No Encryptors, No Problem: The Coinbase Cartel Ransomware Group

By Jade Brown

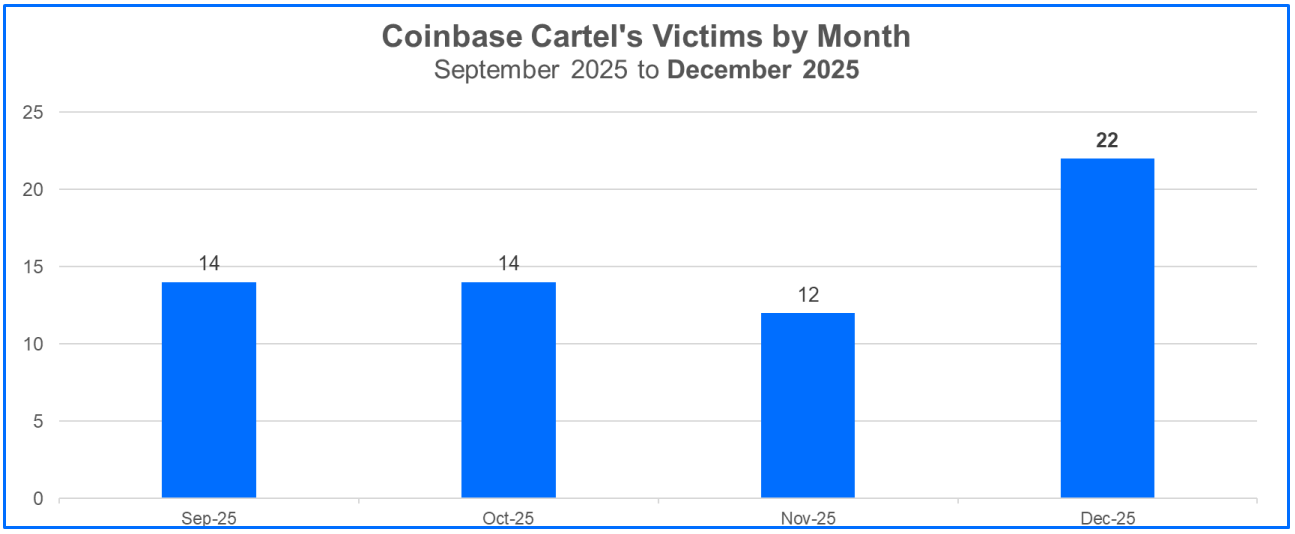
Published: 2026-02-09 · Archived: 2026-04-17 02:00:17 UTC

The ransomware threat actor Coinbase Cartel first emerged in September 2025 and claimed 14 victims that month. The group focuses on data exfiltration, which aligns with a trend Bitdefender is tracking in the ongoing evolution of ransomware.

Currently, the most prolific double-extortion groups, and even emerging single-extortion groups, are increasingly executing data exfiltration-focused ransomware campaigns without encrypting data during attacks.

This approach makes the attacks both quieter and faster to execute while maintaining leverage for a ransom payment: *pay to get your stolen data back, or we'll publish it for the world to see.*

Coinbase Cartel is not only part of this trend but also ranked among Bitdefender's Top 10 Ransomware Groups in September and December 2025, claiming more than 60 victims during its first few months of operation.



