INVESTIGACIÓN DE CIBERSEGURIDAD

Caso Binance Hack (2019)

Robo de 7,000 BTC del hot wallet del exchange Binance mediante compromiso de credenciales de usuario

Información general del caso

Ficha técnica del incidente

Víctima	Binance - Mayor exchange de criptomonedas del mundo por volumen de trading (fundado por Changpeng Zhao, "CZ")
Fecha del ataque	7 de mayo de 2019 (detectado y detenido en los primeros minutos; anunciado públicamente ese mismo día)
Monto sustraído	7,000 – 7,074 BTC (las cifras varían ligeramente entre fuentes)
Valor en el momento	Aproximadamente USD $40–41 millones (a un precio de BTC de ~$6,000)
Wallet afectado	Hot wallet de BTC de Binance (~2% de las reservas totales de Bitcoin de la empresa)
N.° de transacciones	Una sola transacción de retiro
Hash de la transacción	e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea
Vector de ataque	Phishing + malware para obtener claves API y códigos 2FA de usuarios
Fondo de compensación	SAFU (Secure Asset Fund for Users) cubrió el 100% de la pérdida
Suspensión de servicio	Depósitos y retiros suspendidos por ~1 semana; el trading continuó operativo

Cronología del incidente

- **Julio de 2018 —** posible antecedente: Binance ya había sufrido un incidente muy similar (también anunciado como "mantenimiento de emergencia") en el que se retiraron exactamente 7,000 BTC explotando claves API de usuarios. Nunca se confirmó oficialmente si se trató del mismo actor, pero la comunidad cripto lo bautizó como el "hackeo anual de 7,000 BTC de Binance".

- **7 de mayo de 2019 (mañana) —** CZ publica en Twitter que Binance realizará un "mantenimiento de servidor no programado" que afectará depósitos y retiros, añadiendo la frase "funds are #SAFU" para calmar a la comunidad.
- **7 de mayo de 2019 (horas después) —** Binance confirma oficialmente vía comunicado ("Binance Security Breach Update") que sufrió una brecha de seguridad a gran escala y que se retiraron 7,000 BTC en una sola transacción.
- **Inmediatamente después —** Binance suspende todos los depósitos y retiros; anuncia que realizará una revisión de seguridad exhaustiva de aproximadamente una semana; coordina con otros exchanges (incluido Coinbase) para bloquear depósitos provenientes de las direcciones de los atacantes.
- **Mismo día —** CZ realiza una sesión pública de preguntas y respuestas (AMA) en Twitter para mantener la transparencia con la comunidad, y menciona que se evaluó (y luego se descartó) la posibilidad de una reorganización ("reorg") de la cadena de Bitcoin con el 51% del hashrate para revertir la transacción — descartada por el daño reputacional que causaría a Bitcoin como red descentralizada.
- **Semana siguiente —** se restablecen los depósitos y retiros tras completar la revisión de seguridad; Binance anuncia mejoras en sus protocolos de 2FA y de gestión de claves API.
- **Junio de 2019 en adelante —** comienza el rastreo forense de los fondos robados por parte de firmas como Chainalysis, PeckShield, Whale Alert, Coinfirm y Clain, que detectan el uso del mixer ChipMixer para el lavado de una parte significativa del botín.

Declaraciones oficiales clave

Binance explicó el incidente de la siguiente manera en su comunicado oficial:

- *"Hackers were able to obtain a large number of user API keys, 2FA codes, and potentially other info." Los hackers pudieron obtener un gran número de claves API de usuarios, códigos 2FA y potencialmente otra información.*
- *"The hackers had the patience to wait, and execute well-orchestrated actions through multiple seemingly independent accounts at the most opportune time." — Los hackers tuvieron la paciencia de esperar y ejecutar acciones bien orquestadas a través de múltiples cuentas aparentemente independientes en el momento más oportuno.*
- *"The transaction is structured in a way that passed our existing security checks." — La transacción fue estructurada de forma que pasó los controles de seguridad existentes.*

Impacto y reacción del mercado

- El precio de Bitcoin cayó de forma moderada tras la noticia, pero se recuperó con relativa rapidez gracias a la transparencia de la comunicación de Binance.

