SAPTANG™
Proactive Threat Defence

Monthly Threat Report

SEPTEMBER - 2025

Executive Summary

September 2025 marked a significant escalation in cyber threat activity across multiple attack vectors. The month was characterised by aggressive ransomware campaigns, rapid weaponization of enterprise vulnerabilities, sustained hacktivist DDoS operations, and widespread data exposure incidents affecting millions of records globally.

Key Highlights:

- **Ransomware Activity:** 433 confirmed victim organizations across 40+ distinct ransomware operations-a substantial increase demonstrating both the persistence of established actors and continued ecosystem fragmentation
- **Vulnerability Exploitation:** Critical remote code execution flaws in SharePoint, Citrix, and enterprise appliances were weaponized within days of disclosure, with the "ToolShell" cluster driving major ransomware deployments
- **DDoS Campaigns:** Politically motivated hacktivist groups launched coordinated attacks across Europe, Middle East, and Asia-Pacific, targeting government services, critical infrastructure, and healthcare institutions
- **Data Breaches:** Mass exposure incidents affected organizations worldwide, with claims totalling over 26 million records spanning government agencies, healthcare providers, financial institutions, and cloud platforms
- **Supply Chain Impact:** Third-party and vendor compromises produced cascading effects, notably impacting European aviation infrastructure and automotive manufacturing

The threat landscape in September revealed an increasingly opportunistic adversary ecosystem exploiting the convergence of vulnerability disclosure, insufficient patch management, and resource-constrained defenses-particularly in healthcare, education, and public sector organizations.

Ransomware Activity - September 2025

Overview

Ransomware remained one of the most disruptive cyber threats throughout September 2025. The month witnessed **a significant surge in victim disclosures, with 433 confirmed cases across more than 40 distinct ransomware operations**. This reflects both the persistence of dominant actors and the fragmentation of the ecosystem, where smaller or re-branded groups continue to emerge and compete for visibility. The overall landscape was defined by two parallel dynamics:

- **Victim Volume:** 433 organizations publicly disclosed.
- **Most Active Threat Groups:** Qilin, Play, Akira, Incransom, TheGentlemen, Beast, Everest, Safepay.
- **Global Reach:** The United States accounted for more than half of reported victims, though cases spanned Europe, Asia, Africa, and Latin America.
- **Sectoral Impact:** Healthcare, education, manufacturing, financial and legal services, logistics, and SaaS/cloud providers were among the most affected

Major Threat Actor Analysis

Qilin - Large-Scale Industrial & Education Targeting

With nearly **54 victims** in September, Qilin remained one of the most prolific actors. Its campaigns focused heavily on manufacturing, education, and healthcare, while also disrupting logistics providers.

Notable Victims:

- St Thomas More Catholic High School (UK)
- Uganda Electricity Transmission Co. Ltd.
- Haeger & Schmidt Logistics (Germany)
- CIMEXSTEEL (Czech Republic)

Tactics: Qilin follows a systematic playbook involving penetration through exposed services or unpatched vulnerabilities, lateral movement, and selective exfiltration before encrypting systems. The emphasis on supply-chain and public-sector entities highlights a strategy to maximize impact and visibility.

Play - Consistent Global Campaigns

Play registered more than **46 confirmed victims** worldwide. Its portfolio of attacks included engineering, aerospace, logistics, and IT services.

Notable Victims:

- Jamco Aerospace
- Travancore Analytics
- Quartus Engineering

Tactics: Play remains a consistent operator, leveraging unpatched VPN and RDP exposures as initial access points. Its balance of both victim volume and high-value targets underscores its persistence as a global threat.

Akira - Opportunistic Expansion

Akira accounted for around **39 victims** this month, continuing its opportunistic compromise strategy. Its victim pool was broad: law firms, consultancies, IT service providers, logistics firms, and manufacturers.

