bttNG
apura

Ataque Bilionário ao Sistema Financeiro Brasileiro

Atualizado em 03/07/2025

JULHO 2025

TLP:CLEAR

Traffic Light Protocol (TLP) Clear: Não há limites na divulgação.

apura

Sumário

1. Sumário Executivo

Na madrugada de 30 de junho, a C&M Software, empresa brasileira provedora de serviços para o setor financeiro, foi violada por um ator não identificado, supostamente explorando credenciais vazadas de clientes da empresa. Uma vez dentro do sistemas da C&M, o cibercriminoso começou a retirar fundos de ao menos seis instituições financeiras, a partir das contas reservas mantidas no Banco Central para liquidação interbancária.

No dia seguinte, 1º de julho, a imprensa começou a noticiar o incidente cibernético, de características complexas e que desviou valores de proporções sem precedentes no Brasil. O incidente envolveu o acesso indevido a sistemas de instituições financeiras e fintechs através da C&M Software, uma prestadora de serviços com acesso ao coração do Sistema de Pagamentos Brasileiro (SPB).

O valor total desviado ainda está sendo calculado pelas partes envolvidas, com diferentes relatos variando de R$ 400 milhões até R$ 3 bilhões. Segundo estimativas preliminares do Banco Central, apresentadas pelo portal Brazil Journal, o ataque teria drenado ao todo R$ 800 milhões de oito instituições bancárias e não-bancárias. A BMP, uma das instituições prejudicadas, declarou ter tido R$ 400 milhões subtraídos, mas já tendo conseguido recuperar R$ 160 milhões na quinta-feira (03/07).

Como medida preventiva, em 30 de junho a C&M Software foi desconectada temporariamente do Sistema de Pagamentos Brasileiro (SPB) para mitigar riscos de novas movimentações irregulares. A Polícia Federal abriu inquérito para investigar o roubo em 2 de julho, com apoio do Banco Central.

As investigações continuam em andamento no momento da escrita deste relatório de inteligência.

2. Descrição do Incidente

Às 4h da manhã da segunda-feira dia 30/06, um executivo da BMP Money Plus, uma fintech que oferece serviços de “banking as a service”, recebeu uma ligação de um funcionário de outro banco, CorpX Bank, informando que R$18 milhões haviam sido transferidos da conta da BMP para aquele banco. Nesse momento o executivo, que atua como Piloto de reservas da BMP, identificou diversas outras transferências via PIX não autorizadas ocorrendo no mesmo horário. Dessa forma a empresa tomou conhecimento do golpe e começou a agir para identificar e conter o incidente. As 5h do dia 30/06 o executivo acionou a C&M Software. Segundo reportagem do primeiro

veículo a noticiar o caso, o portal Brazil Journal, foram extraviados R$400 milhões da conta reserva da BMP, que conseguiu recuperar R$160 milhões.

Segundo relatos compartilhados com a imprensa, os invasores teriam explorado vulnerabilidades nos sistemas da C&M Software para escalar privilégios de acesso, conseguindo atingir diversas contas de clientes corporativos conectados à plataforma. A partir da obtenção do acesso, eles começaram a movimentar fundos da conta reserva de pelo menos seis entidades bancárias clientes da C&M. Um dos principais alvos foi a BMP Money Plus, instituição financeira especializada em serviços de banking-as-a-service (BaaS).

Após roubar o dinheiro, o cibercriminoso começou a movimentar os valores para diferentes provedores de criptomoedas que trabalham com Pix, como exchanges, gateways, sistemas de swap para cripto integrados com pix e mesas OTC, para comprar USDT e Bitcoin. Em um dos casos, ao identificar um volume expressivo de transações, o provedor teria bloqueado as operações, avisado a BMP (uma das instituições que mais sofreu com o ataque) e impedido a conversão dos valores para USDT.

Para conter a movimentação dos fundos acessados pelo ataque, o Banco Central emitiu uma suspensão cautelar contra a C&M do sistema de transferência bancário nacional, o que afetou a operação do Pix em quase 300 instituições conectadas por meio da empresa.

Apesar do prejuízo milionário, a BMP declarou que nenhum cliente foi impactado ou teve seus recursos acessados e que possui colaterais suficientes para cobrir 100% do valor vilipendiado.

Acionada pelo Banco Central, a Polícia Federal abriu um inquérito para apurar os crimes de organização criminosa, furto mediante fraude, invasão de dispositivo de informática e lavagem de dinheiro.

2.1 Linha do tempo

As notícias publicadas pela imprensa até o momento permitem construir uma linha do tempo aproximada sobre o incidente ocorrido na C&M Software:

- 30/06/2025, 00:18 (Hora de Brasília) — As plataformas da SmartPay e Truther identificaram um movimento atípico de compra de criptomoedas.
- 30/06/2025, 04:00 (Hora de Brasília) — O Piloto de Reserva da BMP é notificado, por um executivo de outro banco, sobre o recebimento de um PIX de R$18 milhões realizado naquele momento. A partir deste evento, a BMP toma conhecimento da realização de algumas transações PIX não autorizadas.

- 30/06/2025, 05:00 (Hora de Brasília) — O piloto de reserva da BMP acionou a C&M Software para comunicar sobre as transações indevidas.
- 30/06/2025 — Como medida preventiva, a C&M foi desconectada temporariamente do Sistema de Pagamentos Brasileiro (SPB) pelo Banco Central.
- 01/07/2025 — O portal Brazil Journal é o primeiro veículo da mídia a noticiar o incidente.
- 02/07/2025 — A BMP publica uma nota oficial em seu site sobre o incidente.
- 03/07/2025, 09:59 — O Banco Central anunciou a retomada parcial das operações da C&M Software.

2.2 Impactos do incidente

O incidente envolveu a transferência ilícita de um valor ainda não determinado de diversas "contas reservas" de instituições financeiras nacionais. As estimativas anunciadas pela imprensa, citando fontes relacionadas às investigações, variam de R$ 400 milhões, R$ 800 milhões, R$ 1 bilhão e podendo chegar a até R$ 4 bilhões.

Mesmo sem a identificação precisa do valor desviado no golpe, é possível afirmar que trata-se do maior crime cibernético da história do Brasil, em termos de valores envolvidos.

