Ataque Billonario al Sistema Financiero Brasileño

Actualizado en 07/07/2025

JULIO 2025

TLP:CLEAR

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

Sumario

1. Resumen ejecutivo

En la madrugada del 30 de junio, C&M Software, una empresa brasileña proveedora de servicios para el sector financiero, fue vulnerada por un actor no identificado, supuestamente mediante la explotación de credenciales filtradas de clientes de la empresa. Una vez dentro de los sistemas de C&M, el ciberdelincuente comenzó a retirar fondos de al menos seis instituciones financieras brasileñas, a partir de las cuentas de reserva mantenidas en el Banco Central de Brasil para la liquidación interbancaria.

Al día siguiente, 1 de julio, la prensa comenzó a informar sobre el incidente cibernético, de características complejas y que desvió fondos de proporciones sin precedentes en Brasil. El incidente involucró el acceso indebido a sistemas de instituciones financieras y fintechs a través de C&M Software, una proveedora de servicios con acceso al corazón del Sistema de Pagos Brasileño (SPB).

El monto total desviado todavía está siendo calculado por las partes involucradas, con diferentes informes que varían desde R$ 400 millones (cerca de US$ 70 millones de dólares) hasta R$ 3 mil millones (cerca de 550 millones de dólares americanos). Según estimaciones preliminares del Banco Central de Brasil, presentadas por el portal Brazil Journal, el ataque habría drenado un total de R$ 800 millones de ocho instituciones bancarias y no bancarias. BMP, una de las instituciones perjudicadas, declaró la sustracción de R$ 400 millones, pero que ya había logrado recuperar R$ 160 millones el jueves (03/07). Sin embargo, según la Policía Civil de São Paulo, BMP declaró en el informe de la denuncia que perdió, por sí sola, R$ 541 millones.

Como medida preventiva, el 30 de junio C&M Software fue desconectada temporalmente del Sistema de Pagos Brasileño (SPB) para mitigar los riesgos de nuevas transacciones irregulares. La Policía Federal abrió una investigación sobre el robo el 2 de julio, con el apoyo del Banco Central. La Policía Civil de São Paulo identificó el vector inicial del ataque: la cuenta de un empleado que fue contactado por el grupo criminal. El rastreo del flujo del dinero indicó que el robo involucró cientos de transacciones PIX realizadas en la madrugada del 30 de junio, que posteriormente los delincuentes intentaron convertir en criptomonedas.

Las investigaciones continúan en curso al momento de la redacción de este informe de inteligencia.

2. Descripción del Incidente

A las 4:00 h de la mañana del lunes 30/06, un ejecutivo de BMP Money Plus, una fintech brasileña que ofrece servicios de “banking as a service”, recibió una llamada de un empleado de otro banco, CorpX Bank, informándole que se habían transferido R$ 18 millones de la cuenta de BMP a ese banco. En ese momento, el ejecutivo, que actúa como Piloto de reservas de BMP, identificó varias otras transferencias no autorizadas vía PIX que estaban ocurriendo en ese mismo momento. De esta forma, la empresa tuvo conocimiento del fraude y comenzó a actuar para identificar y contener el incidente. A las 5:00 h del 30/06, el ejecutivo contactó a C&M Software. Según un reportaje del primer medio en informar sobre el caso, el portal Brazil Journal, se sustrajeron R$ 400 millones de la cuenta de reserva de BMP, la cual consiguió recuperar R$ 160 millones.

Según relatos compartidos con la prensa, los atacantes habrían explotado vulnerabilidades en los sistemas de C&M Software para escalar privilegios de acceso, logrando alcanzar diversas cuentas de clientes corporativos conectados a la plataforma. Tras obtener el acceso, comenzaron a mover fondos de la cuenta de reserva de al menos seis entidades bancarias clientes de C&M. Uno de los principales objetivos fue BMP Money Plus, una institución financiera especializada en servicios de banking-as-a-service (BaaS).

Después de robar el dinero, el ciberdelincuente comenzó a mover los fondos a diferentes proveedores de criptomonedas que operan con Pix, como exchanges, pasarelas de pago, sistemas de swap a cripto integrados con Pix y mesas de operaciones extrabursátiles (OTC), para comprar USDT y Bitcoin. En uno de los casos, al identificar un volumen significativo de transacciones, el proveedor habría bloqueado las operaciones, avisado a BMP (una de las instituciones que más sufrió con el ataque) e impedido la conversión de los fondos a USDT.

Para contener el movimiento de los fondos a los que se accedió en el ataque, el Banco Central emitió una suspensión cautelar contra C&M del sistema de transferencia bancaria nacional, lo que afectó la operación de Pix en casi 300 instituciones conectadas a través de la empresa.

A pesar del perjuicio millonario, BMP declaró que ningún cliente fue afectado ni se accedió a sus recursos y que posee garantías suficientes para cubrir el 100% del monto sustraído.

A requerimiento del Banco Central, la Policía Federal abrió una investigación para indagar sobre los delitos de organización criminal, hurto mediante fraude, invasión de dispositivo informático y lavado de dinero.

2.1 Linea de tiempo

Las noticias publicadas por la prensa hasta el momento permiten construir una línea de tiempo aproximada sobre el incidente ocurrido en C&M Software:

- Marzo de 2025: Un empleado de C&M Software, que trabajaba como Desarrollador Jr., es abordado en un bar y recibe R$ 5 mil por proporcionar su credencial de acceso.
- Mayo de 2025: El empleado de C&M recibe instrucciones para insertar comandos en los sistemas de la empresa para permitir el acceso de los delincuentes.
- 11/06/2025: Se constituye la empresa A Monexa Gateway de Pagamentos, que recibió cinco transferencias durante la intrusión en C&M, por un total de R$ 45 millones.
- 30/06/2025, 00:18 (UTC-3) — Las plataformas de SmartPay y Truther identificaron un movimiento atípico de compra de criptomonedas.
- 30/06/2025, 02:00 (UTC-3) — Las primeras transacciones fraudulentas comienzan a desviar dinero de la Cuenta de Reserva de BMP.
- 30/06/2025, 04:00 (UTC-3) — El Piloto de Reserva de BMP es notificado por un ejecutivo de otro banco sobre la recepción de un PIX de R$ 18 millones realizado en ese momento. A partir de este evento, BMP tiene conocimiento de la realización de algunas transacciones PIX no autorizadas.
- 30/06/2025, 05:00 (UTC-3) — El Piloto de Reserva de BMP contacta a C&M Software para comunicar sobre las transacciones indebidas.
- 30/06/2025, 07:00 (UTC-3) — El equipo de BMP logra interrumpir la secuencia de transacciones fraudulentas.
- 30/06/2025 — Como medida preventiva, C&M fue desconectada temporalmente del Sistema de Pagos Brasileño (SPB) por el Banco Central.
- 01/07/2025 — El portal Brazil Journal es el primer medio de comunicación en informar sobre el incidente.
- 02/07/2025 — BMP publica un comunicado oficial en su sitio web sobre el incidente.
- 03/07/2025, 09:59 — El Banco Central anunció la reanudación parcial de las operaciones de C&M Software.
- 03/07/2025 — El Banco Central anunció la suspensión de tres fintechs que recibieron parte de los fondos desviados de BMP. Entre ellas, Soffy Soluções de Pagamento, que recibió transferencias por un total de 270 millones de reales.

- 04/07/2025 — Se anuncia la detención de un empleado de C&M Software, sospechoso de haber vendido sus credenciales al grupo criminal.
- 03/07/2025 — El Banco Central suspendió el acceso al sistema Pix de otras tres instituciones de pago, de forma cautelar, bajo sospecha de haber recibido fondos desviados de la intermediaria C&M Software.

