09 de julho de 2025

ZenoX

ANÁLISE DO ATAQUE AO SISTEMA FINANCEIRO BRASILEIRO

ZenoX HQ
Av. Dr. Chucri Zaidan, 1550
BR - São Paulo - SP, 04711-130

ZenoX Ai LTDA
Brazil Headquarter
Av. Dr. Chucri Zaidan, 1550 - Sala 3107 - Vila Cordeiro, São Paulo - SP, 04711-130

contact@zenox.ai
+55 (11) 3382-7396
www.zenox.ai
www.vydar.ai

Sumário

As informações, análises e dados contidos neste relatório foram compilados e derivados exclusivamente a partir de fontes de Inteligência de Código Aberto (Open Source Intelligence - OSINT) e em parceria com jornalistas do site de noticias TecMundo.

Estas fontes incluem, mas não se limitam a:

- Notícias publicadas por veículos de comunicação;
- Comunicados de imprensa oficiais de empresas ou entidades governamentais;
- Postagens e discussões em fóruns públicos, incluindo aqueles localizados na Surface Web, Deep Web e Dark Web (como fóruns de cibercrime e canais de Telegram monitorados);
- Redes sociais e plataformas de compartilhamento de informações;
- Relatórios de segurança e análises publicadas por outras empresas de cibersegurança ou pesquisadores independentes;

Importante:

1. **Natureza da Análise**: A ZenoX não realizou, para a elaboração deste relatório, nenhuma atividade de intrusão, acesso não autorizado, engenharia social ou coleta de informações privadas/proprietárias das entidades mencionadas (incluindo a C&M Software, as instituições financeiras impactadas ou o Banco Central) para obter os dados aqui apresentados. Todo o material base é de origem pública ou semi-pública (como postagens em fóruns de cibercrime), acessível através de técnicas OSINT.

2. **Verificação de Alegações**: As alegações, sejam elas de atores de ameaças (como o conteúdo de mensagens de recrutamento em canais de Telegram) ou de fontes não oficiais (como os detalhes sobre a participação de um insider ou a ocorrência de ataques anteriores), são reportadas conforme encontradas nas fontes monitoradas. A ZenoX, no escopo deste documento, não verificou independentemente a veracidade factual ou a precisão absoluta de cada uma dessas alegações junto às supostas vítimas ou fontes primárias. A inclusão dessas informações visa ilustrar o cenário de ameaças conforme percebido e discutido nos ambientes monitorados.

3. **Limitações Inerentes**: A inteligência derivada de OSINT possui limitações inerentes. A ZenoX não pode garantir a exatidão absoluta, a completude ou a atualidade de todas as informações apresentadas, uma vez que estas dependem intrinsecamente da fiabilidade e da disponibilidade das fontes originais, que podem conter erros, omissões, informações desatualizadas ou propaganda/desinformação. A análise de informações provenientes de fontes não oficiais ou de atores de ameaça está sujeita à sua qualidade e formato originais.

4. **Finalidade do Relatório**: Este documento destina-se a fins informativos, analíticos e de conscientização sobre o ataque ao sistema financeiro brasileiro ocorrido em junho de 2025, suas características, as falhas sistêmicas expostas e seu impacto potencial no cenário de fraudes e segurança cibernética no Brasil, com base em dados e alegações publicamente disponíveis até a data de sua elaboração.

5. **Ausência de Responsabilidade**: A ZenoX não se responsabiliza por quaisquer decisões, ações ou omissões tomadas com base exclusiva nas informações contidas neste relatório. Este documento não constitui aconselhamento legal, técnico específico para remediação de incidentes, financeiro ou de investimento.

6. **Diligência Própria**: Recomenda-se enfaticamente que os leitores realizem suas próprias diligências e verificações independentes antes de tomar decisões operacionais, estratégicas ou financeiras críticas baseadas, no todo ou em parte, neste relatório.

1. Sobre Nós

1.1. ZenoX

A ZenoX é uma empresa líder e pioneira no campo da inteligência artificial contra ameaças digitais, dedicada a moldar um futuro mais seguro, eficiente e inovador para todos. Nossa missão é redefinir os limites da tecnologia, impulsionando avanços significativos que beneficiem uma ampla gama de setores, incluindo cibersegurança, marketing, saúde, finanças e muito mais.

1.2. Foco em Pesquisa e Desenvolvimento

No coração da ZenoX está um compromisso inabalável com a pesquisa e desenvolvimento. Nossa equipe de especialistas em IA está constantemente explorando novas fronteiras tecnológicas, desenvolvendo soluções de ponta que abordam desafios complexos e antecipam as necessidades futuras. Nossa abordagem é caracterizada pela inovação contínua, onde questionamos o status quo e procuramos sempre ultrapassar as limitações convencionais.

1.3. Compromisso com a Inovação e Integridade

Em um mundo onde a tecnologia evolui a um ritmo sem precedentes, a ZenoX se destaca como um farol de inovação e integridade. Nossa dedicação à ética e à excelência nos posiciona como um líder confiável na indústria de tecnologia. Trabalhamos incansavelmente para garantir que nossas soluções não apenas resolvam problemas atuais, mas também estejam preparadas para enfrentar os desafios do futuro.

1.4. Vydar

O Vydar é o pilar central de produtos e serviços de inteligência da ZenoX, destacando-se como uma solução avançada de Threat Intelligence que integra tecnologias de ponta em Inteligência Artificial (IA) e GenAI. Desenvolvido para oferecer uma proteção robusta contra ameaças cibernéticas, o Vydar é essencial na missão da ZenoX de garantir um ambiente digital mais seguro e eficiente para todos os seus clientes.

1.5. Inteligência Artificial e GenAI

No núcleo do Vydar está Tellyu, uma IA generativa conectada a um data lake abrangente. Tellyu analisa grandes volumes de dados, identificando padrões de comportamento suspeitos com alta precisão. Isso permite que o Vydar não apenas detecte ameaças conhecidas, mas também antecipe e neutralize novas táticas e técnicas empregadas por atores maliciosos.

