Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 16 - 22, 2025

Report Summary:

- **New Threat Detection Added**
  - TA397/Bitter
  - SantaStealer
  - CastleLoader
  - ZeitLoader

The following threats were added to Crystal Eye this week:

1. SantaStealer

SantaStealer is a relatively new malware that acts as an infostealer. The malware is designed for all kinds of information and data from the infected host. This includes a variety of web data such as credentials, cookies, and finance data. It also searches for applications to install such as Discord, Telegram, and steam to steal sessions and authentication details. SantaStealer is specifically designed to bypass Google Chromes 'App-Bound Encryption'. This is designed to protect login users against credential harvesting.

SantaStealer is sold as part of Malware-as-a-Service (MaaS), allowing it to be used by anyone and distributed in any manner the threat actor chooses.

Threats Protected: 1
Class Type: Malware
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Kill Chain:

Tactic	Technique ID	Technique Name
Collection	T1119	Automated Collection
Exfiltration	T1020	Automated Exfiltration

Current Threat Summary

Known exploited vulnerabilities (Week 3 December 2025)

Vulnerability	CVSS	Description
WatchGuard Firebox	9.4	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to execute arbitrary code. This affects both the Mobile VPN and Office VPN users if the VPN is using IKEv2 (Internet Key Exchange version 2) (This is the protocol that sets up the secure connections for IPsec).
ASUS Live Update	9.3	Certain versions of ASUS Live Updates software contain malicious code due to a supply chain compromise. This software has already reached End-of-Support in October 2021, and no currently supported devices or products are affected by this issue.
SonicWall SMA1000 appliance	6.6	SonicWall SMA1000 contains a missing authorisation vulnerability that could allow for privilege escalation appliance management console (AMC) of affected devices.
Cisco Multiple Products	10	Cisco Secure Email Gateway, Secure Email, AsyncOS Software, and Web Manager appliances contains an improper input validation vulnerability that allows threat actors to execute arbitrary commands with root privileges on the underlying operating system of an affected appliance.
Fortinet Multiple Products	9.8	Fortinet FortiOS, FortiSwitchMaster, FortiProxy, and FortiWeb contain an improper verification of cryptographic signature vulnerability that may allow an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML message.
Gladinet CentreStack and Triofox	7.1	Gladinet CentreStack and TrioFox contain a hardcoded cryptographic keys vulnerability for their implementation of the AES cryptoscheme. This vulnerability degrades security for public exposed endpoints that may make use of it and may offer arbitrary local file inclusion when provided a specially crafted request without authentication.
Apple Multiple Products	8.8	Apple iOS, iPadOS, macOS, watchOS, visionOS, and other Apple products contain a use-after-free vulnerability in WebKit. Processing maliciously crafted web content may lead to memory corruption. This vulnerability could impact HTML parsers that use WebKit, including but not limited to Apple Safari and non-Apple products which rely on WebKit for HTML processing.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-december-2025/627

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. This report provides a detailed analysis of Osiris, a newly emerged ransomware-as-a-service (RaaS) operation that has begun targeting high-value organisations with double extortion tactics.

Ransomware Hits Last Week

Kairos led this week's activity, responsible for 16.6% of all reported incidents. This made it the single most dominant operator in the ecosystem, indicating a focused campaign window or a coordinated disclosure surge that pushed Kairos well ahead of most other groups.

A powerful second tier was formed by Qilin (13.13%), Sinobi (11.58%), and SafePay (7.72%), with Akira (5.02%) close behind. Together, these crews represent a high-volume bloc of operations conducting sustained, multi-industry targeting and regular leak-site publishing, collectively shaping the bulk of visible ransomware pressure for the week.

A mid-tier cluster, DevMan2 (4.25%), DragonForce, PayoutsKing, and LockBit 5 (each 3.47%), along with Play and Inc Ransom (each 3.09%), maintained a steady operational tempo. These groups did not individually match the scale of Kairos or Qilin but, taken together, contributed a significant share of global incidents through ongoing double-extortion and data theft campaigns.

