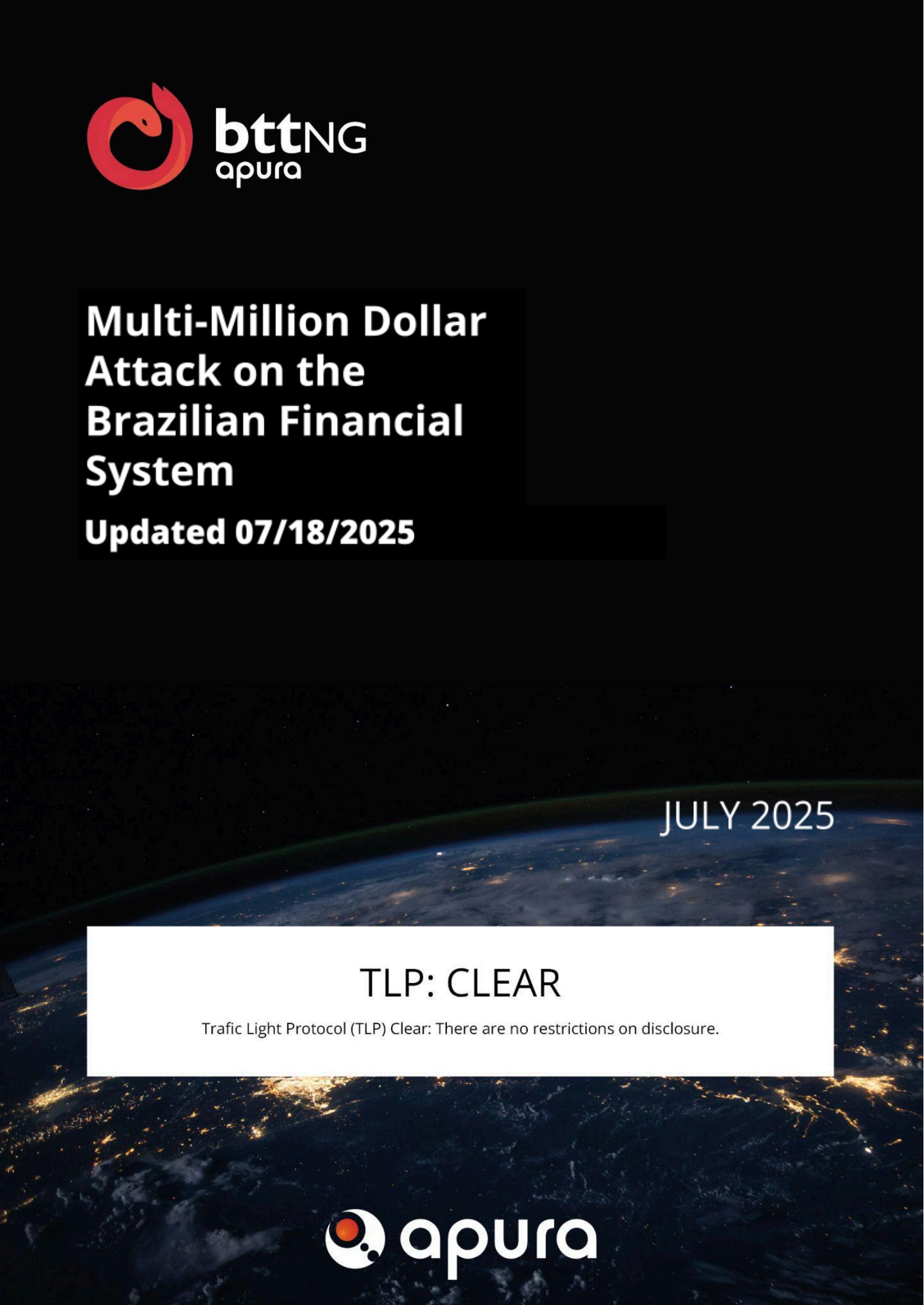


Multi-Million Dollar Attack on the Brazilian Financial System

Updated 07/18/2025

JULY 2025

TLP: CLEAR

Trafic Light Protocol (TLP) Clear: There are no restrictions on disclosure.

Contents

1. Executive Summary

In the early hours of June 30, C&M Software, a Brazilian service provider for the financial sector, was hacked by an unidentified actor, allegedly exploiting leaked credentials of the company's customers. Once inside C&M's systems, the cybercriminal began withdrawing funds from at least six financial institutions, tapping reserve accounts held at the Central Bank for interbank settlement.

The following day, July 1st, the Brazilian press began to report on the cyber incident, which was complex in nature and involved the embezzlement of unprecedented amounts of money in Brazil. The incident involved unauthorized access to the systems of financial institutions and fintechs through C&M Software, a service provider with access to the heart of the Brazilian Payment System (SPB).

The total amount stolen is still being calculated by the parties involved, with different reports ranging from US$ 72 million to US$ 550 million (the equivalent to R$ 400 million to R$ 3 billion, in local currency). According to preliminary estimates by the Central Bank, presented by the Brazil Journal portal, the attack would have drained a total of US$ 144 million from eight banking and non-banking institutions. BMP Money Plus, one of the affected institutions, reported that nearly US$ 72 million had been stolen, but that it had already managed to recover around US$ 29 million on Thursday (July 3). However, according to the São Paulo Civil Police, BMP claimed in the police report that it, alone, had lost US$ 97 million. Other victims did not come forward, and reports indicate that two other banks, whose identities were not revealed, declared losses of another US$ 19 million and US$ 9 million each to the police.

As a preemptive measure, on June 30th, C&M Software was temporarily disconnected from the Brazilian Payment System (SPB) by the Brazilian Central Bank to mitigate the risk of further irregular transactions. The Brazilian Federal Police opened an investigation into the theft on July 2, with the support of the Brazilian Central Bank. The Civil Police of the State of São Paulo identified the initial vector of the attack, an account belonging to an employee who was approached by the criminal group. Mapping the flow of money indicated that the theft involved hundreds of Pix transactions (Brazilian instant payment system) carried out in the early hours of June 30, which the criminals then attempted to convert into cryptocurrency.

Investigations are ongoing at the time of writing this intelligence report.

2. Incident Description

At 4 a.m. on Monday, June 30, an executive at BMP Money Plus, a fintech company that offers banking-as-a-service, received a call from an employee at another bank, CorpX Bank, informing him that nearly US$ 3.3 million (R$18 million) had been transferred from BMP's account to that bank. At that moment, the executive, who acts as BMP's Reserve Pilot, identified several other unauthorized Pix transfers occurring at the same time. Thus, the company became aware of the fraud and began to take action to identify and contain the incident. At 5 a.m. on June 30, the BMP executive contacted C&M Software. According to a report by the first media outlet to report the case, the Brazil Journal portal, US$ 72 million was lost from BMP's reserve account, which managed to recover the equivalent to US$ 29 million.

According to police investigations, the criminals obtained access credentials by bribing a C&M Software employee, allowing them to access the company's systems and to access several corporate client accounts connected to the platform. Once they gained access, they began moving funds from the reserve account of at least six C&M banking clients. One of the main victims was BMP Money Plus, a financial institution specializing in banking-as-a-service (BaaS) services.

