Chaos Ransomware Profile: Tactics, Targets, and Technical Indicators

By Emma Stevens

Published: 2026-11-24 · Archived: 2026-11-26 02:00:36 UTC



Active since 2025, Chaos is a financially motivated ransomware-as-a-service (RaaS) group. Bitsight CTI reports that affiliates rely on social engineering and legitimate remote-access tools to compromise target networks. Their extortion model typically combines data theft, system encryption, threats to publish stolen data, and distributed denial-of-service (DDoS) attacks. To date, Chaos has impacted targets across numerous industries and geographic regions.

Tracking from Bitsight CTI reveals claims spanning diverse sectors and countries. The group operates with clear financial motivation and takes an opportunistic approach, singling out organizations that handle sensitive data or whose operational disruption provides maximum extortion leverage.

Because Chaos operates through an affiliate model, individual operators select their own tools and tactics. As a result, behaviors vary significantly between incidents, meaning no single playbook or set of indicators can identify every attack tied to the group. The name “Chaos” is also associated with an older malware botnet that targeted routers and misconfigured Linux cloud environments. However, this shared name does not indicate that the two operations share operators, tooling, or infrastructure.

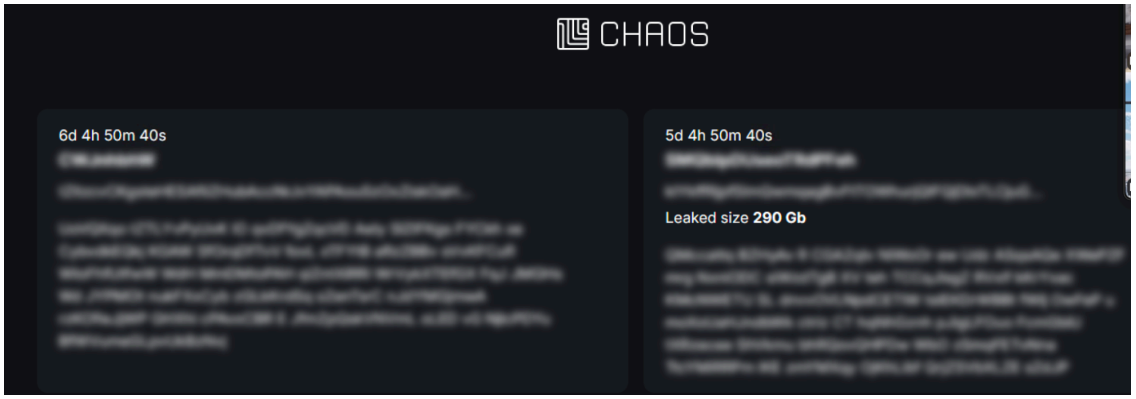


Figure 1: Screenshot from Chaos’s dedicated leak site.

Chaos pairs centralized ransomware infrastructure with affiliate-driven network intrusions. Operators use social engineering and remote-access software to gain initial access, move laterally, exfiltrate data, and deploy ransomware. The group’s multi-layered pressure tactics include:

- Threats to publish stolen data on a leak site
- File encryption that disrupts access to systems and data
- DDoS threats against internet-facing services

Bitsight CTI identified at least ten victim claims on the group's extortion site over a two-month period, primarily targeting U.S.-based entities. Note that these entries reflect the group's public claims and don't independently confirm a successful breach, payload execution, or the scope of exfiltrated data.

Chaos attack lifecycle and techniques

Since affiliates run their own operations, intrusion steps vary from campaign to campaign. The stages below summarize the common techniques observed in Bitsight CTI tracking.

