I. DATOS GENERALES:

Clase de alerta: Ransomware
Tipo de Incidente: Robo de información y amenaza de filtración
Nivel de riesgo: Alta

II. ALERTA

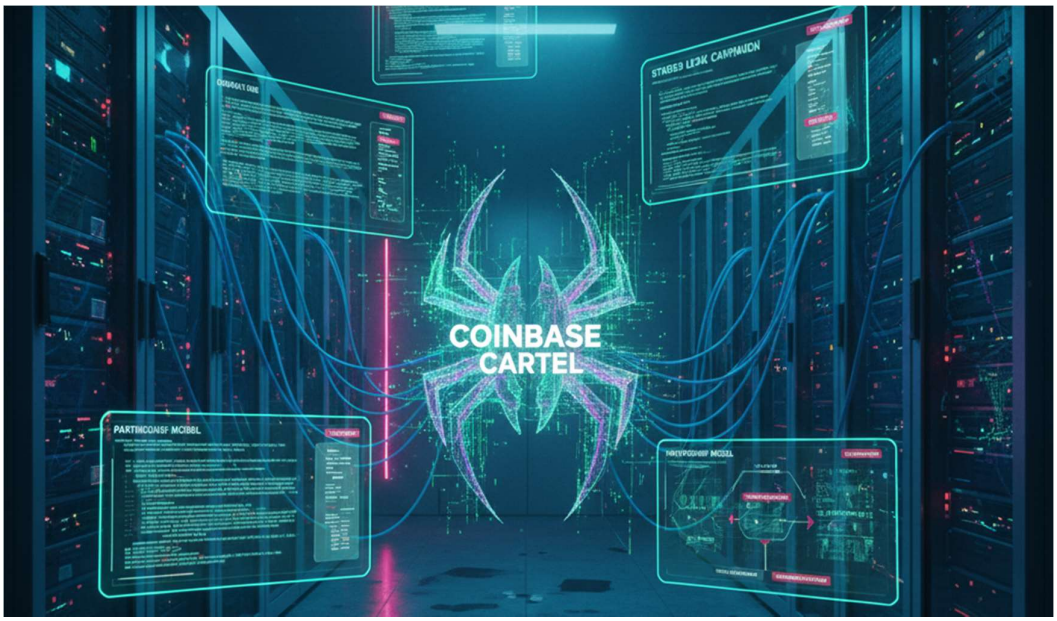

Figura 1.- Coinbase Cartel Ransomware - Figura referencial

En septiembre de 2025 se observó un nuevo actor de amenaza llamado Coinbase Cartel Ransonware, lo que destaca de este nuevo grupo es que no emplea el doble modelo de extorsión que es el cifrado y exfiltración de datos, tampoco opera bajo la modalidad de servicio (RaaS), lo que lo vuelve un actor de amenaza sigiloso dedicado a la ciber-extorsión y robo de datos con la amenaza de publicación en su sitio dedicado a filtración (DLS - Dedicated Leak Site) en la Dark Web.

III. INTRODUCCIÓN

Coinbase Cartel Ransomware es un grupo de ciber-extorsión dedicado únicamente al robo de datos, a diferencia de otros actores de amenaza de ransomware conocidos que utilizan el doble modelo de extorsión como el cifrado/bloqueo de archivos del host de la víctima y la exfiltración de datos de importancia, el grupo se centra en el robo de

datos a gran escala sin comprometer la accesibilidad de los sistemas volviéndolo un ataque más rápido, silencioso y difícil de detectar.

Tras la filtración de datos de las víctimas, Coinbase Cartel Ransomware publica los nombres de las organizaciones afectadas en su sitio web de filtración de datos (DLS) en la dark web y comienza a exigir pagos mediante Bitcoin, estas divulgaciones son escalonadas y tienen el fin de presionar a sus víctimas quienes, dispondrán de 48 horas para responder a través del chat de grupo y una vez establecido el contacto, la víctima tiene 10 días para realizar el pago o solicitar modificaciones al rescate.