Smaller but persistent operators included Obscura, Minteye, Nova, Worldleaks, and Medusa (each 1.93%), alongside The Gentlemen, Handala, BlackShrantac, Lynx (each 1.16%), and Rhysida, KillSec3, Pear, RansomHouse, Interlock, MS13-089, Anubis, and Everest (each 0.77%). These crews continued to appear at lower volumes but maintained a consistent presence across sectors and regions.

At the long tail, a wide spread of low-frequency brands, Nitrogen, Coinbase Cartel, Space Bears, PayoutsKing's smaller peers, Osiris, Crypto24, Leaknet, Termite, TridentLocker (each 0.39%), each accounted for only a small fraction of total incidents. Individually minor but collectively meaningful, this long-tail activity underscores the fragmentation, churn, and resilience of the broader ransomware ecosystem.

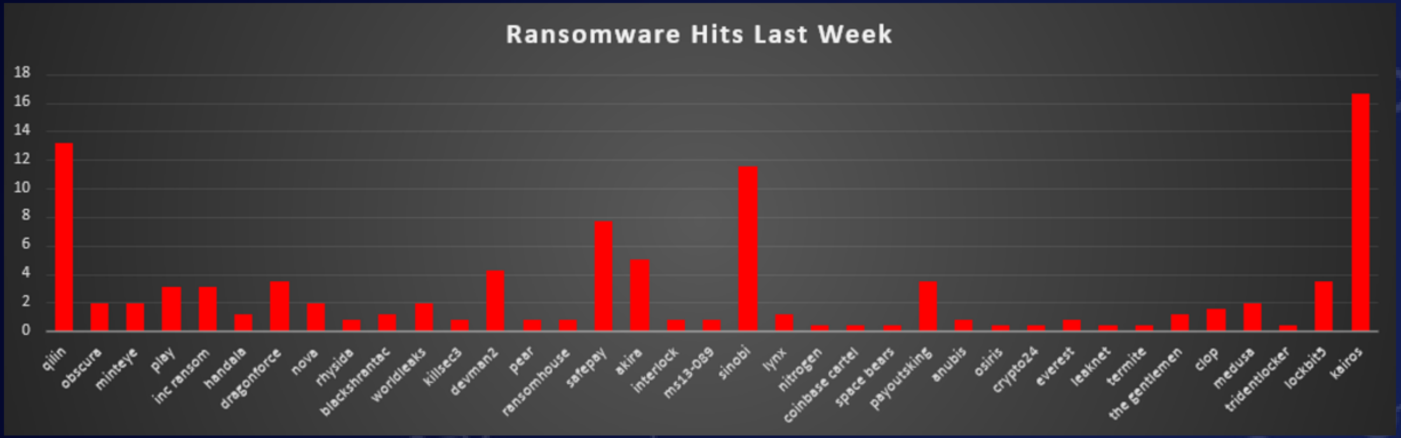


Figure 1: Ransomware Group Hits Last Week

Osiris Ransomware

Osiris is a newly emerged ransomware-as-a-service (RaaS) operation first observed in November 2025. Despite its recent appearance, the group has positioned itself as a sophisticated data broker employing double extortion tactics against high-value corporate targets. The operation shares its name with two unrelated historical threats, the defunct 2016-2017 Locky-Osiris ransomware variant and the Osiris banking trojan but represents an entirely distinct threat actor with modern capabilities. Osiris operates a TOR-hidden leak site accessible at osirisbm3357xrccnid23nlyuqwzbgqheaei6dxvyi34tbkqr3bmvfid[.]onion where the group lists victims and threatens data publication. The leak site features a minimalist design with countdown timers and victim profiles, following established ransomware data broker patterns. As of December 2025, the WatchGuard ransomware tracker lists this operation with an "under construction" status, indicating limited technical intelligence availability.