Stage	Reported activity	Defensive telemetry to review
Initial access	Spam and voice-based social engineering; impersonation of IT support	User reports of unusual email volume followed by unsolicited calls; remote-assistance sessions initiated after contact with an unknown person
Remote access	Abuse of legitimate remote-access and RMM tools	New tool installations, new remote sessions, unexpected remote administrators, and activity outside approved support hours
Persistence and lateral movement	Continued use of RMM tools to retain access and move through the environment	RMM activity across multiple endpoints, unexpected connections between workstations and servers, and changes to accounts used for remote administration
Command and control	Use of custom remote-access tooling and C2 channels is reported, but no validated infrastructure details were provided	Unusual outbound connections from affected hosts, especially when paired with new remote-access tooling or abnormal account activity
Data theft	Exfiltration before encryption	Large or unusual outbound transfers, unexpected use of cloud storage or file-transfer services, and bulk access to sensitive file shares

Impact and extortion	File encryption, leak-site threats, and reported DDoS threats	Rapid changes to many files, loss of access to business systems, public-facing service disruption, and extortion communications

Initial access: Social engineering and remote support

Bitsight CTI highlights spam campaigns and voice phishing (vishing) among the group's primary entry vectors. In IT-support impersonation schemes, attackers often trigger a wave of spam or invent an urgent IT scenario to prompt an employee to initiate contact. They then trick the target into downloading or granting permission for remote-access software. This tactic abuses software that helpdesks regularly use.

Consequently, the presence of remote software alone isn't a clear threat indicator. Security teams should verify who authorized the software, how the session was launched, the user account involved, which systems were accessed, and whether the activity aligns with a valid support request.

Persistence and lateral movement through RMM tools

Bitsight CTI indicates that attackers frequently leverage remote monitoring and management (RMM) platforms for persistence and lateral movement, though specific vendor products are not specified in the current intelligence.

When RMM tools run with elevated privileges or wide network scope, they grant adversaries extensive persistent access across the enterprise. Defenders should inspect installation paths, service creation timestamps, digital signatures, executing accounts, session logs, and destination endpoints. Unsanctioned or unexpected use of standard RMM tools—especially outside regular maintenance windows—should be investigated immediately.

Data exfiltration before encryption

Chaos affiliates generally steal data prior to launching encryption, maintaining leverage even when victims possess clean backups. Because exfiltration tools and destinations vary by affiliate, defenders should focus on detecting anomalous behavior: unusual access to sensitive file shares followed by large outbound network connections. Correlate endpoint activity, file access logs, network proxy and firewall traffic, cloud audit trails, and authentication events. Watch for single accounts opening abnormal volumes of documents, staging files into archives, or transmitting data to unapproved locations.

Encryption and DDoS threats

The group uses ransomware encryption for operational disruption and threatens data exposure if payments are not made. Bitsight CTI tracking also notes DDoS threats as a secondary extortion tactic. A DDoS threat alone does not mean an attack has occurred; verify service metrics and network traffic independently. Organizations must prepare to address concurrent threats: endpoint outages, data exposure risks, and potential disruptions to internet-facing infrastructure. While reliable backups mitigate encryption impact, they do not resolve stolen data or active denial-of-service attempts.

NVD logs CVE-2025-59360 and CVE-2025-59361 as vulnerabilities within Chaos Mesh's Chaos Controller Manager. The shared word "Chaos" between the product and the threat group does not signify any link to the ransomware group.

Type	Indicator
IP	`196.251.107.186`
URL	`http://196.251.107.186/clpr6.exe`
IP	`142.11.210.231`
URL	`http://142.11.210.231/bins/packets.mipe`
URL	`http://91.92.242.236/files-129312398/files/file_583f8856851a870c.exe`
IP	`185.156.73.73`
IP	`185.215.113.209`
SHA-256	`402781973739d057cf3e91d14fce1fb0c12ca95683e2ba43c035ae43314995dd`
SHA-256	`4ab643f49ee2a86c36ba665d7a3e5b91997d1da2840d64a0483d2b477c7ca7e0`
SHA-256	`4b46e7374d148e207d2a4b5d2931b16d0fdce83ece2e05823d211c07ac9eb75d`
SHA-256	`b4fdaf46a9817f828eb7bc29c9319953a9e06fba2bc2325c972bc25d4ed219d5`

Bitsight CTI tracking identifies activity involving the following sectors:

- Manufacturing
- Business services

- Healthcare and wellness
- Engineering
- Technology
- Construction
- Freight and logistics
- Tax preparation