Notable Victims:

- Insero & Co. CPAs (US)
- Cevital Group (Algeria)
- GWU Umwelttechnik GmbH (Germany)
- Sweetener Supply (US)

Tactics: Akira typically exploits vulnerabilities in enterprise VPNs and remote services, showing little regard for sectoral boundaries. Its scattershot targeting makes it a highly unpredictable but widespread threat.

Incransom - Long-tail / Community Targeting

Incransom maintained steady activity with at least **37 confirmed victims**. Unlike top-tier actors, its focus lies on nonprofits, schools, healthcare providers, and SMBs.

Notable Victims:

- Radford City Schools (US)
- Netstar (South Africa)
- Louis Tieu DDS MD (US)

Assessment: These campaigns illustrate the long-tail risk of ransomware, where small but active gangs consistently exploit resource-constrained organizations that cannot afford downtime or extended incident response.

TheGentlemen – SMB & Local Institution Focus

TheGentlemen recorded around **35 victims**, often pursuing SMBs and local institutions with limited cyber resilience capabilities.

Beast - Public Services & Healthcare Focus

Beast logged approximately 30 victims, continuing its pattern of hitting hospitals, schools, and SMEs where operational disruption translates to immediate pressure for ransom payment. **Notable Victims:**

- Huron Regional Medical Center (US)
- Winner School District (US)
- Grand Rapids Metrology (US)

Everest – High-Value, High-Visibility Attacks

Everest was more selective with approximately **15 victims** but stood out for targeting recognizable brands, leveraging public visibility as pressure.

Notable Victims:

- Mailchimp
- Grayscale Investments
- Crumbl
- Pacific HealthWorks

Assessment: Everest's strategy focuses on reputation-driven extortion, where the threat of public exposure may be more damaging than operational downtime.

Safepay – Persistent Opportunistic Activity

Safepay targeted roughly **20 victims**, displaying opportunistic but persistent behavior across various sectors.

Sectoral & Geographic Impact

Healthcare & Education

Healthcare and education continued to bear the brunt of ransomware activity, with numerous hospitals, school districts, and universities impacted.

Examples:

- Cookeville Regional Medical Center
- Radford City Schools
- Franklin Pierce Schools

These sectors remain attractive due to the criticality of patient care and educational continuity, combined with often underfunded cyber security defences.

Financial & Legal Services

Financial and legal services were disproportionately affected, with firms recognizing that data-rich, reputation-sensitive organizations remain prime candidates for extortion.

Examples:

- Insero & Co. CPAs
- Grayscale Investments
- Vinson & Elkins LLP
- Philadelphia Investment Partners

Manufacturing & Industrial Supply Chains

Manufacturing and industrial supply chains faced sustained pressure, with operational disruptions rippling across multiple business partners and customers.

Examples:

- Haeger & Schmidt Logistics
- MGM Transformer
- Hytrol
- Geotec

Cloud & SaaS Providers

The compromise of Mailchimp by Everest reflects a growing emphasis on service providers whose breach could cascade into a broader ecosystem of downstream clients.

Public Sector & Community Services

Community-facing organizations-schools, local governments, nonprofits, and small businesses-remain vulnerable due to limited resources, ensuring rapid payouts and minimal resistance.

Trends & Strategic Assessment

- **Continued Fragmentation:** The ransomware ecosystem revealed clear fragmentation, with dozens of active groups operating simultaneously, though a handful of high-volume actors dominated victim counts.
- **Cloud & SaaS Targeting Shift:** Attacks on service providers like Mailchimp signal recognition that a single breach can magnify leverage across hundreds of downstream clients **Cloud & SaaS Targeting Shift:** Attacks on service providers like Mailchimp signal recognition that a single breach can magnify leverage across hundreds of downstream clients
- **Healthcare & Education Vulnerability:** These sectors face sustained targeting due to criticality of data and service availability, combined with limited investment in cyber resilience.
- **RCE Exploitation:** Operators quickly weaponized flaws such as Citrix Bleed-2, Commvault RCE, and SAP NetWeaver file upload vulnerabilities for initial access.Most Exploited Vulnerabilities - September 2025

Most Exploited Vulnerabilities - September 2025

Executive Summary

September 2025 exploitation activity was defined by **critical remote code execution (RCE) and deserialization vulnerabilities** across widely deployed enterprise platforms.