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. 06 Dec 25 - 12 Dec 25 our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. This report provides a detailed analysis of Osiris, an emerging data extortion group that has rapidly expanded operations targeting healthcare, government, and critical infrastructure sectors.

Detailed Tactics, Techniques, and Procedures (TTPs)

Initial Access
Osiris likely employs multiple initial access vectors common to modern ransomware operations. Based on victim profiles and RaaS operational patterns, probable attack vectors include:

- Valid Accounts & Credential Abuse (T1078) -- Purchasing stolen credentials from infostealer logs or dark web markets; targeting accounts with VPN/RDP access
- External Remote Services (T1133) -- Exploiting exposed RDP, VPN, or remote management interfaces with weak authentication
- Exploit Public-Facing Application (T1190) -- Targeting unpatched web applications, content management systems, or internet-facing services
- Phishing: Spearphishing Attachment (T1566.001) -- Delivering malicious attachments or links via targeted email campaigns

Execution & Persistence
Following successful initial access, Osiris operators likely deploy payload delivery mechanisms and establish persistence for sustained network access:

- Command and Scripting Interpreter (T1059) -- PowerShell, CMD, or bash scripts for execution and lateral movement
- Create or Modify System Process (T1543) -- Installing malicious services or scheduled tasks for persistence
- Boot or Logon AutoStart Execution (T1547) -- Registry Run keys or startup folder modifications
- Defence Evasion
- Impair Defences (T1562) -- Disabling antivirus, EDR agents, or Windows Defender
- Indicator Removal (T1070) -- Clearing event logs, deleting shadow copies, removing forensic artifacts
- Obfuscated Files or Information (T1027) -- Encrypted payloads, packed executables, or code obfuscation

Discovery & Credential Access

- Account Discovery (T1087) -- Enumerating domain accounts, local administrators, privileged users
- System Information Discovery (T1082) -- Identifying OS version, installed software, domain membership
- Network Share Discovery (T1135) -- Mapping accessible file shares for data exfiltration targets
- OS Credential Dumping (T1003) -- LSASS dumping, SAM database extraction, credential harvesting

Lateral Movement

- Remote Services: SMB/Windows Admin Shares (T1021.002) -- Using administrative credentials to access network systems
- Remote Services: RDP (T1021.001) -- Remote desktop access to spread across network

Collection & Exfiltration

- Data from Local System (T1005) -- Collecting sensitive files from compromised endpoints
- Data from Network Shared Drive (T1039) -- Accessing file servers, SharePoint, or cloud storage
- Archive Collected Data (T1560) -- Compressing stolen data for efficient exfiltration
- Exfiltration Over Web Service (T1567) -- Uploading to attacker-controlled cloud storage or file-sharing services

Command-and-Control

- Application Layer Protocol (T1071) -- HTTPS-based C2 communication for stealth
- Encrypted Channel (T1573) -- TOR network usage for anonymity and operational security

Impact

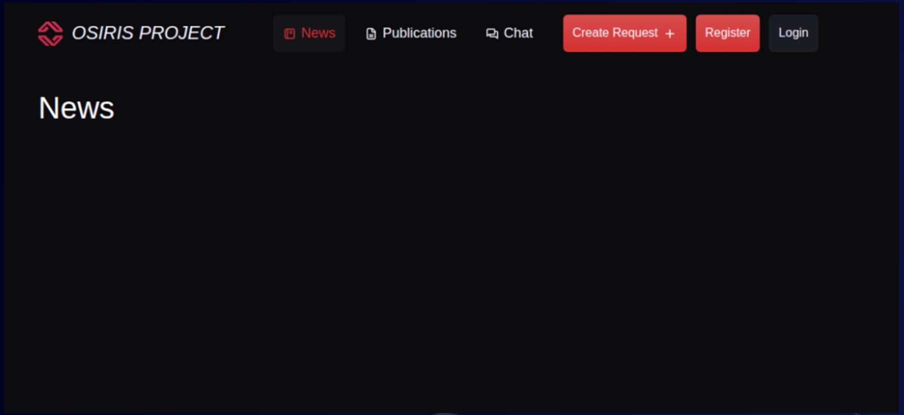
- Data Encrypted for Impact (T1486) -- Deploying encryption payload across network systems (algorithm unknown)
- Inhibit System Recovery (T1490) -- Deleting Volume Shadow Copies, disabling Windows Recovery, removing backup access