Como o pilar de produtos e serviços de inteligência da ZenoX, o Vydar simboliza o compromisso da empresa em oferecer soluções de segurança cibernética de última geração. Sua integração com tecnologias avançadas de IA e GenAI e sua capacidade de oferecer insights acionáveis tornam-no uma ferramenta indispensável para qualquer organização que busca proteger seus ativos digitais contra ameaças em constante evolução. Com o Vydar, a ZenoX reafirma sua posição de liderança na indústria de tecnologia, garantindo que a segurança e a inovação caminhem lado a lado.

VYDAR
powered by ZenoX

2. Sumário Executivo

O ataque de 30 de junho de 2025 representa um marco na história do cibercrime brasileiro, não apenas pelo valor bilionário subtraído, mas por ter exposto uma vulnerabilidade sistêmica no coração do ecossistema financeiro. Este relatório da ZenoX aprofunda-se na anatomia do incidente que comprometeu a prestadora de serviços de tecnologia (PSTI) C&M Software, revelando que a verdadeira porta de entrada não foi uma falha técnica em uma instituição bancária, mas sim uma sofisticada exploração da cadeia de suprimentos digital, utilizada para acessar as contas reserva de múltiplas instituições financeiras.

A análise da ZenoX, fundamentada em inteligência proprietária, contesta as narrativas iniciais e aponta para um cenário mais complexo. Nossa ivestigação aponta indícios de que o ataque pode ter sido uma operação de fraude doméstica, facilitada por um insider, e não uma investida puramente externa. Aparentemente, houve um recrutamento ativo em canais abertos meses antes do incidente, com o objetivo de corromper funcionários bancários com acesso às tesourarias. As mensagens indicavam planos explícitos para executar operações no BACEN que poderiam atingir o valor de **R$ 1 bilhão**. Além disso, nossa análise revela que este não foi um evento isolado, mas a culminação de uma série de ataques de menor escala que, ao longo do tempo, vinham explorando a mesma fragilidade processual em contas reserva em diversas instituições financeiras no Brasil.

O sucesso deste ataque foi catalisado por quatro falhas sistêmicas fundamentais:

1. A ausência de um monitoramento estratégico do submundo da fraude no Brasil, que ignorou os sinais claros de planejamento;
2. A confiança cega na segurança da cadeia de suprimentos, sem a devida verificação contínua;
3. Uma cultura de silêncio no setor financeiro, que impede o compartilhamento de inteligência entre as vítimas e fortalece os criminosos;
4. A falta de uma inteligência centralizada para conectar os pontos entre incidentes aparentemente isolados e transformá-los em um alerta preditivo.

A conclusão é inequívoca: a era da segurança reativa chegou ao fim. Proteger o ecossistema financeiro agora exige uma mudança de paradigma — rumo a uma defesa preditiva, proativa e guiada por inteligência.

3. Introdução

O cenário de cibersegurança brasileiro testemunhou um divisor de águas na madrugada de 30 de junho de 2025. O ataque coordenado que explorou a infraestrutura da C&M Software, uma empresa prestadora de serviços de tecnologia (PSTI) essencial ao ecossistema financeiro – não foi apenas mais um incidente de segurança. Tratou-se de um golpe potencialmente calculado, com grau de sofisticação e escala sem precedentes, que movimentou ilicitamente valores próximos à 1 bilhão de reais e escancarou as fragilidades inerentes de um sistema financeiro cada vez mais digitalizado e interconectado.

Este evento transcende a narrativa de um roubo cibernético. Ele representa a materialização de um risco sistêmico, onde a segurança de centenas de instituições financeiras se mostrou dependente da resiliência de um único parceiro tecnológico. Ao comprometer um provedor com acesso direto ao coração do Sistema de Pagamentos Brasileiro (SPB), os atacantes demonstraram não apenas profundo conhecimento técnico, mas também uma audácia que redefine o perfil das ameaças digitais contemporâneas.

Na ZenoX, entendemos que este incidente não deve ser encarado como um caso isolado, mas sim como o sintoma mais agudo de um problema muito mais amplo: a crescente sofisticação da fraude financeira e a profissionalização do cibercrime. Nossa análise – que vai além das narrativas iniciais – indica que o colapso foi menos resultado de uma vulnerabilidade de software e mais consequência da exploração de falhas sistêmicas: o risco não gerenciado da cadeia de suprimentos, a ameaça apresentada por insiders e, acima de tudo, **a incapacidade de operacionalizar informações de inteligência já disponíveis.**

Este relatório se aprofunda na anatomia do ataque não apenas para documentar o ocorrido, mas para discutir o problema estrutural da fraude que ele representa. Nos tópicos a seguir, a ZenoX detalha as táticas utilizadas, as falhas exploradas e, sobretudo, apresenta estratégias e abordagens orientadas por inteligência – vitais para proteger a integridade do ecossistema financeiro. Nosso objetivo vai além da análise do passado: buscamos contribuir para a construção de um futuro digital mais seguro, em que a tecnologia atue como escudo, e não como vetor de risco.

4. O Relato da Mídia sobre o Ataque Bilionário

O que hoje é considerado o maior assalto cibernético da história do Brasil teve início de forma silenciosa, nas primeiras horas da madrugada de uma segunda-feira, 30 de junho de 2025. Longe dos holofotes, um grupo de cibercriminosos colocava em prática a fase final de um ataque meticulosamente planejado contra a espinha dorsal de uma parcela crítica do sistema financeiro nacional.

4.1. O Alarme Inicial

Segundo relatos da imprensa, o primeiro sinal de que algo estava terrivelmente errado surgiu por volta das 4h da manhã. Um executivo da BMP Money Plus – uma fintech especializada em *banking-as-a-service* (BaaS) – recebeu uma ligação de um funcionário do CorpX Bank. O motivo era uma transferência via PIX de R$ 18 milhões, originada da conta da BMP e direcionada ao banco, uma operação atípica e não autorizada que imediatamente acendeu o alerta. Ao verificar a situação, o executivo da percebeu que não se tratava de um evento isolado, mas de uma série de movimentações fraudulentas que estavam drenando os recursos da conta reserva da empresa, mantida diretamente no Banco Central. Às 5h, a C&M Software foi oficialmente acionada.

