Número 112 | Março 2026

NTT DATA

Radar

A revista de cibersegurança

Ruptura da cadeia de fraude: o papel fundamental das mulas financeiras

Por Miguel Angel Soler Barba e Alejandra Romero Gutiérrez

A fraude financeira se consolidou como um dos grandes desafios globais da atualidade. Seu crescimento acelerado não respeita fronteiras: atinge bancos, empresas, comércio, instituições públicas e cidadãos em todos os continentes. Golpes de investimento cada vez mais sofisticados, falsificações massivas de identidade, fraudes de pagamento e ataques de engenharia social hoje se combinam com um ecossistema criminoso que opera em escala internacional. Nesse cenário, há um elemento comum que continua sendo determinante para o sucesso dos criminosos: as mulas financeiras.

As mulas — pessoas que movimentam fundos ilícitos por meio de suas contas, às vezes enganadas e em outras ocasiões atuando de forma voluntária — tornaram-se a infraestrutura essencial da fraude moderna. Sem elas, os fraudadores não conseguiriam converter seus ganhos em dinheiro utilizável nem esconder o rastro por meio de múltiplas movimentações de recursos e de diferentes jurisdições. A natureza global do sistema financeiro digitalizado multiplicou tanto as oportunidades quanto os riscos, tornando o combate às mulas um desafio transnacional.

O cenário regulatório avança para responder a essa ameaça. Organismos internacionais como o Grupo de Ação Financeira Internacional (GAFI/FATF), novas autoridades europeias como a Autoridade Europeia de Combate à Lavagem de Dinheiro (AMLA) e marcos regulatórios como a Segunda Diretiva de Serviços de Pagamento (PSD2), o futuro Regulamento de Serviços de Pagamento (PSR), o Regulamento de Resiliência Operacional Digital (DORA), a Diretiva NIS2 sobre segurança de redes e sistemas de informação, o futuro padrão global de pagamentos instantâneos e o pacote legislativo do euro digital (Digital Euro Package) vêm impondo requisitos cada vez mais rigorosos em verificação de identidade, monitoramento de transações e gestão do risco operacional e cibernético. A regulação já não se concentra apenas em cumprir procedimentos, mas em demonstrar efetividade real na prevenção da fraude, incluindo a detecção e desarticulação de redes de mulas.

A cibersegurança, por sua vez, tornou-se um pilar inseparável do combate à fraude. Os ataques atuais combinam malware, phishing, spoofing, sequestro de sessão e manipulação psicológica em larga escala. A colaboração entre as equipes de fraude e os centros de operações de segurança (SOC) tornou-se imprescindível para correlacionar indícios técnicos e financeiros a partir das capacidades de ciberinteligência. As mulas são o destino final de muitos desses ataques, de modo que o elo entre as ciberameaças e a fraude transacional se estreitou como nunca.

A complexidade e a velocidade das redes de mulas tornam inviável uma resposta baseada apenas em regras estáticas ou revisões manuais.

A analítica avançada, em seus diferentes níveis de maturidade, tornou-se o principal aliado para antecipar, detectar e desarticular essas redes.

Por meio de painéis gerenciais e análises exploratórias, as organizações conseguem identificar tipologias de fraude, concentrações por canal ou produto e analisar o ciclo de vida das contas-mula. Modelos estatísticos e de machine learning permitem estimar a probabilidade de que uma conta atue como mula, detectar comportamentos anômalos e analisar padrões de rede.

E a combinação de scores de risco, regras dinâmicas e simulações vem permitindo às organizações recomendar as ações de resposta mais adequadas, priorizar investigações e equilibrar fraude, custo e experiência do cliente. Todo esse conjunto torna indispensável um aprendizado contínuo — e é aí que entra a IA (aprendendo de forma contínua, detectando sinais tênues e combinações complexas invisíveis para regras tradicionais, analisando redes completas e escalando a detecção para milhões de transações e relações).

A incorporação da IA Generativa traz uma mudança qualitativa no combate às mulas, permitindo aprimorar o trabalho das equipes humanas.

E o horizonte tecnológico vai ainda mais longe. A computação quântica, embora ainda esteja em sua fase inicial, apresenta desafios e oportunidades: por um lado, pode comprometer os métodos de criptografia atuais no futuro; por outro lado, promete recursos analíticos sem precedentes para rastrear relações complexas entre milhares de contas e transações. Preparar-se para um mundo "pós-quântico" será essencial para manter a resiliência do ecossistema financeiro.

De uma perspectiva estratégica, essa realidade destaca uma mensagem importante para o setor: sem uma visão abrangente e integrada da fraude, de modo geral, e do problema das "mulas", em particular, não haverá prevenção eficaz. As redes de mulas evoluem rapidamente, adaptando-se aos mecanismos de controle existentes, e só podem ser contidas por operações ágeis, controle rígido e recursos analíticos que possam aprender, prever e se ajustar de forma contínua.

O combate às mulas deixa de ser apenas um problema operacional e passa a ser uma decisão estrutural sobre como gerenciar o risco na era digital.