Indicators of Compromise (IOCs)

Network Indicators

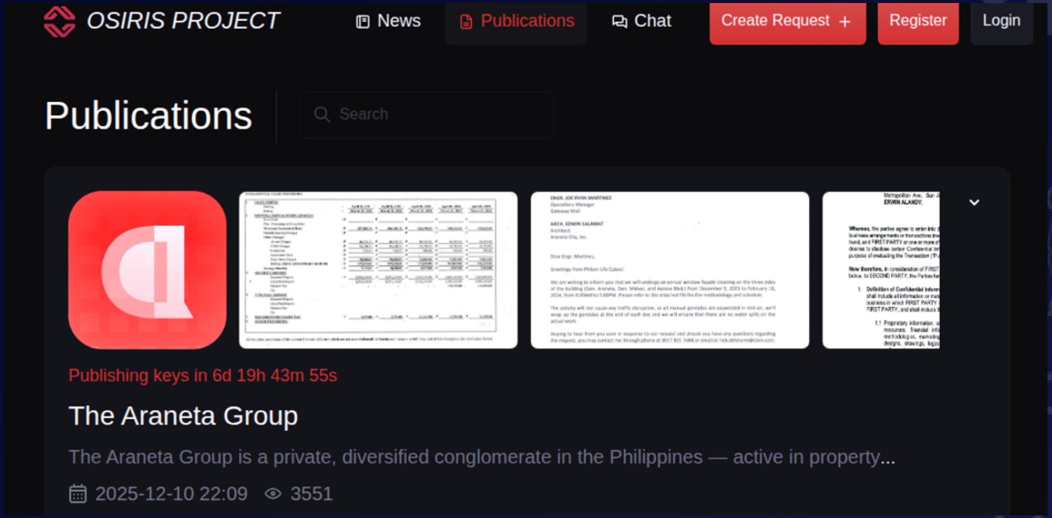
- TOR Leak Site:

https://osirisbm3357xrccnid23nlyuqwzbgqheaei6dxvyi34tbkqr3bmvfid.onion/
http://ausare.net



News

https://osirisbm3357xrccnid23nlyuqwzbgqheaei6dxvyi34tbkqr3bmvfid.onion/app/publications



Publications

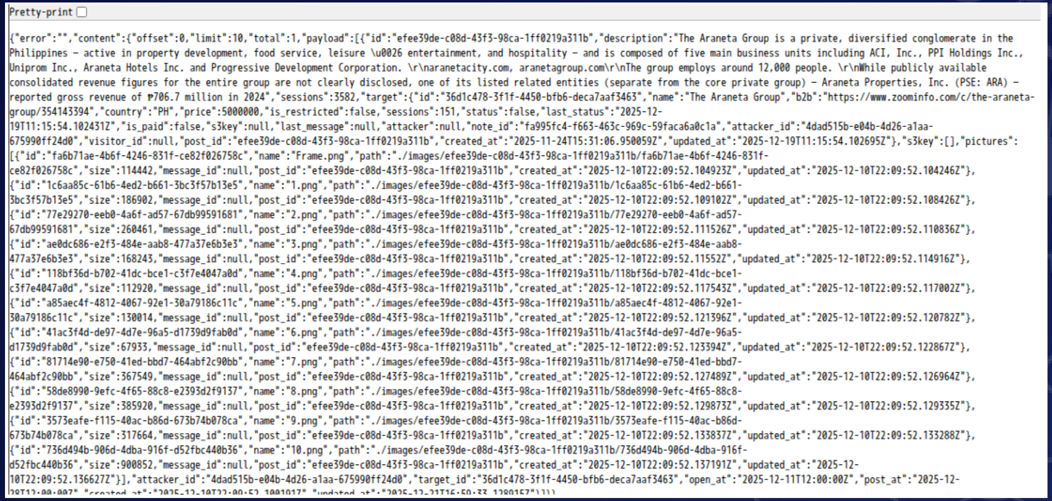
Publishing keys in 6d 19h 43m 55s

The Araneta Group

The Araneta Group is a private, diversified conglomerate in the Philippines — active in property...