4.2. O Suposto Vetor da Invasão

As investigações e reportagens subsequentes – lideradas por veículos como o *Brazil Journal* – rapidamente apontaram para um ponto nevrálgico: o comprometimento da C&M Software. Embora não seja um banco, a C&M Software atua como uma Prestadora de Serviços de Tecnologia da Informação (PSTI), autorizada e supervisionada pelo Banco Central. Seu papel é fornecer a infraestrutura crítica de conexão e comunicação que permite a centenas de instituições financeiras – especialmente aquelas que não possuem estrutura própria – operarem dentro do Sistema de Pagamentos Brasileiro (SPB).

Inicialmente, acreditava-se que os criminosos haviam explorado uma vulnerabilidade ou utilizado credenciais vazadas para obter acesso remoto ao ambiente da C&M Software. Uma vez infiltrados, eles realizaram um mapeamento minucioso do ambiente e conseguiram acessar artefatos altamente sensíveis: as credenciais e os certificados digitais das instituições financeiras atendidas pela C&M. De posse dessas verdadeiras “chaves do cofre”, os atacantes foram capazes de se fazer passar por essas instituições e assinar digitalmente ordens de transferência — fazendo com que as transações parecessem legítimas aos olhos do sistema.

4.3. A Execução

O ataque foi executado com precisão cirúrgica. Os criminosos injetaram transações fraudulentas diretamente no Sistema de Pagamentos Instantâneos (SPI), tendo como alvo as chamadas "contas reserva" – depósitos que as instituições mantêm no Banco Central para fins de liquidação interbancária. Isso significa que os fundos de clientes finais não foram diretamente acessados; o golpe mirou o capital das próprias instituições financeiras.

As estimativas sobre o valor total desviado variaram significativamente à medida que o caso evoluía e novas informações eram reveladas pela mídia. Inicialmente, reportagens mencionavam valores em torno de **R$ 400 milhões**, mas especulações posteriores apontaram para valores superiores a **R$ 1 bilhão**. O portal *Brazil Journal*, citando fontes preliminares do Banco Central, estimou um desvio de aproximadamente **R$ 800 milhões**, envolvendo pelo menos oito instituições financeiras independentes.

4.4. Lavagem de Dinheiro: A Fuga para as Criptomoedas

Após o saque, teve início uma operação frenética de lavagem de dinheiro. Os valores bilionários foram rapidamente pulverizados via PIX para centenas de “contas laranja”, abertas em nome de terceiros junto a instituições de menor porte — muitas vezes caracterizadas por controles de verificação de identidade (*Know Your Customer*, ou KYC) mais brandos ou falhos.

A partir desse ponto, os valores foram rapidamente convertidos em criptoativos — como Bitcoin (BTC) e a stablecoin Tether (USDT) — por meio de diversas exchanges e mesas de balcão (*over-the-counter*, ou OTC) que operam com PIX. A própria

agilidade do PIX acabou se tornando uma aliada dos criminosos, permitindo uma dispersão acelerada dos recursos e dificultando tanto o rastreamento quanto o bloqueio dos valores. Em alguns casos, o volume atípico das transações levantou suspeitas, levando provedores de criptoativos a bloquear as operações e acionar as autoridades competentes.

4.5. A Resposta das Autoridades e o Impacto Sistêmico

A reação foi imediata e drástica. Em 30 de junho, o Banco Central adotou uma medida preventiva severa: determinou a desconexão total da C&M Software do Sistema de Pagamentos Brasileiro (SPB). Embora necessária para conter a sangria financeira, a ação gerou um efeito cascata, deixando cerca de 300 instituições — que dependiam dos serviços da C&M — temporariamente impossibilitadas de realizar transações, comprometendo suas operações por vários dias.

Em 2 de julho, a Polícia Federal anunciou a abertura de um inquérito para investigar possíveis crimes de organização criminosa, furto mediante fraude, invasão de dispositivo de informática e lavagem de dinheiro. No dia seguinte, 3 de julho, o Banco Central autorizou a retomada parcial das operações da C&M, sob condições rigorosas de monitoramento, sinalizando que medidas de contenção haviam sido implementadas.

A crise escancarou a fragilidade da dependência de terceiros críticos, demonstrando como a falha em um único fornecedor pode gerar risco sistêmico e abalar a confiança em um ecossistema financeiro altamente digitalizado e interconectado.

5. O Ataque como um Caso Clássico de Risco na Cadeia de Suprimentos

Para compreender a verdadeira magnitude do incidente de 30 de junho, é preciso enxergá-lo não como um ataque direto a um banco, mas como uma **sofisticada exploração da cadeia de suprimentos digital** do sistema financeiro. O modelo de negócios do setor financeiro moderno – impulsionado pelo *Open Finance* e pelo boom das fintechs – criou um ecossistema dinâmico e eficiente, mas também profundamente interdependente. Hoje, a segurança de uma instituição não depende apenas de suas próprias defesas, mas da **resiliência coletiva de todos os seus parceiros tecnológicos**.

Este ataque não forçou a porta da frente das instituições financeiras — ele visou a chave que todas elas confiavam a um mesmo guardião.

5.1. Identificando os Elos da Cadeia de Suprimentos

Neste incidente, a cadeia de suprimentos digital era composta por três camadas principais, cada uma com diferentes níveis de acesso e confiança.

1. **O Provedor Crítico (O Elo Comprometido): C&M Software**

   A C&M Software atuava como um verdadeiro hub tecnológico. Na condição de Prestadora de Serviços de Tecnologia da Informação (PSTI), ela não era apenas uma fornecedora – mas um elo crítico, homologado pelo Banco Central. Instituições financeiras relevantes a delegaram uma função essencial: a gestão da comunicação segura e da mensageria criptografada com o Sistema de Pagamentos Brasileiro. Ao fazer isso, confiaram à empresa o acesso a certificados digitais e credenciais sensíveis, necessários para autenticar e assinar transações em seu nome. O alegado comprometimento desse elo permitiu os atacantes se passarem por instituições legítimas dentro da infraestrutura central do sistema financeiro.