2.2 Impacto del incidente

El incidente involucró la transferencia ilícita de un monto aún no determinado desde diversas "cuentas de reserva" de instituciones financieras nacionales. Las estimaciones anunciadas por la prensa, citando fuentes relacionadas con las investigaciones, varían entre R$ 400 millones, R$ 800 millones, R$ 1 mil millones y podrían llegar hasta R$ 4 mil millones.

Incluso sin la identificación precisa del monto desviado en el fraude, es posible afirmar que se trata del mayor crimen cibernético de la historia de Brasil, en términos de los montos involucrados.

Además del impacto financiero inmediato causado por el fraude, diversas instituciones financieras que utilizan el servicio de C&M Software se vieron imposibilitadas de realizar transacciones en el sistema financiero nacional del 30 de junio al 3 de julio, causando posibles impactos a sus clientes.

2.3 Entidades involucradas en incidente

La identidad de todas las organizaciones involucradas en el ataque a C&M Software no se conoce, ya que las noticias que han surgido hasta el momento no han identificado a todas las instituciones financieras que fueron víctimas de fraude a raíz del ciberataque. Los informes difieren, incluso, en la cantidad de víctimas, ya que algunos portales de noticias mencionan 6 instituciones perjudicadas, y otros, ocho. El Banco Central no ha informado qué instituciones fueron afectadas.

Al momento de la redacción de este informe, solo BMP Money Plus ha admitido públicamente haber sido víctima del desvío de fondos a través de la intrusión en C&M Software.

C&M Software (CMSW) (https://cmsw.com): Empresa brasileña que presta servicios de infraestructura para el sector financiero, en la categoría de Proveedor de Servicios de Tecnología de la Información (PSTI) autorizada por el Banco Central, incluyendo operaciones críticas como procesamiento de compensaciones, transferencias y liquidaciones. La empresa ha limitado sus comunicados oficiales por orientación jurídica y en respeto al secreto de las investigaciones. El incidente involucró su solución

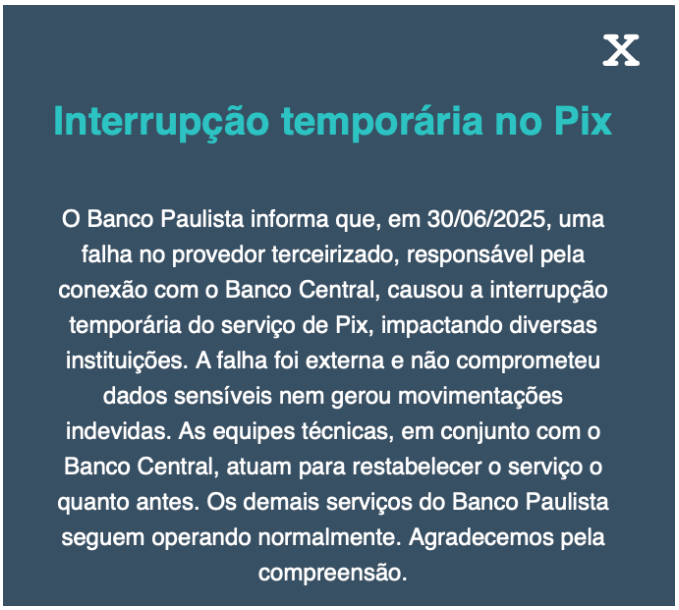
bautizada como “Corner”, una plataforma desarrollada por CMSW que conecta a las instituciones financieras con el Banco Central de Brasil, a través del Sistema de Pagos Brasileño (SPB) y el Sistema de Pagos Instantáneos (SPI). La solución ofrece un portafolio de servicios financieros que incluye el procesamiento de operaciones vía Pix, Open Finance, Nova Plataforma de Cobrança (NPC), Boleto y medios de pago tradicionales. La solución está conectada con la RSFN (Rede do Sistema Financeiro Nacional, Red del Sistema Financiero Nacional) y facilita la integración de las instituciones con el Banco Central.

BMP Money Plus (https://moneyp.com.br): Institución financiera especializada en servicios de banking-as-a-service (BaaS), que ofrece servicios a 92 fintechs y 210 fondos de inversión en Brasil. Según los informes compartidos en la prensa, fue uno de los principales objetivos del fraude, habiéndose desviado R$ 400 millones de su cuenta de reserva. La empresa alega haber recuperado R$ 160 millones. La empresa ha adoptado una postura de transparencia sobre el caso.

Banco Central do Brasil: Entidad gubernamental responsable del sistema financiero brasileño.

Credsystem: Una de las instituciones financieras a la que, supuestamente, se le desviaron activos durante el ataque a C&M Software el 30 de junio.

Banco Paulista (https://www.bancopaulista.com.br): Una de las instituciones financieras que fue afectada por el ataque a C&M Software el 30 de junio. En su sitio web, la institución presenta una ventana emergente (pop-up) que notifica sobre la suspensión temporal de las transacciones PIX el 30/06 y afirma que “el fallo fue externo y no comprometió datos sensibles ni generó transacciones indebidas”.



Soffy Soluções de Pagamento: Pequeña fintech con sede en la Avenida Paulista, en la ciudad de São Paulo, es una de las empresas objetivo de la investigación de la Policía Civil de São Paulo por haber recibido 270 millones de reales del dinero desviado en el ataque a C&M.

2.3 Posicionamiento de Autoridades y empresas involucradas

Según informes compartidos por la prensa brasileña, el Banco Central fue notificado del incidente de inmediato, el 30 de junio, y sigue de cerca las investigaciones. Como medida preventiva, el 30 de junio C&M Software fue desconectada temporalmente del Sistema de Pagos Brasileño (SPB) para mitigar los riesgos de nuevas transacciones irregulares.

En un comunicado al portal Bastidor, el Banco Central confirmó el ataque a C&M y afirmó que ordenó la desconexión del acceso a la plataforma de la empresa: "C&M Software, un proveedor de servicios de tecnología para instituciones que ofrecen cuentas transaccionales y que no poseen medios de conexión propios, comunicó un ataque a su infraestructura tecnológica. El Banco Central ordenó a C&M la desconexión del acceso de las instituciones a las infraestructuras operadas por ella".

El 01/07, BMP publicó un comunicado oficial a los socios de BMP Plus, informando que el servicio PIX estaba temporalmente interrumpido debido a un ataque cibernético que comprometió parcialmente la infraestructura de conexión de C&M Software (sin citar el nombre de la institución).

BMP
O banco do futuro

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.**

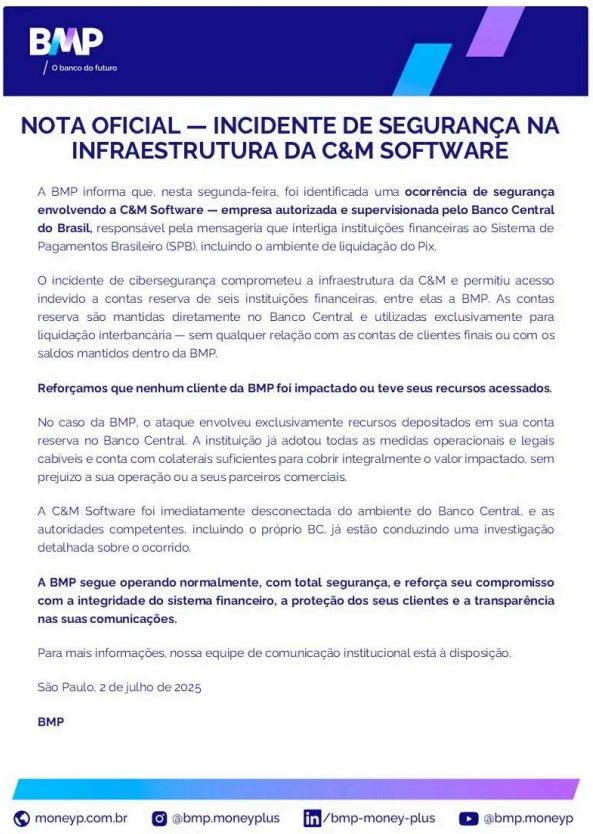
O Banco Central já foi oficialmente comunicado, e medidas de contenção e restabelecimento estão em andamento, com acompanhamento contínuo das autoridades competentes.

