou os artistas a se apresentarem nas chamadas "lives"; temos a telemedicina (teleorientação, telemonitoramento e teleconsulta); comércio eletrônico; serviços *delivery* etc.

Segundo Relatório Digital 2021, promovido pela "We Are Social" em parceria com a Hootsuite, em janeiro de 2021 cerca de 4,66 bilhões de pessoas[1] em todo o mundo usavam a internet, representando um aumento de 316 milhões (7,3%) do ano anterior. Isto equivale dizer que 59,5% da população mundial agora acessa a rede mundial de computadores.

Outro dado importante é que 66,6% da população global já usa telefone celular. Enfim, o tempo de exposição à rede se multiplicou de forma astronômica.

Neste sentido, diante deste novo cenário digital, houve uma corrida desenfreada, principalmente das empresas de e-commerce em migrar para o ambiente online, e, por vezes, os responsáveis se olvidam de implementar ferramentas de proteção aos *softwares*, *hardwares* e redes que garantam a segurança dos dados, transações e tráfego de informações como um todo, tornando mais vulnerável a segurança dos dispositivos eletrônicos e favorecendo a autuação criminosa.

Assim, na área bancária, o reflexo desta sociedade 4.0, apontou que no ano de 2019, o uso dos canais digitais de serviços tais como transferência, pagamento, extrato, contratação de investimento, contratação de seguros, cresceram 11% em relação ao ano anterior, enquanto as operações pelo *Mobile Banking* tiveram um aumento de 19% no mesmo período (FEBRABAN, 2020).

Com o isolamento social imposto pela Pandemia do COVID19, acredita-se que no ano de 2020 e início de 2021, este número tenha crescido vertiginosamente.

Especificamente no sistema financeiro esta transformação tecnológica representa uma grande mudança nos 4D: democratização, digitalização, desburocratização e desmonetização. Assim, o Open Banking e o Open Insurence são uma realidade brasileira em que os dados bancários passam a pertencer aos clientes e não às instituições financeiras (EXAME, 2019).

Em virtude desse processo, ressalta-se a importância na proteção dos sistemas e de redes privadas e governamentais, uma vez que os serviços não podem sofrer interrupções, vazamento de dados ou

1. Considerar que segundo o Relatório Digital 2021, a população mundial era de 7,83 bilhões de pessoas no início de 2021 (https://wearesocial.com/digital-2021).

serem alvos de outras ações danosas, uma vez que podem provocar sérios impactos social, econômico, político e até à segurança nacional.

A preocupação das ameaças cibernéticas no setor financeiro é tão séria que o Banco Central do Brasil (BCB) publicou a Resolução nº 4.658/2018, que dispõe sobre a Política de Segurança Cibernética e dos requisitos e procedimentos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras. No mesmo sentido há a Circular nº 3.909/2018, específica para as instituições de pagamento, que aborda também interessantes aspectos de segurança cibernética.

Já no ano de 2020, o BCB expediu a Circular nº 3.979 a qual dispõe sobre a constituição e a atualização da base de dados de risco operacional e a remessa ao Banco Central de informações relativas a eventos de risco operacional. No bojo deste documento são definidos o que se entende por "risco" e "incidente cibernético".

Outrossim, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) também aborda a questão do incidente de segurança ou *data breach*, na medida em que impõe responsabilidade ao agente de tratamento (controlador e operador de dados) em adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição ou qualquer forma de tratamento inadequado ou ilícito.

É pertinente ressaltar que a Emenda Constitucional Nº 115/22 passou a incluir na Constituição Federal a proteção de dados pessoais entre os direitos e garantias fundamentais, bem como fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Outra questão relevante é que a Medida Provisória Nº 1.124, de 13 de junho de 2022 alterou a Lei Nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, tendo transformado a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transformado cargos em comissão.

Em observância a estes atos normativos, as empresas além de prever medidas preventivas, também definem planos de ação para eventual incidente de segurança, isto é, Plano de Resposta a Incidentes.