After stealing the money, the cybercriminal began moving the funds to different cryptocurrency providers that work with Pix, such as exchanges, gateways, crypto swap systems integrated with Pix, and OTC desks, to buy Tether (USDT) and Bitcoin. In one case, upon identifying a significant volume of transactions, the provider blocked the operations, notified BMP (one of the institutions that suffered most from the attack), and prevented the conversion of the funds to USDT.

To contain the movement of funds accessed by the attack, the Central Bank issued a precautionary suspension against C&M from the national bank transfer system, which affected Pix's operation in almost 300 financial institutions connected through the company.

Despite the million-dollar loss, BMP stated that no customers were impacted or had their funds accessed and that it has sufficient collateral to cover 100% of the amount stolen.

At the request of the Central Bank, the Brazilian Federal Police opened an investigation into crimes of criminal organization, theft by fraud, computer device intrusion, and money laundering. The Civil Police of the State of São Paulo were also involved.

2.1 Timeline

The news published by the brazilian press so far allows us to construct an approximate timeline of the breach that first broke at C&M Software:

- March 2025: An employee of C&M Software, working as a Junior Developer, is approached in a bar in the city of São Paulo and receives nearly US$ 1,000 to provide his access credentials.
- May 2025: The C&M employee receives instructions to enter commands into the company's systems to allow criminals access, in exchange for an extra payment of around US$ 2,000.
- June 11, 2025: The company Monexa Gateway de Pagamentos is opened, which received five transfers during the C&M breach, receiving over US$ 8 million.
- June 30, 2025, 12:18 a.m. (UTC-3) — The SmartPay and Truther platforms identified an abnormal movement of cryptocurrency purchases.
- June 30, 2025, 2:00 a.m. (UTC-3) — The first fraudulent transactions begin to divert money from the BMP Reserve Account.
- June 30, 2025, 4:00 a.m. (UTC-3) — BMP's Reserve Pilot is notified by an executive from another bank about the receipt of a Pix transfer of US$ 3.3 million made at that moment. From this event, BMP becomes aware of some unauthorized Pix transactions.
- June 30, 2025, 5:00 a.m. (UTC-3) — The BMP Reserve Pilot contacted C&M Software to report the unauthorized transactions.
- June 30, 2025, 7:00 a.m. (UTC-3) — The BMP team manages to stop the sequence of fraudulent transactions.
- June 30, 2025 — As a preventive measure, C&M is temporarily disconnected from the Brazilian Payment System (SPB) by the Central Bank.
- 07/01/2025 — The Brazil Journal portal is the first media outlet to report on the incident.
- 07/02/2025 — BMP publishes an official statement on its website about the incident.
- 07/03/2025, 09:59 — The Central Bank announces the partial restoration of C&M Software's operations.
- 07/03/2025 — The Central Bank announces the suspension of three fintech companies that received part of the funds diverted from BMP. Among them is Soffy Payment Solutions, which received transfers of US$ 49 million.
- 07/03/2025 — The Civil Police of São Paulo arrests a C&M Software employee suspected of having sold his access credentials to the criminal group.

- 07/04/2025 — The Central Bank suspended access to the Pix system for three more payment institutions as a cautionary measure, on suspicion of having received funds diverted from the intermediary C&M Software.
- 07/07/2025 — The Central Bank has suspended another institution from Pix, the Creditag credit union. With this addition, there are now seven fintechs suspended.
- 07/16/2025 - The Federal Police and the São Paulo Public Prosecutor's Office conducted Operation Magna Fraus, which resulted in the arrest of two suspects for money laundering proceeds from the attack on C&M Software. Police recovered approximately US$ 1 million in crypto assets, and the court ordered the freezing of nearly US$ 6 million in USDT.

2.2 Incident Impact

The incident involved the illegal transfer of an as yet undetermined amount from various “reserve accounts” of national financial institutions. Estimates announced by the press, citing sources related to the investigations, range from US$ 72 million, US$ 144 million, US$ 179 million, and could reach up to US$ 716 million.

According to the news reports, the São Paulo Civil Police indicated that they were contacted by three financial institutions that had the following amounts diverted:

- R$541 million from BMP Money Plus (around US$ 97 million);
- R$104 million from an undisclosed institution (nearly US$ 19 million);
- R$49 million from another undisclosed institution (around US$ 9 million).

Even without the precise identification of the amount embezzled in the scam, it is possible to say that this is the largest cybercrime in Brazil's history in terms of the amounts involved.

In addition to the immediate financial impact caused by the fraud, several financial institutions that use C&M Software's services were unable to transact in the national financial system from June 30 to July 3, causing possible impacts on their customers.

2.3 Parties involved in the incident

The identities of all the organizations involved in the attack on C&M Software are not known, since the news reports that have appeared so far have not identified all the financial institutions that were defrauded as a result of the cyber-attack. Reports even differ on the number of victims, with some news portals mentioning six institutions affected and others eight. The Central Bank did not say which institutions were affected.

At the time of writing, only BMP Money Plus has publicly admitted to having been a victim of the diversion of funds through the hacking of C&M Software.

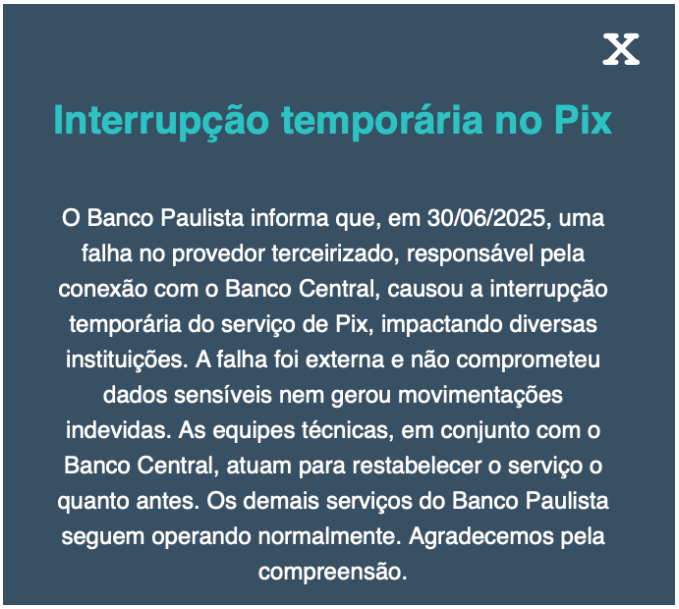
C&M Software (CMSW) (https://cmsw.com): Brazilian company that provides infrastructure services to the financial sector, in the category of Information Technology Service Provider (PSTI) authorized by the Central Bank, including critical operations such as clearing, transfer and settlement processing. C&M's platform also processes real-time settlement payments electronically among U.S. FedNow participant financial institutions. The company has limited its official statements due to legal advice and to respect the confidentiality of the investigations. The incident involved its solution called "Corner", a platform developed by CMSW that connects financial institutions to the Central Bank of Brazil, through the Brazilian Payments System (SPB) and the Instant Payments System (SPI). The solution offers a portfolio of financial services that includes the processing of transactions via Pix, Open Finance, New Collection Platform (NPC), Boleto and traditional means of payment. The solution is connected to the RSFN (National Financial System Network) and facilitates the integration of institutions with the Brazilian Central Bank.

BMP Money Plus (https://moneyp.com.br): Financial institution specialised in banking-as-a-service (BaaS), offering services to 92 fintechs and 210 investment funds. According to reports shared in the press, it was one of the main targets of the scam, with over US$ 97 million being embezzled from its reserve account. The company claims to have recovered US$ 29 million. The company has adopted a transparent stance on the case.