- El token BNB (Binance Coin) sufrió una caída leve inicial, pero también se recuperó y alcanzó nuevos máximos poco después de restablecerse los retiros.
- El caso reforzó el debate sobre la seguridad de los exchanges centralizados frente a la custodia propia ("not your keys, not your coins").
- Otros exchanges y proveedores de wallets colaboraron activamente bloqueando depósitos asociados a las direcciones identificadas de los atacantes, mostrando un nivel de cooperación inusual en la industria.
- Este caso se ubica dentro de una ola de robos a exchanges de criptomonedas en 2019 (Coincheck, Bithumb, DragonEx, entre otros), lo que llevó a un mayor escrutinio regulatorio sobre la seguridad operativa de las plataformas.

Medidas correctivas de Binance

- Cobertura total de la pérdida mediante el fondo SAFU (Secure Asset Fund for Users), constituido con el 10% de las comisiones de trading desde julio de 2018.
- Solicitud a todos los usuarios de cambiar sus claves API y credenciales de 2FA tras el incidente.
- Revisión y actualización de los protocolos de seguridad de autenticación multifactor y gestión de claves API.
- Refuerzo de los sistemas de detección de retiros sospechosos (risk management checks) tanto en la fase previa como posterior al retiro.
- Mantenimiento de comunicación pública constante y transparente durante toda la crisis, lo cual la propia empresa señaló como un factor clave para conservar la confianza de la comunidad.

Técnicas utilizadas

Vector de entrada: phishing + malware

El hackeo se ejecutó mediante una combinación de ataques de phishing y malware que permitió a los atacantes obtener un gran número de códigos de autenticación multifactor (2FA) y claves API. La propia Binance lo confirmó: "Los hackers usaron una variedad de técnicas, incluyendo phishing, virus y otros ataques. Todavía estamos concluyendo todos los métodos posibles utilizados".

Puntos clave del vector de ataque

- **Robo de credenciales, no explotación de blockchain:** no se explotó ningún fallo criptográfico de Bitcoin; el ataque se dirigió contra la capa humana/operativa (usuarios y posiblemente empleados), no contra el protocolo.

- **Recolección paciente y distribuida:** Binance señaló que los atacantes "tuvieron la paciencia de esperar y ejecutar acciones bien orquestadas a través de múltiples cuentas aparentemente independientes en el momento más oportuno".
- **Evasión de controles de riesgo:** un grupo de hackers logró tomar control de varias cuentas de usuario y realizó solicitudes de retiro de tal forma que evadieron los controles de gestión de riesgo previos al retiro (pre-withdrawal risk management checks). El sistema de monitoreo posterior al retiro sí lo detectó de inmediato, y se suspendieron todos los retiros subsecuentes.
- **Estructuración deliberada de la transacción:** agruparon fondos desde múltiples cuentas y sincronizaron el momento del retiro para que pareciera actividad normal y descentralizada, evitando los umbrales y heurísticas que habrían disparado una alerta preventiva.

Posible reincidencia del mismo actor

Un año antes, en julio de 2018, Binance ya había sufrido un incidente prácticamente idéntico (descrito también como "mantenimiento de emergencia") en el que se retiraron exactamente 7,000 BTC explotando claves API de usuarios. La comunidad especuló que podía tratarse del mismo grupo, aunque esto nunca se confirmó oficialmente.

Contexto de la industria en 2019

Este tipo de ataque fue parte de una tendencia observada ese año: Lazarus Group (vinculado a Corea del Norte) perfeccionó esquemas de phishing más sofisticados contra exchanges de criptomonedas durante 2019, aunque no existe atribución oficial confirmada de Lazarus a este caso específico de Binance.

Evidencia digital

Evidencia en blockchain (on-chain, de carácter público)

- **Hash de la transacción del robo:** e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea, visible permanentemente en el explorador de blockchain.
- **Estructura de la transacción:** fue estructurada de forma que pasó los controles de seguridad existentes de Binance, es decir, el diseño mismo de la transacción (fragmentación, timing, agrupación de fondos desde múltiples cuentas) constituye en sí mismo evidencia forense de premeditación.
- **Direcciones de destino:** identificadas y publicadas rápidamente para que otros exchanges pudieran bloquear depósitos provenientes de ellas.

Evidencia del lado de Binance (off-chain / logs internos)

- Registros de acceso a las claves API comprometidas.
- Logs de autenticación 2FA usados de forma fraudulenta.
- Alarmas del sistema de monitoreo post-retiro, que se activaron inmediatamente después de ejecutada la transacción.
- Patrones de actividad de las "múltiples cuentas aparentemente independientes" usadas para camuflar el retiro.

Colaboración externa como fuente de evidencia adicional

Firmas de analítica como PeckShield y Whale Alert comenzaron a rastrear los fondos robados de inmediato, y varios exchanges y proveedores de wallets ofrecieron bloquear depósitos asociados a las direcciones de los atacantes. Esta colaboración amplió la base de evidencia disponible más allá de los sistemas internos de Binance.