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

En 02/07, BMP publicó una nota oficial en su website, reconociendo el incidente que envolvió a C&M Software, y destacando que no hubo impacto ni acceso a datos de sus 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

En dia 03/07, el Banco Central publicó una nota oficial en su portal, anunciando la vuelta parcial de las operaciones de 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.

C&M Software publicó un comunicado oficial en su sitio web, en formato de preguntas y respuestas, donde destaca principalmente que no hubo evidencias de que su entorno fuera comprometido ni de la explotación de una vulnerabilidad, y que el incidente ocurrió debido al uso de las credenciales de un colaborador suyo, que ya ha sido desvinculado de la empresa, las cuales fueron obtenidas por ingeniería social fuera del ambiente de trabajo. El comunicado también informa que C&M consiguió recuperar parte de los montos desviados activando el MED (Mecanismo Especial de Devolución).

2.4 Análisis del ciberataque

Existen indicios de que el ataque a C&M Software involucró el acceso remoto al entorno y a los sistemas de procesamiento de transacciones del SPB mantenidos por la empresa. Una vez con acceso al sistema, el atacante debe haber obtenido acceso a las credenciales de las instituciones financieras clientes de C&M, lo que le dio acceso a los certificados y claves privadas necesarios para ejecutar transacciones PIX fraudulentas, directamente a través del SPI utilizando los sistemas de C&M.

Las características del ataque, junto con la declaración del primer sospechoso identificado por la policía, indican que el crimen fue realizado por un grupo criminal brasileño, formado por, al menos, 5 personas. El fraude fue planeado durante varios meses, por lo menos desde antes de marzo de 2025, y el grupo posee un gran conocimiento técnico y procesal sobre el funcionamiento del sistema financiero brasileño, del sistema de pagos (SPB) y del sistema PIX (Sistema de Pagos Instantáneos).

Con base en el análisis del caso, a continuación se presenta un supuesto *modus operandi* establecido por la investigación de Apura sobre cómo se habrían desarrollado las etapas del fraude.

Acceso al Entorno Interno

Según las investigaciones de la Policía Civil de São Paulo, los delincuentes consiguieron acceso al entorno de C&M Software al captar a un empleado de la empresa, João Nazareno Roque, que trabajaba como desarrollador júnior. Él confesó haber sido captado por otras personas y las ayudó a invadir el sistema. En mayo de este año, Roque ejecutó comandos en los servidores de C&M, siguiendo la orientación de los delincuentes, lo que les permitió el acceso remoto a los sistemas de la empresa.

En un comunicado oficial, publicado en su sitio web, C&M Software destacó que los elementos investigados por las autoridades y por las pesquisas independientes contratadas indican que el episodio tuvo inicio con el uso compartido indebido de credenciales por parte de un colaborador, inducido por terceros por medio de técnicas de ingeniería social. El colaborador fue abordado fuera del entorno de la empresa por

un tercero que se presentó como “vinculado a hackers” y le prometió un beneficio financiero. El acceso comenzó con sus credenciales personales, pero hay indicios de que se utilizaron credenciales adicionales o mecanismos de autenticación auxiliares, lo que está bajo análisis técnico.

La empresa declara que no hubo una intrusión externa ni una violación técnica de la infraestructura de C&M y que no identificaron ningún fallo técnico o vulnerabilidad en sus sistemas.

Reconocimiento y Mapeo

Una vez obtenido el acceso inicial al entorno de C&M Software, los intrusos habrían realizado un mapeo de la infraestructura y del funcionamiento del sistema de transferencias, identificando cómo se estructuraban las transacciones PIX y dónde estaban almacenados los artefactos críticos de autenticación.

En este momento, los atacantes posiblemente mapearon las instituciones financieras clientes de C&M que tenían credenciales almacenadas con la misma, posiblemente usando enumeración. Creemos que, en esa fase, los atacantes identificaron las instituciones financieras en las que era posible tener acceso a sus cuentas de reserva.

Compromiso de Credenciales Sensibles

En nuestro análisis, supuestamente el actor obtuvo acceso a las credenciales de las instituciones financieras y, posiblemente, incluso a las claves privadas y los certificados digitales utilizados por las instituciones clientes de la proveedora para firmar las transacciones PIX. En general, dichas claves se comparten con el PSTI para realizar la firma de las transacciones.

Según el portal G1, en un comunicado, el director comercial de C&M Software, Kamal Zogheib, afirmó que la empresa fue víctima directa de una acción criminal, que involucró el uso indebido de credenciales de clientes para acceder a sus sistemas y servicios de forma fraudulenta.

Con esta información y el acceso privilegiado al sistema de C&M y a las cuentas de las instituciones financieras, los atacantes asumieron la capacidad de inyectar transacciones legítimas en el SPI en nombre de esas instituciones.

Ejecución Masiva de Transacciones PIX

Utilizando las credenciales y los certificados comprometidos, los intrusos habrían inyectado transacciones directamente en el SPI en nombre de las instituciones

financieras, desde la plataforma de C&M Software, las cuales fueron procesadas normalmente por las instituciones financieras, ya que:

- Los mensajes estaban debidamente firmados por las instituciones de origen, puesto que el sistema de C&M estaba comprometido.
- Había respaldo para la realización de esas transacciones, basado en el depósito hecho en la "cuenta de reserva" junto al Banco Central.
- El SPI no realiza validación de saldo, legitimidad del pagador o análisis antifraude; asume que esto fue hecho previamente por la institución.

Las transacciones entre instituciones financieras brasileñas solamente pueden ser insertadas en el sistema de pagos brasileño desde sistemas autorizados y específicos, que tienen acceso a las claves privadas de las instituciones para firmar digitalmente las transacciones, conforme a la exigencia técnica del SPB. Por lo tanto, tal ataque involucró el conocimiento de dichos sistemas y protocolos, además del acceso privilegiado a los mismos, y no podría ser reproducido desde otro sistema.

Además del acceso privilegiado a los sistemas de C&M Software, observamos que los atacantes posiblemente optaron intencionalmente por hacer las transferencias de fondos fuera del horario comercial. Al realizar el fraude en la madrugada del domingo al lunes, lo hicieron probablemente con la expectativa de que sería un horario más difícil para que hubiera monitoreo humano y, así, alguien identificara e interrumpiera las transacciones fraudulentas. En ese momento, la funcionalidad de transferencias instantáneas y a cualquier hora del PIX fue una gran aliada de los ciberdelincuentes.

Creemos que las transacciones habrían ocurrido hasta agotar los saldos en las cuentas de liquidación (cuentas de reserva) o hasta ser identificadas e interrumpidas por las entidades involucradas.

Según la investigación de la Policía Civil de São Paulo, tras acceder a la cuenta de reserva mantenida por el banco BMP en el Banco Central, los delincuentes desviaron R$ 541 millones de la empresa a través de 166 transferencias a 29 instituciones financieras diferentes. Una fintech, Soffy, recibió 69 transacciones que totalizaron R$ 271 millones.

Destino de los Fondos

Hay fuertes indicios de que la mayoría de las transacciones fueron dirigidas inicialmente a cuentas corrientes en instituciones de pago de menor tamaño, que generalmente poseen controles más laxos de incorporación y verificación (KYC), facilitando la apertura

y manipulación de cuentas a nombre de testaferros. La transferencia vía PIX dio agilidad a la evasión de los fondos.