Coinbase Cartel Operations and Victim Demographics

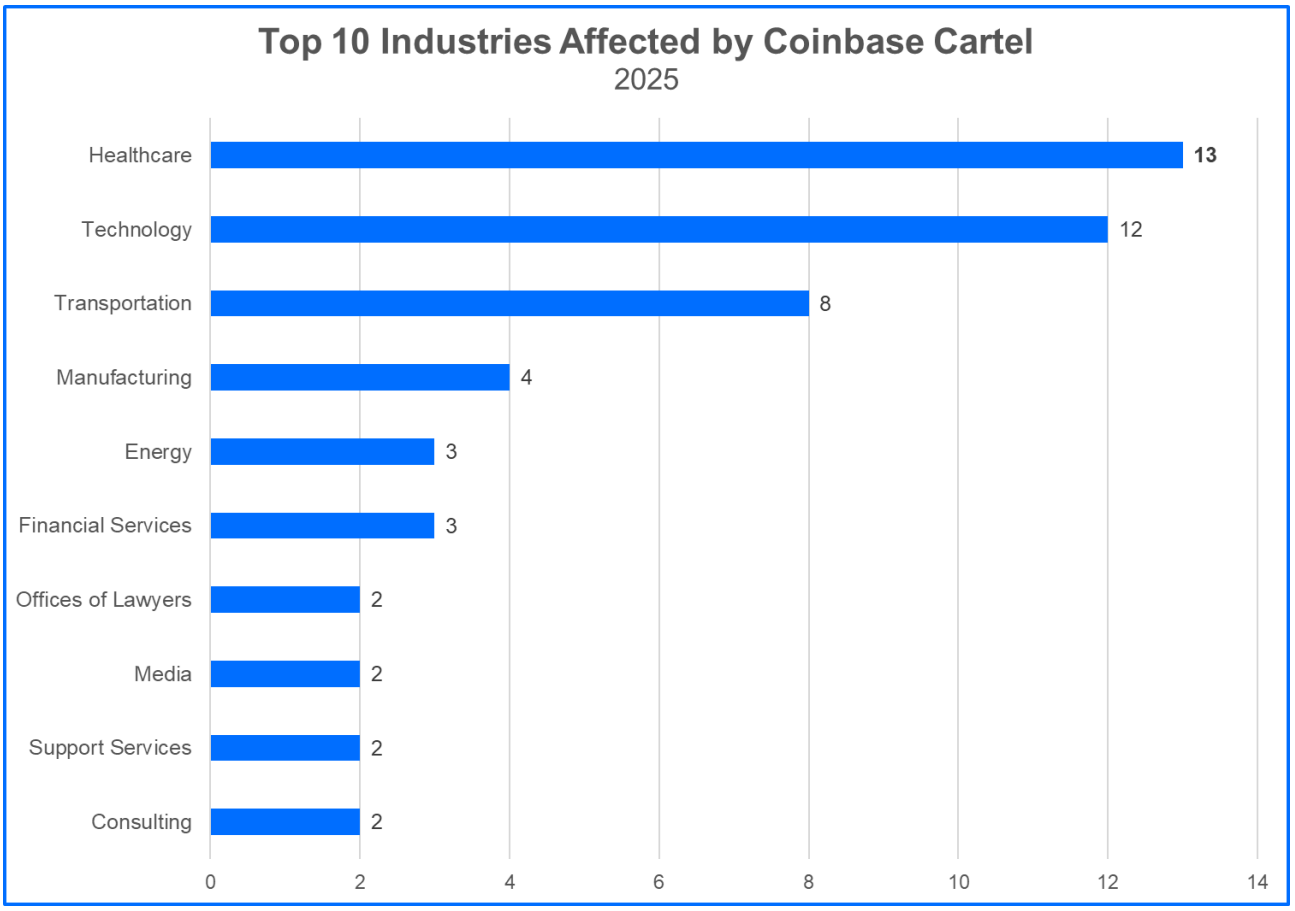
Coinbase Cartel operations are marked by an insistence on stealing data while leaving systems available rather than complementing data theft with the use of encryptors that prohibit system access. Coinbase Cartel's recent activity sparked speculation about their motivations and potential alliances.

Commonalities with other ransomware groups include staging data leaks and targeting organizations in sectors with higher profit margins. The group targets organizations with revenue ranging from millions to several hundred billion dollars. The healthcare, technology, and transportation industries represent Coinbase Cartel's greatest

victim demographic to date. Combined, these industries accounted for more than 50% of the group's victims in 2025.

Interestingly, the healthcare organizations impacted by Coinbase Cartel breaches were primarily based in the United Arab Emirates. Both the reputational damage to healthcare environments, combined with the sensitive nature of PII and PHI data (which contain ample information to perpetrate identity fraud), make healthcare organizations viable targets for extortionist groups.

However, breaching 10 healthcare organizations in the United Arab Emirates in a single month is unusual. This raises questions about motive. Is Coinbase Cartel motivated primarily by financial gain or are other geopolitical considerations in play, such as disrupting the economy of the UAE at large?