Manejo forense de la evidencia

Este caso, al tratarse de un exchange centralizado y no de un dispositivo confiscado, no encaja en el modelo clásico de forense de disco o teléfono. La evidencia está repartida entre la infraestructura interna de Binance y la propia red pública de Bitcoin. A continuación se describe cómo se manejaría esa evidencia siguiendo estándares forenses reconocidos (NIST SP 800-86, ISO/IEC 27037) y las reglas de admisibilidad aplicables en jurisdicciones que siguen las Federal Rules of Evidence (FRE) de EE. UU.

Qué dispositivo contenía la evidencia

- Del lado de Binance: no un único dispositivo, sino un conjunto de sistemas internos del exchange — logs de acceso a las claves API comprometidas, logs del sistema de autenticación 2FA, y las alarmas del motor de gestión de riesgo que se dispararon inmediatamente después del retiro.
- Del lado público: la blockchain de Bitcoin misma, replicada en miles de nodos alrededor del mundo, contiene de forma inmutable la transacción del robo (TXID e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea), verificable independientemente por cualquier perito sin depender de Binance.
- Fuentes externas complementarias: bases de datos de firmas de inteligencia blockchain (Chainalysis, PeckShield, Whale Alert) que agregan y etiquetan las direcciones asociadas al ataque.

Cómo se preservaría la evidencia

- Evidencia on-chain: no requiere preservación activa en el sentido tradicional, porque la blockchain de Bitcoin es de solo-anexado (append-only) e inmutable una vez confirmada la transacción. Preservarla equivale a documentar el bloque exacto, su

altura (block height) y su hash en el momento de la captura, para que cualquier copia posterior sea verificable contra la cadena.

- Evidencia off-chain: sí requiere preservación activa. Binance opera un canal formal para agencias de la ley, el Government Law Enforcement Request System (LERS); al recibir una orden de preservación vinculada a una investigación criminal, la empresa retiene los registros internos por un período inicial de 90 días, prorrogable mediante una solicitud adicional, mientras se tramita el proceso legal formal (subpoena u orden judicial) que autorice su entrega.
- Buena práctica aplicable: aislar los logs originales en modo de solo lectura, trabajar únicamente sobre una copia forense, y documentar cada acceso posterior en un registro de cadena de custodia (quién, cuándo, con qué propósito).

Qué tipo de adquisición se realizaría: física o lógica

No aplica adquisición física clásica, ya que no existe un disco duro o teléfono que clonar bit a bit. Corresponde a una adquisición lógica: exportación selectiva de registros de bases de datos y logs de servidor (accesos a API, eventos de 2FA, alertas de risk management), más la consulta o captura directa de la transacción desde un nodo de Bitcoin o un explorador de blockchain confiable. La adquisición lógica es la norma en casos de exchanges e infraestructura cloud, donde el perito no tiene acceso físico al servidor sino que trabaja mediante exportaciones autorizadas y APIs administrativas.

Qué hash generarían

Conviene distinguir dos hashes que suelen confundirse en este caso:

- El hash de la transacción de Bitcoin (TXID) e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea es un identificador criptográfico generado por el propio protocolo de Bitcoin (doble SHA-256); identifica el ataque, no la integridad de la evidencia recolectada por el investigador.
- El hash de integridad forense es distinto: es el valor SHA-256 (u otro algoritmo equivalente) que el perito calcula sobre cada archivo o log exportado en el momento de la recolección, y que vuelve a calcular antes de presentarlo, para demostrar que el archivo no fue alterado entre la captura y la presentación. Es este segundo hash el que sustenta la cadena de custodia y la admisibilidad legal, no el TXID.

Cómo presentarían la evidencia ante un tribunal

- En jurisdicciones que siguen las Federal Rules of Evidence (FRE) de EE. UU., los registros electrónicos y las copias de datos pueden auto-autenticarse bajo las Reglas 902(13) y 902(14), vigentes desde diciembre de 2017, mediante una certificación escrita de una persona calificada que confirme que el valor hash de la copia coincide con el original — esto evita la necesidad de testimonio en vivo para establecer la autenticidad, aunque no elimina objeciones por otros motivos (relevancia, testimonio de oídas, etc.).