2. **As Vítimas da Dependência (O Elo Final): Instituições Financeiras de Vários Perfis**

   As instituições focadas em negócios como *banking-as-a-service*, produtos financeiros ou serviços bancários tradicionais compõem o elo final da cadeia. Ao delegarem uma função técnica crítica a um provedor especializado, adotaram uma prática comum e eficiente no setor. No entanto, o incidente evidenciou um ponto frágil: a segurança dessas instituições era, na prática, limitada pela segurança do fornecedor ao qual confiaram funções sensíveis. Mesmo possuíssem controles internos robustos, contas reservas no Banco Central foram afetadas porque o ataque visou explorar o nível de confiança e o acesso operacional concedido ao provedor crítico. Elas não foram vítimas de uma falha interna, mas da quebra de um elo anterior em sua cadeia de dependência tecnológica.

5.2. As Falhas Estruturais Expostas no Modelo de Confiança

O aparente sucesso do ataque indica falhas estruturais na gestão de riscos da cadeia de suprimentos de TI — falhas que transcendem uma única empresa ou tecnologia.

- **Centralização de risco em um ecossistema descentralizado**

  O setor financeiro avançou rumo à descentralização, com o crescimento de fintechs e bancos digitais. No entanto, paradoxalmente, concentrou um ponto crítico de falha em um número restrito de PSTIs. A segurança de centenas de “raios” (instituições financeiras) estava ancorada na integridade de um único “cubo” (o provedor), revelando um paradoxo sistêmico de concentração de risco.

- **A Ilusão da segurança por delegação**

  O incidente expôs uma mentalidade perigosa: a crença de que terceirizar uma função é o mesmo que transferir o risco. As instituições continuam sendo responsáveis finais pela segurança de suas operações — perante o regulador, o mercado e os clientes. O ataque demonstrou que diligência prévia (*due diligence*) e contratos não bastam. É imperativo adotar práticas de monitoramento contínuo e validação ativa dos controles de segurança dos parceiros críticos, tratando sua infraestrutura como uma extensão direta do próprio perímetro digital.

- **Acesso privilegiado e ausência do princípio do menor privilégio**

  Em certo momento, os atacantes obtiveram acesso aos certificados digitais de múltiplos clientes, o que sugere privilégios excessivos ou segmentação inadequada. Em um modelo de segurança mais maduro — como o *Zero Trust* — o acesso de fornecedores deve ser estritamente limitado ao mínimo necessário. O comprometimento de um ambiente não pode permitir movimentações laterais para ativos de terceiros. A falha em aplicar esse princípio ampliou exponencialmente o impacto do ataque.

Em suma, o ataque bilionário foi menos sobre a genialidade dos hackers e mais sobre a exploração de um modelo de confiança sistêmico ultrapassado. Ele serve como um alerta claro: **a segurança de uma organização é tão forte quanto a do seu parceiro mais vulnerável**. A gestão de risco da cadeia de suprimentos digital deixou de ser uma boa prática — tornou-se um pilar estratégico da continuidade e sobrevivência do negócio.

6. A Análise da ZenoX Sobre o Incidente

Enquanto a narrativa pública se consolida com base em informações oficiais e reportagens da mídia, a plataforma **Vydar Intelligence**, da ZenoX, e seu time de especialistas conduziram uma investigação interna sobre o caso. Essa análise permite correlacionar dados e levantar hipóteses que podem complementar — ou, em alguns casos, desafiar — as conclusões iniciais.

As informações e análises apresentadas neste tópico baseiam-se em indícios, inteligência em desenvolvimento e eventos publicamente noticiados, cuja veracidade final depende da apuração pelas autoridades competentes. Nenhuma das hipóteses aqui descritas constitui afirmação definitiva de culpa ou conexão direta entre as partes mencionadas. O objetivo é exclusivamente promover a análise de risco e aprofundar a compreensão do cenário de ameaças.

6.1. O Perigo dos Relatórios Precipitados: Por que a Cautela na Análise é Crucial

No vácuo de informações que se segue a um incidente de grande escala, instala-se uma corrida natural por explicações. Empresas de segurança, consultorias e veículos de mídia buscam fornecer respostas rápidas. No entanto, **relatórios baseados em informações parciais ou teorias não corroboradas podem ser mais prejudiciais do que úteis** — gerando ruído, induzindo ações precipitadas e levando organizações a se protegerem contra a ameaça errada.

Um exemplo claro neste caso foi a hipótese, levantada em análises iniciais, de que o **ataque teria sido viabilizado por meio da exploração de uma vulnerabilidade conhecida no Apache ActiveMQ**. A teoria parecia plausível à primeira vista, já que o ActiveMQ é uma tecnologia de mensageria amplamente utilizada na comunicação entre PSTIs e o Banco Central. Essa especulação levou muitas equipes de segurança a uma mobilização reativa — e, como se demonstraria depois, possivelmente equivocada — focada em auditorias e aplicação de patches para um vetor que talvez nem tenha sido explorado.

A narrativa mudou drasticamente em 4 de julho, com a divulgação da prisão de um suspeito em São Paulo pela Polícia Civil. Segundo os relatos, o indivíduo seria um funcionário ou ex-funcionário da C&M Software, acusado de ter recebido valores para facilitar o acesso dos criminosos ao ambiente interno da empresa.

Caso essa linha de investigação se confirme, ela desmonta a teoria da vulnerabilidade externa e revela um cenário ainda mais complexo e sensível: **um ataque facilitado por um insider**. Nesse caso, o vetor de ataque real não teria sido uma falha técnica, mas uma quebra de confiança humana — agravada por falhas nos controles de acesso e na supervisão de pessoal interno.

Isso tudo favorece a conclusão de que a verdadeira inteligência de ameaças não está apenas na velocidade da resposta, mas na precisão da análise — garantindo que as ações de mitigação sejam direcionadas ao ponto certo de ruptura.