Brazil Central Bank: Government entity responsible for the Brazilian financial system.

Credsystem: One of the financial institutions that allegedly had assets embezzled during the attack on C&M Software on June 30.

Banco Paulista (https://www.bancopaulista.com.br): One of the financial institutions that was impacted by the attack on C&M Software on June 30. On its website, the institution displayed a pop-up notifying of the temporary suspension of Pix transactions on June 30 and states that "the failure was external and did not compromise sensitive data or generate improper transactions".



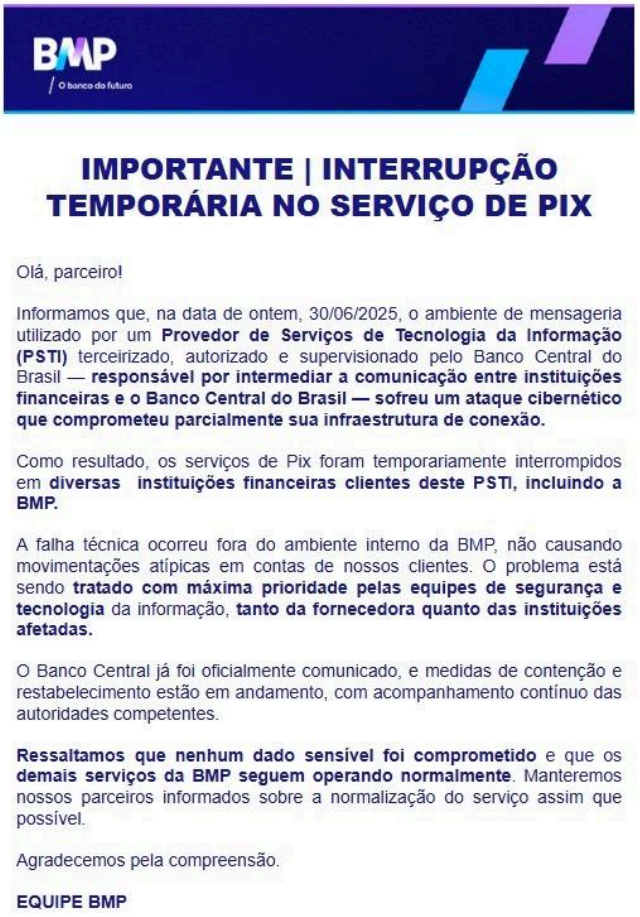
Soffy Payment Solutions: Small fintech located on Avenida Paulista, it is one of the companies targeted by the São Paulo Civil Police for having received nearly US$ 49 million of the money embezzled in the attack on C&M.

2.4 Position of the authorities and companies involved

According to reports shared by the Brazilian press, the Central Bank was notified of the incident immediately, on June 30, and is closely following the investigations. As a preventive measure, on June 30 C&M Software was temporarily disconnected from the Brazilian Payment System (SPB) to mitigate the risk of further irregular transactions.

In a note to the Bastidor portal, the Central Bank confirmed the attack on C&M and said that it had ordered the disconnection of access to the company's platform: "C&M Software, a provider of technology services for institutions that provide transactional accounts that do not have their own means of connection, reported an attack on its technological infrastructure. The Central Bank has ordered C&M to disconnect the institutions' access to the infrastructure it operates."

On July 1, BMP published an official note to BMP Plus partners, informing them that the Pix service was temporarily interrupted due to a cyber attack that partially compromised C&M Software's connection infrastructure (without naming the institution).



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.**

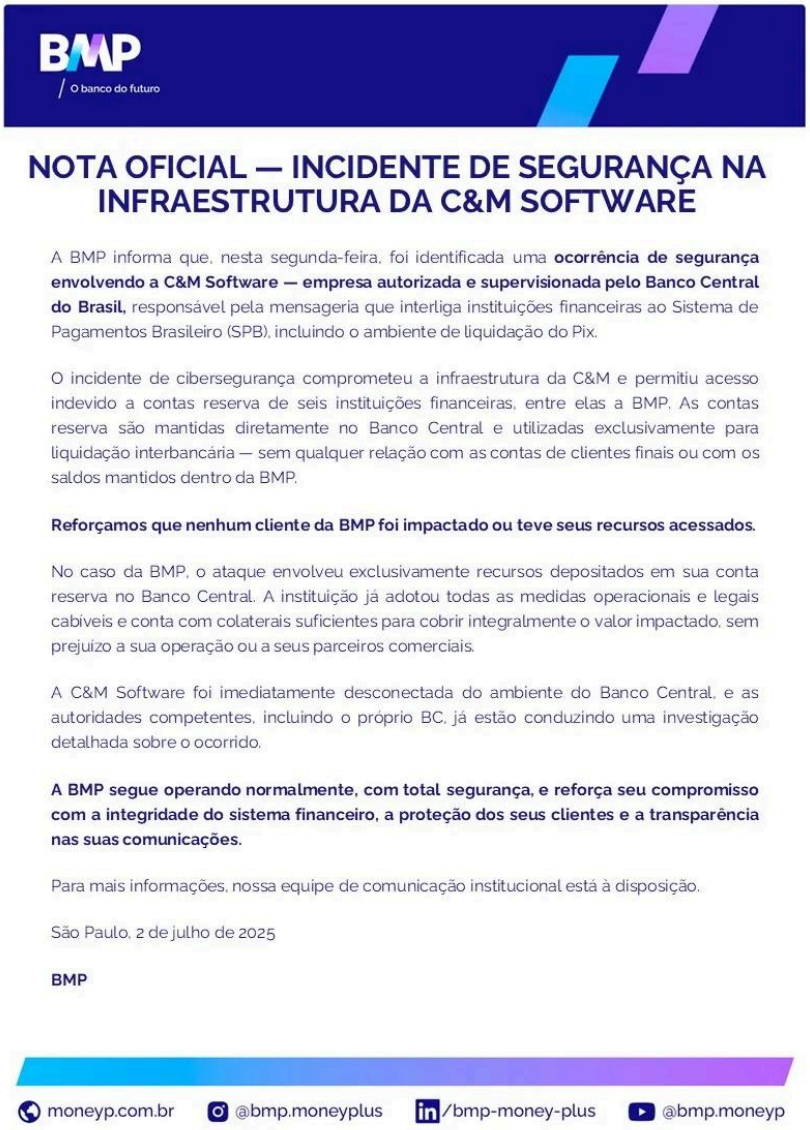
O Banco Central já foi oficialmente comunicado, e medidas de contenção e restabelecimento estão em andamento, com acompanhamento contínuo das autoridades competentes.

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

On July 2, BMP published an official note on its website, acknowledging the incident involving C&M Software, and emphasizing that there was no impact or access to its customers' data:



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

On Thursday, July 3, the Central Bank published an official note on its website announcing the partial resumption of C&M Software's operations, allowing transfers via Pix only from Monday to Friday, between 6:30 am to 6:30 pm:

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.

C&M Software has published an official note on its website, in question and answer format, in which it highlights that there was no evidence of its environment being compromised or a vulnerability being exploited, and that the incident occurred due to the use of the credentials of its employee, who has already left the company, which were obtained through social engineering outside the work environment. The note also states that C&M managed to recover part of the embezzled amounts by activating the MED (Special Return Mechanism).