Entretanto, do outro lado da balança dialética, a criminalidade organizada, atenta às inovações tecnológicas, e ponderando os riscos

no envolvimento em crimes patrimoniais praticados presencialmente, em detrimento dos crimes virtuais, aliado as vantagens econômicas potencialmente possíveis, criminosos vêm migrando para a prática de crimes virtuais.

Além disso, os cibercriminosos conhecedores da forte proteção estratégica das empresas, por vezes, preferem atacar os clientes, protagonistas mais vulneráveis, em virtude da carência ou até mesmo ausência de educação digital acerca dos riscos e armadilhas lançadas no ambiente online.

3.2. PARTICULARIDADES RELEVANTES DOS CRIMES CIBERNÉTICOS DE FRAUDE ELETRÔNICA

Os crimes cibernéticos podem ser entendidos como qualquer crime que é facilitado ou cometido utilizando-se um computador, a internet ou dispositivo de hardware (GORDON; FORD, 2006).

Assim, a fraude bancária na web é o subconjunto de uma categoria mais ampla do cibercrime e é definida por Van Gool (2011, p.13) como

> (...) crime cibernético onde o principal objetivo da atividade é o ganho financeiro para o perpetrador por meio de fraude, onde um banco de varejo está envolvido e onde a infraestrutura de TI é usada como o objeto ou ferramenta para alcançar a fraude e onde o envolvimento do navegador da *web* é relevante (**tradução nossa**).

Analisando o grau de conhecimento do atacante no cenário da fraude bancária, temos os *hackers* experientes com altas habilidades em programação, que desenvolvem *softwares* para outros *hackers*, e os comercializam principalmente na *deepweb* ou em grupos fechados.

Além desses, há também os chamados *script kiddies* que são aqueles novatos que não se preocupam em aprender sobre tecnologia e querem apenas baixar as ferramentas dos hackers para entrar nos sistemas de computadores.

E, por último, temos os indivíduos que não têm nenhum interesse e pouco conhecimento em tecnologia, mas que usam o computador apenas como ferramenta que os auxilia a subtrair valores ou serviços (MITNICK, 2005).

Ao abordar sobre os métodos e ferramentas utilizados na execução da fraude bancária *online*, registra-se que necessariamente se requer algum tipo de falha, seja em um ser humano, sistema ou ambos.

Os métodos de ataque são diversos e estão em constante evolução, porém, os mais comuns são:

> ***Phishing*** – uma forma de engenharia social em que o atacante tenta atrair o usuário em uma falsa sensação de segurança, a fim de obter suas credenciais que podem ser usadas em uma transação financeira que não seja pretendida pelo usuário (JAKOBSSON, MYERS, 2006)

Em linhas gerais, o phishing se refere a mensagens que procuram induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros, ou mensagens que, no próprio conteúdo, apresentam formulários para o preenchimento e envio de dados pessoais e financeiros de usuários (DAMIANO, 2013, p.49).

> ***Softwares* maliciosos** - do mesmo modo que os vírus são devastadores para o corpo humano, guardadas as devidas proporções, os vírus de computadores também representam uma praga para os usuários da tecnologia.

Os programas que visam o uso indevido de dispositivo informático mais usuais neste ambiente são:

> ***Worm*** – *software* que executa ação maliciosa por um processo autônomo e automatizado de propagação de código malicioso na rede que se espalha sem a necessidade do usuário;
>
> **Cavalos de troia (*trojan*)** – *malware* projetado para parecer um *software* legítimo a fim de induzir o usuário a baixa-lo, infectando o sistema informático e permitindo espionagem, subtração de informação ou causação de danos.
>
> **Remote acesses trojan (RAT)** - trata-se de um tipo de cavalo de troia em que se dá ao atacante o acesso total ao seu computador, como se ele estivesse sentado no seu teclado. Há possibilidade ainda, de ativar o microfone e a webcam, e capturar tudo o que ocorre no terminal, mesmo que você ache que estes periféricos estejam desligados.
>
> **Redirecionamento de página (*pharming*)** - o atacante cria uma página idêntica à uma página segura do site legítimo.