Além do impacto financeiro imediato causado pela fraude, diversas instituições financeiras que utilizam o serviço da C&M Software ficaram impossibilitadas de transacionar no sistema financeiro nacional de 30 de junho a 03 de julho, causando possíveis impactos a seus clientes.

2.3 Entidades envolvidas no incidente

A identidade de todas as organizações envolvidas no ataque à C&M Software não é conhecida, uma vez que as notícias que surgiram até o momento não identificaram todas as instituições financeiras que foram fraudadas em função do ciber ataque. Os relatos diferem, inclusive, da quantidade de vítimas, uma vez que alguns portais de notícias mencionam 6 instituições prejudicadas, e outras oito. O Banco Central não informou quais instituições foram afetadas.

Até o momento da escrita deste relatório, somente a BMP Money Plus assumiu publicamente ter sido vítima do desvio de fundos através da invasão da C&M Software.

C&M Software (https://cmsw.com): Empresa brasileira que presta serviços de infraestrutura para o setor financeiro, na categoria de Prestador de Serviços de

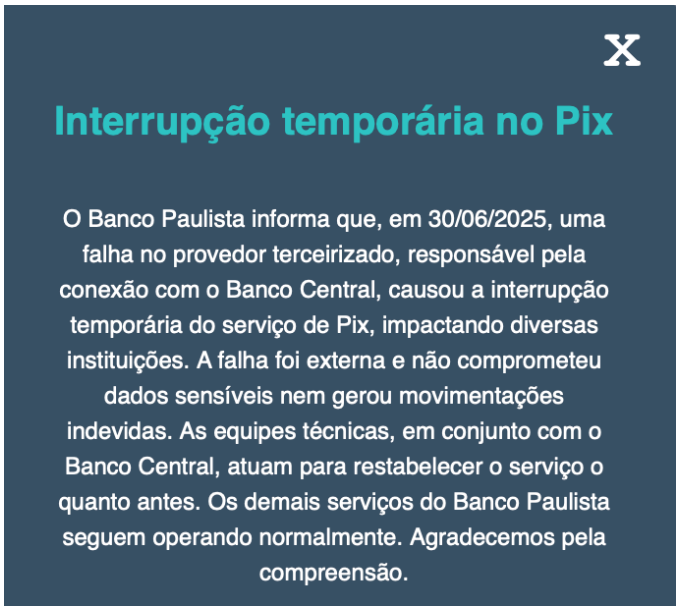
Tecnologia da Informação (PSTI) autorizada pelo Banco Central, incluindo operações críticas como processamento de compensações, transferências e liquidações. A empresa não tem se manifestado oficialmente por orientação jurídica e em respeito ao sigilo das investigações.

BMP Money Plus (https://moneyp.com.br): Instituição financeira especializada em serviços de banking-as-a-service (BaaS), que oferece serviços a 92 fintechs e 210 fundos de investimento. Segundo os relatos compartilhados na imprensa, ela foi um dos principais alvos do golpe, tendo sido desviados R$ 400 milhões de sua conta reserva. A empresa alega ter recuperado R$ 160 milhões. A empresa tem adotado uma postura de transparência sobre o caso.

Banco Central do Brasil: Entidade governamental responsável pelo sistema financeiro brasileiro.

Credsystem: Uma das instituições financeiras que, supostamente, teve ativos desviados durante o ataque à C&M Software em 30 de junho.

Banco Paulista (https://www.bancopaulista.com.br): Uma das instituições financeiras que foi impactada pelo ataque à C&M Software em 30 de junho. Em seu website, a instituição apresenta um pop-up notificando sobre a suspensão temporária de transações PIX em 30/06 e afirma que "a falha foi externa e não comprometeu dados sensíveis nem gerou movimentações indevidas".



2.3 Posicionamento das Autoridades e empresas envolvidas

Segundo relatos compartilhados pela imprensa brasileira, o Banco Central foi notificado do incidente imediatamente, em 30 de junho, e acompanha de perto as investigações. Como medida preventiva, em 30 de junho a C&M Software foi desconectada temporariamente do Sistema de Pagamentos Brasileiro (SPB) para mitigar riscos de novas movimentações irregulares.

Em nota ao portal Bastidor, o Banco Central confirmou o ataque a C&M e afirmou que determinou o desligamento do acesso à plataforma da empresa: "A C&M Software, prestadora de serviços de tecnologia para instituições provedoras de contas transacionais que não possuem meios de conexão própria, comunicou ataque à sua infraestrutura tecnológica. O Banco Central determinou à C&M o desligamento do acesso das instituições às infraestruturas por ela operadas".

Em 01/07 a BMP publicou uma nota oficial aos parceiros da BMP Plus, informando que o serviço de PIX estava temporariamente interrompido devido a um ataque cibernético que comprometeu parcialmente a infraestrutura de conexão da C&M Software (sem citar o nome da instituição).

IMPORTANTE | INTERRUPÇÃO TEMPORÁRIA NO SERVIÇO DE PIX

Olá, parceiro!

Informamos que, na data de ontem, 30/06/2025, o ambiente de mensageria utilizado por um **Provedor de Serviços de Tecnologia da Informação (PSTI)** terceirizado, autorizado e supervisionado pelo Banco Central do Brasil — **responsável por intermediar a comunicação entre instituições financeiras e o Banco Central do Brasil — sofreu um ataque cibernético que comprometeu parcialmente sua infraestrutura de conexão.**

Como resultado, os serviços de Pix foram temporariamente interrompidos em **diversas instituições financeiras clientes deste PSTI, incluindo a BMP.**

A falha técnica ocorreu fora do ambiente interno da BMP, não causando movimentações atípicas em contas de nossos clientes. O problema está sendo **tratado com máxima prioridade pelas equipes de segurança e tecnologia** da informação, **tanto da fornecedora quanto das instituições afetadas.**