2.5 Cyberattack Analysis

There are indications that the attack on C&M Software involved remote access to the SPB environment and transaction processing systems maintained by the company. Once the threat actor obtained access to the system, he accessed the credentials of the financial institutions, C&M's clients, which in turn gave him access to the certificates and private keys needed to execute fraudulent Pix transactions, directly via SPI through C&M's systems.

The characteristics of the attack, in light of the testimony of the first suspect arrested by the police, indicate that the crime was carried out by a Brazilian criminal group made up of at least five people. The attack was planned for several months, at least since before March 2025, and the group has a strong technical and procedural knowledge about how the Brazilian financial system works, including the payment system (SPB) and the Pix system (Instant Payment System).

Based on the analysis of the case, the following is an assumed modus operandi established by Apura's research into how the stages of the fraud would have taken place.

Access to the Internal System

According to investigations by the São Paulo Civil Police, the criminals gained access to the C&M Software environment by luring a company employee, João Nazareno Roque, who worked as a junior developer. He confessed that other people convinced him to help break into the system. In May of this year, Roque carried out commands on C&M's servers, following the criminals' instructions, which allowed them remote access to the company's systems.

In an official statement published on its website, C&M Software pointed out that the elements ascertained by the authorities and the independent investigations contracted indicate that the episode began with the improper sharing of credentials by an employee, induced by third parties using social engineering techniques. The employee was approached outside the company environment by a third party who introduced himself as “connected to hackers” and promised him a financial benefit. Access began with his personal credentials, but there are indications that additional credentials or auxiliary authentication mechanisms were used, which is under technical analysis.

The company states that there was no external intrusion or technical breach of C&M's infrastructure and that they have not identified any technical flaws or vulnerabilities in their systems.

Reconnaissance and Mapping

Once they had gained initial access to the C&M Software environment, the attackers mapped out the infrastructure and operation of the transfer system, identifying how Pix transactions were structured and where critical authentication artifacts were stored.

At this point, the attackers may have mapped the financial institutions that were clients of C&M and had credentials stored with it, possibly using enumeration. We believe that, at this stage, the attackers identified the financial institutions where it was possible to access their reserve accounts.

Compromise of Sensitive Credentials

In our analysis, the actor supposedly gained access to the credentials of financial institutions and possibly even the private keys and digital certificates used by C&M

Software's client institutions to sign Pix transactions. In general, these keys are shared with the PSTI to sign transactions.

According to Brazilian news outlet G1, in a statement, C&M Software's commercial director, Kamal Zogheib, said that the company was the direct victim of a criminal action, which involved the misuse of customer credentials to fraudulently access its systems and services.

With this information and privileged access to C&M's system and the accounts of financial institutions, the attackers gained the ability to inject legitimate transactions into SPI on behalf of these institutions.

Massive execution of Pix transactions

By using the compromised credentials and certificates, the attackers would have injected transactions directly into the SPI on behalf of the financial institutions, from the C&M Software platform, which were processed normally by the financial institutions, since:

- The messages were correctly signed by the institutions of origin, since C&M's system was compromised;
- There was backing for these transactions, based on the deposit made in the "reserve account" with the Central Bank;
- The SPI does not validate the balance, legitimacy of the payer or anti-fraud analysis - it assumes that this has been done in advance by the financial institution.

Transactions amongst Brazilian financial institutions can only be done through the Brazilian payment system by authorized and specific systems, which have access to the institutions' private keys to digitally sign the transactions - in accordance with the SPB's technical requirements. Therefore, this attack involved knowledge of these systems and protocols, as well as privileged access to them, and could not be reproduced from another system.

In addition to privileged access to C&M Software's systems, we observed that the attackers may have intentionally chosen to make the fund transfers outside of business hours. By conducting the fraud in the early hours of Sunday to Monday, they probably expected that it would be time less subject to human monitoring, decreasing the likelihood of someone identifying and stopping the fraudulent transactions. At this point, Pix's instant and anytime transfer functionality was a great ally for the cybercriminals.

We believe that the transactions took place until the balances in the liquidation accounts (reserve accounts) were exhausted or until they were identified and stopped by the entities involved.

According to the São Paulo Civil Police investigation, after accessing the reserve account held by BMP bank at the Central Bank, the criminals diverted funds from the company's reserve account through 166 Pix transfers to the accounts of 29 different companies and 79 individuals. The fraudulent transactions began at 2:03 a.m. on June 30th (GMT-3), and the last Pix withdrawal from BMP's reserve account was recorded at 7:04 a.m. In total, R$541,019,034.96 was stolen (nearly US$ 97 million). A fintech in particular, Soffy, stood out to investigators because it received the largest volume of funds: 69 transactions totaling approximately US$ 49 million.

Destination of the funds

There are strong indications that most of the transactions were initially directed to current accounts at smaller payment institutions, which generally have more lenient onboarding and verification (KYC) controls, making it easier to open and manipulate accounts in the name of money mules. The transfer via Pix facilitated the evasion of funds.

The destination accounts were used as a bridge to the criminal group's ultimate goal: hiding the embezzled money in cryptocurrencies.

Laundering and Dispersal

After the funds were exfiltrated to moley mule accounts, the amounts were quickly dispersed in small transactions and allegedly also converted into crypto-assets, making it difficult to trace and block the embezzled amounts. According to news reports, some of these transactions were identified as suspicious and blocked on some exchanges.

According to a report on the Cointelegraph portal, the CEO of SmartPay and Truther, Rocelo Lopes, said he detected atypical movement on both platforms at 00:18 on June 30 (GMT-3), and automatically raised the validation filters on USDT and Bitcoin purchases. According to him, large sums of money were withheld and, at the same time, the process of returning them to the institutions involved was carried out. SmartPay operators identified a Pix worth over US$ 1 million from the BMP, which caught their attention. The employees then noticed a much higher than normal number of new account movements and many transfer requests in a short interval of around two hours.

According to an article published on the Bleeping Computer portal, the criminals responsible for diverting money from the Brazilian financial system managed to convert between US$30 and US$40 million (approximately R$160 million and R$220 million) of the stolen money into cryptocurrencies such as BTC, ETH and USDT, through various brokerages and over-the-counter (OTC) markets.

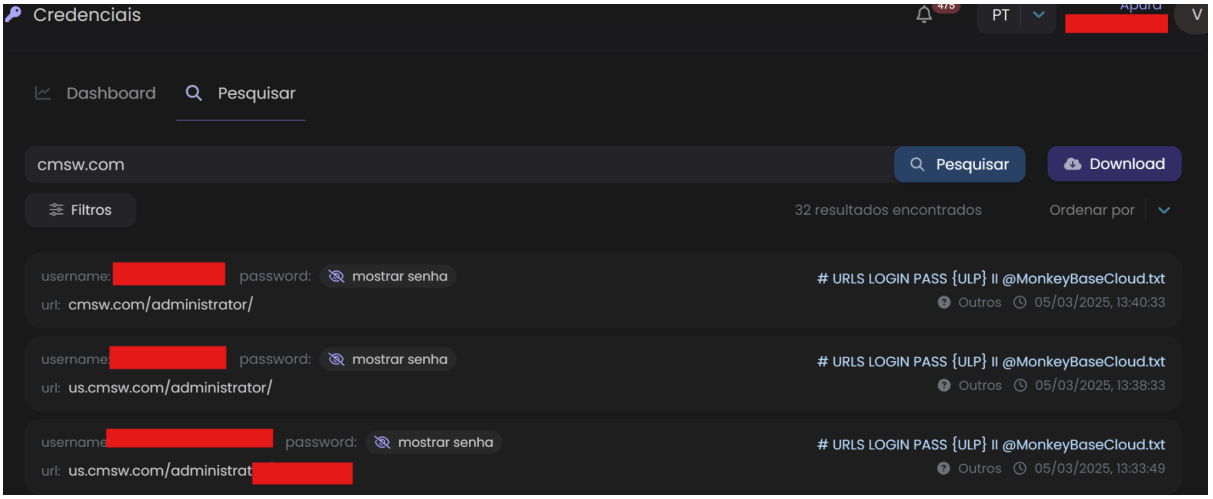
2.6 Ongoing investigations

Initial Hypotheses

In the first few hours after learning about the incident at C&M Software, various hypotheses were put forward by the press and by professionals in the industry.