Naquela tela *fake* há um campo de login que não dá acesso ao sistema de computadores que o usuário está tentando, mas sim, passa o seu login e senha para o criminoso.

***Main-in-the-middle* (MITM)** – homem do meio – infrator intercepta as comunicações entre remetente e destinatário ou assume a identidade do remetente ou do destinatário e se comunica fazendo-se passar por um deles. É uma interceptação ilegal.

As ameaças cibernéticas direcionadas aos sistemas informáticos das instituições financeiras normalmente não são simples e exige-se do atacante um alto nível técnico em cybersegurança, tecnologia da informação (TI), engenharia da computação, etc e, para tanto é preciso muito tempo, dedicação e investimento para buscar identificar a explorar eventuais vulnerabilidades do sistema. Assim, dada a complexidade das camadas de segurança e ferramentas avançadas de proteção e alta capacidade técnica das equipes de resposta a incidentes, a probabilidade de êxito financeiro do cracker é mínima.

Todavia, por outro lado, diante da heterogeneidade dos usuários do sistema financeiro, com diversos níveis de maturidade digital, para burlar as medidas de segurança os criminosos preferem mirar seus ataques nos seres humanos, quer sejam os proprietários dos dados ou terceiros que deles tenham acesso e possa fornecê-los.

Desta forma, os cyberinfratores utilizam a engenharia social para ludibriar as pessoas com e-mails (*spoofing*), SMS e *links* de anúncios com propagandas oferecendo produtos ou serviços com descontos em eletrônicos, eletrodomésticos, viagens, maneiras de melhorar a saúde ou a vida sexual, informações confidenciais, pornografia grátis, brindes, enfim, temas que atraem a atenção de muitas pessoas.

Mensagens para que você atualize o cadastro, redefina senha, são outras formas bastante utilizadas pelos bandidos para atrair suas vítimas.

Muitos ataques de engenharia social são complicados e envolvem diversas etapas e planejamento elaborado, além de combinar o conhecimento da manipulação e tecnologia.

A engenharia social explora a vulnerabilidade humana com ataques visando a permissão em sistema de computadores para acesso e obtenção de vantagens indevidas, assim, não há *firewall*, sistemas

de detecção de intrusos (*Intrusion Detection Systems*) ou dispositivos avançados de autenticação, tais como tokens baseados no tempo ou cartões biométricos inteligentes que irão impedir o golpe.

3.3. DO ECOSSISTEMA DO CRIME ORGANIZADO EM CRIMES ELETRÔNICOS FINANCEIROS

O esquema da fraude bancária no meio cibernético em larga escala, necessariamente precisa da atuação de diversas pessoas com divisão escalonada das tarefas, o que dificulta a identificação de todos os seus componentes. Contudo, é possível que uma única pessoa execute todos os papéis, porém, em razão dos atuais limites de valores estabelecidos pelos bancos para as transações, o bandido terá que realizar poucas operações e em baixo valor para que não seja facilmente descoberto.

Neste contexto, como forma de pirâmide, iremos discorrer acerca dos níveis de atuação das entidades e suas respectivas atuações.

No primeiro nível, no topo da pirâmide, estão os **programadores** que possuem grandes conhecimentos na área de ciência da computação, análise de sistemas e TI e são responsáveis por explorar as vulnerabilidades de um sistema e desenvolver os códigos ou programas maliciosos, já citados no capítulo anterior.

Os programadores não costumam usar suas invenções, logo, as comercializam, principalmente na *darkweb*, para outros cybercriminosos que efetivamente realizam a captura de informações sensíveis como login, senhas e dados creditícios.

A conduta do desenvolvedor do *software* será de partícipe dos delitos que venham a ser consumados a partir do seu programa, ou seja, furto qualificado mediante fraude, estelionato e quiçá, organização criminosa, pois quem, de qualquer modo, concorre para o crime incide nas penas a ele cominadas, na medida de sua culpabilidade (art. 29 do Código Penal).