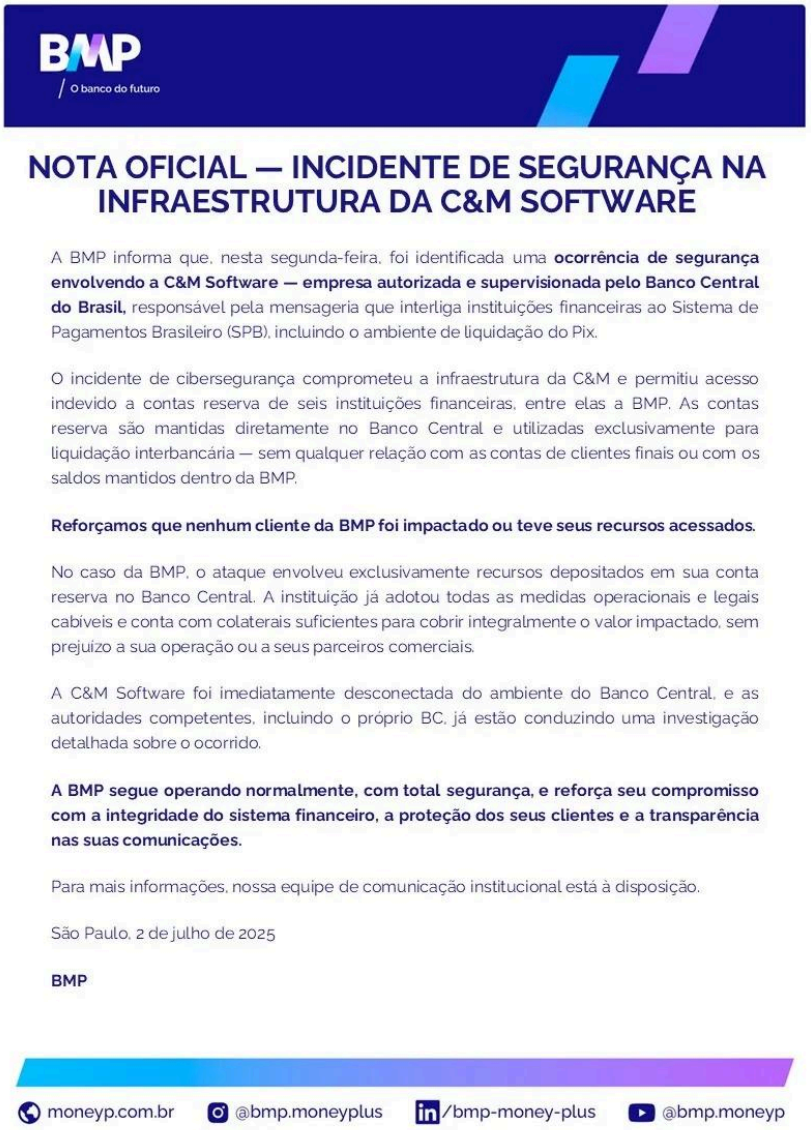
O Banco Central já foi oficialmente comunicado, e medidas de contenção e restabelecimento estão em andamento, com acompanhamento contínuo das autoridades competentes.

Ressaltamos que nenhum dado sensível foi comprometido e que os **demais serviços da BMP seguem operando normalmente**. Manteremos nossos parceiros informados sobre a normalização do serviço assim que possível.

Agradecemos pela compreensão.

EQUIPE BMP

Em 02/07 a BMP publicou uma nota oficial em seu website, reconhecendo o incidente que envolveu a C&M Software, e destacando que não houve impacto nem acesso a dados de seus clientes:



BMP

O banco do futuro

NOTA OFICIAL — INCIDENTE DE SEGURANÇA NA INFRAESTRUTURA DA C&M SOFTWARE

A BMP informa que, nesta segunda-feira, foi identificada uma **ocorrência de segurança envolvendo a C&M Software — empresa autorizada e supervisionada pelo Banco Central do Brasil,** responsável pela mensageria que interliga instituições financeiras ao Sistema de Pagamentos Brasileiro (SPB), incluindo o ambiente de liquidação do Pix.

O incidente de cibersegurança comprometeu a infraestrutura da C&M e permitiu acesso indevido a contas reserva de seis instituições financeiras, entre elas a BMP. As contas reserva são mantidas diretamente no Banco Central e utilizadas exclusivamente para liquidação interbancária — sem qualquer relação com as contas de clientes finais ou com os saldos mantidos dentro da BMP.

Reforçamos que nenhum cliente da BMP foi impactado ou teve seus recursos acessados.

No caso da BMP, o ataque envolveu exclusivamente recursos depositados em sua conta reserva no Banco Central. A instituição já adotou todas as medidas operacionais e legais cabíveis e conta com colaterais suficientes para cobrir integralmente o valor impactado, sem prejuízo a sua operação ou a seus parceiros comerciais.

A C&M Software foi imediatamente desconectada do ambiente do Banco Central, e as autoridades competentes, incluindo o próprio BC, já estão conduzindo uma investigação detalhada sobre o ocorrido.

A BMP segue operando normalmente, com total segurança, e reforça seu compromisso com a integridade do sistema financeiro, a proteção dos seus clientes e a transparência nas suas comunicações.

Para mais informações, nossa equipe de comunicação institucional está à disposição.

São Paulo, 2 de julho de 2025

BMP

moneyp.com.br @bmp.moneyplus /bmp-money-plus @bmp.moneyp

No dia 03/07, quinta-feira, o Banco Central publicou uma nota oficial em seu portal, anunciando a retomada parcial das operações da C&M Software:

A suspensão cautelar da C&M foi substituída por uma suspensão parcial

Publicado 03/07/2025 às 09:59
Atualizado 03/07 às 09:59

Compartilhe: Imprimir

A decisão foi tomada após a empresa adotar medidas para mitigar a possibilidade de ocorrência de novos incidentes.

As operações da C&M poderão ser restabelecidas em dias úteis, das 6h30 às 18h30, desde que haja anuência expressa da instituição participante do Pix e o robustecimento do monitoramento de fraudes e limites transacionais.