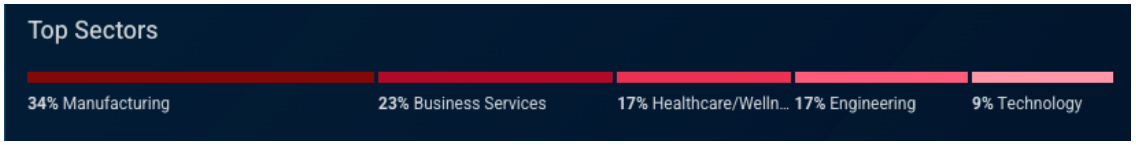


Figure 2: Sector targeting according to Bitsight Threat Intelligence.

The United States represents the most frequent target location in tracking reports, with additional claims across Canada, the United Kingdom, Italy, and Austria. These patterns reflect observed leak-site postings and will evolve over time.

Bitsight CTI tracking notes victim claims involving Carolina Asthma & Allergy Center, Advantech, Park Dental, Astrana Health, and Optima Tax Relief. Unless independently confirmed by the victim organization, these should be treated strictly as group claims.

In the Optima Tax Relief case, Chaos claimed to have exfiltrated 69 GB of data. A filing with the Maine Attorney General confirms a breach affecting 3,114 individuals between May 1 and May 6, 2025. While the regulatory filing verifies the breach occurred, it does not confirm the volume or contents of the claimed stolen data.

1. Protect identity and remote-support workflows

- Require MFA for remote access and privileged accounts.
- Establish a verification process for help-desk requests, password resets, and MFA re-enrollment. Use a trusted, previously recorded contact method to verify sensitive requests.
- Alert on new remote-access tools, unexpected support sessions, new administrator accounts, and unusual account or password changes.
- Review active sessions and revoke tokens or sessions after suspected account compromise.

2. Reduce RMM and third-party risk

- Maintain an inventory of MSPs, RMM products, vendor accounts, and systems with remote access.
- Restrict RMM access to approved devices, named accounts, and documented support windows.
- Segment RMM infrastructure from critical systems and limit which endpoints each vendor can reach.
- Log and review remote sessions, software deployments, scripts, and configuration changes initiated through RMM platforms.
- Include incident notification, access logging, and response responsibilities in MSP agreements.

3. Detect data theft and encryption

- Alert on unusual bulk file access, unexpected file staging, large outbound transfers, and new external destinations.
- Monitor activity involving sensitive repositories, file shares, cloud storage, and backup systems.
- Use endpoint detection and response tools to detect suspicious remote control, security-tool tampering, and rapid changes to files.
- Treat unexplained data staging or outbound movement as a possible pre-ransomware event, even if no encryptor has been detected.

4. Prepare for recovery and extortion

- Maintain offline or immutable backups with credentials separate from the production environment.
- Test restoration of critical systems and data.
- Include data theft, encryption, leak-site claims, and possible DDoS threats in ransomware exercises.
- Define roles for incident response, legal, privacy, communications, executive leadership, and service providers.

Bitsight CTI consolidates intelligence on ransomware groups, threat actors, vulnerabilities, identities, and attack surfaces. Security operations can leverage these insights to track emerging activity, conduct targeted investigations, and enhance threat-hunting programs.

Bitsight's Dynamic Vulnerability Exploit (DVE) Intelligence delivers threat context to help prioritize patching based on real-world exploitation likelihood. Note that DVE insights do not confirm Chaos exploited the specific CVEs discussed in this overview.

Bitsight Identity Intelligence detects exposed corporate credentials across surface, deep, and dark web forums, mapping compromise risk directly to your attack surface to mitigate credential-based intrusions.

If a critical vendor or MSP suffers an incident, Bitsight Beacon delivers verified alerts with actionable threat context and remediation guidance, empowering third-party risk teams to evaluate and manage supply chain exposure.

For further technical details or assistance, contact your Cyber Threat Intelligence team.

Source: https://www.bitsight.com/blog/threat-actor-profile-chaos-ransomware-group