The majority of observed cases affected Microsoft SharePoint, Citrix NetScaler, Fortinet FortiWeb, Cisco ISE, and browser engines (Chromium, Android runtime). Attackers demonstrated both rapid weaponization of newly disclosed flaws and persistent exploitation of previously patched or end-of-life (EOL) products.

The exploitation landscape highlights three dominant vectors:

- **SharePoint exploitation (ToolShell cluster):** Multiple deserialization and patchbypass flaws formed the core of September's ransomware and intrusion activity, chained together for unauthenticated RCE in enterprise environments
- **Browser zero-days:** Exploitation of Chromium V8, ANGLE/GPU, and Android runtime vulnerabilities provided attackers with sandbox escapes and full device compromise, driving emergency patch releases
- **Appliance & infrastructure exploitation:** External-facing systems (Citrix, Fortinet, Cisco, Ivanti, TP-Link) remained prime targets, with opportunistic scanning escalating into botnet recruitment and targeted intrusions

The speed of weaponization was striking-proof-of-concept exploits surfaced within days of public advisories, with automated scanning campaigns quickly following. Many incidents linked exploitation directly to ransomware deployment, credential/session theft, and data exfiltration.

Key Highlights

- **SharePoint "ToolShell" cluster:** Multiple deserialization and patch-bypass vulnerabilities (CVE-2025-53770, -53771, -49704, -49706) drove the month's most impactful intrusions, observed in ransomware campaigns and APT targeting
- **Browser exploitation surge:** Chromium V8 type-confusion (CVE-2025-10585), Android runtime UAF (CVE-2025-48543), and GPU/ANGLE sandbox escapes (CVE2025-6558) were all exploited as zero-days in the wild

Appliance/gateway exploitation: Citrix NetScaler "Bleed 2" (CVE-2025-5777), Fortinet FortiWeb SQLi (CVE-2025-25257), Cisco ISE file-upload RCE (CVE-2025-
20282), and Ivanti EPMM flaws were actively targeted

- **Legacy and consumer IoT exploitation:** EOL TP-Link routers and

authentication flaws (CVE-2023-50224, CVE-2025-9377) continued to be abused for botnet recruitment and persistence in consumer networks

Top CVEs Actively Exploited

Browser & Runtime Exploits

- **CVE-2025-10585 (Chromium V8 type-confusion) – CVSS 8.8** Heap corruption flaw enabling RCE via crafted web payloads. Exploited as a zero-day, patched with emergency updates.
- **CVE-2025-6558 (Chromium ANGLE/GPU sandbox escape) – CVSS ~8.8** Validation failure allowing sandbox breakout from crafted content. Used in chained exploit kits.
- **CVE-2025-10584 family (Chromium rendering engine chain) – CVSS 7.5-9.0** Cluster of rendering flaws exploited together for browser-based persistence and code execution.

Enterprise Deserialization & Authentication Issues

- **CVE-2025-53770 (SharePoint ToolShell zero-day) – CVSS 9.8** Unauthenticated deserialization RCE. Central to ransomware campaigns and targeted APT activity.
- **CVE-2025-53771 (SharePoint patch-bypass) – Critical** Bypassed prior fixes, extending exploitation windows for threat actors.
- **CVE-2025-49704 (SharePoint deserialization/code injection) – CVSS 8.8** Enabled code injection when combined with spoofing flaws.
- **CVE-2025-49706 (SharePoint authentication spoofing) – CVSS 6.3** Allowed crafted requests to bypass validation and chain into RCE.
- **CVE-2025-53690 (Sitecore deserialization) – CVSS 9.0** Unauthenticated deserialization leading to RCE. Public PoCs released; observed exploitation of externally exposed servers.
- **CVE-2025-5086 (DELMIA Apriso deserialization) – CVSS ~9.0** Targeted exploitation in PLM/industrial environments with high-value IP theft potential.