Las cuentas de destino fueron usadas como puente para el objetivo final del grupo criminal: ocultar el dinero desviado en criptomonedas.

Lavado y Dispersión

Tras la exfiltración de los fondos a cuentas de testaferros, los montos fueron rápidamente dispersados en pequeñas transacciones y supuestamente también convertidos en criptoactivos, dificultando el rastreo y bloqueo de los valores desviados. Según las noticias, parte de esas transacciones fueron identificadas como sospechosas y bloqueadas en algunas exchanges.

Según un reportaje del portal Cointelegraph, el CEO de SmartPay y Truther, Rocelo Lopes, informó haber detectado un movimiento atípico en ambas plataformas a las 00:18 del día 30 de junio, y automáticamente elevó los filtros de validación en las compras de USDT y Bitcoin. Según él, se retuvieron grandes sumas de dinero y, en ese mismo momento, se realizó el proceso de devolución a las instituciones involucradas.

Los operadores de SmartPay identificaron un PIX por un valor de R$ 6 millones desde BMP, lo que llamó la atención. Los empleados, entonces, se percataron de una cantidad muy por encima de lo normal de movimientos de nuevas cuentas y muchas solicitudes de transferencias en un intervalo corto, de cerca de dos horas.

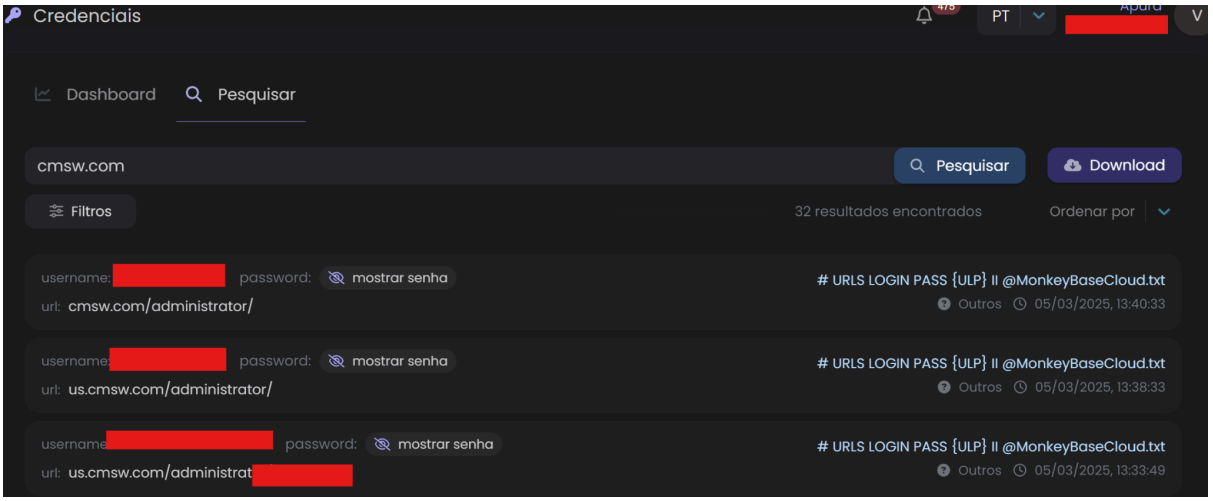
2.5 Investigações actuales

Hipótesis iniciales

Pocas horas después de conocerse el incidente en C&M Software, diversas hipótesis fueron barajadas por la prensa y por profesionales del sector.

Supuestamente, según diversos informes reproducidos por la prensa, los atacantes habrían explotado posibles vulnerabilidades en el entorno tecnológico de C&M Software y utilizado herramientas de acceso remoto (RMM) para entrar en el entorno de C&M.

A partir de BTTng, identificamos la filtración de 32 credenciales de C&M, incluyendo contraseñas supuestamente de administrador. Dichas credenciales, en caso de que fueran válidas en el momento del incidente, podrían haber sido un posible vector de acceso.



Un informe creado por una empresa tercera, no involucrada oficialmente en las investigaciones, planteó la hipótesis de que C&M Software supuestamente operaba un bróker de mensajería Java, ActiveMQ 5.x, para orquestar las colas de mensajes de liquidación para el Banco Central. Esta plataforma podría, supuestamente, ser explotada y ofrecer acceso remoto a los delincuentes, ya que sería vulnerable a la CVE-2023-46604[1]. El mismo informe declara que las claves privadas de cifrado estarían accesibles en el servidor de C&M, en lugar de estar almacenadas en un dispositivo HSM. La empresa no mostró evidencias de estas afirmaciones.

Analizando las especificidades de este caso y comparándolo con el escenario actual de actores de amenaza en Brasil, es posible percibir similitudes con el grupo Plump Spider. Este actor brasileño, ya conocido por la comunidad de inteligencia, se enfoca en instituciones financieras, no solo bancos, sino también empresas que tienen actividades financieras. El grupo, de origen brasileño, está activo desde 2023 y acumula casi dos años de actividades de ciberdelincuencia sin ninguna identificación por parte de las autoridades.

Prisión de sospechoso por facilitar el acesso

En dos artículos publicados por el portal G1 el 4 de julio, se confirmó la detención de un sospechoso de participar en el ataque a C&M Software el jueves (03/07), realizada por el Departamento Estatal de Investigaciones Criminales (DEIC), de la Policía Civil de São Paulo. El sospechoso, identificado en el reportaje como João Nazareno Roque, de 48 años, es un operador de TI de C&M (aunque en su perfil de LinkedIn se presenta como electricista y Desarrollador Back-End Jr.). Fue detenido en el barrio de City Jaraguá, en la

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

Zona Norte de la ciudad de São Paulo. La investigación indaga la participación de otras personas. La policía incautó equipos en su casa y bloqueó sus cuentas.

Según los investigadores, el hombre bajo custodia es empleado de la propia C&M Software desde 2022 y dio acceso a través de su equipo al sistema del banco a los delincuentes que efectuaron el ataque. El sospechoso habría confirmado informalmente a la policía que entregó la contraseña de acceso a terceros, que cometieron el fraude. Él los ayudó a ingresar al sistema y a realizar las transferencias vía PIX. En su declaración, afirmó que recibió R$ 15 mil, en efectivo, por facilitar el acceso.

De acuerdo con la declaración de João Nazareno Roque, recibió dos pagos:

- R$ 5 mil por proporcionar el usuario y la contraseña corporativos de la empresa C&M. El pago se realizó a través de un mensajero en motocicleta (*motoboy*), quien también recogió las credenciales de acceso.
- R$ 10 mil por continuar insertando comandos en el sistema desde su propio equipo, al servicio del grupo criminal. Recibió las instrucciones a través de notas compartidas en Notion. Este segundo monto también fue pagado en billetes de R$ 100,00, nuevamente a través de un mensajero en motocicleta (*motoboy*).

El reportaje de G1 también destaca que se desviaron R$ 541 millones de BMP y que una cuenta con R$ 270 millones, que fue usada para recibir el dinero desviado, ya ha sido bloqueada.

C&M Software dijo, en un comunicado, que “el colaborador trabajaba en CMSW desde 2022 y fue desvinculado de la empresa justo después de la investigación inicial de los hechos. La decisión fue tomada con base en los elementos técnicos recopilados, de forma criteriosa y en línea con los procedimientos internos de la compañía.”

Participación de entidades de pago

Según un artículo del portal Finsiders Brasil, el Banco Central informó en la noche del jueves (03/07) la suspensión cautelar de las Instituciones de Pago (IP) Transfeera, Nuoro Pay y Sofffy del sistema Pix, como consecuencia del ataque a C&M Software.

Según fuentes consultadas por el reportaje, estas tres IP fueron las que recibieron el mayor volumen de fondos desviados y no consiguieron identificar y bloquear los depósitos. Todas recibieron cientos de millones e hicieron la conexión con las exchanges de criptomonedas.