6.2. De Atacante Internacional a Fraude Doméstica: A Pista do Insider

A notícia da prisão de um suposto funcionário ou ex-funcionário da C&M Software, que teria recebido pagamentos em espécie, entregues por motoboy, para facilitar o acesso inicial, enfraquece consideravelmente a hipótese de um ataque conduzido exclusivamente por um agente externo e internacional.

Nossa análise indica que, embora a participação de um ator externo não possa ser descartada, a estrutura do golpe apresenta **fortes indícios de uma fraude com componentes essencialmente nacionais**. O grau de conhecimento necessário para transitar pelas complexas burocracias do Sistema de Pagamentos Brasileiro, identificar gargalos nos processos de liquidação e compreender a dinâmica de confiança entre PSTIs e o Banco Central impõe uma barreira de entrada extremamente alta para quem não tem experiência direta no ecossistema financeiro brasileiro.

Caso a atuação de um insider se confirme, ele se configura como o elemento-chave que tornou a operação viável, convertendo um plano audacioso em um golpe executável. Isso desloca o foco do suposto arquiteto principal: de um “hacker” anônimo operando do exterior para um fraudador – ou grupo – com base no Brasil, especializado em ataques sofisticados e com capacidade de recrutamento e execução logística em território nacional.

6.3. Ataque Oportunista ou Plano Bilionário? A Contradição sobre a Escala

Uma segunda linha de investigação levanta dúvidas sobre a intenção original dos criminosos. **Há suspeitas de que o sucesso da operação possa ter superado até mesmo as expectativas dos próprios atacantes.** A aparente dificuldade na fase de lavagem dos recursos, com a pulverização de valores que acabou gerando alertas em exchanges, e o valor supostamente pago ao insider, que embora elevado, parece desproporcional ao montante final subtraído, sugerem a possibilidade de um plano que ganhou escala de forma oportunista.

Contudo, informações obtidas por nossa inteligência interna levam a acreditar em uma situação diversa e apontam para um ataque possivelmente concebido, desde o início, com o objetivo de alcançar valores na casa do bilhão. A complexidade da invasão e o grau de detalhamento no mapeamento do ambiente da C&M sugerem meses de preparação e reconhecimento. **Cremos que o plano sempre foi extrair o maior valor possível que as contas reserva pudessem suportar**. A falha na etapa de lavagem, portanto, pode ter sido fruto de um erro de cálculo logístico — e não de uma surpresa com o volume obtido.

6.4. O Recrutamento Ativo de Insiders

Corroborando a hipótese da atuação de um insider e de um planejamento prévio, é crucial analisar mensagens — incluindo conversas e sinais — compartilhadas em grupos do Telegram nos meses que antecederam o ataque. É importante destacar que a ZenoX **não pode, neste momento, confirmar uma ligação direta** entre essas mensagens e o incidente envolvendo a C&M Software. Ainda assim, tratam-se de elementos relevantes de inteligência, especialmente por conterem menções a instituições como o Banco Central e valores que, segundo os interlocutores, poderiam chegar à casa de R$ 1 bilhão.

Mesmo na ausência de uma conexão comprovada com o caso, o fato de agentes suspeitos, atuando em grupos voltados à fraude, estarem recrutando para operações supostamente direcionadas ao Bacen — com expectativas explícitas de movimentações bilionárias — configura, no mínimo, uma coincidência significativa.

Em canais abertos do Telegram monitorados pela Vydar Intelligence, já em **maio de 2025**, identificamos agentes de ameaça conduzindo um recrutamento explícito e alarmante:

- **Busca por insiders em posições-chave**: Os recrutadores procuravam abertamente por “gerentes bancários de grandes bancos físicos com acesso direto às contas da tesouraria”.

- **Capacidade operacional definida**: O objetivo era claro, realizar transferências (TEDs) de valores extremamente elevados, “a partir de R$ 50 milhões” e “capacidade de até R$ 1 bilhão”.

  Conexão com o Banco Central: Em tom ainda mais ousado, os recrutadores demonstravam “interesse em trabalhos diretamente ligados ao pessoal do Banco Central (Bacen)” e prometiam uma “operação rápida e discreta junto com o pessoal do Bacen”.

- **Ofertas de pagamento milionárias**: A proposta para corromper os insiders era direta e agressiva: “Pagamento 30 milhões. Exemplo: 5 milhões pro intermediário e 25 milhões pro gerente”.

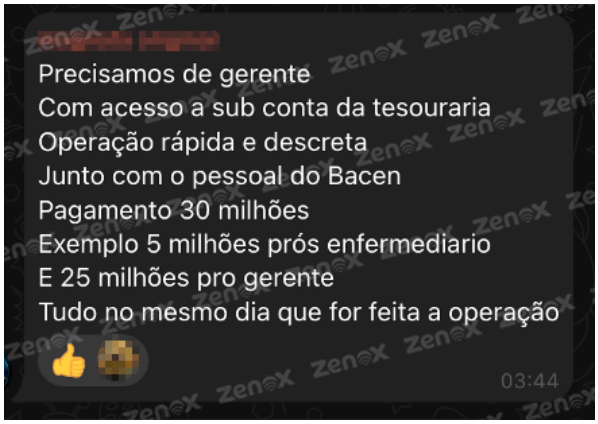

Figura 1 - Suposta Mensagem de Recrutamente para **Ataque ao Bacen em Maio de 2025.**

