Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

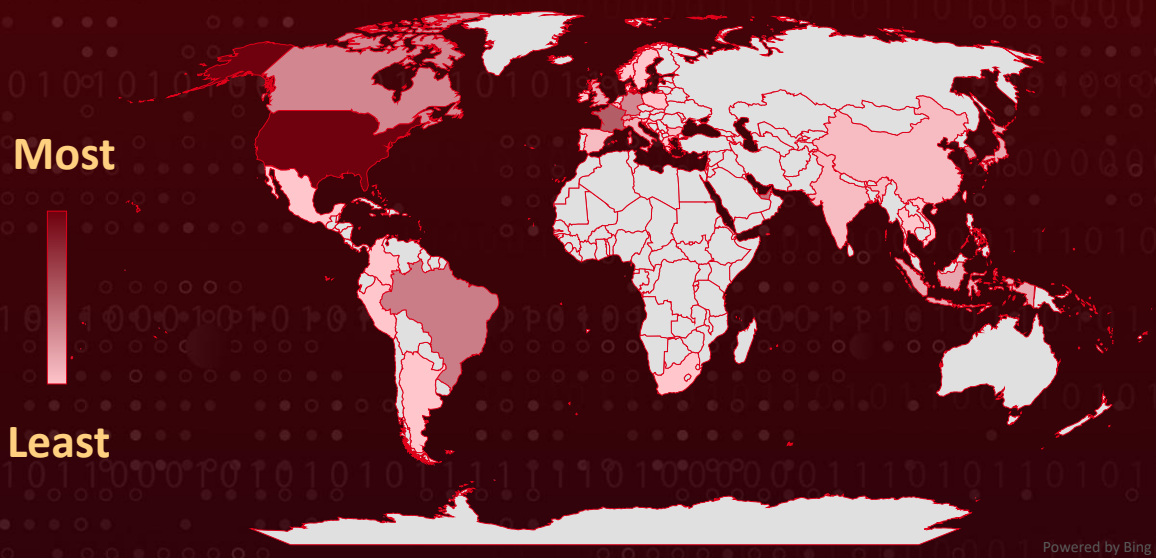
Coinbase Cartel: The Encryption-Free Data Extortion Group

Date of Publication	Admiralty Code	TA Number
July 10, 2026	A2	TA2026194

Summary

First Seen: September 2025
Targeted Regions: United States, France, United Arab Emirates, Brazil, Canada, Germany, South Korea, Switzerland, United Kingdom, Indonesia, Japan, Italy, Spain, Belgium, India, Taiwan, China, Bulgaria, Vietnam, Thailand, Croatia, Norway, Colombia, Denmark, Sweden, Ireland, Argentina, Slovenia, Mexico, South Africa, Peru, Greece, Poland, Malta
Targeted Platforms: Windows, Linux, VMware ESXi (projected), cloud SaaS environments
Targeted Industries: Technology, Manufacturing, Business Services & Consulting, Real Estate, Transportation, Retail, Financial Services, Healthcare, Telecommunications, Legal, Energy, Pharmaceutical, Casino & Gambling, Education, Media, Agriculture, Aviation, Food Service, Hospitality, Aerospace and Defense, Government
Threat Actor: Coinbase Cartel (aka shinysp1d3r); assessed as part of the Scattered Lapsus$ Hunters (SLSH) collective
Attack: Coinbase Cartel is a financially motivated, data-theft-only extortion group active since September 2025 with over 160 claimed victims globally, assessed as an affiliate operation within the Scattered Lapsus$ Hunters (SLSH) collective spanning ShinyHunters, Scattered Spider, and Lapsus$. The group avoids encryption entirely, relying on legitimate credentials sourced from commodity infostealer logs, with approximately 80% of victims showing prior infostealer exposure, to exfiltrate data and pressure victims via a Tor-based leak site with 48-hour contact and 10-day Bitcoin payment windows. Impacted sectors concentrate in technology, transportation, manufacturing, and business services, making behavioral detection, enforced MFA, infostealer credential monitoring, and OAuth governance the highest-leverage defenses.

Attack Regions



Attack Details

#1 Coinbase Cartel is a financially motivated data-theft-only extortion group that first surfaced in September 2025 and has since claimed over 160 victim organizations across five continents. Despite the branding, the group has no affiliation with the legitimate cryptocurrency exchange, and multiple analysts assess it to consist of affiliates drawn from the ShinyHunters, Scattered Spider, and Lapsus$ ecosystem, collectively referred to as the Scattered Lapsus$ Hunters (SLSH) collective. The SLSH linkage is assessed on the basis of overlapping TTPs, shared affiliate pools, and shared infrastructure.

#2 The group's distinguishing characteristic is the absence of encryption. Operations are exfiltration-only: sensitive data is stolen and staged for publication on a Tor-based data leak site unless a Bitcoin ransom is paid. Victims are given 48 hours to establish contact through a designated chat interface and a subsequent 10-day window to pay or negotiate, with an AUCTIONS page recently added to allow third-party bidding on stolen datasets before the timer expires. This model extends dwell time and removes backup-based recovery as a defense.