Essential Mechanisms for Compromise

Coinbase Cartel leverages several mechanisms to gain initial access to a system, including traditional avenues such as social engineering, support from Initial Access Brokers, and the acquisition of exposed credentials. The ransomware group is then equipped with admin accounts and tools it can use to manipulate systemwide settings, tamper with log files to reduce the odds of detection, and exfiltrate data of interest.

After victim data is exfiltrated, Coinbase Cartel publishes the names of victim organizations on its data leak site and begins issuing ransom demands. Victims are contacted and have 48 hours to respond via Coinbase Cartel's designated chat interface. Once contact with the victim is established, the victim has 10 days to submit payment or request changes to the ransom demand. The victim must submit payment via Bitcoin.

The Data Leak Site

Coinbase Cartel's data leak site features multiple webpages, including HOME, the newly added AUCTIONS page, PARTNERSHIPS, and CONTACTS. From the home page, visitors can view featured victim blog posts, including the active, leaking, and leaked statuses associated with each victim disclosure. The AUCTIONS webpage appears to be a pending initiative; no auctions have been added.

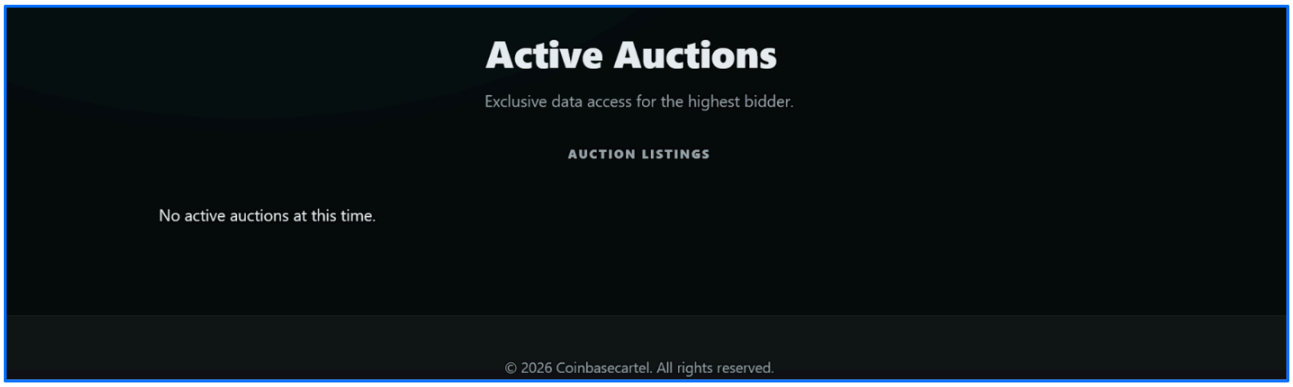


Figure 1: Auctions page on Coinbase Cartel Data Leak Site

Coinbase Cartel maintains that they are a ransomware group that is "redefining data extortion."

Figure 2: Coinbase Cartel branding that claims they are redefining data extortion.

Coinbase Cartel operates without using the RaaS model, which raises many questions about how they collaborate with other cybercriminals. The threat actor previously promoted their brand in other dark web communities, going so far as to market the sale of stolen data. This makes their recent addition of an auction site expected; it is not a significant departure from their initial correspondence and objectives.

Other groups in the past year, including FunkSec, have implemented a similar strategy for auctioning stolen data to increase their earnings. By design, it is a practical approach for ransomware groups that claim a steady volume of victims and have the means to thrive. However, it does not "redefine" the current expectations and trends that have been observed across cybercrime forums.

Coinbase Cartel Partnerships

It is important to note that while Coinbase Cartel may not have in-house offensive security specialists and developers at the forefront of their operations, they have the business acumen to recruit other cybercriminals, seeking the personnel (and tools) vital for weaponization.

One example occurred last fall, when Coinbase Cartel requested exploitation development services in an underground community, announcing a business need for zero-day exploits and a flexible budget exceeding $2 million.