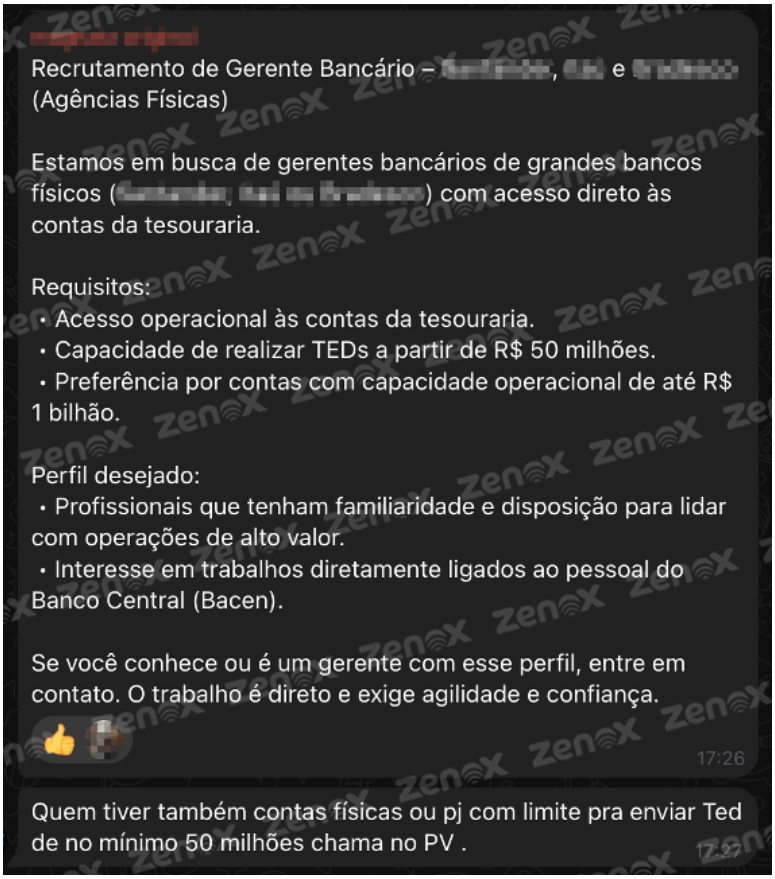

Figura 2 - Suposta Mensagem de Recrutamente para **Ataque ao Bacen em Maio de 2025.**

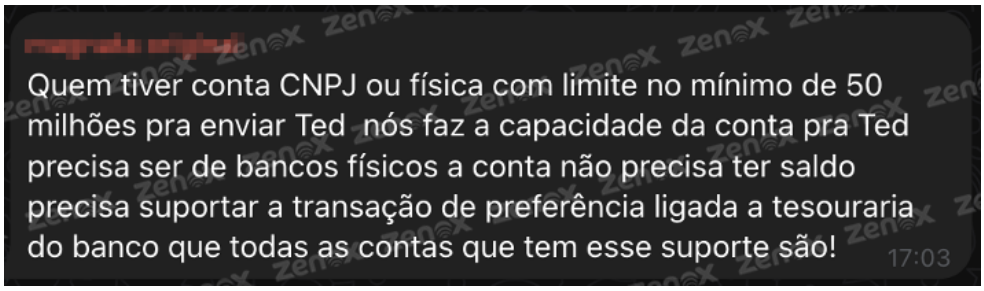

Figura 3 - Supostas Mensagens de Recrutamente **para Ataque ao Bacen em Maio de 2025.**

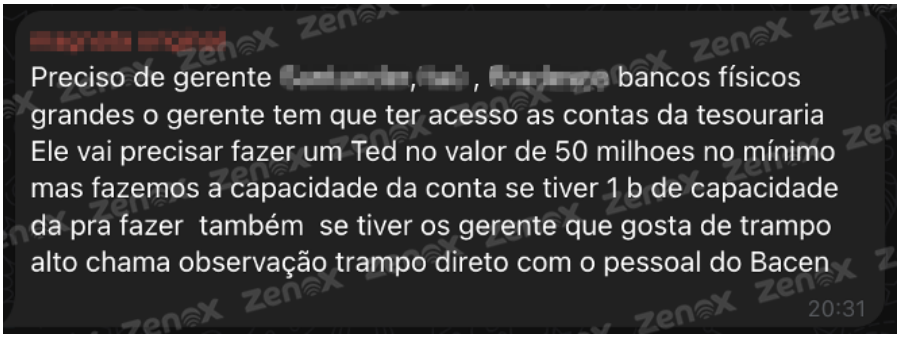

Figura 4 - Supostas Mensagens de Recrutamente para **Ataque ao Bacen em Maio de 2025.**

Independentemente de uma ligação direta com este caso, essa inteligência é irrefutável: a estratégia de recrutar funcionários de alto escalão em bancos e, possivelmente, no próprio órgão regulador para a execução de fraudes bilionárias não é mera especulação. Trata-se de um plano real, que já estava em fase de recrutamento no ambiente underground.

O ataque de 30 de junho pode ter sido, ou não, a concretização bem-sucedida de um desses esquemas que vinham sendo articulados de forma aberta.

6.5. Este Não Foi o Primeiro Ataque às Contas Reserva

A análise da ZenoX, com base em fontes de inteligência cujas informações ainda aguardam validação oficial, indica que o ataque de 30 de junho, apesar de sua escala sem precedentes, não foi um evento isolado nem a primeira vez que este *modus operandi* foi utilizado no Brasil. **Ao contrário, tudo indica que ele seja a culminação de uma série de ataques menores que vêm sendo executados nos últimos meses.**

Nossas pesquisas e inteligências apontam que incidentes com características semelhantes foram reportados às autoridades em diferentes estados do país. Somente em São Paulo, teriam ocorrido pelo menos três ataques recentes a instituições financeiras distintas, todos explorando a mesma brecha fundamental: **a transferência de valores a partir de contas reserva.**

O que torna esse padrão ainda mais preocupante é a diversidade dos vetores de entrada observados nos casos anteriores. Alguns exploraram falhas técnicas em sistemas, outros utilizaram meios distintos de acesso não autorizado. A semelhança entre eles não estava no modo de entrada, mas no objetivo final: uma vez dentro da rede, o foco era sempre o mesmo.

Isso nos leva a uma hipótese crítica: **um ou mais grupos de ameaça teriam identificado — e começado a explorar sistematicamente — uma possível fragilidade nas regras de negócio que regulam as transferências a partir de contas reserva no Brasil.**

Essa não seria uma vulnerabilidade de software, no sentido tradicional, passível de correção com um patch. Trata-se, ao que tudo indica, de uma falha de processo, de lógica de autorização ou da ausência de verificações mais robustas em transações desse tipo. Os criminosos parecem ter percebido que, com o nível certo de acesso privilegiado, o caminho para movimentar fundos diretamente das contas de liquidação interbancária apresentava pouco atrito e alto retorno.