Network Appliances & Gateways

- **CVE-2025-5777 (Citrix NetScaler "Bleed 2") – CVSS ~9.3** Memory over-read exposing session tokens. Mass scanning and exploitation observed.
- **CVE-2025-25257 (FortiWeb Fabric Connector SQLi → RCE) – CVSS ~9.6** Preauthentication SQL injection enabling remote execution. Public PoC; actively exploited.
- **CVE-2025-20282 (Cisco ISE unauth file-upload → root RCE) – CVSS 9.8** Unauthenticated API flaw permitting root-level compromise.
  CVE-2025-54309 (CrushFTP AS2 validation bypass) – CVSS 9.0 Unauthenticated admin access leading to service takeover. Exploited in multiple attacks.
- **CVE-2025-4427 / 4428 (Ivanti EPMM chain) – CVSS 7.5-8.8** Authentication

bypass combined with RCE in mobile device management platforms. Exploited together for admin takeover.

Consumer IoT & Legacy Devices

- **CVE-2025-9377 (TP-Link router RCE) – High/Critical** Authenticated RCE in parental control module of EOL firmware. Exploited for botnet recruitment.
- **CVE-2023-50224 (TP-Link TL-WR841N improper authentication) – High** Authentication bypass exposing configuration data. Active in ongoing scans.

Observations & Trends

- **Deserialization dominance:** Over half of top exploited CVEs involve unsafe deserialization or input validation flaws, underscoring poor serialization hygiene as a systemic weakness
- **Browser zero-days as first access:** Multiple zero-days across Chromium/Android show that browser exploitation remains the most common delivery mechanism for state-aligned actors
- **Appliance abuse for mass scanning:** Citrix, Fortinet, Cisco, and Ivanti devices continue to draw opportunistic exploitation at scale due to constant external exposure
- **Chaining behaviour:** Exploits are increasingly chained (authentication bypass + RCE) to maximize impact, particularly in SharePoint ToolShell campaigns
- **Weaponization speed:** Time between disclosure and weaponization is shrinking, with active scanning beginning within days of advisory release

Impact Profile

Severity: Majority fall into High (7.5-8.9) or Critical (9.0-10.0) categories.

Exploitation outcomes observed:

- Initial access and persistence in enterprise networks
- Credential/session theft (Citrix NetScaler, Cisco ISE)
- Data exfiltration (CrushFTP, Sitecore, DELMIA Apriso)
- Ransomware deployment (SharePoint ToolShell, Fortinet FortiWeb)
- Botnet recruitment (TP-Link routers)

Threat type balance: Opportunistic (IoT/appliances) versus targeted (SharePoint, PLM, enterprise SaaS). DDoS Activity

DDoS

Executive Summary

September 2025 witnessed a surge in **hacktivist-driven Distributed Denial-of-Service (DDoS) campaigns**, with operations spanning Europe, the Middle East, and Asia-Pacific. The majority of activity was **politically motivated**, often aligned with ongoing geopolitical conflicts such as the Russia-Ukraine war and Middle Eastern unrest.

Key actors included **NoName, Dark Storm Team, HEZI RASH, Red Wolf Cyber, Keymous+, and Fire Wire**, supported by a range of smaller regional groups. Their campaigns primarily targeted **government ministries, municipal councils, energy utilities, telecoms, airports, and healthcare institutions**, sectors where even short-lived outages generate visibility and public concern.

While the technical impact of these operations was generally **short-lived service degradation**, their value lay in **propaganda amplification**. Groups claimed responsibility on Telegram and social media, often exaggerating operational success to project strength and undermine public trust.