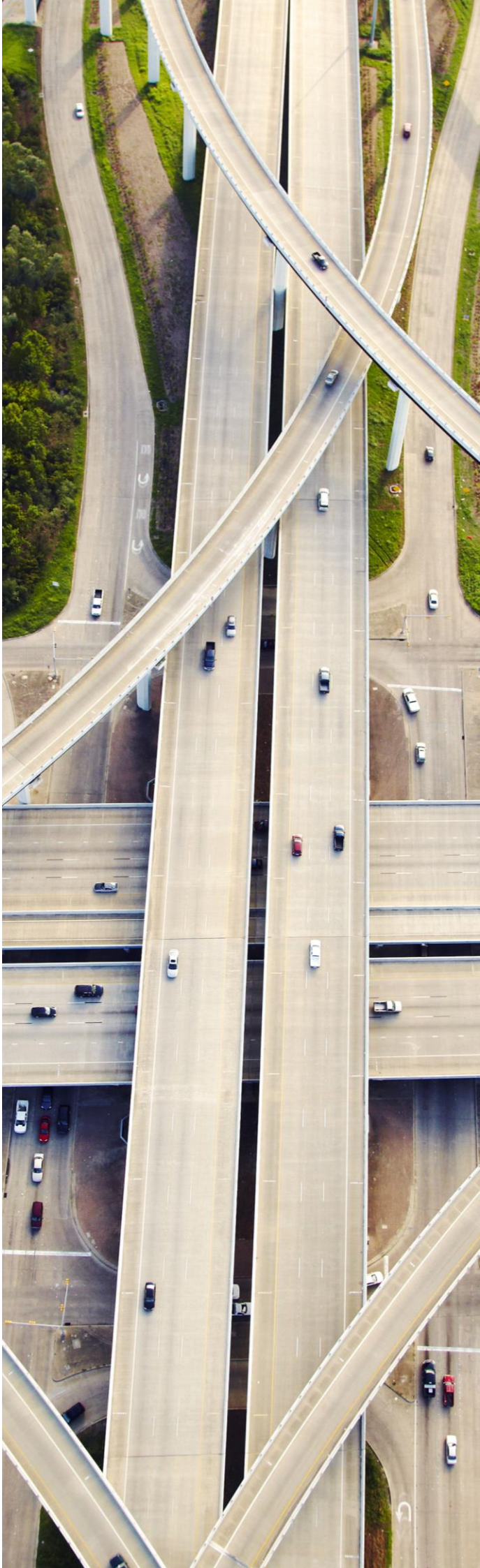
Portanto, o problema das mulas financeiras vai muito além de ser uma questão operacional, é um desafio global que exige uma regulação inteligente (que não restrinja as ações legítimas dos cidadãos), tecnologia que conecte fraude e cibersegurança, analítica avançada e colaboração transfronteiriça. Enfraquecer esse elo crítico nos permitirá reduzir de forma significativa a fraude e proteger a confiança que sustenta o sistema financeiro mundial.

Ao longo desta edição da nossa publicação Radar, vamos aprofundar como as instituições financeiras gerenciam a detecção e a mitigação de contas-mula ao longo do seu ciclo de vida. Esse processo está dividido em três etapas críticas: o onboarding do cliente, o período de latência e a análise da transacionalidade em tempo real. Também vamos destacar a evolução tecnológica com o uso de modelos de machine learning proativos e reativos, que ajudam a identificar padrões suspeitos com muito mais precisão.

Além disso, vamos analisar como as ferramentas de inteligência artificial facilitam tanto a criação de identidades falsas pelos criminosos quanto a sua detecção pelo banco. Por fim, esta edição refletirá sobre a implementação futura de sistemas de agentes para automatizar a análise de alertas e melhorar a eficiência operacional.

Miguel Angel Soler Barba
Diretor de FinCrime

Alejandra Romero Gutiérrez
Diretora de Prevenção e Gestão a Fraudes



Ataques às instituições europeias

Cibercrônica por Leire Cubo Arce

Os primeiros meses de 2026 confirmaram que o cenário de cibersegurança segue pressionado e em constante evolução. No último mês, foram registrados incidentes relevantes que afetam instituições públicas europeias, grandes eventos internacionais e setores estratégicos, enquanto os relatórios consolidados apontam um crescimento contínuo do ransomware e da fraude digital.

Um dos episódios mais significativos ocorreu no âmbito institucional europeu. No fim de janeiro, a Comissão Europeia confirmou um acesso não autorizado à sua plataforma corporativa de gestão de dispositivos móveis (MDM). O incidente, detectado e controlado em menos de nove horas, permitiu que os atacantes acessassem um conjunto limitado de dados pessoais de alguns colaboradores, incluindo nomes e números de telefone profissionais. Embora os dispositivos móveis gerenciados pela plataforma não tenham sido comprometidos diretamente, as autoridades alertaram para o risco de que as informações extraídas sejam usadas em campanhas de phishing altamente direcionadas contra os colaboradores dessas instituições. O caso volta a evidenciar a exposição de ferramentas críticas de gestão interna, que se tornaram cada vez mais atraentes para agentes de ameaça avançados.

Em paralelo, o contexto geopolítico voltou a se projetar no ciberespaço. Nas semanas que antecederam os Jogos Olímpicos de Inverno, na Itália, a agência nacional de cibersegurança italiana confirmou tentativas coordenadas de ataques distribuídos de negação de serviço (DDoS) contra portais oficiais do evento e contra infraestruturas ligadas ao ecossistema turístico e logístico em Cortina d'Ampezzo. As ações, atribuídas a um grupo hacktivista pró-Rússia, tinham como objetivo provocar interrupções e ganhar visibilidade na mídia em um evento de alto perfil internacional. As medidas de mitigação adotadas conseguiram neutralizar o tráfego malicioso sem causar interrupções significativas de serviço, mas o episódio confirma que os grandes eventos globais seguem sendo alvos simbólicos no confronto digital.

No âmbito nacional, os dados mais recentes mostram um aumento considerável da atividade criminosa. O Instituto Nacional de Ciberseguridad (Incibe) informou que, ao longo de 2025, foram gerenciados mais de 122 mil incidentes, o que representa um aumento de 26% em relação ao ano anterior. Um fato que merece destaque é o aumento de 171% nos casos de roubo de informação digital, além da persistência de milhares de campanhas de phishing e fraude on-line. Além disso, mais de 400 incidentes afetaram operadores considerados essenciais, incluindo setores como bancos, transporte e energia. Esses números mostram que a ameaça não só se tornou mais frequente, como também impacta diretamente infraestruturas críticas e serviços estratégicos.