Sob essa ótica, **o ataque contra a C&M Software não representaria a descoberta da falha — mas sim sua industrialização**. Em vez de atacar bancos individualmente, os criminosos teriam mirado um alvo muito mais estratégico: um provedor de tecnologia (PSTI) que lhes daria acesso simultâneo às contas reserva de diversas instituições. Com isso, o golpe ganharia escala e poderia atingir valores bilionários.

7. As Falhas Sistêmicas que o Ataque Revelou

O ataque bilionário de 30 de junho não foi um raio em céu azul. Foi a consequência inevitável de um conjunto de falhas sistêmicas, culturais e estratégicas que há muito tempo fragilizam o ecossistema financeiro brasileiro. Isso fortalece nossa visão, de que focar apenas no incidente é tratar o sintoma, não a causa. A seguir, observa-se os quatro problemas fundamentais que permitiram que este ataque não apenas ocorresse, mas alcançasse uma escala tão devastadora.

1. A Cegueira Proativa: A Falta de Monitoramento Estratégico do Submundo da Fraude

O problema mais gritante é a falha na inteligência proativa. O plano para um suposto ataque de grande escala ao sistema financeiro, com movimentações que poderiam chegar a R$ 1 bilhão, não era segredo bem guardado. Relatórios indicam **mensagens de recrutamento de insiders circulando abertamente no Telegram quase dois meses antes do ataque** — um sinal que, mesmo sem confirmação de vínculo direto com o caso, merecia atenção.

Isso significa que havia tempo suficiente para que o Banco Central e sua cadeia crítica de fornecedores, especialmente as PSTIs, se preparassem. A ausência de um monitoramento sério e contínuo dos grupos de fraude que operam no Brasil, com profundo conhecimento das particularidades do sistema nacional, representou uma cegueira estratégica. Uma inteligência de ameaças mais estruturada poderia ter transformado esses indícios em alertas acionáveis, elevando o nível de prontidão e, possivelmente, impedindo o ataque antes mesmo de sua execução.

2. A Confiança Cega na Cadeia de Suprimentos (Supply Chain)

O incidente é a materialização de um dos maiores pesadelos em gestão de risco: a falha catastrófica em um elo da cadeia de suprimentos. O setor financeiro moderno depende da delegação de funções críticas a parceiros especializados. No entanto, a confiança depositada nesses fornecedores tem sido, muitas vezes, excessiva e pouco verificada. A segurança foi tratada como um item contratual, e não como uma responsabilidade conjunta, que exige auditoria contínua. A mentalidade de "contratar e esquecer" se mostrou um erro grave. Na prática, as defesas de dezenas de instituições estavam niveladas pela segurança do fornecedor mais vulnerável.

3. A Cultura do Silêncio: O Isolamento que Fortalece o Inimigo

No setor financeiro, a reputação é um ativo valioso. Por receio de prejuízos à imagem, penalidades regulatórias ou perda de confiança do mercado, é comum que instituições financeiras que sofrem ataques escolham o silêncio. Esse isolamento enfraquece a capacidade coletiva de resposta. As táticas, técnicas e procedimentos (TTPs) utilizados pelos atacantes acabam ficando restritos à instituição que sofreu o ataque, impedindo que outras se preparem ou aprendam com o ocorrido.

Essa cultura do silêncio cria o ambiente ideal para os criminosos. Eles atacam uma instituição, aprendem com os erros e repetem a estratégia na próxima, que permanece completamente alheia ao risco iminente. Essa falta de compartilhamento de informações impede a criação de uma defesa coletiva mais robusta — algo que poderia funcionar como uma espécie de "imunidade de rebanho" cibernética.

4. O Elo Que Falta: A Ausência de uma Inteligência Centralizada e Acionável

Todos os problemas anteriores convergem para uma falha central: **a inexistência de um hub de inteligência de ameaças que concentre, analise e dissemine informações relevantes em tempo hábil.**

A informação de que múltiplos ataques a contas reserva já haviam sido registrados em diferentes estados era o ponto A. As mensagens de recrutamento para um golpe de R$ 1 bilhão, circulando na dark web e em canais abertos de Telegram, eram o ponto B. Sem uma estrutura centralizada para ligar esses pontos, cada instituição permaneceu isolada — **cega ao padrão que estava se formando.**

Se esse tipo de central existisse, os ataques menores teriam sido documentados, o *modus operandi* identificado, e, ao serem cruzados com os sinais captados em canais de recrutamento, um alerta prioritário poderia ter sido disparado a todo o sistema financeiro com semanas ou até meses de antecedência. Algo como: "**Atenção: Atores de ameaça estão ativamente explorando uma brecha processual em transferências de contas reserva. Recomenda-se a revisão imediata de todos os**

controles de segurança em torno deste processo, tanto internos quanto em seus provedores de tecnologia.". A ausência desse elo pode ter sido o que deixou a porta aberta para o maior roubo cibernético da história do país.

8. Recomendações

A análise deste incidente deixa claro que a prevenção de um futuro ataque de escala semelhante não virá de soluções paliativas ou de um reforço isolado nas defesas técnicas. Será necessário repensar de forma estrutural a maneira como o ecossistema financeiro brasileiro trata a segurança. As recomendações da ZenoX estão organizadas em três pilares estratégicos, voltados a corrigir as falhas sistêmicas na raiz do problema.

Pilar 1: Adoção de Inteligência de Ameaças Acionável (CTI)

A defesa reativa se mostrou insuficiente. O futuro da segurança está na capacidade de antecipar os movimentos do adversário.

- **Monitoramento Contínuo do Submundo da Fraude**

  Instituições financeiras, PSTIs e o próprio Banco Central devem investir em capacidade de inteligência ativa para monitorar ambientes onde fraudadores brasileiros operam — fóruns na dark web, mercados ilegais e canais de Telegram. Se os sinais de recrutamento para um suposto ataque bilionário, que estavam visíveis meses antes, tivessem sido captados e analisados, o desastre talvez pudesse ter sido evitado.