According to various press reports, the attackers supposedly exploited any vulnerabilities in C&M Software's technological environment and used remote access tools (RMM) to enter C&M's environment.

From BTTng, we identified the leak of 32 credentials belonging to C&M, including supposedly administrator passwords. These credentials, if valid at the time of the incident, could have been a possible access vector.



A report created by a third-party company, not officially involved in the investigations, hypothesized that C&M Software allegedly operated a Java message broker, Active MQ 5.x, to orchestrate the settlement message queues for the Central Bank. This platform could supposedly be exploited and offer remote access to criminals since it would be vulnerable to CVE-2023-46604.[1] The same report states that the private encryption keys would be accessible on C&M's server, rather than stored on an HSM device. The company has shown no evidence of these claims.

[1] https://nvd.nist.gov/vuln/detail/CVE-2023-46604

Analyzing the specifics of this case and comparing it to the current scenario of threat actors in Brazil, it is possible to see similarities with the Plump Spider group. This Brazilian actor, already known to the global intelligence community, focuses on financial institutions, not just banks, but also companies that have financial activities. The group, of Brazilian origin, has been active since 2023 and has accumulated almost two years of cybercriminal activity without any identification by the authorities.

Arrest of suspect for facilitating access

In two articles published by the G1 portal on July 4, the arrest of a suspect involved in the attack on C&M Software on Thursday (July 3) was confirmed by the State Department of Criminal Investigations (DEIC) of the São Paulo Civil Police. The suspect, identified in the report as João Nazareno Roque, 48 years old, is an IT operator at C&M (although on his Linkedin profile he introduces himself as an electrician and Junior Back-End Developer) He was arrested in the neighborhood of City Jaraguá, in the North Zone of São Paulo. Authorities are investigating the involvement of additional people. The police seized equipment from his home and blocked his accounts.

According to investigators, the man in custody has been an employee of C&M Software since 2022 and gave the criminals who carried out the attack access to the bank's system via his computer. The suspect is said to have informally confirmed to the police that he gave the access password to a third party, who committed the fraud. He helped them enter the system and make the transfers via Pix. In a statement, he said that he received approximately US$ 3,000 in cash to facilitate access.

According to João Nazareno Roque's testimony, he received two payments:

- Around US$ 1,000 for supplying the C&M company's corporate login and password. The payment was made via motorcycle courier, who also collected the access credentials;
- Nearly US$ 2,000 for continuing to enter commands into the system from his own computer, at the service of the criminal group. He received the instructions via notes shared on Notion. This second amount was also paid in R$100 bills, again via a courier.

Roque claimed to have maintained online contact with four different members of the criminal group, who provided them with the necessary guidance. Contact was made by phone, which was changed every 15 days.

C&M Software said in a statement that "the employee had been working at CMSW since 2022 and was dismissed from the company shortly after the initial investigation of the

facts. The decision was taken based on the technical elements collected, in a careful manner and in line with the company's internal procedures."

Involvement of Payment Institutions

According to an article on the Finsiders Brasil portal, the Central Bank announced on Thursday night (03/07) the precautionary suspension of the Payment Institutions (PI) Transfeera, Nuoro Pay and Sofffy from the Pix arrangement, as a result of the attack on C&M Software.

According to sources heard by the report, these three IPs received the largest volume of embezzled funds and were unable to identify and stop the deposits. They all received hundreds of millions and connected to the crypto exchange.

Later, on the evening of July 4th, the Central Bank suspended access to the Pix system for three more payment institutions: Voluti Gestão Financeira, Brasil Cash, and S3 Bank. On July 7th, the Central Bank suspended another institution, the Creditag credit union, bringing the total suspension to seven fintechs for alleged links to the illicit movement of millions of brazilian reais.

Progress in the Investigations

On July 15th and 16th, the Brazilian Federal Police and the São Paulo Public Prosecutor's Office conducted Operation Magna Fraus, which resulted in the arrest of two suspects involved in the group responsible for laundering money originating from the attack on C&M Software. The searches took place at five addresses in the states of Goiás and Pará.

During the operation, officers recovered R$5.5 million in crypto assets (around US$ 1 million), as the private key for accessing the cryptocurrencies was found at one of the addresses searched by police, allowing the immediate transfer of the funds to the custody of the Public Prosecutor's Office. Furthermore, the court ordered the freezing of R$32 million (nearly US$ 6 million) in USDT in collaboration with Tether. Cash, vehicles, and weapons were also seized by law enforcement.

2.7 The case and the Brazilian cybercrime scenario in 2025

The incident at C&M Software involved the compromise of very specific technological components and processes of the Brazilian financial system. This leads us to believe that the actor responsible for the incident is familiar with the country and, possibly, there may have been collaboration from people with experience in the financial sector.

At the time of writing, there is still no evidence or news about the possible identity of the actors responsible for the attack on C&M Software, their modus operandi or affiliation.

Characteristics of the criminal group

It is possible to deduce from João Nazareno Roque's statements that the criminal group responsible for the attack on C&M Software was made up of at least 5 individuals: one who approached him in person offering him money to provide his access credentials, and another four different people with whom he communicated via cell phone, who sent instructions for Roque to facilitate their remote access.

As the first contact with Roque took place in March of this year, it is clear that the group planned the scam for at least four months. The group has advanced knowledge of how the financial system works, and technical knowledge of the Brazilian payment system (SPB) and the instant payment system (SPI) responsible for Pix.