O ransomware, por sua vez, mantém uma tendência elevada em escala global. Relatórios setoriais referentes a janeiro de 2026 apontam um volume de ataques acima da média histórica, com incidência especial sobre organizações dos setores de saúde, governo e indústria. Os grupos criminosos continuam aperfeiçoando modelos de dupla extorsão, combinando a criptografia dos sistemas com a ameaça de vazar dados exfiltrados. A profissionalização dessas estruturas criminosas e a diversificação de seus vetores de acesso — muitas vezes por meio de credenciais comprometidas ou vulnerabilidades em serviços expostos — tornam mais difícil conter os ataques ainda nas fases iniciais.

Ao mesmo tempo, especialistas vêm alertando para a exploração em larga escala de dispositivos residenciais conectados, em especial televisores inteligentes e sistemas de streaming baseados em Android. Esses equipamentos, muitas vezes mal configurados ou sem atualizações de segurança, vêm sendo recrutados para compor botnets usados em ataques distribuídos de negação de serviço. Essa tendência mostra que a superfície de ataque já não se limita ao perímetro corporativo tradicional, mas se estende ao ecossistema digital da residência conectada, que pode se transformar, sem que o usuário perceba, em infraestrutura a serviço do atacante. De modo geral, o último mês apresentou um cenário em que a atividade cibercriminosa combinou motivações políticas, ganhos financeiros e exploração sistemática de vulnerabilidades técnicas. A rapidez na detecção, a capacidade de resposta coordenada e a gestão do ciclo de vida tecnológico consolidam-se como fatores essenciais para reduzir o impacto. O início de 2026 confirma, portanto, que a cibersegurança continua sendo um componente estratégico fundamental para a estabilidade institucional, econômica e social em um ambiente cada vez mais interconectado.

Leire Cubo Arce
Engenheira de Cibersegurança

Mulas financeiras: repensando a relação entre PLD e fraude

Artigo por José Frías Hernando

Na última década, praticamente todos os aspectos da atividade financeira mudaram da noite para o dia. Os clientes operam dentro e fora dos canais digitais com uma facilidade que há alguns anos parecia impossível, e as organizações tiveram de adaptar seus modelos a uma relação muito mais digital. Mas, no meio dessa transformação, surgiu um convidado desagradável: o crime financeiro. O crime financeiro também mudou de forma silenciosa, explorando brechas no sistema e, em muitos casos, atuando mais rápido do que os controles já existentes.

A essa realidade soma-se uma discrepância crucial: enquanto as instituições financeiras operam sob marcos regulatórios cada vez mais exigentes — cumprindo obrigações de prevenção à lavagem de dinheiro (PLD), proteção ao consumidor, privacidade, governança e resiliência operacional —, os cibercriminosos não estão sujeitos a nenhuma dessas restrições. Os cibercriminosos não precisam conciliar inovação e conformidade, nem velocidade e controle; essa ausência de obrigações dá a esses grupos uma agilidade que, na prática, se traduz em uma vantagem estrutural em relação às organizações que precisam proteger seus clientes sem deixar de cumprir as exigências regulatórias.

Mas um dos movimentos que essa nova realidade trouxe é o que mais preocupa os supervisores: as mulas financeiras estão crescendo e se diversificando. Durante muito tempo, o setor assumiu que uma mula se encaixava no modelo clássico do indivíduo que emprestava sua conta e recebia alguma remuneração financeira ou um bom retorno.

Um ator de boa-fé, quase sempre consciente da própria participação. Hoje, essa caricatura já não se sustenta. As instituições agora se deparam com estudantes atraídos por ofertas que, à primeira vista, parecem inocentes, trabalhadores que buscam renda adicional sem perceber que estão sendo explorados, vítimas de roubo de identidade e, cada vez mais, identidades sintéticas que escapam aos controles iniciais por meio de técnicas cada vez mais sofisticadas.

Esse cenário não apenas torna a detecção mais difícil, como também muda a forma como o risco é percebido e obriga a repensar como se define e se estabelece a proteção desde o início da relação com o cliente.

Um problema que chegou ao centro da agenda regulatória

Esse cenário não é novo; o órgão regulador já tinha previsto essa prática em seu roteiro muito antes de chegar aos noticiários. A questão das mulas não é novidade para as autoridades responsáveis pela supervisão.

Os supervisores também enxergam esse fenômeno como um sintoma: quando uma instituição permite que seus produtos sejam usados para movimentar recursos de origem ilícita, mesmo que o cliente tenha sido enganado, isso pode revelar fragilidades em suas políticas de credenciamento, na capacidade de realizar revisões analíticas periódicas e na integridade de seus modelos de risco.

Com o tempo, os supervisores elevaram o nível de exigência. A verificação de identidade e os registros já não são mais suficientes para atender às exigências. Eles querem saber o máximo possível sobre o que a instituição faz para entender se o comportamento do cliente é consistente com o seu perfil, se há inconsistências em suas atividades iniciais, se está exposto a práticas de manipulação ou se apresenta padrões já associados a redes criminosas.

Por isso, o onboarding deixou de ser apenas uma fase de validação e passou a ser a primeira linha de defesa para definir a qualidade do crescimento da instituição.

Outra mudança relevante diz respeito à responsabilidade. É evidente que a mula pode ser, em muitos casos, uma vítima; no entanto, o orgão regulador não considera isso um escudo para a instituição.

A expectativa é clara, o banco precisa demonstrar que existe um programa de controles robusto o suficiente para identificar comportamentos anormais antes que se transformem em risco operacional ou reputacional.

PLD e fraude: dois mundos historicamente conectados que agora precisam atuar de forma integrada

Um dos fatores que mais favoreceu o avanço das mulas foi a distância operacional entre as equipes de prevenção à lavagem de dinheiro e as equipes de combate à fraude, que existe há anos. Essas equipes analisavam sinais complementares, mas raramente os integravam em uma visão única do cliente.