2.4 Análise do Ciberataque

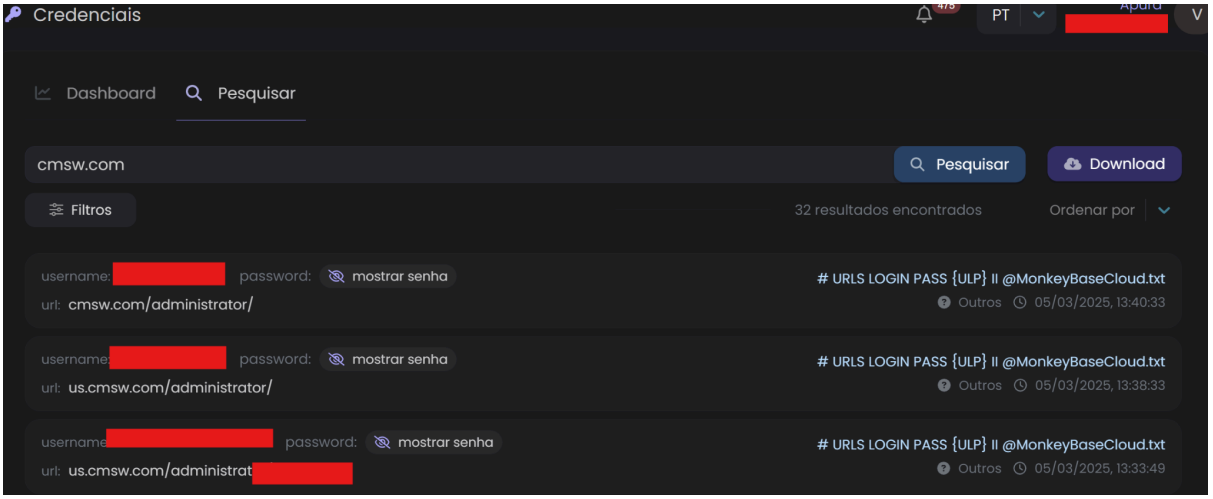
Há indícios de que o ataque a C&M Software envolveu acesso remoto ao ambiente e aos sistemas de processamento de transações do SPB mantidos pela empresa. Uma vez com acesso ao sistema, o atacante deve ter obtido acesso às credenciais das instituições financeiras, clientes da C&M, o que lhe deu acesso aos certificados e chaves privadas necessários para executar transações PIX fraudulentas, diretamente via SPI através dos sistemas da C&M.

Com base na análise do caso, segue um suposto modus operandi estabelecido pela pesquisa da **Apura** de como teria se dado as etapas da fraude.

Acesso ao Ambiente Interno

Supostamente, segundo diversos relatos reproduzidos pela imprensa, os atacantes exploraram eventuais vulnerabilidades no ambiente tecnológico da C&M Software e utilizaram ferramentas de acesso remoto (RMM) para entrar no ambiente da C&M. O vetor inicial não foi confirmado, mas o uso de credenciais vazadas ou vulnerabilidades de acesso remoto é cogitado.

A partir do BTTng, identificamos o vazamento de 32 credenciais da C&M, incluindo senhas supostamente de administrador. Tais credenciais, caso estivessem válidas no momento do incidente, poderiam ser um possível vetor de acesso.



Reconhecimento e Mapeamento

Uma vez obtido acesso inicial ao ambiente da C&M Software, os invasores teriam realizado um mapeamento da infraestrutura e do funcionamento do sistema de transferências, identificando como as transações PIX eram estruturadas e onde estavam armazenados os artefatos críticos de autenticação.

Neste momento, os atacantes possivelmente mapearam as instituições financeiras clientes da C&M e que possuíam credenciais armazenadas com a mesma, possivelmente usando enumeração. Acreditamos que, nessa fase, os atacantes identificaram as instituições financeiras em que era possível ter acesso às suas contas reservas.

Comprometimento de Credenciais Sensíveis

Em nossa análise, supostamente o ator obteve o acesso às credenciais das instituições financeiras e, possivelmente, até mesmo às chaves privadas e os certificados digitais utilizados por instituições clientes da fornecedora para assinar as transações PIX. Em geral, tais chaves são compartilhadas com o PSTI para realizar a assinatura das transações.

Segundo o G1, em nota, o diretor comercial da C&M Software, Kamal Zogheib, afirmou que a empresa foi vítima direta de uma ação criminosa, que envolveu o uso indevido de credenciais de clientes para acessar seus sistemas e serviços de forma fraudulenta.

Com essas informações e o acesso privilegiado ao sistema da C&M e às contas das instituições financeiras, os atacantes assumiram a capacidade de injetar transações legítimas no SPI em nome dessas instituições.

Execução Massiva de Transações PIX

Utilizando as credenciais e os certificados comprometidos, os invasores teriam injetado transações diretamente no SPI em nome das instituições financeiras, a partir da plataforma da C&M Software, que foram processadas normalmente pelas instituições financeiras, já que:

- As mensagens estavam devidamente assinadas pelas instituições de origem, uma vez que o sistema da C&M estava comprometido;
- Havia lastro para realização dessas transações, baseado no depósito feito na "conta reserva" junto ao Banco Central;
- O SPI não realiza validação de saldo, legitimidade do pagador ou análise antifraude — assume que isso foi feito previamente pela instituição.

As transações entre instituições financeiras brasileiras somente podem ser inseridas no sistema de pagamentos brasileiro a partir de sistemas autorizados e específicos, que têm acesso às chaves privadas das instituições para assinar digitalmente as transações - conforme exigência técnica do SPB. Portanto, tal ataque envolveu o conhecimento de tais sistemas e protocolos, além do acesso privilegiado aos mesmos, e não poderia ser reproduzido a partir de outro sistema.

Além do acesso privilegiado aos sistemas da C&M Software, observamos que os atacantes possivelmente optaram intencionalmente por fazer as transferências de fundos fora do horário comercial. Ao realizar a fraude no período da madrugada de domingo para segunda-feira, o fizeram provavelmente na expectativa de que seria um horário mais difícil para haver monitoramento humano e, assim, alguém identificar e interromper as transações fraudulentas. Nesse momento, a funcionalidade de transferências instantâneas e a qualquer hora do PIX foi uma grande aliada dos cibercriminosos.

Acreditamos que as movimentações teriam ocorrido até o esgotamento dos saldos nas contas de liquidação (contas de reserva) ou até serem identificadas e interrompidas pelas entidades envolvidas.