#3 Initial access relies almost entirely on legitimate credentials rather than zero-days or custom malware. The primary vector is credentials sourced from commodity infostealer malware logs traded through dark web markets and Telegram channels; cross-referenced analysis identified that approximately 80% of confirmed victim organizations had documented prior infostealer exposures, in some cases years before the intrusion. The group supplements this with social engineering, exposed credentials in cloud repositories, and initial access broker sourcing, and it solicits collaboration through a PARTNERSHIPS intake channel targeted at individuals with access to corporate systems. In October 2025, the operators publicly advertised a budget exceeding USD 2 million for zero-day exploits.

#4 Post-access activity is documented at a coarser level of granularity than for many peer groups. Sources directly attribute administrative account abuse, systemwide configuration manipulation, log tampering to reduce detection, and staged data exfiltration to Coinbase Cartel operations. Finer-grained tradecraft, vCenter API discovery, SSH across ESXi hypervisors, RDP or PsExec lateral movement, and Salesforce Data Loader mimicry via custom Python scripts, is reported as tradecraft associated with the broader SLSH cluster and is assessed as consistent with Coinbase Cartel operations under a shared-playbook hypothesis rather than as directly observed activity.

#5 Targeted sectors concentrate in technology, transportation, manufacturing, and business services, with notable clusters in the United States, UAE, Germany, France, and Brazil. Detection must be behavioral rather than signature-based, and the highest-leverage defenses are enforced MFA, infostealer credential monitoring, OAuth application governance, and ESXi hardening.

Recommendations

Enforce MFA Across All Remote Access and SaaS Entry Points: Make multi-factor authentication mandatory (not optional) across VPN concentrators, RDP-facing hosts, SaaS application portals, administrative consoles, and any account with elevated privileges. Given that credential compromise is the group's dominant access vector, MFA should be treated as a system-enforced control rather than a user preference.

Deploy Infostealer Credential Exposure Monitoring: Subscribe to threat intelligence services that continuously index infostealer dump datasets (such as Hudson Rock's Cavalier database) and alert when organizational domains, email addresses, or SSO tokens appear in leaked logs. With approximately 80% of confirmed victims exhibiting prior documented credential exposure, this is a direct early-warning control against Coinbase Cartel's primary access pattern.

Audit and Restrict OAuth Application Permissions: Review every OAuth application authorized to connect to Microsoft 365, Google Workspace, Salesforce, and other SaaS tenants; remove unused or unrecognized grants, enforce administrator approval before new OAuth applications can be connected, and set token lifetimes as short as operationally feasible to limit vishing-driven persistence.

Harden VMware ESXi and vCenter Infrastructure: Disable SSH on ESXi hosts by default and enable it only for maintenance windows; forward ESXi logs to a secured, external syslog server that cannot be silenced by a local operator; implement snapshot and datastore protection policies that block unauthorized disablement; and restrict vCenter API access to a defined administrative subnet.

Implement Identity Threat Detection and Response (ITDR): Deploy a dedicated identity-layer control that establishes behavioral baselines for authentication events and flags deviations such as impossible-travel logins, new device fingerprints, access from Tor or commercial VPN egress ranges, and privilege-escalation anomalies that signature-based detection will not catch.

Monitor for Data Exfiltration Behavior: Establish DLP and egress monitoring rules that flag sustained outbound transfers to cloud storage services with no established business relationship, high-volume CRM or Salesforce Data Loader-style API exports, and large compressed archive creation on file servers outside normal working hours.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
	T1199: Trusted Relationship	
	T1566: Phishing	T1566.004: Spearphishing Voice
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1136: Create Account	
	T1528: Steal Application Access Token	
Privilege Escalation	T1078: Valid Accounts	T1078.004: Cloud Accounts
Credential Access	T1003: OS Credential Dumping	
Defense Evasion	T1070: Indicator Removal	
	T1562: Impair Defenses	
	T1090: Proxy	T1090.003: Multi-hop Proxy

Tactic	Technique	Sub-technique
Discovery	T1580: Cloud Infrastructure Discovery	
Lateral Movement	T1021: Remote Services	T1021.004: SSH
		T1021.001: Remote Desktop Protocol
Collection	T1213: Data from Information Repositories	
	T1119: Automated Collection	
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
Emails	shinycorp[@]tuta[.]com, shinygroup[@]tuta[.]com
Tox ID	1225DDE01980D7C7890A90E359EF4406D74DF7DB94F6C5F3B8378BB78444473022675C49FACB
TOR Address	fjg4zi4opkxkvdz7mvwp7h6goe4tcby3hhkrz43pht4j3vakhy75znyd[.]onion

Recent Breaches

https://www.pragmatic.solutions
https://www.openmindnetworks.com
https://www.cognizant.com
https://www.panasonic.aero
https://www.cmtelematics.com
https://www.demand.io
https://www.zywave.com
https://www.grafana.com
https://www.alpinion.com
https://www.ijs.si
https://www.tabservice.com
https://www.cassinfo.com

References

https://www.fortiguard.com/threat-actor/6386/coinbase-cartel-ransomware

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/coinbase-cartel

https://www.ecucert.gob.ec/wp-content/uploads/2026/05/AI-2026-022-Coinbase-Cartel-Ransomware.pdf

https://www.halcyon.ai/threat-group/coinbasecartel

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 10, 2026 • 07:30 AM

More at www.hivepro.com