Posteriormente, el 04/07, el Banco Central suspendió el acceso al sistema Pix de otras tres instituciones de pago: Voluti Gestão Financeira, Brasil Cash y S3 Bank.

2.6 El caso y el escenario del cibercrimen brasileño en 2025

El incidente en C&M Software involucró la vulneración de componentes tecnológicos y procesos muy específicos del sistema financiero brasileño. Esto nos lleva a creer que el actor responsable del incidente tiene familiaridad con el país y, posiblemente, puede haber habido colaboración de personas con experiencia en el sector financiero
Al momento de la redacción de este informe, todavía no hay evidencias ni noticias sobre la posible identidad de los actores responsables del ataque a C&M Software, su modus operandi o su afiliación.

Características del grupo criminal

Es posible deducir, a partir de las declaraciones de João Nazareno Roque, que el grupo criminal responsable del ataque a C&M Software estaba formado por al menos 5 personas: una que lo abordó presencialmente ofreciéndole dinero para que cediera sus credenciales de acceso, y otras cuatro personas diferentes con las que se comunicó vía teléfono celular, que le enviaron instrucciones para que Roque facilitara el acceso remoto de los mismos.

Como el primer contacto con Roque ocurrió en marzo de este año, queda claro que el grupo planeó el fraude durante al menos 4 meses. El grupo posee conocimientos avanzados sobre el funcionamiento del sistema financiero, y conocimientos técnicos sobre el sistema de pagos brasileño (SPB) y el sistema de pagos instantáneos (SPI), responsable de PIX.

3. Mapeamiento con MITRE ATT&CK

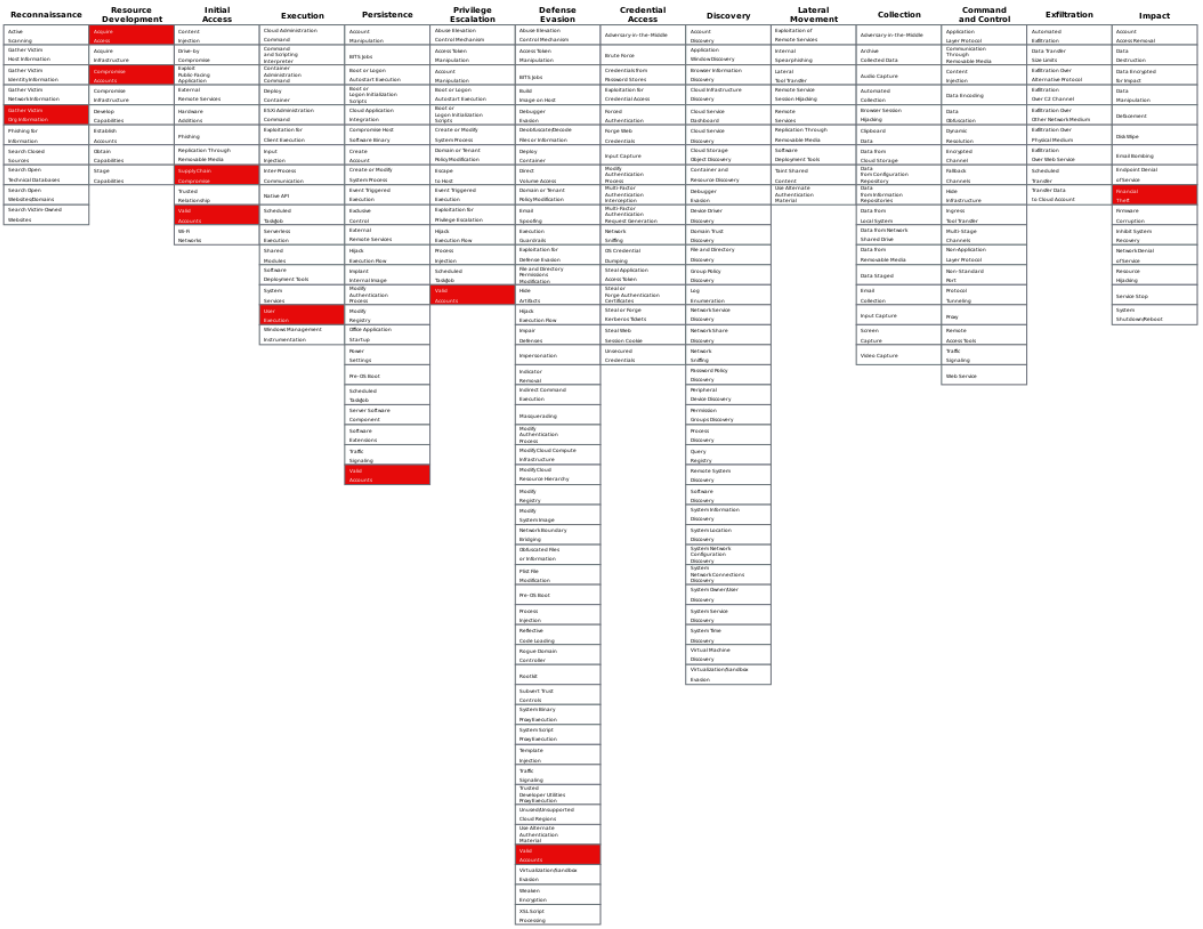
Basado en la información pública del incidente, podemos señalar algunos de los posibles pasos realizados por el actor durante la explotación de C&M Software, en términos de Tácticas, Técnicas y Procedimientos (TTP) conocidos, con base en el framework MITRE ATT&CK.

El siguiente mapeo fue realizado considerando la información disponible en la prensa sobre el incidente, ya que los detalles del ataque no han sido divulgados. De esta forma, mucha información importante para entender el ataque y mapearlo correctamente no se conoce hasta el momento.

A continuación, presentamos los supuestos pasos del ciberataque, mapeados según el framework MITRE ATT&CK (Enterprise ATT&CK v17):

Reconocimiento (Reconnaissance)		
T1591.002	Recolectar Informaciones sobre la Organización Víctima	Los criminales mapean una empresa que actúa como PSTI junto al SPB e identifican las organizaciones financieras a las cuales presta servicio.
Desarrollo de Recursos (Resource Development)		
T1650	Obtener Acesso	Según investigaciones de DEIC, los criminales sobornaron a un funcionario de C&M, que les proporcionó sus credenciales de acceso.
T1586	Cuentas comprometidas	Los delincuentes explotaron cuentas comprometidas relacionadas con los servicios de C&M Software y de sus clientes financieros, que fueron usadas posteriormente para el acceso y la transferencia de fondos de las cuentas de reserva.
Acesso Inicial (Initial Access)		
T1195.002	Compromiso de la Cadena de Suministro / Comprometer la Cadena de Suministro de Software	Los actores manipularon los sistemas transaccionales de C&M Software utilizados por sus clientes, con el objetivo de inyectar transacciones fraudulentas en el SPI sin el conocimiento de los mismos.
T1078	Cuentas Válidas	Según las investigaciones del DEIC, los delincuentes utilizaron las credenciales de un empleado de C&M para obtener acceso a los sistemas de la empresa.
Execução (Execution)		
T1204	Execución peor usuário	Según las investigaciones del DEIC, los delincuentes sobornaron a un empleado de C&M y lo orientaron para que ejecutara comandos en los sistemas de la empresa.
Persistencia (Persistence)		
T1078	Cuentas Válidas	Según las investigaciones del DEIC, los delincuentes utilizaron las credenciales de un empleado de C&M para obtener acceso a los sistemas de la empresa.
Escalada de Privilegios (Privilege Escalation)		

T1078	Cuentas Válidas	Según las investigaciones del DEIC, los delincuentes utilizaron las credenciales de un empleado de C&M para obtener acceso a los sistemas de la empresa.
Evasión de las Defensas (Defense Evasion)		
T1078	Cuentas Válidas	Según las investigaciones del DEIC, los delincuentes utilizaron las credenciales de un empleado de C&M para obtener acceso a los sistemas de la empresa.
Impacto (Impact)		
T1657	Robo Financiero	Un volumen significativo de recursos financieros fue desviado de instituciones financieras que utilizaban la plataforma de C&M Software.