E, caso não seja possível comprovar que o programa gerado foi utilizado, ainda assim, a conduta será típica e configurará a invasão de dispositivo informático, na figura equiparada (art. 154-A, § 1º do CP).

Como se percebe, a conduta deste arquiteto de sistema é imprescindível para execução criminosa, não obstante, na prática o que se percebe é que, a princípio, ele não possui relação de hierarquia com

a rede criminosa, sendo que sua função se extingue com a venda do programa.

No segundo nível, portanto abaixo dos desenvolvedores de softwares, temos os **coletores** que armazenarão as informações captadas pelo programa malicioso ou uso de outra técnica.

A coleta e armazenamento de dados pessoais há tempos virou um comércio e alimenta uma indústria bilionária. Esta metodologia de coleta de informações pessoais de consumidores, aliado a revenda e compartilhamento de dados é conhecida como "*data brockers*".

Os *data brockers* interagem com as plataformas digitais e capturam nossos dados pessoais de maneira invisível, e muitas vezes com ausência de transparência ou *accountability*, e depois os revendem para empresas especializadas em predizer comportamentos dos consumidores, marketing, serviços de mitigação de riscos ou serviços de busca de pessoas.

De um modo geral, é um comércio lícito, porém sem qualquer fiscalização ou controle governamental, até a chegada da LGPD.

O problema desta mercancia e ausência de supervisionamento é que nossos dados legitimamente coletados, tais como nome, CPF, e-mail, endereço, telefone, podem estar expostos nesses grandes vazamentos de dados, e, por conseguinte, abastecer redes criminosas que os utilizarão para fins ilícitos.

Nesta senda, a partir dos dados pessoais armazenados, os coletores facilmente encaminham SMS, e-mails ou links maliciosos que comprometem os dispositivos eletrônicos e viabilizam a captura de informações financeiras confidenciais.

Em outra camada da organização criminosa estão os **aliciadores,** que tendo a confiança dos coletores, recebe uma porcentagem para exercer a função operacional de cooptar os "laranjas", isto é, angariar, atrair pessoas para emprestarem suas contas, trocar dinheiro em casas de câmbio e serem beneficiárias de boletos fraudulentos, ou até mesmo identificar pessoas dispostas a emprestar documentos e abrir empresas de fachada que servirão para ocultar e lavar as vantagens ilicitamente auferidas com a fraude.

Estas pessoas, também conhecidas como **intermediador, cabeça ou plaqueiro** são extremamente difíceis de serem identificados, pois seus nomes não aparecem claramente como beneficiários, e muitas

vezes, são identificados apenas em cruzamento de transações pós fraude, isto é, os laranjas transferem porcentagens para eles, e esta nominação só vem à tona com a quebra de sigilo bancário, analisando o extrato bancário.

Por derradeiro, na base da pirâmide, e em maior quantidade, estão as pessoas que são as destinatárias finais dos recursos subtraídos e isto pode ocorrer de diferentes formas, tais como: transferência para contas disponibilizadas por terceiros (**laranjas**), em troca de alguma contrapartida; pagamento de boletos de cobrança e de tributos emitidos em nome de terceiros; carga de crédito em cartões pré-pagos emitidos em nome de terceiros, etc.

A conduta dessas pessoas que emprestam a conta para recebimento de valores é crime, pois atuam como partícipes, e mesmo que aleguem desconhecimento, para situações análogas a esta, a doutrina desenvolveu a Teoria da Cegueira Deliberada, que, segundo o Superior Tribunal de Justiça, sua aplicabilidade está condicionada à demonstração "no quadro fático apresentado na lide que o agente finge não perceber determinada situação de ilicitude para, a partir daí, alcançar a vantagem pretendida". (STJ – Agravo Regimental no Recurso Especial nº 1565832/RJ).