2025-12-10 22:09 3551

https://osirisbm3357xrccnid23nlyuqwzbgqheaei6dxvyi34tbkqr3bmvfid.onion/rest/blog/posts?offset=0&limit=10&search=



```
{"error":"","content":{"offset":0,"limit":10,"total":1,"payload":[{"id":"efee39de-c08d-43f3-98ca-1ff0219a311b","description":"The Araneta Group is a private, diversified conglomerate in the
Philippines – active in property development, food service, leisure \u0026 entertainment, and hospitality – and is composed of five main business units including ACI, Inc., PPI Holdings Inc.,
Uniprom Inc., Araneta Hotels Inc. and Progressive Development Corporation. \r\naranetacity.com, aranetagroup.com\r\nThe group employs around 12,000 people. \r\nWhile publicly available
consolidated revenue figures for the entire group are not clearly disclosed, one of its listed related entities (separate from the core private group) – Araneta Properties, Inc. (PSE: ARA) –
reported gross revenue of ₱706.7 million in 2024","sessions":3582,"target":{"id":"36d1c478-3f1f-4450-bfb6-deca7aaf3463","name":"The Araneta Group","b2b":"https://www.zoominfo.com/c/the-araneta-
group/354143394","country":"PH","price":5000000,"is_restricted":false,"sessions":151,"status":false,"last_status":"2025-12-
19T11:15:54.102431Z","is_paid":false,"s3key":null,"last_message":null,"attacker":null,"note_id":"fa995fc4-f663-463c-969c-59faca6a0c1a","attacker_id":"4dad515b-e04b-4d26-a1aa-
675990ff24d0","visitor_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-11-24T15:31:06.950059Z","updated_at":"2025-12-19T11:15:54.102695Z"},"s3key":[],"pictures":
[{"id":"fa6b71ae-4b6f-4246-831f-ce82f026758c","name":"Frame.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/fa6b71ae-4b6f-4246-831f-
ce82f026758c","size":114442,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.104923Z","updated_at":"2025-12-10T22:09:52.104246Z"},
{"id":"1c6aa85c-61b6-4ed2-b661-3bc3f57b13e5","name":"1.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/1c6aa85c-61b6-4ed2-b661-
3bc3f57b13e5","size":186902,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.109102Z","updated_at":"2025-12-10T22:09:52.108426Z"},
{"id":"77e29270-eeb0-4a6f-ad57-67db99591681","name":"2.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/77e29270-eeb0-4a6f-ad57-
67db99591681","size":260461,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.111526Z","updated_at":"2025-12-10T22:09:52.110836Z"},
{"id":"ae0dc686-e2f3-484e-aab8-477a37e6b3e3","name":"3.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/ae0dc686-e2f3-484e-aab8-
477a37e6b3e3","size":168243,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.11552Z","updated_at":"2025-12-10T22:09:52.114916Z"},
{"id":"118bf36d-b702-41dc-bce1-c3f7e4047a0d","name":"4.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/118bf36d-b702-41dc-bce1-
c3f7e4047a0d","size":112920,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.117543Z","updated_at":"2025-12-10T22:09:52.117002Z"},
{"id":"a85aec4f-4812-4067-92e1-30a79186c11c","name":"5.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/a85aec4f-4812-4067-92e1-
30a79186c11c","size":130014,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.121396Z","updated_at":"2025-12-10T22:09:52.120782Z"},
{"id":"41ac3f4d-de97-4d7e-96a5-d1739d9fab0d","name":"6.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/41ac3f4d-de97-4d7e-96a5-
d1739d9fab0d","size":67933,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.123394Z","updated_at":"2025-12-10T22:09:52.122867Z"},
{"id":"81714e90-e750-41ed-bbd7-464abf2c90bb","name":"7.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/81714e90-e750-41ed-bbd7-
464abf2c90bb","size":367549,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.127489Z","updated_at":"2025-12-10T22:09:52.126964Z"},
{"id":"58de8990-9efc-4f65-88c8-e2393d2f9137","name":"8.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/58de8990-9efc-4f65-88c8-
e2393d2f9137","size":385920,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.129873Z","updated_at":"2025-12-10T22:09:52.129335Z"},
{"id":"3573eafe-f115-40ac-b86d-673b74b078ca","name":"9.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/3573eafe-f115-40ac-b86d-
673b74b078ca","size":317664,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.133837Z","updated_at":"2025-12-10T22:09:52.133288Z"},
{"id":"736d494b-906d-4dba-916f-d52fbc440b36","name":"10.png","path":"./images/efee39de-c08d-43f3-98ca-1ff0219a311b/736d494b-906d-4dba-916f-
d52fbc440b36","size":900852,"message_id":null,"post_id":"efee39de-c08d-43f3-98ca-1ff0219a311b","created_at":"2025-12-10T22:09:52.137191Z","updated_at":"2025-12-
10T22:09:52.136627Z"}],"attacker_id":"4dad515b-e04b-4d26-a1aa-675990ff24d0","target_id":"36d1c478-3f1f-4450-bfb6-deca7aaf3463","open_at":"2025-12-11T12:00:00Z","post_at":"2025-12-
28T12:00:00Z","created_at":"2025-12-10T22:09:52.100101Z","updated_at":"2025-12-21T16:59:33.128015Z"}]}}
```