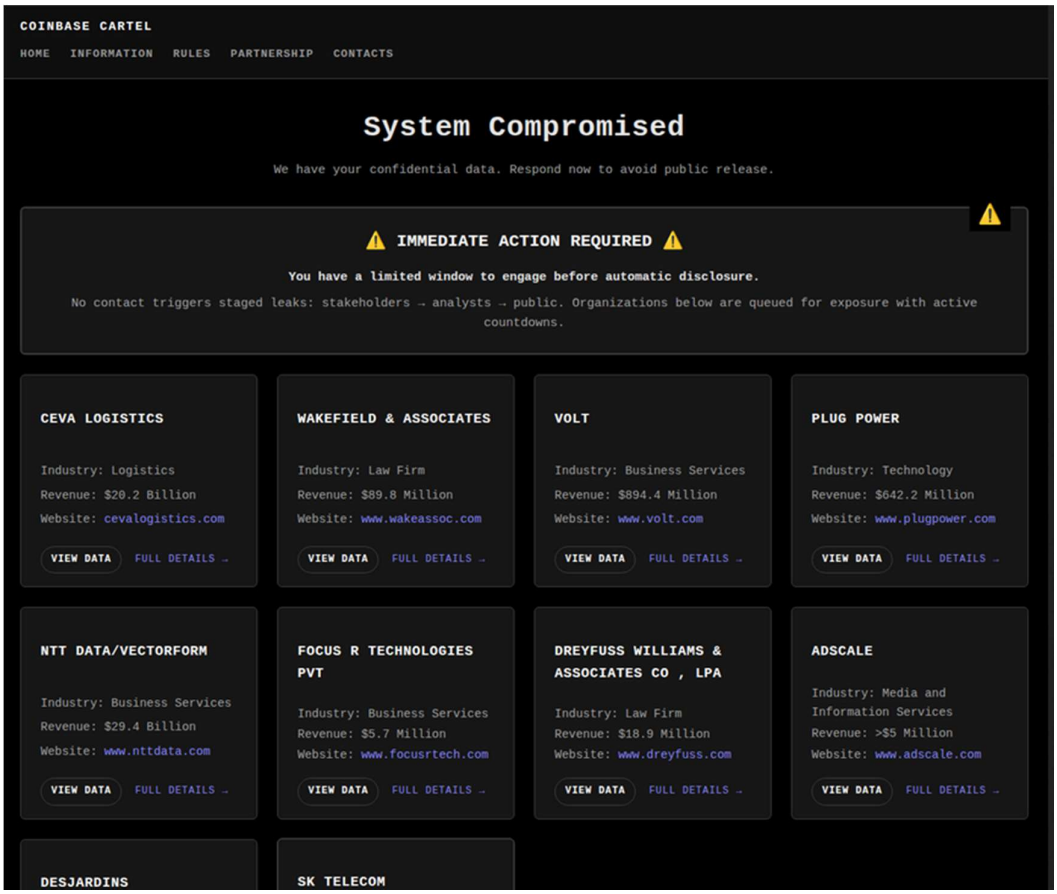

Figura 2.- Sitio de filtración de datos (DLS) - Coinbase Cartel Ransomware

En su sitio web registra ataques a organizaciones de los sectores de logística, banca, telecomunicaciones, tecnología, bufetes de abogados y servicios empresariales, con víctimas confirmadas en Corea del Sur, Canadá, Israel, Estados Unidos, Japón, Ecuador y Europa.