When it comes to Coinbase Cartel's connection(s) to other ransomware groups, things are still murky. In October 2025, several security firms reported hypotheses suggesting that Coinbase Cartel was a potential offshoot of ShinyHunters. The exact connection beyond contacts or infrastructure has not yet been validated.

Coinbase Cartel is open to cooperation with others if collaborators meet certain requirements. Groups interested in partnering with the threat actor must submit a proposal with evidence that supports a successful compromise. Additional correspondence in the review process is then sent via the Coinbase Cartel chat channel.

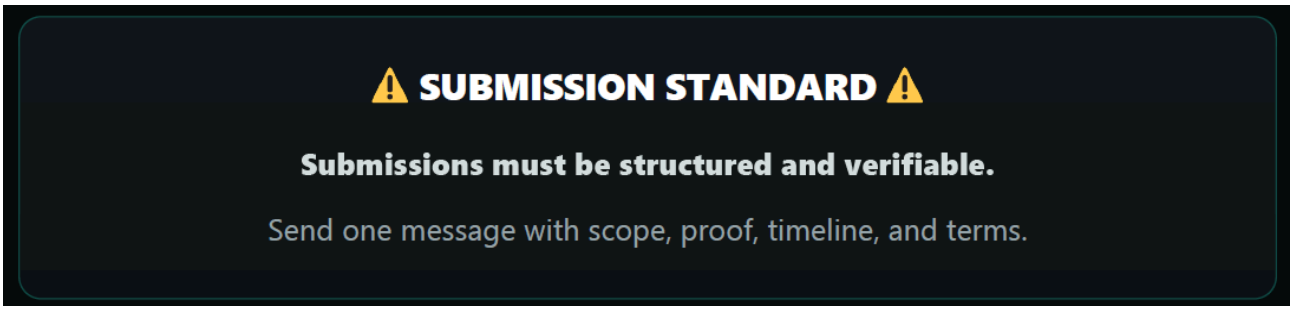


Figure 3: Coinbase Cartel partnership submission requirements

Partnership payment terms and conditions are unclear. However, according to Coinbase Cartel, payment arrangements are not as restrictive in nature as those defined by other groups. There are "options…including fixed-rate agreements or revenue-sharing models based on the nature and value of the collaboration."

Is Coinbase Cartel a True Cartel?

A "cartel" refers to a criminal group that exerts their perceived influence and power to intimidate or force other competing entities to limit their growth and submit to them. Currently, there is no evidence to support the notion that Coinbase Cartel is operating under a framework to reflect that of a cartel.

This is due to the fact that a cartel model of behavior, applying a level of sustained control and/or intimidation, has not yet been identified that matches the tactics that have been observed with other groups such as DragonForce. DragonForce was unique as they were among the first ransomware groups to diverge from the traditional RaaS model and assume the title of "ransomware cartel"; they were also involved in compromising the infrastructure of competing ransomware groups.

How Does Coinbase Cartel Compare to Another Group Focused on Data Theft?

Over the past few quarters, many ransomware groups have organized targeted campaigns against organizations that do not leverage encryptors and instead only issue a ransom demand for stolen data.