MITRE ATT&CK TTPs:

Tactic	ID	Technique
Initial Access	T1078	Valid Accounts
	T1133	External Remote Services
	T1190	Exploit Public-Facing Application
	T1566.001	Phishing: Spearphishing Attachment
Execution	T1059	Command and Scripting Interpreter
	T1569.002	System Services: Service Execution
Persistence	T1543.003	Create or Modify System Process: Windows Service
	T1547.001	Boot/Logon AutoStart: Registry Run Keys
Defence Evasion	T1562.001	Impair Defences: Disable or Modify Tools
	T1070	Indicator Removal
	T1027	Obfuscated Files or Information
Discovery	T1087	Account Discovery
	T1082	System Information Discovery
	T1135	Network Share Discovery
Credential Access	T1003	OS Credential Dumping
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares
	T1021.001	Remote Services: Remote Desktop Protocol
Collection	T1005	Data from Local System
	T1039	Data from Network Shared Drive
	T1560	Archive Collected Data
Exfiltration	T1567	Exfiltration Over Web Service
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
	T1573	Encrypted Channel
Impact	T1486	Data Encrypted for Impact
	T1490	Inhibit System Recovery

Mitigation and Detection with Crystal Eye 6.0

1. Access Control & Credential Protection
    - Implement multi-factor authentication (MFA) on all remote access services (VPN, RDP, webmail, cloud applications)
    - Disable or restrict RDP access; use VPN with MFA for remote management
    - Rotate administrative credentials regularly; disable unused accounts
    - Monitor dark web for compromised credentials; subscribe to breach notification services
2. Vulnerability Management
    - Patch public-facing applications immediately (web servers, VPNs, email gateways)
    - Conduct regular Vulnerability Assessments and Penetration Testing
    - Implement web application firewalls (WAF) for internet-facing services
3. Backup & Recovery Protection
    - Maintain offline, immutable backups with air-gapped storage
    - Test backup restoration procedures monthly
    - Restrict backup system access; monitor for shadow copy deletion attempts
4. Endpoint Detection & Response (EDR)
    - Deploy EDR solutions with behavioural detection capabilities
    - Enable tamper protection on security agents
    - Monitor for suspicious PowerShell, WMI, or service execution
5. Network Segmentation & Monitoring
    - Segment critical systems (domain controllers, backup servers, databases) from general network
    - Block TOR exit nodes at perimeter firewalls
    - Monitor for large outbound data transfers and unusual network traffic patterns
6. Data Loss Prevention (DLP)
    - Implement DLP policies for sensitive data (PII, financial records, intellectual property)
    - Alert on bulk data downloads or transfers to external services