4. Sobre el Sistema de Pago Brasileño e los Proveedores de Servicios de Tecnología de la Información

Entre bastidores del sistema financiero brasileño, buena parte de la tecnología que hace que todo funcione —apertura de cuentas, pagos vía Pix, análisis de crédito, onboarding, prevención de fraudes— no está directamente en manos de los bancos o fintechs, sino de terceros. Son empresas que operan APIs, procesan transacciones, validan identidades, gestionan la infraestructura y, a menudo, mantienen el core bancario de instituciones enteras, los llamados PSTI — Proveedores de Servicios de Tecnología de la Información.
Este modelo, que ganó fuerza con el auge de las fintechs y el avance del open finance, aportó agilidad, reducción de costos y acceso rápido a soluciones financieras. Pero también creó un ecosistema altamente dependiente de terceros críticos, donde un fallo puntual puede escalar y afectar a múltiples actores al mismo tiempo.

4.1 Definición de PSTIs

PSTI es la sigla de Proveedor de Servicios de Tecnología de la Información, dentro del ecosistema del sistema financiero brasileño. Son empresas terceras autorizadas por el Banco Central, contratadas por instituciones financieras para ejecutar funciones esenciales de tecnología para el acceso al sistema bancario —desde el desarrollo de sistemas hasta la oferta de plataformas enteras que sustentan operaciones críticas, como pagos, validación de identidad, gestión de datos e incluso el core bancario.
Estos proveedores están detrás de servicios que van mucho más allá del soporte técnico tradicional. Son ellos los que ofrecen, por ejemplo:

- Plataformas de Banking as a Service (BaaS);
- Integración con el SPB;
- Plataformas de comunicación y transacción con el Sistema Financiero Nacional (SFN);
- Desarrollo y mantenimiento de software a medida;
- Almacenamiento en la nube y servicios de infraestructura;

- Gestión de identidad y acceso (IAM, autenticación, KYC);
- Soporte, help desk y gestión de operaciones en tiempo real.

Para fines de acceso a la Red del Sistema Financiero Nacional (RSFN), las PSTI actúan como pasarelas transaccionales entre las instituciones financieras, procesando operaciones de liquidación e integración con el sistema bancario nacional, incluyendo, por ejemplo, transferencias vía TED y Pix, emisión y pago de boletos, etc.

.

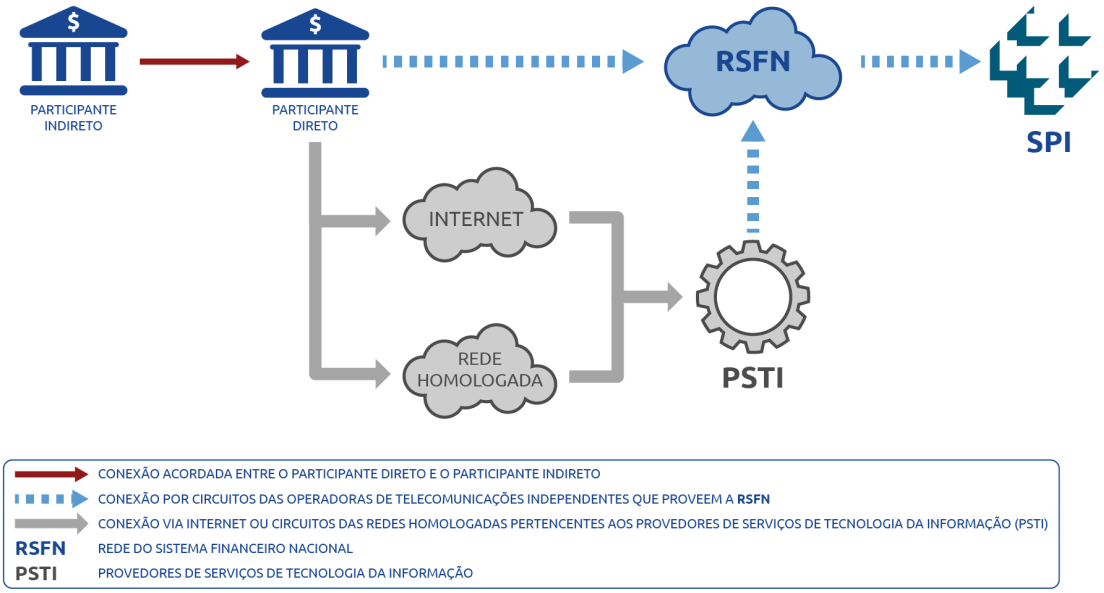


Imagen: Formas de acceso al Sistema de Pago Instantaneos, a través de PSTIs

En sectores altamente regulados, como el financiero, un PSTI puede ser clasificado como un tercero crítico, lo que significa que, desde el punto de vista regulatorio, la responsabilidad por fallos, filtraciones o indisponibilidad no es solo suya, sino también de quien lo contrató. Las obligaciones de seguridad, continuidad y cumplimiento deben ser tratadas con el mismo rigor que la operación interna.

Principales proveedores autorizados por el Banco Central de Brasil:

- ABBC – Associação Brasileira de Bancos;
- C&M Software – Proveedora de compensaciones, interconexión de cuentas y acceso al sistema de pagos. Fue el origen del reciente ataque;

- GOKEI Tecnología - Se diferencia por ofrecer un entorno Cloud de alto rendimiento y disponibilidad, utilizando la comunicación cliente-PSTI a través de recursos 100% en la nube;
- JD Consultores - Ofrece soluciones financieras desde hace 24 años;
- MAPS - Desde hace 30 años provee soluciones para pagos y liquidación financiera a través del SPB y SPI;
- Sinqia (antes MasterSAF, Icaro) – Soluciones para liquidación e integración bancaria;
- Stark – Creada en 2022, provee infraestructura para instituciones financieras y fintechs.

También figuran como PSTI homologados TIVIT y TOPAZ.

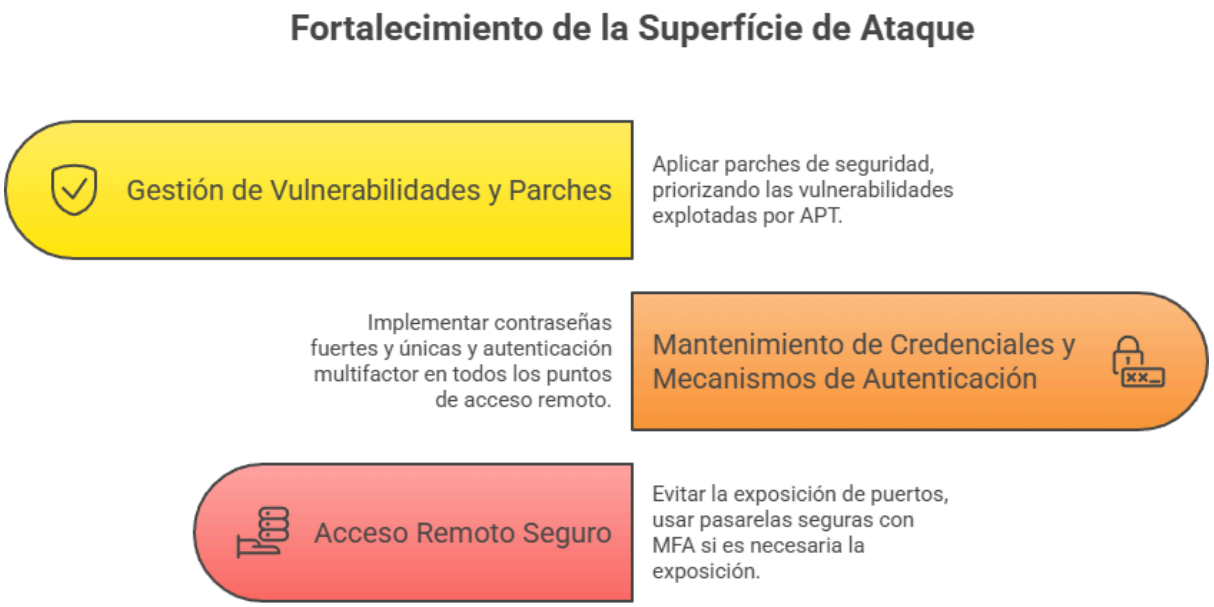
5. Recomendaciones

Los análisis presentados anteriormente en este informe demuestran que los actores de amenaza representan un riesgo estratégico directo, capaz de generar pérdidas financieras significativas, daños a la reputación de la marca e interrupciones operativas severas.