Destino dos Recursos

Há fortes indícios de que a maioria das transações foram direcionadas inicialmente a contas correntes em **instituições de pagamento de menor porte**, que geralmente possuem controles mais brandos de onboarding e verificação (KYC), facilitando a abertura e manipulação de contas em nome de laranjas. A transferência via PIX deu agilidade na evasão dos recursos.

Lavagem e Dispersão

Após a exfiltração dos recursos para contas laranjas, os valores foram rapidamente dispersos em pequenas transações e supostamente também convertidos em criptoativos, dificultando o rastreio e bloqueio dos valores desviados. Segundo notícias, parte dessas transações foram identificadas como suspeitas e bloqueadas em algumas exchanges.

2.5 O caso e o cenário do cibercrime brasileiro em 2025

O incidente na C&M Software envolveu o comprometimento de componentes tecnológicos e processos muito específicos do sistema financeiro brasileiro. Isso nos leva a crer que o ator responsável pelo incidente tem familiaridade com o país e, possivelmente, pode haver colaboração de pessoas com experiência no setor financeiro.

Analisando as especificidades deste caso e comparando com o cenário atual de atores de ameaça no Brasil é possível perceber similaridades com o grupo Plump Spider. Este ator brasileiro, já conhecido pela comunidade de inteligência, tem foco em instituições financeiras, não apenas bancos, mas também empresas que têm atividades financeiras.

O grupo, de origem brasileira, está ativo desde 2023 e acumula quase dois anos de atividades cibercriminosas sem qualquer identificação pelas autoridades.

Até o momento da escrita deste relatório, ainda não há evidências nem notícias sobre a possível identidade dos atores responsáveis pelo ataque à C&M Software, seu modus operandi ou afiliação.

3. Mapeamento MITRE ATT&CK

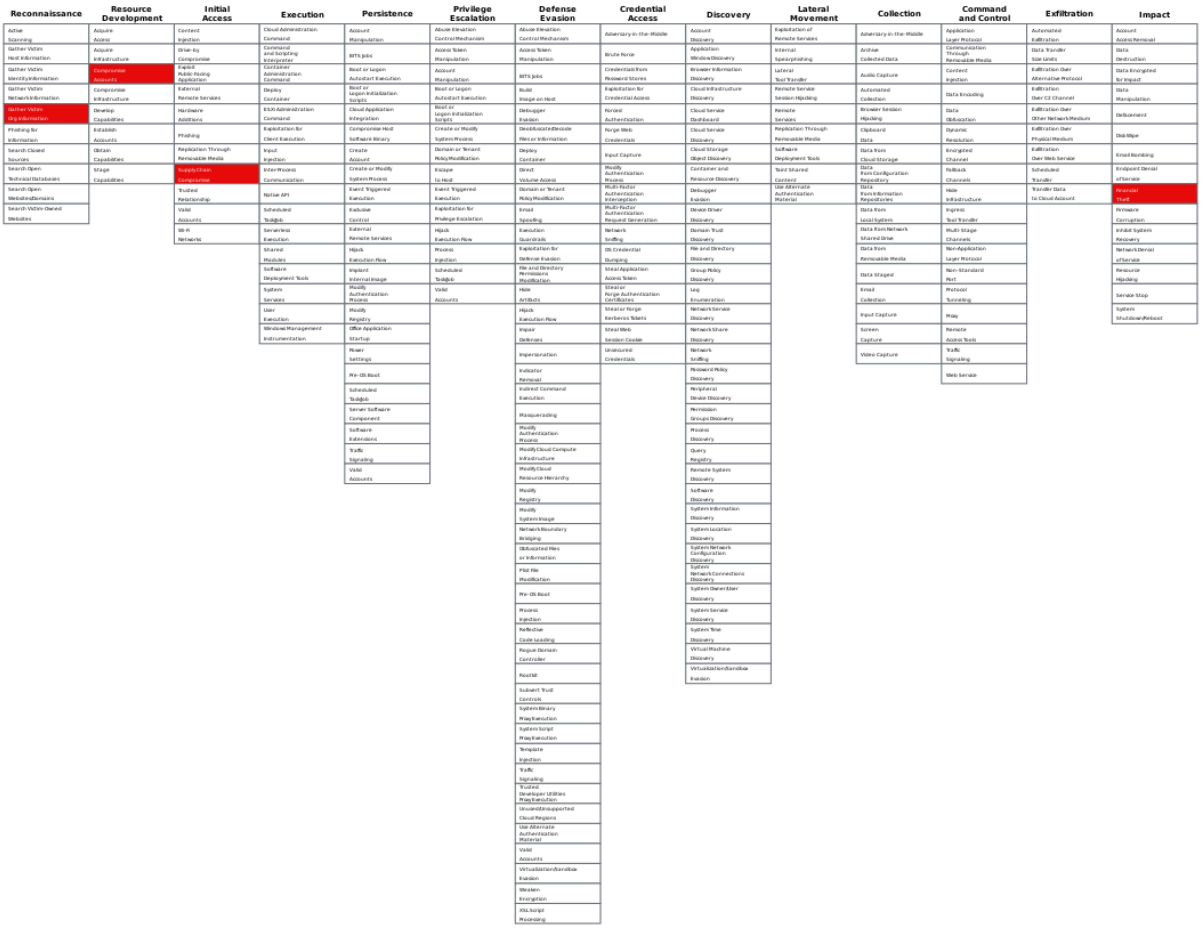
Baseado nas informações públicas do incidente, podemos apontar alguns dos possíveis passos realizados pelo ator durante a exploração da C&M Software, em termos de Táticas, Técnicas e Procedimentos (TTPs) conhecidos, com base no framework MITRE ATT&CK.[1]

O mapeamento abaixo foi realizado considerando as informações disponíveis na imprensa sobre o incidente, uma vez que os detalhes do ataque não foram divulgados. Desta forma, muitas informações importantes para entender o ataque e mapeá-lo corretamente não são conhecidas até o momento.