The **European region remained the most heavily targeted**, followed by **Middle Eastern and Asian institutions**. Patterns suggest that DDoS will continue to serve as a **low-cost, high-visibility tactic**, increasingly paired with other forms of disruption such as website defacements or false data-leak claims to maximize reputational damage.

Key Threat Groups Observed

NoName

Remained one of the most prolific actors, conducting sustained campaigns across **Europe**. Key targets included **municipal governments in Finland**, Spanish ministries, Italian port authorities, and French state agencies. The group also struck Ukrainian regional administrations, ISPs, and industrial firms, consistent with its **pro-Russian operational narrative**. The focus on **European government and infrastructure** aligns with ongoing attempts to disrupt EU support for Ukraine.

Hider Nex

Focused its campaigns on the **Middle East and North America**, with notable attacks against ministries, hospitals, and utilities in **Israel and Bahrain**, as well as **financial regulators in the United States**. The breadth of targets suggests access to **sizeable botnet infrastructure** capable of sustaining concurrent campaigns across geographically distant regions.

Keymous+

Stood out for targeting **symbolic and reputationally sensitive organisations**, including **ministries of health, financial regulators, and international institutions such as the International Court of Justice**. Unlike other groups that pursue volume, Keymous+ sought **high-profile headlines** to increase political and psychological impact.

Dark Storm Team

Conducted opportunistic DDoS operations across **Turkey, Iran, Japan, and the United States**. Notable campaigns included **airports in Turkey and Japan**, Iranian oil and gas organisations, and academic institutions. Dark Storm displayed less consistency in victimology but demonstrated **broad opportunism**, hitting diverse regions with no clear thematic restriction.

HEZI RASH

Targeted **Ukraine, Germany, Turkey, and Japan**, striking entities such as **Spetstechnoexport, KEPCO, Nippon Animation, and children's hospitals in Kyiv and Berlin**. The blend of **industrial, healthcare, and media organisations** shows a tendency to select sensitive targets that can generate reputational harm rather than technical disruption.

Red Wolf Cyber

Focused on **South Korea**, attacking government ministries, KEPCO (the national electric utility), universities, and port authorities. It also claimed responsibility for targeting NATOrelated entities, signalling ambitions to extend beyond regional objectives.

Other regional actors

Smaller groups such as **Fire Wire**, **NOTCTBER404**, **Kxichixxsec**, and **NullSec Philippines** were active in **Algeria, Thailand, and the Philippines**. Their operations tended to concentrate on **local ministries, educational institutions, and municipal services**, often mirroring the tactics of larger collectives but on a smaller scale.

Targeted Regions and Sectors

Regions most affected:

- **Europe:** Finland, Spain, Germany, Czech Republic, Italy, France, Norway.
- **Middle East:** Israel, Bahrain, Iraq, Syria, Algeria, Iran.
- **Asia-Pacific:** Japan, Taiwan, Thailand, Philippines, South Korea.
- **North America:** United States.

Sectors most frequently targeted:

- **Government and municipal services** - Ministries, municipal councils, customs agencies, parliaments.
- **Critical infrastructure** - Energy utilities, gas/oil companies, telecom providers, port authorities, airports.
- **Financial services** - Banks, stock exchanges, regulators.
- **Healthcare** - National hospitals, children's hospitals, and medical societies.
- **Education** - Universities, schools, and research institutions.
- **Private corporations** - Telecoms, ISPs, insurance, and retail platforms.

Attack Characteristics

Types of Attacks*:* Predominantly volumetric floods (UDP, SYN) and application-layer HTTP floods against public-facing portals. Multi-vector campaigns were observed where actors simultaneously launched attacks on several institutions within the same region.

Duration & Impact: Most attacks lasted minutes to a few hours, causing temporary service degradation. No confirmed prolonged outages or physical infrastructure damage was attributed to these campaigns.