Como o crime virtual não conhece fronteiras, os fraudadores utilizam a amplitude do nosso território nacional para praticar o crime em diversos locais de onde se situam fisicamente. Assim, muitas vezes, as entidades de cada camada estão em Estados diferentes, se tornando mais uma pedra no caminho da persecução penal.

3.4. ANÁLISE DE VÍNCULO COMO FERRAMENTA DE AGREGAÇÃO TECNOLÓGICA

Os profissionais da justiça criminal no Brasil (Polícias Civis e Federal, Ministério Público, Defensoria e Poder Judiciário) são os responsáveis pela detecção, investigação, prevenção, mitigação, acusação e julgamento dos crimes cibernéticos.

Nesta toada, especificamente em relação aos profissionais da segurança pública, além das aptidões necessárias para investigar crimes comuns, devem ter conhecimentos especializados, habilidades e atitude para pôr em prática esses conhecimentos técnicos. Tais exigências se fazem necessárias para identificar, obter, preservar e analisar as provas digitais de uma maneira que garanta sua admissibilidade em juízo,

respeitando principalmente a cadeia de custódia, que são exigências impostas pela norma processual penal quando da apreensão da prova, garantindo sua licitude.

Diante da escassez de mão de obra qualificada nesta área, e em contrapartida com a criminalidade organizada cada vez mais sofisticada e em franco crescimento, para otimização dos recursos humanos e materiais, uma das ações esperadas está na necessidade de promover cooperação público-privada, com empresas e órgãos da justiça criminal trabalhando lado a lado com a aplicação da lei.

A cooperação entre todos os espectros da sociedade, entes públicos e privados vem ao encontro de um novo paradigma de enfrentamento sistemático à essa ameaça, aumentando os riscos para os cibercriminosos, pois há um interesse mútuo e benefícios de trabalho juntos em direção a um objetivo comum.

Certo é que, já existem iniciativas colaborativas dos setores, contudo elas são fragmentadas e insuficientes para as necessidades atuais de um cenário de ameaças de crimes eletrônicos em constante evolução.

Outro ponto importante que precisa de aprimoramento é a necessidade na adoção de padrões internacionais e de leis modelos no enfrentamento do cibercrime, por isso, a importância de adesão do Brasil à Convenção de Budapeste, uma vez que a harmonização e a simetria nos procedimentos investigatórios são fatores premente para o sucesso na identificação da autoria e materialidade delitiva.

Na cognição investigativa, uma boa alternativa é utilizar a área da computação para automatizar e acelerar a solução de problemas através de técnicas de Inteligência Artificial, em particular de Aprendizado de Máquina.

Para tanto, a proposta é que exista um Projeto Estadual de combate a fraudes bancárias eletrônicas, em que a Polícia Civil possa dispor, de modo centralizado, de uma base de dados estruturado que, através da sistematização de associação de elementos e identificação de correlação de vínculo, auxilie na cognição policial para tomada de decisões. Isto é, automatização da análise de B*ig Data*[2] de fraudes,

2. O termo Big Data refere-se a situações em que as tecnologias digitais são utilizadas para lidar com grandes e diversas quantidades de dados e às várias possibilidades de combinações, avaliação e processamento desses dados por autoridades privadas e públicas em diferentes contextos (HOFFMANN-REIM, 2021, p.16).

indicando pontos convergentes que posteriormente auxiliarão na identificação do ecossistema de organizações criminosas.

A análise de dados busca dar sentido às informações encontradas, definindo padrões e obtendo conclusões.

As ferramentas disponíveis para compreensão de grande volume de dados também são úteis na medida em que proporcionam uma inteligência visual, pois representam em forma de gráficos, imagens e tabelas toda informação sobre o alvo da investigação, apontando toda relação com outras entidades.

A título de exemplo, temos as seguintes ferramentas de análise de vínculo dispostas no mercado: software "I2" (banco de dados Ibase Analyst´s Notebook, TextChart, Ixa, Pattern Tracer) de propriedade da IBM, o sistema NEXUS, da Dígitro e o WEBTIGER, da Wytron.