A equipe de PLD analisa os fluxos, a coerência das receitas, a origem dos recursos. A equipe de fraudes avalia operações — incluindo a saída de recursos —, dispositivos, padrões de acesso, volume de transações e comportamento transacional. Cada área gera alertas segundo a sua própria lógica, sem construir uma visão integrada sobre o cliente. Esse modo de operar já não é mais sustentável. As mulas cruzam exatamente a fronteira entre esses dois mundos e, se as peças não estiverem todas conectadas, o risco não será detectado.

As instituições mais proativas já perceberam isso. Aquelas que estão reagindo entendem e defendem que a PLD e a fraude devem atuar em conjunto e construir modelos integrados, compartilhando dados, critérios e decisões. Isso implica transformar a governança, assim como os fluxos de trabalho, como casos integrados, análise conjunta, pontuação que integre perspectivas e, acima de tudo, uma leitura do comportamento do cliente - não apenas observando o comportamento do cliente, mas também a maneira como ele age e a intenção aparente do motivo que o levou a agir assim.

O resultado é uma visão muito mais ampla. Em vez de interpretar sinais desconectados, a instituição passa a enxergar o cliente como uma entidade em evolução e consegue agir antes, tomando decisões com um impacto muito mais amplo.

O papel da área de negócios continua sendo impulsionar o crescimento, mas com uma nova visão de risco. O setor empresarial é profundamente afetado por todas essas mudanças regulatórias e operacionais. A aquisição de clientes já não pode ser avaliada apenas em números. Volume, sozinho, já não basta.

Agora, a busca é pelo que muitas instituições estão começando a chamar de “crescimento limpo,” ou seja, um crescimento em que o comportamento não se desgasta, não produz alertas excessivos e não se torna um fator de risco para a organização.

Quando o crescimento ignora essa dimensão do risco, o impacto não se limita a métricas internas ou regulatórias, se traduz em clientes que se sentem desprotegidos, que, mesmo sem sofrer uma perda econômica direta, reduzem sua confiança, diminuem o relacionamento com a instituição e enfraquecem oportunidades importantes de fidelização e cross-selling.

O primeiro resultado dessa mudança de mentalidade são os ajustes na política de admissão de clientes. As instituições vêm incorporando filtros menos visíveis, porém mais relevantes, baseados em indicadores antecipados de risco tanto de PLD quanto de fraude.

Isso não significa tornar o processo mais rígido, e sim ser mais flexível quando não há indícios de risco e aprofundar a análise nos casos em que as evidências apontam vulnerabilidade ou exposição à manipulação.

A adaptação do negócio: políticas dinâmicas, jornadas conscientes e um novo equilíbrio entre crescimento e qualidade

Ao mesmo tempo, as jornadas do cliente estão sendo redesenhadas. Já não são vistas como jornadas lineares projetadas para maximizar a conversão. Além disso, essas jornadas passam a incorporar pontos de controle mais sofisticados, mensagens preventivas e, em alguns casos, restrições dinâmicas acionadas quando o comportamento do cliente se afasta do padrão esperado.

Sem comprometer a experiência do cliente, essa estratégia promove um ambiente digital mais seguro e aumenta a conscientização sobre os riscos emergentes.

Os indicadores internos também vêm mudando. A conversão se torna uma conversão qualificada; o valor do cliente é avaliado utilizando fatores que não eram considerados há alguns anos. Até mesmo os incentivos comerciais começam a ser ajustados para favorecer um crescimento que já não recompensa segmentos de negócio que, no longo prazo, geram mais atrito operacional e maior exposição regulatória.

Conclusão: um desafio que redefine a forma de fazer negócios no setor financeiro

As mulas financeiras não são uma tendência ou uma raridade estatística. Representam um crime financeiro que ganhou complexidade e explora as vulnerabilidades dos sistemas.

Seu crescimento exponencial forçou o setor a acelerar as mudanças necessárias que estavam sendo planejadas há algum tempo. Entre elas estão uma maior harmonização das práticas de AML e fraude, políticas flexíveis, caminhos mais deliberados e uma mentalidade de risco que analisa os clientes no decorrer de seu ciclo de vida.

O órgão regulador indicou o caminho, no entanto, a responsabilidade recai sobre as próprias organizações, que devem perceber que o crescimento sustentável depende da capacidade de detecção dessa ameaça.

As instituições que integrarem essa abordagem não apenas conseguirão cumprir melhor as exigências regulatórias, reforçar a confiança dos clientes e desenvolver um modelo de negócios mais flexível, como também consolidarão a credibilidade e a solidez desse modelo em um ambiente acelerado, em que o crime financeiro segue em expansão em um mundo cada vez mais incerto.

José Frías Hernando
Diretor de Prevenção à Lavagem de Dinheiro

Evolução tecnológica das ferramentas de prevenção à fraude

Artigo por Francisco José García Spina

A fraude financeira entrou em uma fase radicalmente diferente. As mulas de dinheiro e as fraudes avançadas deixaram de ser incidentes pontuais para se tornar ameaças coordenadas, capazes de impactar simultaneamente múltiplas instituições. A combinação de pagamentos imediatos, ecossistemas fintech abertos e identidades digitais vulneráveis ampliou o perímetro de risco e obrigou o setor financeiro a evoluir seu conjunto tecnológico antifraude com uma velocidade sem precedentes.

Nesse contexto, o desafio já não é identificar uma transação incomum, mas interromper redes inteiras, dinâmicas e distribuídas, que se adaptam continuamente para burlar os controles.

Durante anos, as ferramentas de prevenção se basearam em regras estáticas e em controles elaborados para um ecossistema digital mais estável. Essa estratégia ficou para trás. A fraude atual se caracteriza por engenharia social sofisticada, manipulação direta do usuário, falsificação de identidade, uso de identidades sintéticas e redes de mulas que executam padrões de colocação (Placement), ocultação (Layering) e integração (Integration) em alta velocidade. Para responder de forma efetiva, as ferramentas modernas precisam ir além da análise transacional e compreender o que o cliente faz, como faz, de qual dispositivo, sob quais sinais digitais e em qual rede de relacionamento.