En respuesta a esta amenaza, hemos elaborado una guía estratégica de mitigación diseñada para aumentar la resiliencia corporativa y proteger el valor del negocio a partir de cuatro pilares fundamentales:

- **Fortalecimiento Proactivo de las Defensas:** Medidas preventivas para reducir la superficie de ataque y dificultar la intrusión inicial.
- **Capacidad de Detección y Respuesta Avanzada:** Implementación de tecnologías y procesos para identificar y neutralizar rápidamente las amenazas que penetran en el perímetro.
- **Inteligencia de Amenazas Accionable:** Utilización de inteligencia para anticipar y cazar amenazas de forma proactiva.
- **Gestión de Riesgos de la Cadena de Suministro:** Controles rigurosos para mitigar los riesgos introducidos por socios y proveedores de TI.

5.1 Fortalecimento de la Superfície de Ataque contra el compromiso inicial



Gestión de Vulnerabilidades y Parches: Aplicar parches de seguridad en sistemas orientados a internet, especialmente en pasarelas de VPN, RDP y software empresarial común. Priorizar las vulnerabilidades conocidas por ser explotadas por APT y grupos de ransomware.

Mantenimiento de Credenciales y Mecanismos de Autenticación: Implementar contraseñas fuertes y únicas y, de forma más crítica, exigir la Autenticación Multifactor (MFA) resistente al phishing en todos los puntos de acceso remoto, correo electrónico y aplicaciones en la nube. Este es el control más eficaz contra los ataques basados en credenciales.

Acceso Remoto Seguro: Evitar la exposición de puertos que proporcionen acceso a servicios críticos como RDP, Server Message Block (SMB), Telnet y NetBIOS, por ejemplo. En caso de que sea absolutamente necesaria la exposición de dicho puerto, realice el acceso remoto a través de una pasarela segura, con la MFA activa.

5.2 Defensa Pos Compromiso

Detección Basada en el Comportamiento: Implementar soluciones de seguridad avanzadas que utilicen Indicadores de Comportamiento además de los tradicionales Indicadores de Compromiso (IOC). Esto permite la detección de cadenas de actividades maliciosas sutiles, como una herramienta de administración legítima siendo utilizada para iniciar PowerShell para el movimiento lateral.

Visibilidad de Endpoints y Red: Implementar soluciones robustas de Detección y Respuesta en Endpoints (EDR) y segmentación de red. El EDR proporciona visibilidad sobre la ejecución de procesos en los endpoints (por ejemplo, winword.exe generando regsvr32.exe, un TTP de TA551), mientras que la segmentación puede contener el movimiento lateral de un atacante.

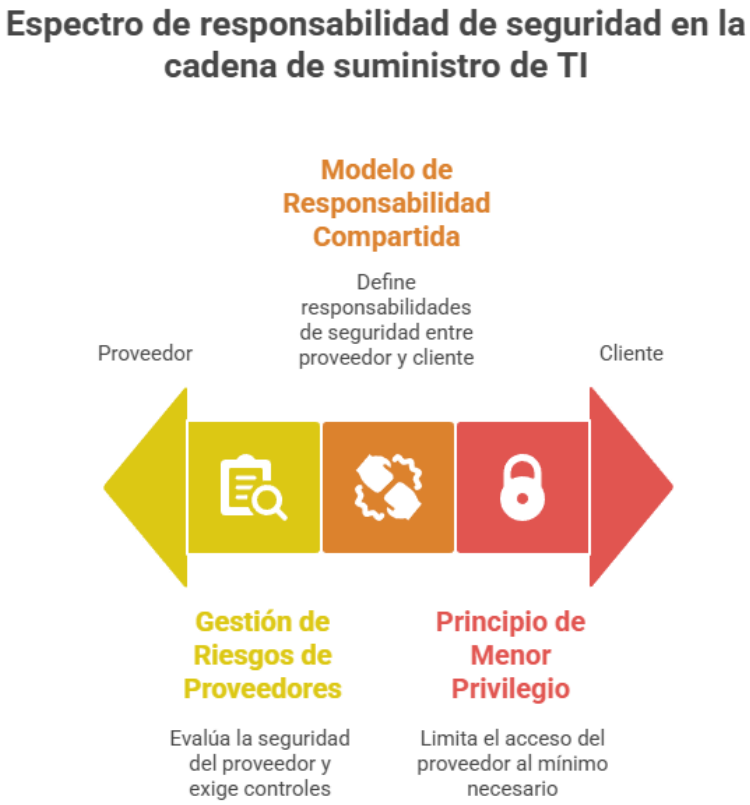
Registro y Monitoreo: Garantizar el registro exhaustivo de toda la actividad de la red, especialmente de las cuentas privilegiadas y las conexiones de terceros. Auditar regularmente estos registros (logs) en busca de comportamientos anómalos.

5.3 Inteligencia Proativa y Threat Hunting

Monitoreo de la Dark Web: Monitorear activamente foros de la *d*ark web, mercados ilegales y canales de Telegram en busca de menciones del nombre de su organización, dominios o credenciales comprometidas.

Monitoreo de Logs de Infostealers: Utilizar servicios que rastrean y analizan *logs* de *malware infostealer* para descubrir proactivamente si las credenciales de empleados o corporativas han sido comprometidas y están en circulación. Esto permite el restablecimiento de las credenciales antes de que sean utilizadas por un actor de amenaza.

5.4 Protegiendo la Cadena de Suministro de TI



Gestión de Riesgos de Proveedores: Para las organizaciones que utilizan PSTI, realizar evaluaciones de seguridad rigurosas de su proveedor. Los contratos deben exigir controles de seguridad específicos, incluyendo la MFA en todas las cuentas utilizadas para acceder a su entorno.

Principio de Menor Privilegio para Terceros: Garantizar que las cuentas del PSTI tengan solo el nivel mínimo de acceso necesario para realizar sus funciones. Su acceso debe ser estrictamente monitoreado y auditado.

Modelo de Responsabilidad Compartida: Definir claramente en los contratos quién es responsable de las funciones de seguridad como el fortalecimiento (hardening), la detección y la respuesta a incidentes.

6.Conclusiones hasta la fecha

El incidente ocurrido en C&M Software el día 30 de junio ya ha pasado a la historia como el mayor robo cibernético de Brasil, gracias a los montos exorbitantes involucrados.

El ataque presenta niveles complejos de sofisticación, que exigen un conocimiento profundo del funcionamiento del Sistema de Pagos Brasileño (SPB), incluyendo sus protocolos, sistemas y terceros involucrados. De hecho, tales operaciones fraudulentas, por sus características, sólo podrían haber sido manipuladas e insertadas en el sistema financiero a partir del acceso indebido y malicioso a los sistemas de procesamiento de transacciones conectados al SPB (Sistema de Pagos Brasileño).