Ensina Ferro Junior (2007, p.70) que a análise de vínculo e a técnica baseada em tecnologia da informação, sugere uma moderna metodologia de investigação que amplia a capacidade de visualização da complexidade do crime com recurso gráfico. Prossegue ensinando que:

> Facilita a verificação de elementos associados numa relação em teia complexa, por meio de ligações dos fatos, associações de pessoas, empresas, vínculos de contatos telefônicos, do fluxo financeiro et. Torna possível a construção da informação com significado (conhecimento) para a investigação.

Assim, investigar crimes cibernéticos implica em lidar com relações numerosas, diversificadas e difíceis de analisar e compreender, fazendo com que o sucesso do trabalho policial dependa do uso da tecnologia e da capacidade de analisar e perceber o contexto em sua completude, sintetizando dados distintos e reunindo em só ambiente gráfico para melhor compreensão do esquema criminoso.

3.5. EXPOSIÇÃO DE CASO - OPERAÇÃO FREENET

A operação desencadeada no mês de fevereiro de 2021, teve sua gênese a partir de petição de uma instituição financeira de alto renome nacional, narrando que no início de 2020, quatro contas correntes de clientes pessoas jurídicas, haviam sido invadidas por cibercriminosos, os quais, realizaram diversas transações espúrias, causando um prejuízo em torno de R$ 4 milhões de reais.

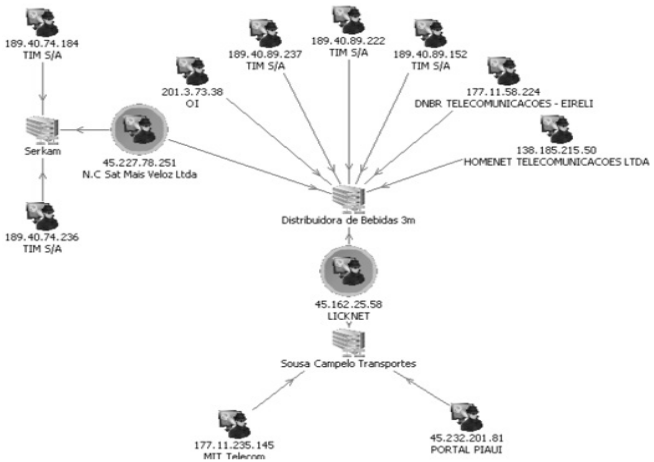
Apurou-se que os ataques investidos consistiram na abordagem das vítimas, principalmente por meio de mensagens via e-mail ou SMS, induzindo a clicar em links maliciosos, a partir daí os dispositivos utilizados eram infectados, e, posteriormente, as credenciais e senhas eram descobertas.

Na posse dos dados sensíveis financeiros, os invasores liberaram o uso de dispositivos pertencentes à quadrilha, possibilitando o acesso e realização de transações financeiras espúrias.

Pois bem, eram quatro vítimas pessoas jurídicas, e o banco apresentou sessenta e oito transações contestadas e seus correspondentes dados capturados pelo sistema bancário.

Neste sentido, utilizando-se de técnicas de investigação criminal tecnológica, por meio de análise de vínculo, foi possível identificar que os registros de conexão (IPs) utilizados para as invasões estavam robustamente correlacionados nos quatro casos.

Segue diagrama ilustrativo inserindo na mesma cena de crime, as empresas vítimas:



Uma investigação cibernética preliminarmente é conduzida por um exame dos arquivos de log, ou seja, os registros de eventos que são arquivos resultantes da atividade do sistema, que podem conter informações sobre o ato delituoso.

Os *logs* de eventos registram automaticamente fatos que ocorrem em um computador propiciando futura auditoria que possa ser

usada para monitorar, entender, diagnosticar atividades e problemas no sistema, e quiçá revelar o IP usado no cybercrime. Um exemplo desses registros são os logs de aplicativos que assimilam eventos que são registrados por programas e aplicações, e os logs de segurança que gravam todas as tentativas de login, tanto válidos quanto inválidos, e a criação, abertura ou exclusão de arquivos ou programas feitos por usuários de computador.