Essa transformação vem dando origem a uma nova geração de plataformas que incorporam a inteligência artificial (IA) avançada, analítica de grafos, biometria comportamental, orquestração inteligente e arquiteturas capazes de antecipar comportamentos suspeitos em tempo real.

Nesse contexto, a analítica avançada se consolida como o núcleo do modelo antifraude moderno. A analítica descritiva permite entender a dimensão real do cenário das mulas e priorizar as ações. Os modelos preditivos e de machine learning antecipam o risco ao identificar comportamentos anômalos e padrões de rede. A analítica prescritiva traduz esse risco em decisões acionáveis, equilibrando impacto econômico, experiência do cliente e atendimento às exigências regulatórias.

A Inteligência Artificial acrescenta ainda capacidade de aprendizado contínuo e escalabilidade, o que permite manter a eficácia dos controles antifraude mesmo frente a táticas criminosas em constante evolução.

Nessa abordagem, a IA Generativa atua como um acelerador operacional: analisa informações não estruturadas, apoia os analistas na investigação de casos complexos e melhora a explicabilidade das decisões. Essa tecnologia não substitui o julgamento humano; reforça sua capacidade e eficiência.

Compreender o ciclo da mula: ponto de partida da nova abordagem

O ciclo das mulas — que abrange as fases de colocação, ocultação e integração — continua válido, mas hoje se desenrola em uma velocidade que ultrapassa a capacidade dos modelos tradicionais de acompanhar esse movimento. A evolução natural foi migrar de um monitoramento de PLD reativo para um modelo mais proativo e tecnológico, que integra:

- controles avançados no onboarding digital e avaliação antecipada de risco;
- alertas inteligentes gerados por modelos de IA;
- identificação de relações por meio de grafos;
- análise contextual baseada em canal, dispositivo e velocidade.

Esse modelo de relação permite detectar não apenas o usuário suspeito, mas também todo o grupo a que pertence.

Agentic AI: o novo braço operacional antifraude

Uma das inovações mais relevantes é o surgimento de agentes de IA especializados, que automatizam tarefas críticas do ciclo de fraude e tomam decisões em milissegundos:

- **Agente de onboarding seguro:** identifica contas sintéticas, dispositivos repetidos e sinais de "fábricas de contas";
- **Agente de ativação e integração:** monitora transações de passagem rápida (pass through) e recomenda retenções preventivas;
- **Agente de orquestração:** combina regras, modelos e propensão a riscos para decidir se deve permitir, escalar ou bloquear uma transação.

Esses agentes permitem operar no ritmo da fraude moderna, em que a velocidade é fator decisivo.

Arquiteturas modernas: do transacional ao relacional

As ferramentas atuais deixaram de funcionar como motores independentes e passaram a operar como ecossistemas antifraude integrados, que combinam:

- analítica de grafos para detectar clusters de risco;
- modelos híbridos (regras+IA) para reduzir falsos positivos;
- sinais digitais avançados (Behavioural Biometrics, IP Intelligence, detecção de Remote Access Trojan (RAT));
- rastreabilidade completa por meio de capacidades de logging e, em alguns casos, de blockchain.

O resultado é uma detecção mais precisa e contextual, capaz de antecipar padrões de manipulação humana ou automatizada.

O futuro: colaboração interbancária e aprendizado federado

O próximo avanço evolutivo está na detecção colaborativa entre instituições. Com o uso de aprendizado federado, os bancos podem compartilhar inteligência sem expor dados sensíveis. Isso permitirá:

- detectar mulas que operam em múltiplas instituições;
- identificar dispositivos ou identidades repetidas no ecossistema;
- antecipar campanhas criminosas antes de sua disseminação.

Conclusão

O setor financeiro vive uma transformação estrutural no combate à fraude. As regras estáticas já não são suficientes. As ferramentas modernas incorporam IA, analítica de grafos, sinais digitais e arquiteturas inteligentes que permitem desmantelar redes inteiras e antecipar ataques.

A missão já não é apenas impedir as operações fraudulentas, é compreender a rede, antecipar o risco e agir antes que a fraude se materialize.

Francisco José García Spina
Diretor de Soluções de FinCrime

Impacto operacional das mulas

Artigo por Carlos Campos Hervas

Do ponto de vista de operações, quando os mecanismos de prevenção não conseguem impedir sua entrada, a gestão de mulas busca detectar o quanto antes para interromper sua atuação, identificar outras possíveis mulas e, na sequência, encerrar o relacionamento (cancelamento de contas e encerramento do cadastro do cliente etc.).
Do ponto de vista operacional, é possível identificar uma mula em três momentos do seu "ciclo de vida": onboarding, latência e transacionalidade.

Onboarding

Do ponto de vista operacional, o onboarding consiste na verificação da identidade, da documentação e dos demais dados do cliente. Exceto em casos muito evidentes, como o uso do mesmo celular ou endereço por diferentes pessoas, irregularidades na documentação ou alertas na verificação de identidade (fotos/vídeos). É realmente muito complexo identificar uma mula logo na entrada, motivo pelo qual vêm sendo desenvolvidos modelos específicos para reforçar a detecção já no onboarding.

Esse último ponto — a verificação de identidade — é onde as ferramentas mais vêm avançando, permitindo identificar com maior precisão rostos repetidos ou já presentes em bases de dados de identidades ilegítimas. Por outro lado, as ferramentas de inteligência artificial (IA) permitem ao crime gerar imagens com muito mais precisão e rapidez. Há casos de pessoas com centenas de tentativas de onboarding com faces e identificações diferentes, de modo que os avanços na detecção acabam sendo compensados pelos avanços na geração de identidades falsas.