- **Inteligência Focada em Insiders e Credenciais Vazadas**

  A estratégia de segurança precisa reconhecer que a ameaça interna pode ser tão ou mais perigosa que a externa. É fundamental monitorar continuamente vazamentos de credenciais corporativas e indicadores de aliciamento de funcionários em grupos criminosos, permitindo respostas rápidas e preventivas.

- **Plataformas de CTI como a Vydar da ZenoX**

  Organizações devem adotar soluções de inteligência que não apenas coletem dados, mas usem inteligência artificial para cruzar sinais e transformar ruído em alertas claros, preditivos e acionáveis. Isso permite enxergar os riscos antes que eles se tornem incidentes.

Pilar 2: Gestão de Risco da Cadeia de Suprimentos (Third-Party Risk Management)

A confiança, por si só, não é uma política de segurança. Ela precisa ser conquistada e, continuamente, verificada.

- **Da Diligência Prévia ao Monitoramento Contínuo**

  O modelo de “contratar e esquecer” precisa dar lugar a um ciclo de acompanhamento permanente. Instituições financeiras devem ter visibilidade contínua sobre a postura de segurança de seus fornecedores, tratando a infraestrutura terceirizada como uma extensão de seu próprio perímetro.

- **Mandato Contratual e Auditoria de Controles Essenciais**

  Acordos com PSTIs e outros parceiros críticos devem incluir, de forma clara, exigências técnicas como a adoção de arquiteturas Zero Trust, Autenticação Multifator (MFA) resistente a *phishing* e monitoramento detalhado de acessos privilegiados, além de auditorias regulares para garantir conformidade.

- **Revisão do Modelo de Acesso a Contas Reserva**

  A lógica de negócio que permite transferências a partir de contas reserva precisa ser reavaliada com urgência. A introdução de camadas adicionais de verificação pode reduzir riscos e dificultar que um único ponto de falha, seja ele humano ou técnico, comprometa grandes volumes financeiros.

Pilar 3: Criação de um Ecossistema de Inteligência Colaborativa

O isolamento fortalece o adversário. A colaboração fortalece a defesa. É preciso quebrar a cultura do silêncio.

- **Estabelecimento de um Hub Centralizado de Compartilhamento de Ameaças**

Seja liderado pelo Banco Central ou por uma entidade como a FEBRABAN, é fundamental criar (ou reforçar) um centro de inteligência setorial — um ISAC (Information Sharing and Analysis Center) — voltado ao compartilhamento ágil de informações. Ele deve receber relatos de incidentes, conectar os pontos entre diferentes eventos e emitir alertas em tempo real para todo o setor.

- **Anonimização e Padronização de Dados**

  Para vencer a resistência ao compartilhamento, os dados devem ser anonimizados e tratados de forma padronizada. O foco precisa estar nas táticas, técnicas e procedimentos (TTPs) utilizados pelos atacantes — e não na identidade das vítimas. Isso permite que o setor aprenda com cada ataque sem expor publicamente as instituições afetadas.

- **Desenvolvimento de Playbooks de Resposta Coordenada**

  Com base nas informações compartilhadas, o setor deve desenvolver e exercitar planos conjuntos de resposta a ameaças sistêmicas. Se um padrão de ataque contra contas reserva tivesse sido identificado com antecedência, um *playbook* coordenado poderia ter orientado instituições a agir simultaneamente, neutralizando o risco de forma mais eficiente.

9. Conclusão

O ataque de 30 de junho de 2025 não foi o fim de uma história; foi o prólogo de um novo capítulo na cibersegurança do Brasil. Este evento sísmico não deve ser lembrado apenas pelo valor bilionário subtraído, mas pelas falhas tectônicas que revelou na estrutura de confiança, tecnologia e estratégia do nosso sistema financeiro. Olhar para este incidente como um simples "ataque hacker" é perder a lição mais importante que ele nos oferece.

Como este relatório da ZenoX demonstrou, o colapso não se deu por uma única vulnerabilidade de software, mas pela confluência de falhas sistêmicas que, juntas, criaram a tempestade perfeita:

1. **A surdez estratégica** a um submundo da fraude que supostamente planejava abertamente o ataque.
2. **A confiança cega** em uma cadeia de suprimentos digital, tratando parceiros críticos como caixas-pretas seguras, em vez de extensões do próprio perímetro de risco.
3. **A cultura do silêncio**, que isola as vítimas e permite que os criminosos reutilizem e refinem suas táticas livremente, atacando um alvo após o outro.
4. **A ausência de um cérebro de inteligência centralizado**, capaz de conectar os pontos entre ataques menores e o planejamento de um golpe maior, transformando dados dispersos em um alerta preditivo.

A resposta para esta nova realidade não está em construir muros mais altos em torno de cada instituição, mas em desenvolver uma visão mais ampla e profunda que transcenda as fronteiras organizacionais. A defesa reativa, baseada em esperar pelo alerta, se provou tragicamente inadequada. A nova fronteira da segurança é **preditiva, proativa e orientada por inteligência.**

O incidente de 30 de junho deve servir como o catalisador definitivo para uma mudança de paradigma. A segurança do sistema financeiro brasileiro não depende mais apenas da robustez de seus sistemas individuais, mas da sua capacidade coletiva de antecipar, colaborar e responder com base em uma inteligência de ameaças compartilhada e de alta fidelidade.

Organizações que atuam com pesquisa aplicada e monitoramento avançado — como as utilizadas na construção deste relatório — têm um papel relevante nesse novo cenário, não como protagonistas do discurso, mas como parte da solução. O futuro não pertence a quem reage mais rápido, mas a quem enxerga mais longe.

Zenox

Brazil Headquarter
Av. Dr. Chucri Zaidan, 1550 - Sala 3107 - Vila Cordeiro, São Paulo - SP, 04711-130

Email: contact@zenox.ai
Phone: +55 (11) 3382-7396
Website: www.zenox.ai