[1] https://attack.mitre.org

A seguir apresentamos os **supostos** passos do ciberataque, mapeados segundo o framework MITRE ATT&CK (Enterprise ATT&CK v17):

Reconhecimento (Reconnaissance)		
T1591.002	Coletar Informações sobre a Organização da Vítima / Relacionamentos de Negócio	Os criminosos mapearam uma empresa que atuasse como PSTI junto ao SPB e identificaram as organizações financeiras a qual presta serviço.
Desenvolvimento de Recursos (Resource Development)		
T1586	Contas comprometidas	Os criminosos exploraram contas comprometidas relacionadas aos serviços da C&M Software e de seus clientes financeiros, que foram usadas posteriormente para acesso e transferência de fundos.
Acesso Inicial (Initial Access)		
T1195.002	Comprometimento da Cadeia de Suprimentos / Comprometimento de Softwares Adversários da Cadeia de Suprimentos	Os atores manipularam os sistemas transacionais da C&M Software utilizados por seus clientes, com o objetivo de injetar transações fraudulentas no SPI à revelia dos mesmos.
Impacto (Impact)		
T1657	Roubo Financeiro	Um volume significativo de recursos financeiros foi desviado de instituições financeiras que utilizavam a plataforma da C&M Software.



4. Sobre o Sistema de Pagamentos Brasileiro e os Provedores de Serviços de Tecnologia da Informação

Nos bastidores do sistema financeiro brasileiro, boa parte da tecnologia que faz tudo funcionar — abertura de contas, pagamentos via Pix, análise de crédito, onboarding, prevenção a fraudes — não está diretamente nas mãos dos bancos ou fintechs, mas com terceiros. São empresas que operam APIs, processam transações, validam identidades, cuidam da infraestrutura e, muitas vezes, mantêm o core bancário de instituições inteiras, os chamados **PSTIs — Prestadores de Serviços de Tecnologia da Informação**.

Esse modelo, que ganhou força com o boom das fintechs e o avanço do open finance, trouxe agilidade, redução de custos e acesso rápido a soluções financeiras. Mas também **criou um ecossistema altamente dependente de terceiros críticos**, onde uma falha pontual pode escalar e atingir múltiplos players ao mesmo tempo.

4.1 Definição de PSTIs

PSTI é a sigla para Prestador de Serviço de Tecnologia da Informação, dentro do ecossistema do sistema financeiro brasileiro. São empresas terceiras autorizadas pelo Banco Central, contratadas por instituições financeiras para executar funções essenciais de tecnologia para acesso ao sistema bancário — desde o desenvolvimento de sistemas até a oferta de plataformas inteiras que sustentam operações críticas, como pagamentos, validação de identidade, gestão de dados e até mesmo o core bancário.

Esses prestadores estão por trás de serviços que vão muito além do suporte técnico tradicional. São eles que oferecem, por exemplo:

- Plataformas de Banking as a Service (BaaS)
- Integração com o SPB
- Plataformas de comunicação e transação com o Sistema Financeiro Nacional (SFN)
- Desenvolvimento e manutenção de software sob medida
- Armazenamento em nuvem e serviços de infraestrutura
- Gerenciamento de identidade e acesso (IAM, autenticação, KYC)
- Suporte, helpdesk e gestão de operações em tempo real

Para fins de acesso à Rede do Sistema Financeiro Nacional (RSFN), as PSTIs atuam como gateways transacionais entre as instituições financeiras, processando operações de liquidação e integração com o sistema bancário nacional, incluindo, por exemplo, transferências via TED e Pix, emissão e pagamento de boletos, etc.

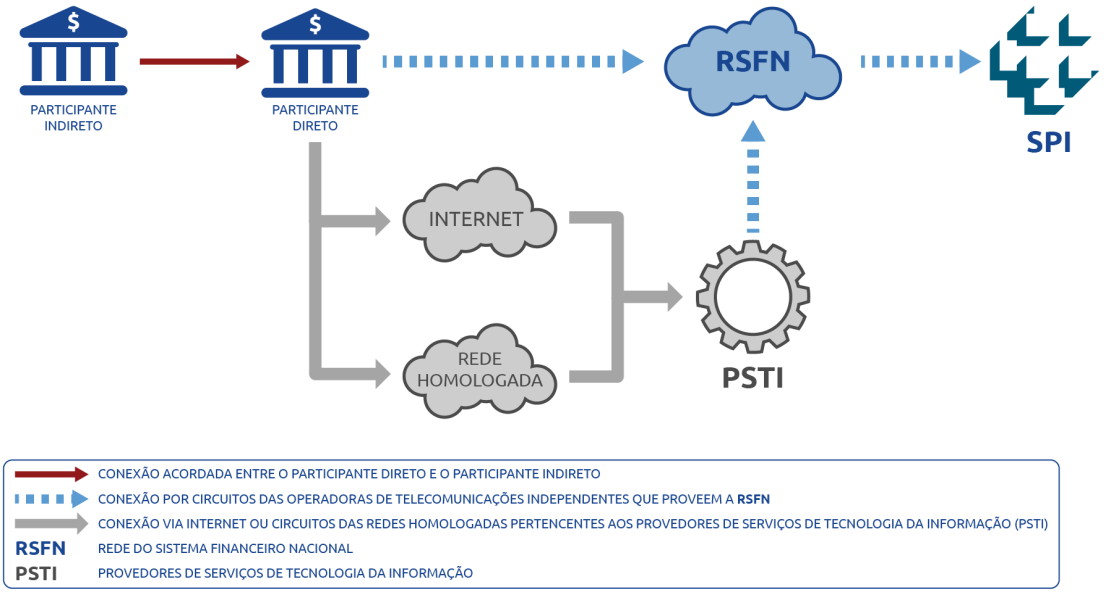


Imagem: Formas de acesso ao Sistema de Pagamentos Instantâneos, através dos PSTIs

Em setores altamente regulados, como o financeiro, o PSTI pode ser classificado como **terceiro crítico**, o que significa que, do ponto de vista regulatório, a responsabilidade por falhas, vazamentos ou indisponibilidade não é só dele mas também de quem o contratou. As obrigações de segurança, continuidade e conformidade precisam ser tratadas com o mesmo rigor que a operação interna.