Os processos de controle no contexto de prevenção à lavagem de dinheiro (PLD), como o 'conheça seu cliente (KYC)', também não trazem muita informação adicional que permita essa detecção, pois muitas pessoas se cadastram como estudantes, donas de casa e outros perfis que não exigem muita documentação.

Latência

Durante o ciclo de vida das mulas, ao analisar a movimentação de suas contas, é possível começar a detectá-las com maior confiabilidade.

Modelos proativos de machine learning (ML) vêm sendo desenvolvidos para gerar um score individual por pessoa e conta, estimando a probabilidade de envolvimento em atividades fraudulentas. Esses modelos se baseiam na tipologia, na quantidade de produtos, serviços, perfil de uso, entre outros fatores, associados à conta.

Por exemplo, uma conta com pagamentos em débito automático, que recebe salário e na qual são debitadas parcelas de um empréstimo, tem muito menos chance de ser uma conta mula do que uma conta recém-criada, com onboarding digital, perfil de cliente estudante, sem produtos ou serviços associados, com saldo médio baixo e movimentação frequente de entrada e saída.

A importância e a efetividade desses modelos ficam evidentes quando são integrados às ferramentas de monitoramento de transações, seja de entrada (PLD) ou de saída (Fraude).

Transacionalidade

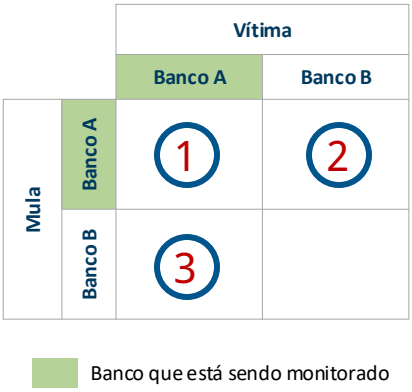
O monitoramento de transações é a peça central na cadeia operacional de detecção de mulas e, basicamente, envolve:

- análise dos alertas gerados pelas ferramentas de monitoramento;
- adoção de ações conforme o resultado da análise, ações que podem gerar muito atrito com clientes, como: bloqueio de contas, usuário, cartões etc.
- verificação de legitimidade – solicitação de informações e documentação adicionais para validar se é de fato uma mula ou se se trata de falso positivo;
- encerramento do relacionamento em caso de confirmação ou reversão das ações adotadas em caso de falso positivo.

As ferramentas de monitoramento de transações, sejam de fraude ou de PLD, baseiam-se em modelos de machine learning, porém são reativas, analisando cada transação em conjunto com outros dados relacionados ao cliente, dispositivos, assinaturas, entre outras informações, no momento em que ocorrem.

Como o monitoramento é em tempo real e, apesar de ter evoluído muito, a capacidade de processamento do volume de informações ainda é limitado; por isso, integrar o resultado dos modelos proativos a essas ferramentas tem sido um grande avanço.

Dependendo da origem e do destino dos fundos, as mulas são tratadas de forma diferente.



1. São operações em que a conta da vítima e a conta da mula estão na mesma instituição, que é o que estamos "monitorando".
Nesse caso, tenta-se detectar a mula com as ferramentas de monitoramento de fraude (operações de saída da conta de origem), que se baseiam em validar o padrão habitual do tipo de operação que a "vítima" está realizando.
Nessas operações, integrar os modelos proativos às ferramentas de monitoramento (fraude) é muito importante, pois as regras são enriquecidas com informações que as tornam mais confiáveis e reduzem falsos positivos.

2. Uma conta ("mula") do banco que estamos monitorando recebe fundos de um banco externo, seja nacional ou internacional. As ferramentas de fraude se baseiam em analisar operações de saída; neste caso, por se tratar de entrada, o tratamento deve ser feito pelas ferramentas de PLD. Assim como no caso anterior, integrar os modelos proativos às ferramentas de monitoramento (PLD) é muito importante.

3. A conta da vítima está no banco que estamos monitorando, mas os fundos são enviados para outro banco, nacional ou estrangeiro.
Trata-se de uma operação de saída de fundos, mas, neste caso, não há nenhuma informação sobre a conta de destino, por se tratar de uma conta em outra instituição.
Projetos estão sendo desenvolvidos para compartilhar informações sobre contas fraudulentas, mas ainda não estão 100% operacionais.

Impacto dos sistemas de agentes nas operações

Além das melhorias baseadas em machine learning para otimizar a detecção, os sistemas de agentes vão se tornar uma peça fundamental na eficiência das operações.

Por exemplo, na análise de um alerta, pode-se contar com agentes que façam uma pré-análise dos dados do cliente, das transações, da conta, de serviços e produtos; e um agente "orquestrador" que, com base no resultado dos agentes anteriores, realiza uma pré-análise, facilitando bastante o trabalho que hoje é feito por um analista de alertas.

Carlos Campos Hervas
Diretor de Operações de FinCrime

 © Copyright NTT DATA, Inc.

O que vem pela frente: mulas quânticas?

Tendências por María Angeles Gutiérrez Puente

O panorama das mulas financeiras é um dos pilares operacionais da fraude bancária contemporânea. Essas pessoas, conscientes ou não, atuam como intermediárias para movimentar fundos ilícitos e dificultar o seu rastreio. No entanto, a chegada da computação quântica e da criptografia quântica pode transformar radicalmente tanto a forma de atuação dos cibercriminosos quanto as capacidades de defesa dos bancos, dos órgãos reguladores e das autoridades de segurança pública.

O risco quântico: um novo ecossistema para a fraude

A principal ameaça da computação quântica para o setor financeiro é sua capacidade teórica de quebrar os esquemas criptográficos clássicos nos quais se baseiam as transações bancárias, a autenticação digital e os canais seguros.

Algoritmos como RSA ou ECC podem se tornar obsoletos quando existirem computadores quânticos suficientemente potentes.