Coinbase Cartel Ransomware no cuenta con una red afiliados, no funciona bajo el modelo tradicional de RaaS que suelen integrar otros actores de amenazas con la re-partición de ganancias para poder usar su malware y parece no contar con especialistas internos en seguridad ofensiva ni con desarrolladores líderes para sus operaciones, sin embargo, demuestra una impresionante astucia empresarial al reclutar a otros ciberciminales, obteniendo así el personal y las herramientas necesarias para convertir vulnerabilidades en exploits. Como ocurrió al inicio de sus actividades, en el cual acudió a una comunidad clandestina en busca de servicios de desarrollo de exploits, anunciando su necesidad de exploits de 0-day con un presupuesto flexible que superaba los 2 millones de dólares. Coinbase Cartel Ransomware está abierto a la cooperación con demás actores de amenazas si cumplen ciertos requisitos, como la presentación de una propuesta con pruebas sólidas que respalden una intrusión exitosa, los solicitantes que cumplan estos requisitos se les asigna una canal de comunicación a través de un chat cifrado y privado.

Figura 3.- Requisitos para solicitar la colaboración - Coinbase Cartel Ransomware

Diversos analistas estiman que el grupo podría estar compuesto por afiliados de ShinyHunters, Scattered Spider y Lapsus$ y se cree que están desarrollando un ransomware dirigido a ESXi, lo que sugiere un posible cambio hacia la doble extorsión en el futuro.

IV. VECTOR DE ATAQUE

Coinbase Cartel Ransomware destaca por el uso de varios mecanismos para obtener acceso inicial a un sistema, entre los que se incluyen vías tradicionales como la ingeniería social, la ayuda de intermediarios de acceso inicial y la obtención de credenciales expuestas.

Luego el grupo dispone de cuentas de administrador y herramientas que puede utilizar para manipular la configuración de todo el sistema, alterar los archivos de registro con el fin de reducir las posibilidades de detección y sustraer datos de interés.

V. IMPACTO

- Windows OS
- Distribuciones Linux

VI. INDICADORES DE COMPROMISO

Sitio web dedicado a filtración DLS
fjg4zi4opkxkvdz7mvwp7h6goe4tcby3hhkrz43pht4j3vakhy75znyd[.]onion

Tabla 1.- Sitio web dedicado a filtración - Coinbase Cartel Ransomware

VII. RECOMENDACIONES:

- Aplicar una gestión estricta de la rotación de credenciales y del acceso junto con la activación de la autenticación multifactor (MFA)
- Proteger los entornos y repositorios en la nube contra la exposición de claves.
- Adoptar un proceso para verificar y aplicar parches periódicamente y de manera oportuna puede marcar la diferencia entre un ataque exitoso y un intento fallido.
- Para garantizar que los datos se conserven en su estado original, programa y prueba copias de seguridad y guárdalas en una ubicación segura, por ejemplo, un repositorio en la nube o un medio externo al servidor principal.
- Supervisar las transferencias de datos salientes inusuales y los archivos de datos almacenados temporalmente.
- Se recomienda encarecidamente implementar controles para restringir y auditar el acceso a los datos fuera de las ubicaciones seguras.
- Implementar controles de supervisión de amenazas internas y de segmentación.
- Llevar a cabo actividades periódicas de detección proactiva de amenazas alineadas con las técnicas del marco MITRE ATT&CK.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

FORTIGUARD LABS (2026). Coinbase Cartel Ransomware. https://www.fortiguard.com/threat-actor/6386/coinbase-cartel-ransomware

BITDEFENDER (2026). No Encryptors, No Problem: The Coinbase Cartel Ransomware Group. https://www.bitdefender.com/en-us/blog/businessinsights/coinbase-cartel-ransomware-group-extortion-tactics

CYBERNEWS (2026). SK Telecom Hackers "CoinbaseCartel" Threaten to Leak Source Code. https://cybernews.com/news/sk-telecom-hackers-coinbasecartel-threaten-to-leak-source-code/

JOE SHENOUDA (2026). New Threat Actor: Coinbase Cartel. https://www.linkedin.com/pulse/new-threat-actor-coinbase-cartel-joe-shenouda-m2lue