Principais fornecedores autorizados pelo Banco Central:

- **ABBC –** Associação Brasileira de Bancos.
- **C&M Software** – Provedora de compensações, interligação de contas e acesso ao sistema de pagamentos. Foi a origem do ataque recente.
- **GOKEI Tecnologia -** Diferencia-se por oferecer em um ambiente Cloud de alta performance e disponibilidade, utilizando a comunicação cliente com o PSTI através de recursos 100% em nuvem.
- **JD Consultores** - Oferece soluções financeiras há 24 anos.
- **MAPS** - Há 30 anos fornece soluções para pagamentos e liquidação financeira pelo SPB e SPI.
- **Sinqia (ex-MasterSAF, Icaro)** – Soluções para liquidação e integração bancária.
- **Stark** – Criada em 2022, fornece infraestrutura para instituições financeiras e fintechs.

Também constam como PSTIs homologadas a TIVIT e a TOPAZ.

5. Recomendações

As análises apresentadas anteriormente neste relatório demonstram que os atores de ameaça, representam um risco estratégico direto, capaz de gerar perdas financeiras significativas, danos à reputação da marca e interrupções operacionais severas.

Em resposta a esta ameaça, elaboramos um guia estratégico de mitigação projetado para aumentar a resiliência corporativa e proteger o valor do negócio a partir de quatro pilares fundamentais:

- **Fortalecimento Proativo das Defesas:** Medidas preventivas para reduzir a superfície de ataque e dificultar o comprometimento inicial.
- **Capacidade de Detecção e Resposta Avançada:** Implementação de tecnologias e processos para identificar e neutralizar rapidamente as ameaças que penetram o perímetro.
- **Inteligência de Ameaças Acionável:** Utilização de inteligência para antecipar e caçar ameaças de forma proativa.
- **Gestão de Risco da Cadeia de Suprimentos:** Controles rigorosos para mitigar os riscos introduzidos por parceiros e fornecedores de TI.

5.1 Fortalecimento da Superfície de Ataque Contra o Comprometimento Inicial

Gestão de Vulnerabilidades e Patches: Aplicar patches de segurança em sistemas voltados para a internet, especialmente em gateways de VPN, RDP e softwares empresariais comuns. Priorizar vulnerabilidades conhecidas por serem exploradas por APTs e grupos de ransomware.

Manutenção de Credenciais e Mecanismos de Autenticação: Implementar senhas fortes e únicas e, mais criticamente, exigir Autenticação Multifator (MFA) resistente a

phishing em todos os pontos de acesso remoto, e-mail e aplicações em nuvem. Este é o controle mais eficaz contra ataques baseados em credenciais.

Acesso Remoto Seguro: Evitar a publicação de portas que forneçam acesso a serviços críticos como RDP, Server Message Block (SMB), Telnet, e NetBIOS por exemplo. Caso seja absolutamente necessária a exposição de tal porta, execute o acesso remoto através de um gateway seguro, com MFA ativo.

5.2 Defesa Pós Comprometimento

Detecção Baseada em Comportamento: Implantar soluções de segurança avançadas que utilizem Indicadores de Comportamento além dos tradicionais Indicadores de Comprometimento (IOCs). Isso permite a detecção de cadeias de atividades maliciosas sutis, como uma ferramenta de administração legítima sendo usada para iniciar o PowerShell para movimento lateral.

Visibilidade de Endpoint e Rede: Implementar soluções robustas de Detecção e Resposta de Endpoint (EDR) e segmentação de rede. O EDR fornece visibilidade sobre a execução de processos nos endpoints (por exemplo, winword.exe gerando regsvr32.exe, um TTP do TA551) , enquanto a segmentação pode conter o movimento lateral de um invasor.

Registro e Monitoramento: Garantir o registro abrangente de toda a atividade da rede, especialmente de contas privilegiadas e conexões de terceiros. Auditar regularmente esses logs em busca de comportamento anômalo.

5.3 Inteligência Proativa e Threat Hunting

Monitoramento da Dark Web: Monitorar ativamente fóruns da dark web, mercados ilegais e canais do Telegram em busca de menções ao nome da sua organização, domínios ou credenciais comprometidas.

Monitoramento de Logs de Infostealer: Utilizar serviços que rastreiam e analisam logs de malware infostealer para descobrir proativamente se credenciais de funcionários ou corporativas foram comprometidas e estão em circulação. Isso permite a redefinição de credenciais antes que sejam usadas por um ator de ameaças.

5.4 Protegendo a Cadeia de Suprimentos de TI

Gestão de Risco de Fornecedores: Para organizações que utilizam PSTIs, conduzir avaliações de segurança rigorosas do seu provedor. Os contratos devem exigir controles de segurança específicos, incluindo MFA em todas as contas usadas para acessar seu ambiente.

Princípio do Menor Privilégio para Terceiros: Garantir que as contas do PSTI tenham apenas o nível mínimo de acesso necessário para realizar suas funções. O acesso delas deve ser estritamente monitorado e auditado.

Modelo de Responsabilidade Compartilhada: Definir claramente nos contratos quem é responsável por funções de segurança como fortalecimento, detecção e resposta a incidentes.

6. O Que Podemos Concluir Até Agora

O incidente ocorrido na C&M Software no dia 30 de junho já entrou para a história como o maior roubo cibernético do Brasil, graças aos valores exorbitantes envolvidos.

O ataque traz níveis complexos de sofisticação, que demandam um conhecimento profundo do funcionamento do Sistema de Pagamentos Brasileiro (SPB), incluindo seus protocolos, sistemas e terceiros envolvidos. De fato, tais operações fraudulentas, por suas características, somente poderiam ser manipuladas e inseridas no sistema financeiro a partir do acesso indevido e malicioso aos sistemas de processamento de transações conectados ao SPB (Sistema de Pagamentos Brasileiro).

Isso, aliado ao esforço necessário para exfiltrar grandes valores monetários via PIX e criptomoedas, indicam que a operação foi complexa e demandou grande planejamento e preparação. Acreditamos, portanto, que o incidente foi realizado por um grupo preparado e especializado, e não um ator solitário. Não descartamos a hipótese de participação de insiders, dado a grande especificidade dos sistemas envolvidos.

As investigações estão em andamento e qualquer conclusão sobre a natureza e autoria do ataque, neste momento, seria precipitada.