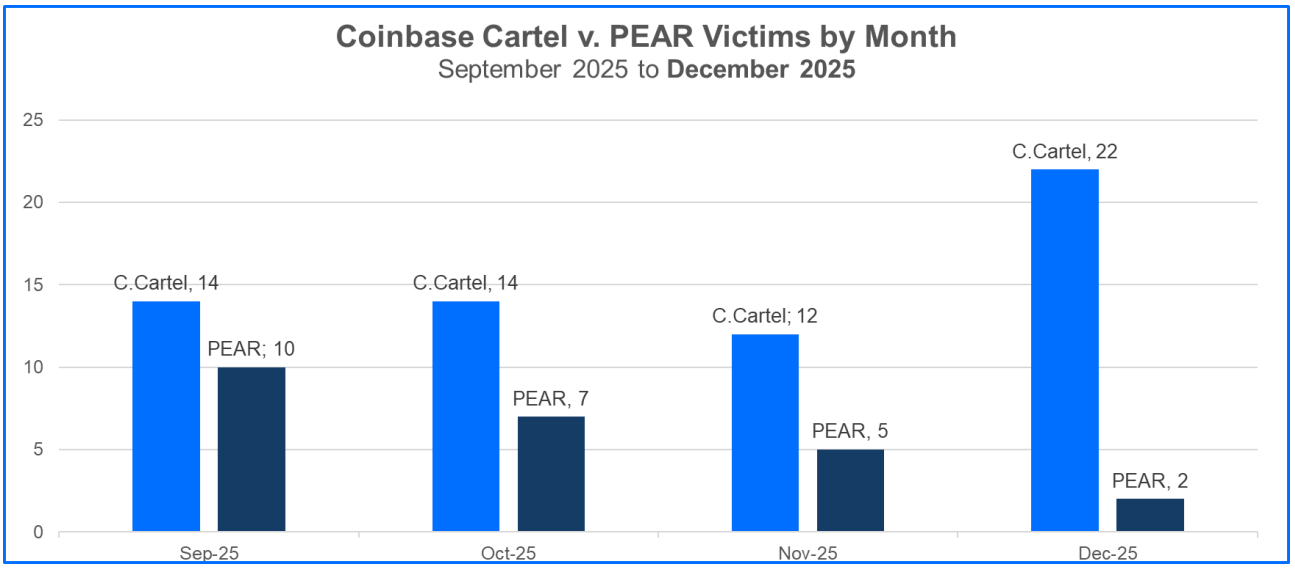
World Leaks is one ransomware group that has toed the line between encryption-based attacks and data theft-only attacks, however PEAR (Pure Extraction and Ransom) is a group that is a more apt comparison with Coinbase Cartel.

Historically, PEAR has avoided using encryptors and focused on data theft to drive ransom demands, much like

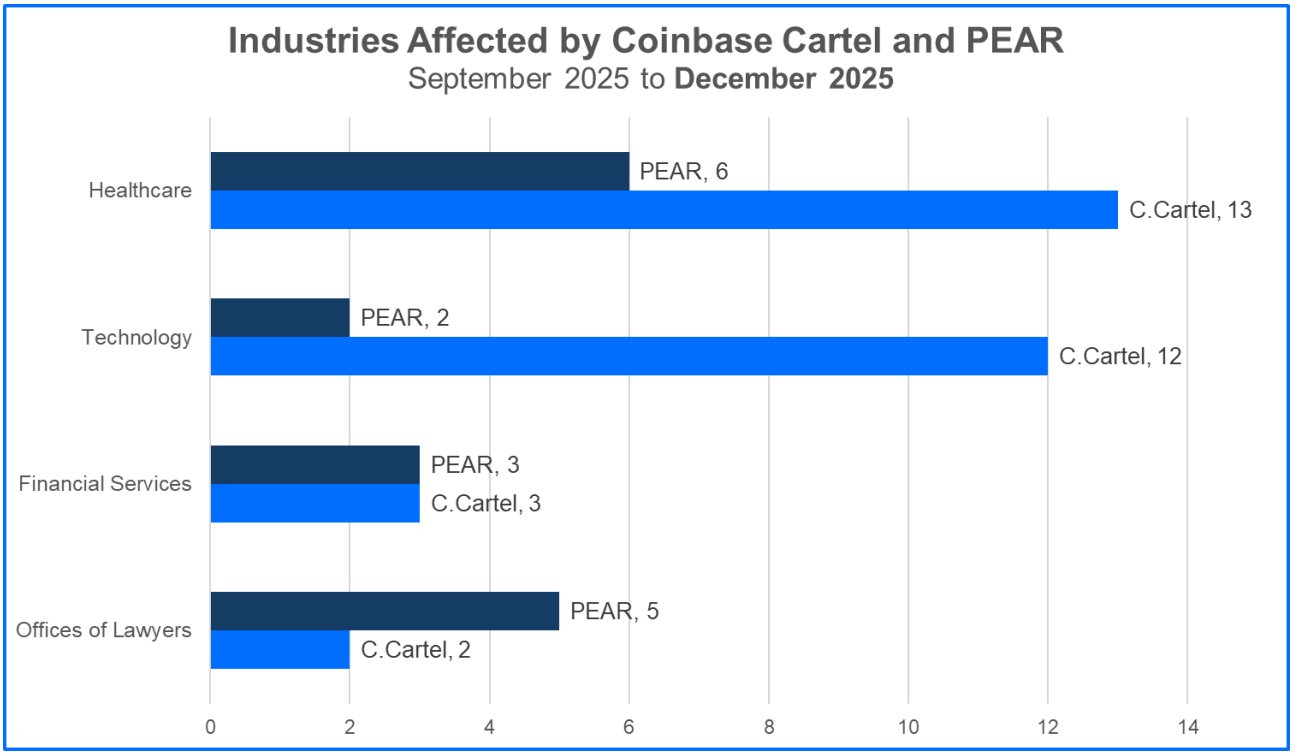
Coinbase Cartel. And PEAR claimed more than 45 victims over the last half of 2025. However, Coinbase Cartel has exceeded PEAR's claimed victims each month since September.