- La naturaleza pública y verificable de la blockchain de Bitcoin es en sí misma una ventaja probatoria: cualquier perito de la contraparte puede reproducir de forma independiente la verificación del TXID contra la cadena, sin depender únicamente de la palabra de Binance.
- Para los registros internos de Binance, la vía formal de acceso legal es su portal de solicitudes para agencias de la ley (LERS), donde se presenta la orden judicial correspondiente y se documenta la respuesta oficial de la empresa como parte de la cadena de custodia.

Nota metodológica: Binance nunca publicó un informe forense detallado con esta metodología específica para el caso de 2019 — la empresa mantuvo la mayoría de los detalles técnicos internos por razones de seguridad operativa (ver sección de Limitaciones más adelante). Lo descrito en esta sección es la metodología estándar que se aplicaría siguiendo el marco de NIST SP 800-86, ISO/IEC 27037 y las reglas FRE 902(13)-(14), no un procedimiento confirmado públicamente por Binance para este caso puntual.

Análisis forense posterior

Metodología: forense de blockchain

El análisis forense en este caso fue esencialmente forense de blockchain (no forense clásico de disco o memoria), ya que la evidencia central era pública y trazable en la cadena de Bitcoin. Chainalysis recomendó como buenas prácticas ante hackeos de este tipo: usar software de investigación blockchain para rastrear el flujo de fondos en tiempo real, mantener transparencia para que la comunidad pueda colaborar, y publicar las direcciones usadas por los atacantes para que otros exchanges puedan bloquear conversiones.

Fase 1 — Dispersión inicial

Tras el robo, los fondos se movieron desde el wallet del atacante hacia un conjunto de direcciones intermedias, un patrón típico para dificultar el clustering automático de direcciones por parte de los analistas.

Fase 2 — Lavado a través del mixer ChipMixer

La firma forense Clain documentó en detalle cómo, a partir del 12 de junio de 2019, los atacantes comenzaron a enviar los fondos robados al mixer de Bitcoin ChipMixer. Hallazgos clave de ese análisis:

- Se identificaron alrededor de 150 clusters en los que se agregaron 10 BTC o más durante el período activo de lavado, con un total estimado superior a 5,300 BTC circulando por esos clusters.

- Al menos 4,836 BTC del total robado fueron lavados a través de ChipMixer; otras fuentes sitúan la cifra en un rango similar, de aproximadamente 5,000 bitcoins del total sustraído.
- 183 BTC fueron identificados como fondos de los hackers ya lavados, y otros 814 BTC como fondos pendientes de iniciar el proceso de lavado.
- **Técnica de detección:** los investigadores correlacionaron direcciones de entrada y salida del mixer, partiendo de la premisa de que el atacante necesitaría fusionar ("merge") periódicamente los fondos fragmentados para poder controlarlos efectivamente; ese patrón de fusión fue lo que permitió reconstruir los clusters.
- Los investigadores concluyeron que, dado el volumen anómalo de fondos ingresados, era razonable asumir que cualquier salida de fondos desde ChipMixer en ese período estaba relacionada con el mismo propietario (los atacantes).

Fase 3 — Resultado del rastreo

- Se detectaron al menos 6.4634 BTC adicionales enviados específicamente a direcciones de otros mixers, aparte de las cifras principales ya mencionadas.
- Dado que muchos exchanges pequeños operan en jurisdicciones no reguladas, los analistas concluyeron que era probable que los fondos lograran convertirse a moneda fiat u otras criptomonedas más difíciles de rastrear, como Monero o Zcash.
- **Sin atribución pública:** a diferencia de otros casos (como el hackeo de Bitfinex de 2016, donde hubo arrestos años después), en el caso Binance 2019 no hubo atribución oficial ni detenciones confirmadas; el rastro se pierde progresivamente en el mixer y en exchanges de bajo cumplimiento KYC.

Limitaciones del análisis forense en este tipo de casos

- Los mixers rompen la trazabilidad determinística: agrupan fondos de múltiples usuarios y solo permiten inferencia estadística/heurística (clustering), no prueba criptográfica directa.
- La atribución depende en gran medida de errores operativos del atacante (reutilización de direcciones, fusión de fondos, retiro hacia exchanges con KYC) la misma lógica que permitió, años después, resolver otros grandes robos de criptomonedas.
- **Discreción operativa de Binance:** CZ explicó públicamente que no podía compartir demasiados detalles técnicos porque los hackers estaban "leyendo cada palabra que publicamos y viendo cada AMA", y que compartir demasiada información de seguridad debilitaba la estrategia de respuesta de la empresa.

Versión interactiva de este informe

Este documento también está disponible como sitio interactivo, con navegación por secciones, gráficos y tablas ordenables.

Enlace aquí - Caso Binance Hack 2019