Worldwide Ransomware Victims

The United States remained the clear epicentre of ransomware activity, accounting for 52.9% of all identified victims this week. That level of concentration means more than half of all known cases were U.S.-based, reinforcing its position as the primary hunting ground for most major ransomware operations.

A strong second tier consisted of the United Kingdom (7.72%), Canada (6.56%), and Germany (4.63%). Together with the U.S., this core group of mature economies represents the bulk of visible global activity, reflecting large digital footprints, higher reporting/disclosure rates, and significant financial upside for threat actors.

A broader mid band followed, including India (2.32%), Australia, Argentina, and Italy (each 1.93%), as well as Spain, Singapore, and France (each 1.54%), plus Malaysia, Chile, Turkey, Sweden (each 1.16%). These countries show that ransomware remains deeply embedded across both established and emerging markets, especially where services, manufacturing, and IT-heavy businesses are concentrated.

Below that, a long tail of countries, Brazil, Taiwan, Croatia, Philippines (each 0.77%), and a wide spread of single-incident geographies such as Mexico, Paraguay, New Zealand, South Korea, Greece, Japan, Venezuela, Belgium, Poland, Bolivia, Dominican Republic, South Africa, Indonesia, Colombia, Slovakia, Portugal, Denmark, China, Estonia (each 0.39%), appeared at low but non-zero volumes. Individually small, their combined footprint underscores that ransomware remains a global problem, with opportunistic and campaign-driven attacks touching almost every region rather than being confined to a handful of high-profile countries.

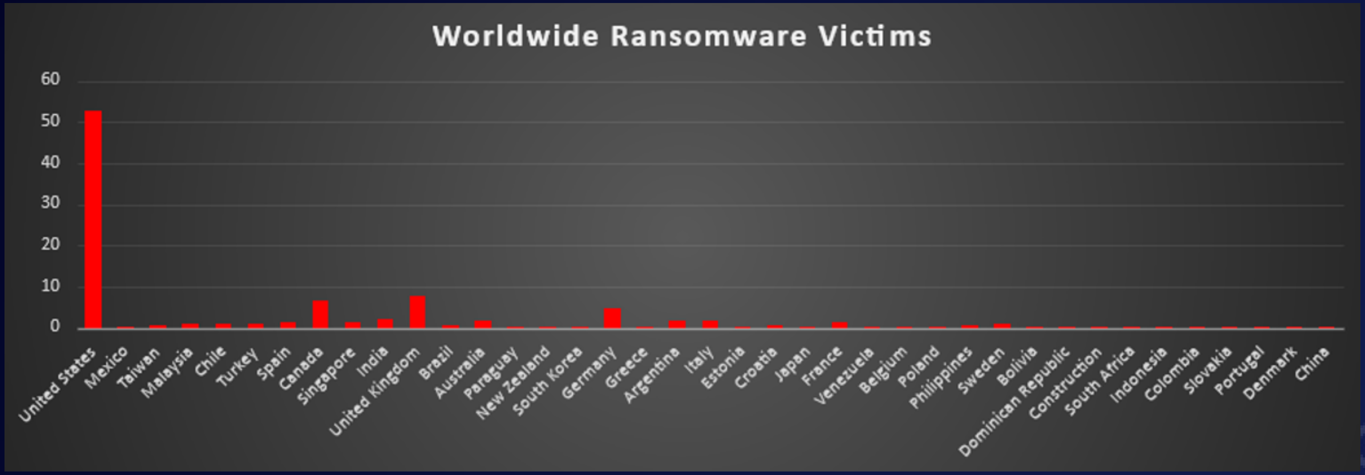


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Construction was the most heavily targeted sector this week, accounting for 15.06% of all identified ransomware victims. That puts project-driven, contract-heavy environments at the very top of the risk ladder, where any disruption can stall sites, delay deliveries, and immediately impact cash flow, perfect leverage for extortion.