3. MITRE ATT&CK mapping

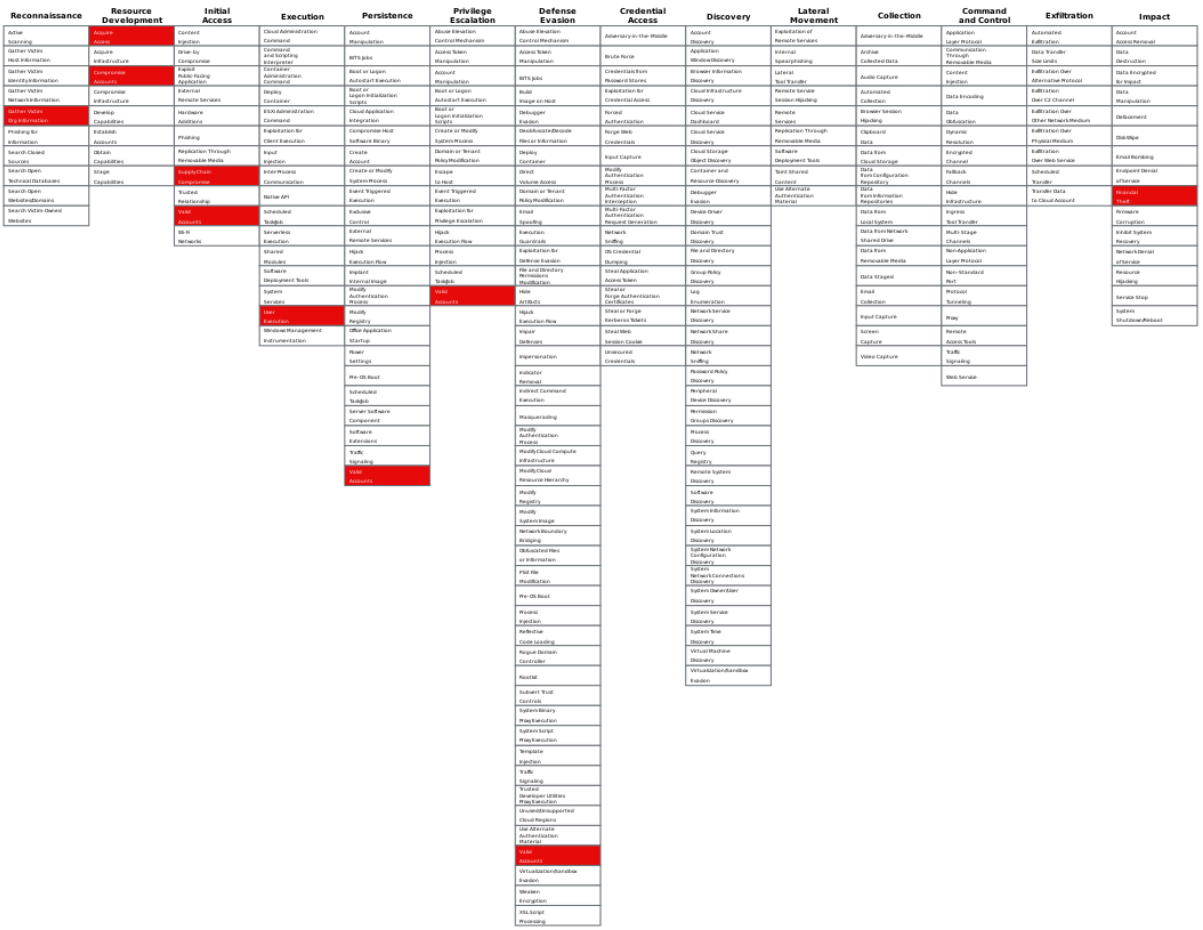
Based on the public information about the incident, we can point to some of the possible steps taken by the actor during the exploitation of C&M Software, in terms of known Tactics, Techniques and Procedures (TTPs), based on the MITRE ATT&CK framework.

The mapping below was carried out considering the information available in the press about the incident, since the details of the attack were not made public. As such, a lot of important information for understanding the attack and mapping it correctly is not known at this time.

Below we present the **supposed** steps of the cyber-attack, mapped according to the MITRE ATT&CK framework (Enterprise ATT&CK v17):

Reconnaissance		
T1591.002	Gather Victim Org Information / Business Relationships	The criminals mapped out a company that acted as a PSTI with the SPB and identified the financial organizations it serves..
Resource Development		
T1650	Acquire Access	According to DEIC investigations, the criminals bribed a C&M employee, who provided them with his access credentials.

T1586	Compromised Accounts	The criminals exploited compromised accounts related to C&M Software's services and its financial customers, which were later used to access and transfer funds from reserve accounts.
Initial Access		
T1195.002	Supply Chain Compromise / Compromise Software Supply Chain	The actors manipulated C&M Software's transactional systems used by its customers in order to inject fraudulent transactions into the SPI without their knowledge.
T1078	Valid Accounts	According to DEIC investigations, the criminals used the credentials of a C&M employee to gain access to the company's systems.
Execution		
T1204	User Execution	According to DEIC investigations, the criminals bribed a C&M employee and instructed him to execute commands on the company's systems.
Persistence		
T1078	Valid Accounts	According to DEIC investigations, the criminals used the credentials of a C&M employee to gain access to the company's systems.
Privilege Escalation		
T1078	Valid Accounts	According to DEIC investigations, the criminals used the credentials of a C&M employee to gain access to the company's systems.
Defense Evasion		
T1078	Valid Accounts	According to DEIC investigations, the criminals used the credentials of a C&M employee to gain access to the company's systems.
Impact		
T1657	Financial Theft	A significant amount of financial resources was diverted from financial institutions using the C&M Software platform.



4. The Brazilian Payment System and Information Technology Service Providers

Behind the scenes of the Brazilian financial system, much of the technology that makes it all work - account opening, Pix payments, credit analysis, onboarding, fraud prevention - is not directly in the hands of banks or fintechs, but with third parties. These are companies that operate APIs, process transactions, validate identities, take care of the infrastructure and often maintain the core banking of entire institutions, the so-called **PSTIs - Information Technology Service Providers**.

This model, which has gained momentum with the fintech boom and the advance of open finance in Brazil, has brought agility, cost reduction and quick access to financial solutions. But it has also **created an ecosystem highly dependent on critical third parties**, where a one-off failure can escalate and affect multiple players at the same time.

4.1 Definition of PSTIs

PSTI is the acronym for Information Technology Service Provider, in Portuguese, within the ecosystem of the Brazilian financial system. They are third-party companies authorized by the Brazilian Central Bank, hired by financial institutions to perform essential technology functions for access to the banking system - from developing systems to offering entire platforms that support critical operations, such as payments, identity validation, data management and even core banking.

These providers are behind services that go far beyond traditional technical support. They offer, for example:

- Banking as a Service (BaaS) platforms;
- Integration with the SPB;
- Communication and transaction platforms with the National Financial System (SFN);
- Tailor-made software development and maintenance;
- Cloud storage and infrastructure services;
- Identity and access management (IAM, authentication, KYC);
- Support, helpdesk and real-time operations management.

For the purposes of access to the National Financial System Network (RSFN), PSTIs act as transactional gateways between financial institutions, by processing settlement operations and integration with the national banking system, including, for example, transfers via TED and Pix, issuing and payment of ticket bills, etc.