Neste sentido, a primeira linha de investigação foi identificar os infratores que manipularam e acessaram indevidamente as contas bancárias. Para tanto, foram oficiados os provedores de conexão.

Em uma das respostas, a operadora de telefonia móvel, apontou que três IPs foram utilizados por um mesmo cliente, que se tornou nosso primeiro alvo.

No banco de dados policial descobriu-se que este alvo, ainda quando adolescente, foi acusado de ato infracional de furto qualificado, consistente na subtração de cartão bancário, e realização de compras indevidas.

Uma segunda linha de investigação foi direcionada para análise dos beneficiários das movimentações contestadas.

Nesta senda, oficiados aos Bancos para que apresentassem os dados cadastrais dos beneficiários, algumas informações chamaram a atenção, pois alguns elementos identificadores se repetiram, a título de exemplo podemos citar: linha telefônica, e-mail, endereço. E alguns desses dados pessoais, por meio de pesquisas internas no banco de dados policial, claramente demonstravam não corresponder com o beneficiário direto, indicando fortes indícios de que terceiros, com ciência do correntista estavam manipulando as contas agraciadas.

Assim, oficiou-se às instituições bancárias no sentido de informar se aqueles dados do cadastro se repetiram em outras contas não vinculadas à nossa investigação. E a resposta foi frutífera, uma vez que estes dados qualificativos foram identificados em outras contas as quais também já haviam sido utilizadas para recebimento de transferências fraudulentas, indicando seguramente tratarem-se de aliciadores que obtém vantagem indevida por meio de laranjas.

Na sequência, em fontes abertas, principalmente em redes sociais, identificou-se que diferentes investigados eram seguidores uns dos outros, e inclusive haviam fotografias juntos, indicando fortes laços

e vínculos, e por vezes, esbanjando alto padrão de vida incompatível com a renda declarada para Receita Federal.

Em decorrência do cumprimento de onze Mandados de Busca e Apreensão, foram apreendidos diversos aparelhos celulares, quase 50 cartões bancários em nome de diversas pessoas distintas, notebooks, pen drives, máquinas de cartão e chips de celulares.

Sobreleva ponderar, por derradeiro, que na data da operação, em razão de haver prévia autorização judicial para análise e extração dos dados contidos nos equipamentos eletrônicos, foi possível realizar uma prisão em flagrante, pois horas antes o indiciado estava empreendendo investidas em possíveis vítimas de golpes e estava trocando informações de dados qualificativos e números de cartões. Além disso, o preso também possuía um documento falso e com este havia aberto ilicitamente conta em banco digital.

3.6. CONSIDERAÇÕES FINAIS

O crybercrime apresenta características de autuação sem limite territorial, facilidade de comunicação e acesso à informação, e as organizações criminosas exercem suas atividades demonstrando poder de articulação, planejamento e sofisticação, por isso, cada vez mais a atividade policial se depara com situações complexas que exige mais conhecimento para êxito da investigação.

Nesta metodologia investigativa, faz-se necessário cada vez mais procedimentos disruptivos, em razão das características idiossincráticas dos delitos cibernéticos, assim, exige-se novas estratégias de modo a acompanhar as mudanças de paradigmas.

Nesta toada, a investigação tradicional (intuitiva, artesanal, empírica) já não é suficiente, e a atividade de inteligência de segurança pública aliada aos modernos sistemas tecnológicos de suporte à investigação é que são os instrumentos eficazes e aptos a antecipar e agir com celeridade e efetividade diante do fenômeno criminal.

Saber trabalhar a informação é uma condição estratégica e a análise de vínculo representa um elevado poder de identificação das relações ocultas e das variáveis consideradas na conduta delitiva e, principalmente, na complexidade do crime.

Além disso, a análise de vínculo proporciona um melhor entendimento do crime, na medida em que amplia a cognição investigati-