Como isso afeta as mulas? De duas formas principais:

1. **Fraudes mais rápidas e difíceis de rastrear**
   Caso um atacante consiga quebrar senhas ou falsificar identidades digitais em grande escala, poderá gerar transações fraudulentas que exijam mulas humanas ou digitais para movimentar dinheiro antes que o ataque seja detectado.

2. **Desaparecimento gradual da mula humana**
   A fraude evoluiria para esquemas totalmente automatizados, em que bots e carteiras digitais criptografadas com técnicas pós-quânticas assumiriam o trânsito de fundos. A "mula quântica" seria um software distribuído e anônimo, muito difícil de bloquear.

Criptografia quântica e pós-quântica: medidas de prevenção que favorecem os proponentes

Por outro lado, as comunicações quânticas, em especial a distribuição quântica de chaves (QKD), oferecem uma capacidade inédita, detectar qualquer tentativa de interceptação graças ao princípio da não clonagem quântica.

Os bancos que adotarem o QKD em seus centros críticos, tornarão as comunicações interbancárias praticamente impossíveis de serem espionadas até mesmo por um adversário com um computador quântico.

Além disso, a criptografia pós-quântica (PQC), já padronizada pelo NIST, permitirá que órgãos reguladores e instituições migrem para sistemas resistentes a ataques quânticos antes mesmo que eles aconteçam.

Isso significa:

- Menor probabilidade de ataques que gerem transferências fraudulentas, reduzindo o volume de dinheiro ilícito que precisaria passar por lavagem de dinheiro.
- Melhor rastreabilidade, já que muitos algoritmos pós-quânticos permitem autenticação forte sem comprometer metadados necessários para investigações.
- Maior proteção de identidades e evidências digitais em investigações policiais.

Os benefícios para a investigação criminal

A computação quântica também tem potencial para aprimorar as capacidades forenses, por exemplo:

- Analisar grandes grafos de transações para detectar padrões de mulas com maior profundidade e velocidade.
- Otimizar a correlação entre contas, dispositivos e comportamentos.
- Acelerar a análise de blockchain em investigações de fraude criptográfica.

Não se trata apenas de rastrear melhor, mas de antecipar comportamentos com modelos quânticos aplicados a séries temporais e fluxos financeiros.

Órgãos reguladores diante do desafio quântico

Os órgãos reguladores terão que:

- Exigir a migração obrigatória para criptografia pós-quântica.
- Estabelecer normas claras para o uso de QKD em infraestruturas críticas.
- Estabelecer marcos regulatórios para cenários em que as mulas sejam software autônomo.

Maria Angeles Gutiérrez Puente
Diretor de Cibersegurança/
Quantum FinCrime

 © Copyright NTT DATA, Inc.

Vulnerabilidades

Vulnerabilidade crítica no SolarWinds Web Help Desk

Data: 29 de janeiro de 2026
CVE: CVE-2025-40551

CVSS: 9.8

CRÍTICA

Descrição

Uma vulnerabilidade crítica, listada como **CVE-2025-40551**, foi identificada afetando o SolarWinds Web Help Desk. A falha está relacionada a um problema de desserialização de dados não confiáveis.

A desserialização é o processo pelo qual um aplicativo converte um fluxo de dados, como uma cadeia de texto ou uma sequência de bytes, em objetos utilizáveis no ambiente operacional.

Nesse caso, a vulnerabilidade pode permitir a execução remota de código (RCE), o que possibilita que um atacante não autenticado execute comandos arbitrários no servidor afetado, comprometendo a segurança do sistema.

Solução

Recomedação:

- Limitar a exposição à Internet e analisar os registros.
- Atualizar os servidores vulneráveis do Web Help Desk para a versão 2026.01.

Produtos afetados

SolarWinds Web Help Desk na versão 12.8.8 HF1 e anteriores.

Referências

- thehackernews.com
- incibe.es
- solarwinds.com

 © Copyright NTT DATA, Inc.

TLP:WHITE

Vulnerabilidades

Vulnerabilidade crítica no Ivanti EPMM

Data: 30 de janeiro de 2026
CVE: CVE-2026-1281 e uma mais

CVSS: 9.8

CRÍTICA

Descrição

Vulnerabilidades críticas de injeção de código foram identificadas no Ivanti Endpoint Manager Mobile (EPMM).

Essas vulnerabilidades (**CVE-2026-1281** e **CVE-2026-1340**) permitem que um atacante execute código remoto sem autenticação, afetando os componentes internos do EPMM. A Ivanti confirmou que pelo menos uma das vulnerabilidades foi ativamente explorada em um número limitado de casos.

Uma exploração bem-sucedida poderia permitir o controle total do sistema EPMM, comprometendo o gerenciamento de dispositivos móveis e o acesso a recursos corporativos.

Solução

Recomedação:

- Executar imediatamente o hotfix fornecido pela Ivanti: RPM 12.x.0 ou 12.x.1 (observando que o hotfix não permanece após uma atualização de versão e precisará ser executado novamente).
- Atualizar para a versão 12.8.0.0.0, que incluirá a correção permanente (planejada para o primeiro trimestre de 2026).

Produtos afetados

Ivanti Endpoint Manager Mobile (EPMM) nas seguintes versões:

- 12.5.1.0 e anteriores
- 12.6.1.0 e anteriores
- 12.7.0.0 e anteriores

Referências

- nvd.nist.gov
- hub.ivanti.com

 © Copyright NTT DATA, Inc.

A Microsoft corrige uma vulnerabilidade crítica de dia zero no Microsoft Office

Data: 26 de janeiro de 2026
CVE: CVE-2026-21509

Crítica

Descrição

A vulnerabilidade **CVE-2026-21509** permite contornar (bypass) os mecanismos de segurança do Microsoft Office. Com isso, um atacante pode contornar as proteções por meio de documentos especialmente elaborados.

A exploração exige que a vítima abra o arquivo malicioso, o que pode resultar na execução de ações não autorizadas que comprometem a segurança do computador.