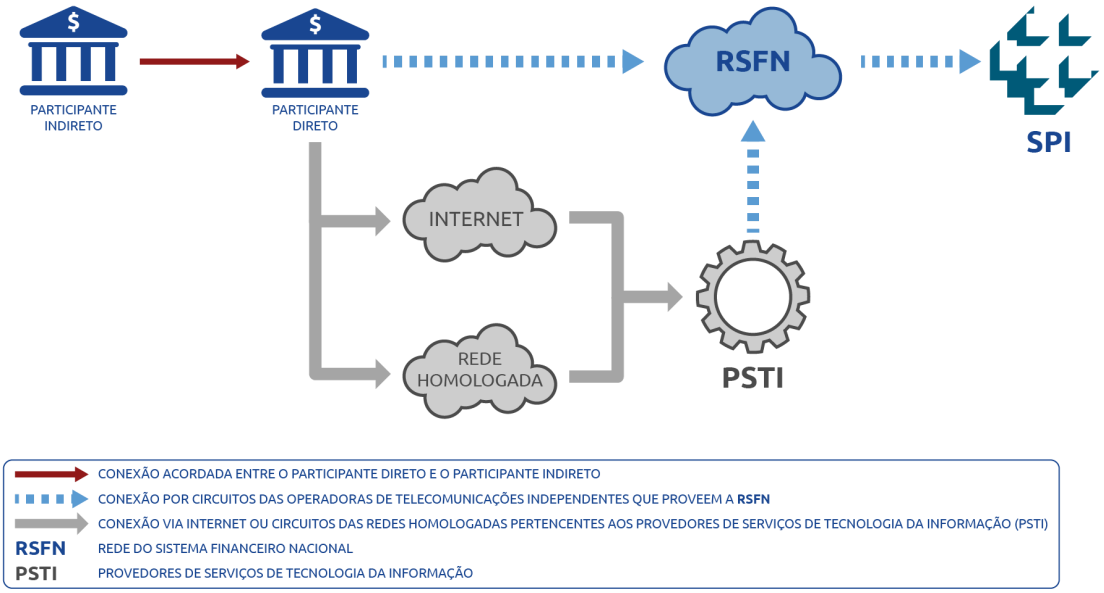


Image: Ways of accessing the Instant Payment System via PSTIs

In highly regulated sectors such as finance, the PSTI can be classified as a **critical third party**, which means that, from a regulatory point of view, the responsibility for failures, leaks or unavailability lies not only with it but also with whoever hired it. Security, continuity and compliance obligations need to be treated with the same rigor as internal operations.

Main suppliers authorized by the Central Bank:

- **ABBC –** Brazilian Banking Association;
- **C&M Software** –Provider of clearing, interconnection of accounts and access to the payment system. It was the source of the recent attack;
- **GOKEI Tecnologia -** Differentiates itself by offering a high-performance, high-availability cloud environment, using client communication with the PSTI through 100% cloud resources;
- **JD Consultores** - Has been offering financial solutions for 24 years;
- **MAPS** - Has been providing payment and financial settlement solutions for the SPB and SPI for 30 years;
- **Sinqia (former MasterSAF, Icaro)** – Settlement and banking integration solutions;
- **Stark** – Created in 2022, it provides infrastructure for financial institutions and fintechs.

TIVIT and TOPAZ are also listed as approved PSTIs.

5.Recommendations

The analyses presented earlier in this report show that the threat actors represent a direct strategic risk, capable of generating significant financial losses, damage to brand reputation and severe operational disruptions.

In response to this threat, we have drawn up a strategic mitigation guide designed to increase corporate resilience and protect business value based on four fundamental pillars:

- **Proactive Defense Strengthening:** Preventive measures to reduce the attack surface and make initial compromise more difficult;
- **Advanced Detection and Response Capability:** Implementation of technologies and processes to quickly identify and neutralize threats that penetrate the perimeter;
- **Actionable Threat Intelligence::** Using intelligence to proactively anticipate and hunt threats;
- **Supply Chain Risk Management:** Strict controls to mitigate risks introduced by IT partners and suppliers.

5.1 Strengthening the Attack Surface Against Initial Compromise

Vulnerability and Patch Management: Apply security patches to internet-facing systems, especially VPN gateways, RDP and common enterprise software. Prioritize vulnerabilities known to be exploited by APTs and ransomware groups.

Maintain Credentials and Authentication Mechanisms: Implement strong, unique passwords and, most critically, require phishing-resistant Multifactor Authentication (MFA) on all remote access points, email and cloud applications. This is the most effective control against credential-based attacks.

Secure Remote Access: Avoid publishing ports that provide access to critical services such as RDP, Server Message Block (SMB), Telnet, and NetBIOS, for example. If it is absolutely necessary to expose such a port, perform remote access through a secure gateway with active MFA.

5.2 Post-Compromise Defense

Behavior-Based Detection: Deploy advanced security solutions that use Behavior Indicators in addition to traditional Indicators of Compromise (IOCs). This enables the

detection of subtle malicious activity chains, such as a legitimate administration tool being used to launch PowerShell for lateral movement.

Endpoint and Network Visibility: Implement robust Endpoint Detection and Response (EDR) and network segmentation solutions. EDR provides visibility into the execution of processes on endpoints (e.g. winword.exe generating regsvr32.exe, a TA551 TTP), while segmentation can contain the lateral movement of an attacker.

Logging and Monitoring: Ensure comprehensive logging of all network activity, especially privileged accounts and third-party connections. Regularly audit these logs for anomalous behavior.

5.3 Proactive Intelligence and Threat Hunting

Dark Web Monitoring: Actively monitor dark web forums, illegal marketplaces and Telegram channels for mentions of your organization's name, domains or compromised credentials.

Infostealer Log Monitoring: Use services that track and analyze infostealer malware logs to proactively find out if employee or corporate credentials have been compromised and are in circulation. This allows credentials to be reset before they are used by a threat actor.

5.4 Protecting the IT Supply Chain

Supplier Risk Management: For organizations using PSTIs, conduct rigorous security assessments of your provider. Contracts should require specific security controls, including MFA on all accounts used to access your environment.

Least Privilege Principle for Third Parties: Ensure that PSTI accounts have only the minimum level of access necessary to perform their functions. Their access must be strictly monitored and audited.

Shared Responsibility Model: Clearly define in contracts who is responsible for security functions such as strengthening, detecting, and responding to incidents.

6. What We Can Conclude So Far

The incident that occurred at C&M Software on June 30 has already gone down as the largest cyber theft in Brazil's history, thanks to the exorbitant amounts involved.

The attack involves complex levels of sophistication, requiring in-depth knowledge of how the Brazilian Payment System (SPB) works, including its protocols, systems, and third parties involved. In fact, due to their characteristics, such fraudulent operations could only be manipulated and inserted into the financial system through unauthorized and malicious access to the transaction processing systems connected to the SPB (Brazilian Payment System).

This, combined with the effort required to exfiltrate large amounts of money via Pix and cryptocurrencies, indicates that the operation was complex and required extensive planning and preparation. We therefore believe that the incident was carried out by a prepared and specialized group, rather than a lone actor. We do not rule out the possibility of insider involvement, given the highly specific nature of the systems involved.

The Central Bank of Brazil and the authorities acted swiftly to contain and to investigate the incidents. Investigations are ongoing, and any conclusions about the nature and perpetrator of the attack at this time would be hasty and irresponsible. Many questions remain, which should be clarified as the investigation progresses.

Due to the significant impact involved, it is believed that this incident will prompt a review of the National Financial System's security protocols. Although the National Financial System (SFN) adopts technically robust security protocols for communication and messaging, the incident with C&M Software on June 30, 2025, demonstrated the fragility of the entire system, resulting from the compromise of systems at a single supplier — a classic scenario for supply chain compromise.

Apura Cyber Intelligence customers have access, through the BTTng platform, to detailed reports, which are updated promptly with every relevant development regarding the incident.