Pelo grande impacto envolvido, acredita-se que este incidente vai motivar uma grande revisão dos protocolos de segurança do Sistema Financeiro Nacional. Embora o SFN adote protocolos tecnicamente robustos de comunicação e mensageria, o incidente com a C&M Software em 30 de junho de 2025 mostrou a fragilidade de todo o sistema a partir do comprometimento de um único fornecedor - um cenário clássico de comprometimento na cadeia de suprimentos.

Clientes da Apura Cyber Intelligence tem acesso, através da plataforma BTTng, ao relatório detalhado, que é atualizado tempestivamente, a cada novidade relevante sobre o incidente.

7. Referências

Exclusivo: Hackers levam mais de R$ 1 bilhão de ‘banking as a service’ - https://braziljournal.com/exclusivo-hackers-levam-mais-de-r-1-bilhao-em-ataque-a-banking-as-a-service/

Ataque ao sistema financeiro - https://obastidor.com.br/economia/ataque-ao-sistema-financeiro-8979

Na madrugada, um pix de R$ 18 milhões. Começava o ataque: https://braziljournal.com/na-madrugada-um-pix-de-r-18-milhoes-comecava-o-assalto/

Hackers roubam R$ 1 bilhão em contas do sistema financeiro nacional e tentam converter em Bitcoin e USDT - https://br.cointelegraph.com/news/hackers-steal-r-1-billion-from-the-central-bank-of-brazil-s-reserve-account-and-convert-it-into-bitcoin-and-usdt

CEO da BPM conta passo a passo os bastidores do roubo que fez R$ 400 milhões sumirem da conta da empresa - https://neofeed.com.br/negocios/a-anatomia-de-um-crime-ceo-da-bmp-conta-passo-a-passo-os-bastidores-do-roubo-que-fez-r-400-milhoes-sumirem-da-conta-da-empresa/

PF abre inquérito para apurar ataque a sistemas de instituições financeiras; BC não foi afetado - https://g1.globo.com/economia/noticia/2025/07/02/pf-vai-abrir-inquerito-para-apurar-ataque-a-sistemas-de-instituicoes-financeiras-bc-nao-foi-afetado.ghtml

Nota oficial da BMP: https://moneyp.com.br/comunicados/nota-oficial-bmp-ataque-c-m-software/

Nota do Banco Central: A suspensão cautelar da C&M foi substituída por uma suspensão parcial: https://www.bcb.gov.br/detalhenoticia/20752/nota

Comunicação eletrônica de dados no sistema financeiro - https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados

8. Glossário

Certificados (Digitais) - Documentos eletrônicos emitidos por uma Autoridade Certificadora (AC) que atestam a identidade de uma entidade (pessoa, empresa ou sistema) e vinculam essa identidade a uma chave criptográfica.

Contas reserva - Depósitos mantidos pelas instituições financeiras diretamente no Banco Central e utilizadas exclusivamente para liquidação interbancária.

Contas Laranja - Contas bancárias abertas em nome de terceiros (pessoas físicas ou jurídicas) para fins de fraude, geralmente com pouca ou nenhuma consciência sobre o uso ilícito da conta.

Criptoativos - Ativos digitais criptografados, transferidos e armazenados por meio de tecnologias de registro distribuído, como o blockchain.

Fintechs - Empresas que introduzem inovações nos mercados financeiros por meio do uso intenso de tecnologia, com potencial para criar novos modelos de negócios. Atuam por meio de plataformas online e oferecem serviços digitais inovadores relacionados ao setor.

Participante do SFN – refere-se a qualquer instituição autorizada pelo Banco Central ou ente de governo cujos sistemas se comunicam eletronicamente através da SFN. Os participantes do SFN interagem por meio de mensagens e de arquivos, nas redes homologadas pelo Banco Central.

Piloto de Reservas - Profissional responsável por monitorar e gerenciar as contas de reservas bancárias ou de liquidação de uma instituição financeira. Sua principal função é garantir a liquidez da instituição, através da precisão e confiabilidade dos saldos dessas contas, verificando e registrando todos os lançamentos a débito ou crédito.

Provedores de Serviços de Tecnologia da Informação (PSTI) - Entidades autorizadas pelo Banco Central a prestar serviços de processamento de dados, para fins de acesso à RSFN, a instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Rede do Sistema Financeiro Nacional (RSFN) - A RSFN é uma estrutura de comunicação de dados entre instituições financeiras brasileiras que tem por finalidade amparar o tráfego de informações no âmbito do SFN para serviços autorizados.

Remote Monitoring and Management (RMM) - Tecnologia utilizada por equipes de TI para monitorar, gerenciar e acessar remotamente computadores, servidores e dispositivos de rede.

Sistema Financeiro Nacional (SFN) - Entidade formada por um conjunto de entidades e instituições que promovem a intermediação financeira, isto é, o encontro entre credores e tomadores de recursos. É por meio do sistema financeiro que as pessoas, as empresas e o governo circulam a maior parte dos seus ativos, pagam suas dívidas e realizam seus investimentos.

Sistema de Pagamentos Brasileiro (SPB) - Um conjunto de regras, procedimentos, instituições e sistemas gerenciado pelo Banco Central que, através de infraestruturas, regras e procedimentos, viabilizam as transações financeiras no Brasil. Ele engloba desde operações de transferência de recursos, como TEDs e Pix, até a liquidação de pagamentos com cartões e boletos.

Sistema de Pagamentos Instantâneos (SPI) - Infraestrutura centralizada e única para liquidação de pagamentos instantâneos entre instituições distintas no Brasil. A operação do SPI, gerida pelo BCB, teve início em Novembro de 2020. O SPI é um sistema que faz liquidação bruta em tempo real (LBTR), ou seja, que processa e liquida transação por transação. Uma vez liquidadas, as transações são irrevogáveis.

0800 719 1902

info@apura.io

apura.io

linkedin.com/company/apura

BRASÍLIA
SNH Qd. 1 Lote A,
Ed. Le Quartier, sala 1413
CEP: 70.077-000
Tel: +55 (61) 3255-1245

SÃO PAULO
Av. Paulista 2.421,
1° andar, Jardins
CEP: 01.310-300
Tel: +55 (11) 5504-1966

MIAMI
299 Alhambra Circle, Suite 403
Coral Gables, Flórida
Zip Code: 33134
Tel./FAX: +1 (305) 5504-1966