Tactics & Infrastructure:

- Heavy reliance on **botnets and DDoS-for-hire platforms**, giving relatively unsophisticated actors significant amplification capacity.
- Many attacks were **timed in waves**, maximising visibility across social media by striking multiple organisations in quick succession.
- Propaganda was central: claims of success often exceeded actual operational effect, with actors pushing narratives of "government collapse" or "critical outage" to bolster reputational weight.

Threat Actor Motivation

The motivations behind these campaigns remain consistent with observed hacktivist behaviour:

- **Political Alignment:** Pro-Russian activity targeting EU and Ukrainian institutions; anti-Israel operations; opportunistic strikes against U.S. assets.
- **Propaganda & Visibility:** High reliance on **Telegram and social platforms** to amplify claims of success, regardless of real impact.
- **Psychological Effect:** Designed to **erode public confidence** in the resilience of government and essential services, often coinciding with **politically sensitive events** such as sanctions votes, military escalations, or anniversaries.

Outlook

Looking ahead, DDoS activity is expected to remain a **low-cost, high-visibility tactic** for hacktivist actors.

- **European and Middle Eastern organisations** will remain the most frequent targets, particularly in sectors tied to **political, military, or humanitarian developments**.
- Campaigns are likely to **evolve into multi-vector operations**, where DDoS is paired with **website defacements, credential dumps, or false data-leak claims** to maximise reputational impact.

Cyber Incidents

Executive summary

September 2025 saw a continued focus on three dominant patterns: large-scale social engineering and fraud campaigns affecting Indian citizens and institutions, ransomware and supply-chain attacks causing operational outages at scale (notably in aviation and manufacturing), and rapid exploitation of network and vendor misconfigurations (firewalls, SharePoint/Jira misconfigurations) with broad downstream impact.

In India, law enforcement achieved several high-profile arrests for remote-access frauds and impersonation scams, while globally, third-party and vendor compromises produced the most disruptive incidents of the month.

India - Confirmed incidents (September 2025)

- **Phagwara hotel-run cyber-fraud racket dismantled**
  Police arrested 38 people operating from a hotel call-center in Phagwara, Punjab. The gang used fake virus warnings, remote-access tools (screen sharing/remote-control apps), and social engineering to coerce victims into transferring funds and providing card details. Victims included overseas nationals (U.S./Canada). Authorities recovered devices and seized proceeds; investigations include moneylaundering and cross-border victim notifications.
- **High-value “digital arrest” impersonation extortion**
  Prominent ex-banker was coerced by attackers posing as law-enforcement into transferring substantial sums under threat of arrest. The case reported in national press illustrates increasing sophistication in impersonation scams where legalstyle social-pressure is combined with threats to freeze or seize assets. Investigations and banking-freeze actions are in progress.
- **YouTuber account takeover and extortion**
  A high-follower Indian content creator had their channel taken over; suspects

demanded ₹8 lakh and had already extorted ~₹1.6 lakh before arrests. Local police arrested two suspects from Bihar. This is a confirmed account-compromise + extortion case showing direct monetization of credential theft.

- **Telangana directive: tracking habitual cyber offenders**
  Telangana police issued a directive for cyber cells to maintain history sheets for habitual cybercriminals formalizing an administrative measure aimed at tracking recidivism among fraudsters (financial scams, job frauds, impersonations). This is a confirmed policy action with operational implications for enforcement.
- **Elderly lawyer extorted via CBI-impersonation (Pune)**
  An older lawyer was coined by actors impersonating Central Bureau of Investigation
  (CBI) officers; nearly ₹1.8 crore was transferred before partial freezing. The incident was confirmed to police and is being prosecuted.
- **Fake police-raid extortion & digital asset theft (Ludhiana area)**
  An incident surfaced in which individuals posing as cyber wing officers kidnapped victims and forcibly requisitioned digital assets including 4,600 USDT and phones. Local police investigations are ongoing; arrests and FIRs were reported. This demonstrates violent tactics combined with digital-asset theft.
- **Sudha Murthy impersonation scam attempt (Bengaluru)**
  High-profile scam call targeted a public figure; the caller was recorded, and a FIR was registered. The confirmed incident is emblematic of continued targeting of public figures to extract data or payments via impersonation.
- **Indian airports: precautionary advisories after European airport outages** Following disruptive ransomware incidents that affected checkin/boarding systems at multiple European airports, Indian airport authorities issued advisories and conducted precautionary checks. No confirmed systems breach in India was reported; these are confirmed operational monitoring and preparedness actions.
- **Supplementary verified fraud & compromise updates**
  Multiple regional law-enforcement units reported arrests in smaller organized fraud cells (SIM-swap, fake-investment/ trading app rings, and fake job/employment scams). These confirmed takedowns-while often localized collectively illustrate the persistent fraud ecosystem active in September.