Foi confirmado que a vulnerabilidade está sendo explorada ativamente por atacantes. Em resposta, a Microsoft emitiu um patch de emergência para corrigir a vulnerabilidade imediatamente.

Produtos afetados

Os produtos afetados por esta vulnerabilidade incluem:

- Microsoft Office 2016
- Microsoft Office 2019
- Office LTSC 2021/2024
- Microsoft 365 Apps

Solução

Recomedação:

- Instalar imediatamente as atualizações de segurança lançadas pela Microsoft por meio do Windows Update ou do Microsoft Update.

Referências

- cyber.gov.rw
- msrc.microsoft.com

 © Copyright NTT DATA, Inc.

TLP:WHITE

Fortinet corrige vulnerabilidade crítica de “bypass” de autenticação

Data: 28 de janeiro de 2026
CVE: CVE-2026-24858

Crítica

Descrição

A vulnerabilidade crítica **CVE-2026-24858** está relacionada a um contorno (bypass) de autenticação no FortiOS, o sistema operacional baseado no kernel do Linux usado pelos dispositivos Fortinet.

A vulnerabilidade poderia permitir que um atacante com uma conta FortiCloud e um dispositivo registrado conseguisse acessar outros computadores e contas sem autenticação. Essa capacidade teria sido usada para criar contas locais com privilégios de administrador, manter a persistência, modificar configurações, habilitar o acesso à VPN e exfiltrar configurações de firewall.

A vulnerabilidade afetou vários produtos do ecossistema da Fortinet, incluindo o FortiManager e o FortiProxy.

Produtos afetados

Os produtos afetados por esta vulnerabilidade incluem:

- Serviços FortiManager e FortiANalyzer na versão 7.6.0 e anteriores.
- FortiProxy na versão 7.6.4 e anteriores.
- FortiWeb da versão 7.4.0 a 8.0.3.

Solução

Recomedação:

- Atualizar para as versões mais recentes do software.
- Redefinir as credenciais possivelmente afetadas.

Referências

- thehackernews.com
- incibe.es

 © Copyright NTT DATA, Inc.

Eventos

RootedCON 2026
De 5 a 7 de março

A cidade de Madri se prepara para sediar uma nova edição do RootedCON 2026, um dos congressos de cibersegurança mais relevantes no cenário nacional e internacional. O evento, que mais uma vez reunirá especialistas técnicos, pesquisadores, gerentes de segurança, agências de aplicação da lei e empresas de tecnologia, se estabeleceu como um espaço estratégico para a troca de conhecimento e atualização contra ameaças emergentes.

Link

Ohio Information Security Conference
11 de março

A Ohio Information Security Conference (OISC) 2026 se prepara para ser um dos eventos mais importantes do calendário de cibersegurança para profissionais técnicos e gestores de risco. Organizada pela Technology First, essa conferência anual reunirá especialistas, analistas, CISOs e equipes de segurança no dia 11 de março de 2026 no Sinclair Conference Center em Dayton, Ohio, nos Estados Unidos, para discutir as ameaças mais recentes, estratégias de resposta em tempo real e soluções inovadoras para riscos emergentes, como os impulsionados pela IA, além de oferecer networking, workshops e demonstrações de tecnologias de defesa.

Link

RSAC Conference
De 23 a 26 de março

A RSAC Conference 2026, considerada um dos eventos mais influentes do calendário global de cibersegurança, reunirá novamente milhares de profissionais do setor de 23 a 26 de março de 2026 no Moscone Center em São Francisco, nos Estados Unidos. O evento - onde "o mundo fala sobre segurança" - serve como uma plataforma para explorar as tendências que estão definindo o futuro digital, com palestras, sessões técnicas e exposições sobre os principais tópicos, como inteligência artificial, gestão de riscos, identidade e defesa contra ameaças emergentes, assim como oportunidades de networking entre pesquisadores, CISOs e fornecedores de soluções. A conferência se estabeleceu como um dos principais locais para compartilhar estratégias de defesa, analisar incidentes recentes e promover a inovação em cibersegurança.

Link

5º Congreso de Ciberseguridad de Andalucía
De 24 a 26 de março

A cidade de Málaga se prepara para sediar o 5º Congresso Andaluz de Cibersegurança nos dias 24 e 25 de março de 2026. Esse fórum anual é considerado um ponto de encontro fundamental para o ecossistema de segurança digital no sul da Espanha. Organizado pela Agência Digital da Andaluzia em colaboração com a Prefeitura de Málaga, o evento reunirá especialistas, líderes institucionais, empresas de tecnologia, startups e PMEs para discutir a proteção de dados, a resiliência cibernética, a segurança em ambientes em cloud, a inteligência artificial aplicada à defesa digital e a crescente necessidade de talentos especializados em cibersegurança.

Link

Recursos

- ***Checklist* de melhores práticas**

Lista atualizada de ações de cibersegurança com foco operacional: controles de identidade, atualizações críticas, *backups* verificados, *vendor controls*... ideal como *checklist* para inspeções rápidas ou auditorias internas.

Link

- **Global Cybersecurity Outlook 2025 – Fórum Econômico Mundial (WEF)**

Relatório estratégico e global que examina como a cibersegurança está evoluindo frente a tecnologias emergentes, tensões geopolíticas e desafios de resiliência. Fornece dados-chave sobre riscos relacionados à dependência de cadeias de suprimentos, sofisticação de ataques e disparidades entre organizações, com recomendações para líderes que enfrentam esse cenário em constante evolução.

Link

- **GCA Cybersecurity Toolkit (Global Cyber Alliance)**

Kit de ferramentas e guias práticos para avaliar a postura de segurança, reforçar controles comuns e acessar soluções gratuitas com foco em defesas básicas amplamente recomendadas.

Link

Inscreva-se na RADAR
up.nttdata.com/suscribetearadar

Powered by the Cybersecurity NTT DATA Team

br.nttdata.com