Close behind, Manufacturing (14.67%), Hospitality (10.42%), and Business Services (9.65%) formed a strong second tier. These sectors combine operational dependency, tight timelines, and large volumes of customer or client data. For attackers, that mix offers both pressure (downtime costs real money fast) and monetisation paths (data theft, regulatory exposure, reputational impact).

A substantial mid-band followed, led by Law Firms and Retail (each 7.34%), Education (5.02%), Finance (4.25%), and Energy (3.47%), as well as Organisations (3.09%), with Transportation, IT, and Federal entities (each 2.32%) also regularly appearing in victim data. This layer shows that legal, financial, public sector, and core service providers remain routine fixtures on leak sites rather than exceptions.

Lower-volume but still active verticals included Real Estate, Healthcare, and Consumer Services (each 1.93%), Electronics and Media & Internet (each 1.54%), plus Telecommunications (1.16%), followed by Agriculture, Insurance, Minerals & Mining (each 0.77%), and Software (0.39%) forming the long tail. Individually small, this spread makes it clear that ransomware pressure cuts across almost every major industry, if an organisation holds valuable data or depends on uptime, it sits somewhere inside this threat envelope.

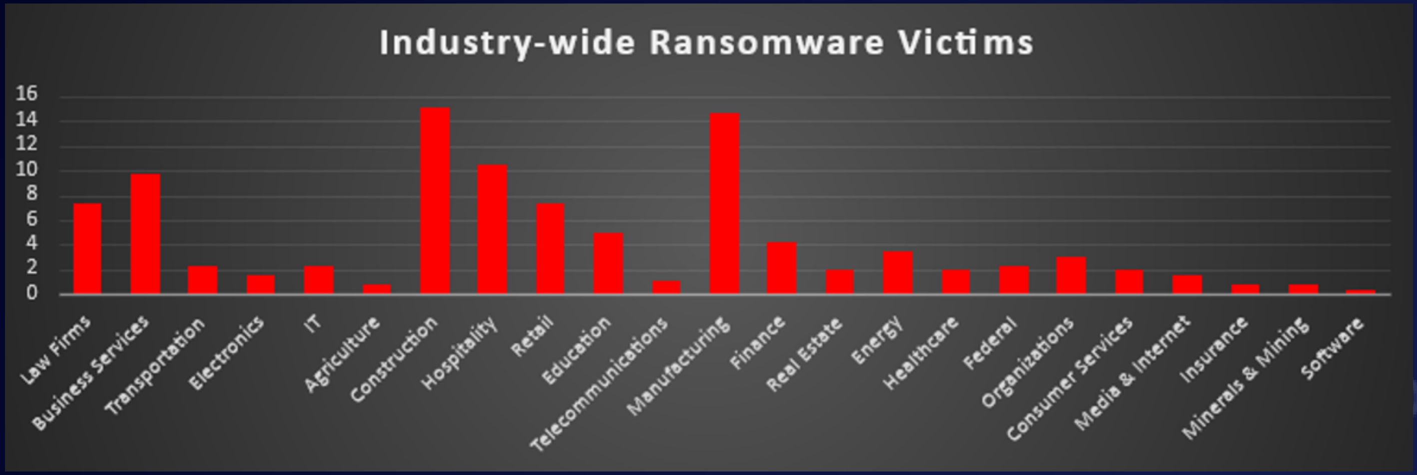


Figure 6: Industry-wide Ransomware Victims