7. References

- Exclusive: Hackers steal over R$1 billion from 'banking as a service' - https://braziljournal.com/exclusivo-hackers-levam-mais-de-r-1-bilhao-em-ataque-a-banking-as-a-service/
- Attack on the financial system - https://obastidor.com.br/economia/ataque-ao-sistema-financeiro-8979
- In the early hours of the morning, a Pix payment worth R$18 million. The attack began: https://braziljournal.com/na-madrugada-um-pix-de-r-18-milhoes-comecava-o-assalto/
- Hackers steal R$1 billion from national financial system accounts and attempt to convert it into Bitcoin and 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
- BPM CEO gives a step-by-step account behind the scenes of the theft that led to R$400 million disappearing from the company's account - 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/
- Federal Police open investigation to investigate attack on financial institution systems; The Central Bank was not affected - 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
- Official statement from the BMP: https://moneyp.com.br/comunicados/nota-oficial-bmp-ataque-c-m-software/
- Statement from the Central Bank: https://www.bcb.gov.br/detalhenoticia/20752/nota
- Electronic data communication in the financial system - https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados
- Civil Police arrest suspect in São Paulo for hacking system that connects banks to PIX - https://g1.globo.com/sp/sao-paulo/noticia/2025/07/04/policia-civil-prende-em-sp-suspeito-envolvido-em-ataque-hacker-contra-o-banco-central.ghtml
- Attack on the Pix system: IT operator received R$15,000 to give password to hackers, police say; Find out who the suspect is https://g1.globo.com/sp/sao-paulo/noticia/2025/07/04/ataque-hacker-quem-e-suspeito-de-entregar-acesso-ao-sistema-que-liga-bancos-do-pix.ghtml

- BC suspends Pix participants Transfeera, Nuoro Pay, and Soffy (update) - https://finsidersbrasil.com.br/reportagem-exclusiva-fintechs/bc-suspende-os-participantes-do-pix-transfeera-nuoro-pay-e-soffy/
- Schedule, focus on Bitcoin, persistence: the clues that helped reveal the attack against the company that connects banks to PIX - https://g1.globo.com/tecnologia/noticia/2025/07/04/horario-tipo-de-transacao-e-insistencia-as-pistas-que-levaram-a-descoberta-do-ataque-hacker-ao-sistema-ligado-ao-pix.ghtml
- Official statement from C&M Software: https://cmsw.com/blog/qa-incidente-de-seguranca/
- Central Bank suspends three more payment institutions during hacker attack investigation - https://www1.folha.uol.com.br/tec/2025/07/banco-central-suspende-mais-tres-instituicoes-de-pagamentos-durante-investigacao-de-ataque-hacker.shtml
- Open 19 days before the multi-million dollar Pix embezzlement, the company received R$45 million - https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/07/06/empresa-aberta-19-dias-antes-de-desvio-milionario-do-pix-recebeu-r-45-mi.htm
- Hacker attack: BMP alone lost R$541 million; other institutions were also affected- https://g1.globo.com/economia/noticia/2025/07/04/ataque-hacker-recursos-desviados.ghtml
- Hacker attack transferred R$541 million from BMP to 29 institutions; Part of the amount was recovered - https://www1.folha.uol.com.br/tec/2025/07/ataque-hacker-pulverizou-r-541-mi-da-bmp-em-29-instituicoes-parte-do-valor-foi-recuperado.shtml
- Employee gets $920 for credentials used in $140 million bank heist - https://www.bleepingcomputer.com/news/security/employee-gets-920-for-credentials-used-in-140-million-bank-heist/
- Hacker attack that drained R$541 million via Pix lasted 5 hours in the early morning - https://www.metropoles.com/sao-paulo/ataque-hacker-que-drenou-r-541-milhoes-via-pix-durou-5h-na-madrugada
- Millions stolen in hacker attack transferred to 79 people - https://www.metropoles.com/sao-paulo/milhoes-roubados-em-ataque-hacker-foram-transferidos-para-79-pessoas
- Money diverted in the country's biggest hacking scam reportedly passed through at least 40 institutions - https://finsidersbrasil.com.br/noticias-sobre-fintechs/fraudes/dinheiro-desviado-em-maior-golpe-hacker-do-pais-teria-passado-por-pelo-menos-40-instituicoes/

- Exclusive: Losses from the hacker attack on C&M could exceed R$1 billion and more banks were affected, police say - https://valor.globo.com/financas/noticia/2025/07/11/exclusivo-policia-diz-que-prejuizo-com-ataque-hacker-pode-superar-r-1-bilhao-e-que-mais-bancos-foram-afetados-1.ghtml
- Operation Magna Fraus recovers R$5.5 million and blocks R$32 million in crypto assets - https://www.mpsp.mp.br/w/operacao-magna-fraus-resulta-em-recuperacao-de-r-5-5-mi-em-criptos-e-bloqueio-de-outros-r-32-mi-de-esquema-de-lavagem

8. Glossary

Brazilian Payment System (SPB) - A set of rules, procedures, institutions, and systems managed by the Central Bank that, through infrastructure, rules, and procedures, enable financial transactions in Brazil. It encompasses everything from fund transfer operations, such as TEDs and Pix, to the settlement of payments with cards and slips.

Cryptoassets - Encrypted digital assets transferred and stored using distributed ledger technologies, such as blockchain.

Digital Certificates - Electronic documents issued by a Certification Authority (CA) that attest to the identity of an entity (person, company, or system) and link that identity to a cryptographic key.

Fintechs - Companies that introduce innovations in financial markets through the intensive use of technology, with the potential to create new business models. They operate through online platforms and offer innovative digital services related to the sector.

Information Technology Service Providers (PSTI) - Entities authorized by the Central Bank to provide data processing services for the purpose of accessing the RSFN to financial institutions and other institutions authorized to operate by the Central Bank of Brazil.

Instant Payment System (SPI) - A centralized and unique infrastructure for the settlement of instant payments between different institutions in Brazil. The SPI, managed by the BCB, began operating in November 2020. The SPI is a real-time gross settlement (RTGS) system, meaning that it processes and settles transactions on a transaction-by-transaction basis. Once settled, transactions are irrevocable.

Money Mule Accounts - Bank accounts opened in the name of third parties (individuals or legal entities) for fraudulent purposes, usually with little or no awareness of the illicit use of the account.

National Financial System (SFN) - An entity formed by a group of entities and institutions that promote financial intermediation, i.e., the meeting between lenders and borrowers. It is through the financial system that individuals, companies, and the government circulate most of their assets, pay their debts, and make their investments.

National Financial System Network (RSFN) - The RSFN is a data communication structure between Brazilian financial institutions that aims to support the flow of information within the SFN for authorized services.

PIX - Brazilian instant payment system, created by the Central Bank, which enables real-time transfers and payments, 24 hours a day, 7 days a week, between different banks and financial institutions in the country.

Reserve Accounts - Deposits held by financial institutions directly with the Central Bank and used exclusively for interbank settlement.

SFN participant – refers to any institution authorized by the Central Bank or government entity whose systems communicate electronically through the SFN. SFN participants interact through messages and files on networks approved by the Central Bank.

Remote Monitoring and Management (RMM) - Technology used by IT teams to remotely monitor, manage, and access computers, servers, and network devices.

Reserve Pilot - Professional responsible for monitoring and managing the bank reserve or settlement accounts of a financial institution. Their main function is to ensure the institution's liquidity through the accuracy and reliability of these account balances, verifying and recording all debit and credit entries.

0800 719 1902

info@apura.io

apura.io

linkedin.com/company/apura

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