In addition, when looking at the industries impacted by both Coinbase Cartel and PEAR, Coinbase Cartel's breaches have affected a wider range of industries (17 in total compared to PEAR's 13). And, Coinbase Cartel has claimed more victims in high-impact industries such as Healthcare and Technology.

As of early 2026, Coinbase Cartel continues to impact victims in the healthcare and technology industries. Since the rise in reports of their activity in the last few months of 2025, the group has also maintained great stealth and avoided any significant OPSEC (operational security) failures. As a result, published indicators affiliated with their tools and attack methods remain limited. Here is a side-by-side comparison of these two threat actors:



Coinbase Cartel vs. PEAR ransomware victims by month



Coinbase Cartel and PEAR ransomware target victims listed by industry vertical

Recommendations

There are several best practices your organization can follow to minimize attack pathways into your environment and decrease the odds of a successful ransomware attack.

- **Enforce MFA**: MFA should be implemented across all accounts, especially those with administrative privileges. The Principle of Least Privilege (PoLP) should also be strictly enforced, ensuring that no user has more permissions than necessary to fulfill essential job functions.
- **Continuously assess patch management practices**: Unpatched vulnerabilities can leave services and specific software open to attack. Adopting a process to regularly check for and apply patches in a timely manner can be the difference between a successful compromise and an attempted compromise that fails.
- **Regularly schedule backups**: While Coinbase Cartel does not encrypt systems and, therefore, allows business operations to remain intact, it is common for ransomware groups to tamper with or modify critical data. To ensure that data is preserved in its original state, schedule and test backups and store them in a secure location, e.g., a cloud repository and/or external media external to a primary server.
- **Maintain an inventory of critical data**: Listing and charting out an inventory, identifying the types of sensitive data that are handled, in addition to where it is stored and transmitted, is helpful in recognizing areas to secure and potential weaknesses. Enforcing controls to restrict and audit access to data beyond secured locations is highly recommended.
- **Implement a threat intelligence solution**: Context and security awareness both play significant parts in threat intelligence, which informs incident response. Staying up to date on threat actor TTPs and

understanding the patterns associated with ransomware and other attacks allows organizations to save time in building a defensive strategy and responding to future incidents.

- **Implement an MDR plus an attack surface reduction solution**: Time is of the essence when it comes to incident detection, analysis, and response. An MDR service will help you detect and respond to threats based on current indicators. It relieves your internal team of burdens and helps you rapidly implement best practices within your environment. Understanding and dynamically reducing your attack surface is also crucial. This can be accomplished by deploying a solution such as GravityZone PHASR. PHASR monitors your organization's environment and leverages machine learning to establish a baseline of normal activity while assessing and blocking use cases for LOTL (living off the land) attacks, and other ransomware playbook tactics that are now used in a majority of high-severity attacks and may go undetected by traditional tools.

Tracking Ransomware Developments

Coinbase Cartel is part of a growing number of ransomware groups focused on data exfiltration without encryption, and Bitdefender will continue to track developments with this threat actor. We also track and report on changes throughout the ransomware threat landscape in our monthly Bitdefender Threat Debrief.

Source: https://businessinsights.bitdefender.com/coinbase-cartel-ransomware-group-extortion-tactics