Esto, sumado al esfuerzo necesario para exfiltrar grandes sumas de dinero a través de PIX y criptomonedas, indica que la operación fue compleja y exigió una gran planificación y preparación. Creemos, por lo tanto, que el incidente fue realizado por un grupo preparado y especializado, y no por un actor solitario. No descartamos la hipótesis de la participación de insiders, dada la gran especificidad de los sistemas involucrados.

Las investigaciones están en curso y cualquier conclusión sobre la naturaleza y autoría del ataque, en este momento, sería precipitada.

Debido al gran impacto que tuvo, se cree que este incidente motivará una gran revisión de los protocolos de seguridad del Sistema Financiero Nacional de Brasil. Aunque el SFN adopta protocolos técnicamente robustos de comunicación y mensajería, el incidente de C&M Software del 30 de junio de 2025 mostró la fragilidad de todo el sistema a raíz de la vulneración de un único proveedor, un escenario clásico de compromiso en la cadena de suministro.

Los clientes de Apura Cyber Intelligence tienen acceso, a través de la plataforma BTTng, al informe detallado, que se actualiza oportunamente con cada novedad relevante sobre el incidente.

7. Referencias

- Exclusivo: Hackers se llevan más de R$ 1 mil millones de 'banking as a service' - https://braziljournal.com/exclusivo-hackers-levam-mais-de-r-1-bilhao-em-ataque-a-banking-as-a-service/
- Ataque al sistema financiero - https://obastidor.com.br/economia/ataque-ao-sistema-financeiro-8979
- En la madrugada, un Pix de R$ 18 millones. Comenzaba el ataque: https://braziljournal.com/na-madrugada-um-pix-de-r-18-milhoes-comecava-o-assalto/
- Hackers roban R$ 1 mil millones en cuentas del sistema financiero nacional e intentan convertirlos en Bitcoin y 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
- El CEO de BMP cuenta paso a paso los entretelones del robo que hizo que R$ 400 millones desaparecieran de la cuenta de la 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/
- La PF abre una investigación para indagar el ataque a sistemas de instituciones financieras; el BC no fue afectado - 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
- Comunicado oficial de BMP: https://moneyp.com.br/comunicados/nota-oficial-bmp-ataque-c-m-software/
- Comunicado del Banco Central: https://www.bcb.gov.br/detalhenoticia/20752/nota
- Comunicación electrónica de datos en el sistema financiero - https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados
- La Policía Civil detiene en SP a sospechoso de ataque hacker al sistema que conecta a los bancos con 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
- Ataque al sistema Pix: operador de TI recibió R$ 15 mil por entregar contraseña a hackers, dice la policía; sepa quién es el sospechoso 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
- El BC suspende de Pix a los participantes Transfeera, Nuoro Pay y Soffy (actualización) -

https://finsidersbrasil.com.br/reportagem-exclusiva-fintechs/bc-suspende-os-participantes-do-pix-transfeera-nuoro-pay-e-soffy/

- Horario, enfoque en bitcoin, insistencia: las pistas que ayudaron a revelar el ataque contra la empresa que conecta a los bancos con 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
- Comunicado oficial de C&M Software: https://cmsw.com/blog/qa-incidente-de-seguranca/
- El Banco Central suspende a otras tres instituciones de pago durante la investigación del ataque hacker - https://www1.folha.uol.com.br/tec/2025/07/banco-central-suspende-mais-tres-instituicoes-de-pagamentos-durante-investigacao-de-ataque-hacker.shtml
- Constituida 19 días antes del desvío millonario de Pix, una empresa recibió R$ 45 millones - 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
- Ataque hacker: BMP perdió, por sí sola, R$ 541 millones; otras instituciones también fueron afectadas - https://g1.globo.com/economia/noticia/2025/07/04/ataque-hacker-recursos-desviados.ghtml
- Ataque hacker transfirió R$ 541 millones de BMP a 29 instituciones; parte del monto fue recuperado - 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

8. Glosario

Aquí tienes la traducción del glosario:

Certificados (Digitales) - Documentos electrónicos emitidos por una Autoridad de Certificación (AC) que acreditan la identidad de una entidad (persona, empresa o sistema) y vinculan esa identidad a una clave criptográfica.

Cuentas de Testaferros (*Contas Laranja*) - Cuentas bancarias abiertas a nombre de terceros (personas físicas o jurídicas) con fines de fraude, generalmente con poca o ninguna conciencia sobre el uso ilícito de la cuenta.

Cuentas de reserva - Depósitos mantenidos por las instituciones financieras brasileñas directamente en el Banco Central de Brasil y utilizados exclusivamente para la liquidación interbancaria.

Criptoactivos - Activos digitales cifrados, transferidos y almacenados por medio de tecnologías de registro distribuido, como la *blockchain*.

Fintechs - Empresas que introducen innovaciones en los mercados financieros por medio del uso intensivo de tecnología, con el potencial de crear nuevos modelos de negocio. Actúan a través de plataformas en línea y ofrecen servicios digitales innovadores relacionados con el sector.

Participante del SFN – Se refiere a cualquier institución autorizada por el Banco Central de Brasil o ente gubernamental cuyos sistemas se comunican electrónicamente a través de la SFN. Los participantes del SFN interactúan por medio de mensajes y de archivos, en las redes homologadas por el Banco Central.

Piloto de Reservas - Profesional responsable de monitorear y gestionar las cuentas de reservas bancarias o de liquidación de una institución financiera. Su principal función es garantizar la liquidez de la institución, a través de la precisión y confiabilidad de los saldos de esas cuentas, verificando y registrando todos los asientos de débito o crédito.

PIX - Sistema brasileño de pago instantáneo, creado por el Banco Central, que permite transferencias y pagos en tiempo real, las 24 horas del día, los 7 días de la semana, entre diferentes bancos e instituciones financieras en el país.

Proveedores de Servicios de Tecnología de la Información (PSTI) - Entidades autorizadas por el Banco Central de Brasil para prestar servicios de procesamiento de datos, para fines de acceso a la RSFN, a instituciones financieras y demás instituciones autorizadas para operar por el Banco Central de Brasil.

Red del Sistema Financiero Nacional (RSFN) - La RSFN es una estructura de comunicación de datos entre instituciones financieras brasileñas que tiene por finalidad soportar el tráfico de información en el ámbito del SFN para servicios autorizados.

Remote Monitoring and Management **(RMM)** - Tecnología utilizada por equipos de TI para monitorear, gestionar y acceder remotamente a computadoras, servidores y dispositivos de red.

Sistema Financiero Nacional (SFN) - Entidad brasileña formada por un conjunto de entidades e instituciones que promueven la intermediación financiera, es decir, el encuentro entre acreedores y prestatarios de recursos. Es por medio del sistema

financiero que las personas, las empresas y el gobierno circulan la mayor parte de sus activos, pagan sus deudas y realizan sus inversiones.

Sistema de Pagos Brasileño (SPB) - Un conjunto de reglas, procedimientos, instituciones y sistemas gestionado por el Banco Central que, a través de infraestructuras, reglas y procedimientos, viabilizan las transacciones financieras en Brasil. Abarca desde operaciones de transferencia de fondos, como TEDs y Pix, hasta la liquidación de pagos con tarjetas y boletos.

Sistema de Pagos Instantáneos (SPI) - Infraestructura centralizada y única para la liquidación de pagos instantáneos entre distintas instituciones en Brasil. La operación del SPI, gestionada por el BCB, comenzó en noviembre de 2020. El SPI es un sistema de liquidación bruta en tiempo real (LBTR), es decir, que procesa y liquida transacción por transacción. Una vez liquidadas, las transacciones son irrevocables.

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