Global - Confirmed incidents (September 2025)

- **Major European airport disruptions stemming from third-party ransomware**
  Multiple large European airports (including Heathrow and major continental hubs) experienced widespread loss of automated check-in/boarding availability following a ransomware compromise linked to a vendor/third-party system (Collins Aerospace MUSE-related disruption reported). ENISA and other EU agencies confirmed ransomware as the causal factor; the UK National Crime

Agency later arrested an individual suspected of involvement. Operational recovery proceeded with manual fallbacks; passenger disruption was significant.

- **CISA emergency advisory - exploitation campaign targeting Cisco ASA 5500-X appliances**
  U.S. authorities issued an emergency warning after detection of active exploitation attempts against Cisco ASA 5500-X firewall appliances. The advisory required immediate patching or application of workarounds to prevent compromise of critical perimeter devices. This is a confirmed, high-priority exploitation campaign affecting enterprises and government agencies.
- **Jaguar Land Rover production disruption after cyberattack**
  Jaguar Land Rover reported a cyber incident that temporarily shut down IT systems and halted production at several UK plants. The company confirmed containment and phased restoration of systems; investigations continued. The attack's operational impact on manufacturing underscores ransomware/IT disruption risk to automotive supply chains.
- **Stellantis third-party vendor data exposure (~18 million records)**
  Stellantis disclosed that a compromise of a third-party vendor exposed around 18 million customer contact records. The incident was reported by industry outlets and vendor disclosure channels; samples appeared in public leak forums, prompting regulatory notifications and customer alerts.
- **Optus network outage (Australia) - emergency calling disruption**
  Australia's Optus experienced a major outage caused during a firewall/upgrade change that disrupted calls to the national emergency number for many users. The incident had severe public-safety consequences and prompted investigations and regulator inquiries. Although described operationally as a failed upgrade rather than a confirmed breach, the real-world impact on emergency services made this an urgent confirmed incident.
- **Co-op Group (UK) malicious cyberattack affecting ~6.5 million member**
  Co-op publicly confirmed a malicious cyber intrusion impacting member data; the company revised profit forecasts downward due to remediation costs and customer support. This confirmed incident affected member privacy and the retailer's operations.
- **Inotiv pharmaceutical firm - Qilin ransomware**
  Inotiv confirmed a ransomware attack (attributed to Qilin) that encrypted systems and resulted in exfiltration of roughly 176 GB (~162,000 files) of internal data. The firm reported disruption to operations and initiated containment and forensic response.
- **Orange Belgium telecom breach - ~850,000 customers impacted**
  Orange Belgium acknowledged a breach impacting nearly 850,000 customers, including exposure of names, phone numbers, and SIM/PUK codes. While financial data remained protected, the incident posed significant privacy and SIM-security concerns.

- **Data I/O operational ransomware attack**
  Electronics manufacturer Data I/O confirmed a ransomware incident that disrupted manufacturing, shipping and operational workflows. The company reported widespread operational impacts and ongoing recovery.
- **ManpowerGroup breach / RansomHub exfiltration (~500 GB, ~144k individuals)**
  ManpowerGroup confirmed a security incident involving exfiltration of large volumes of data; third-party reporting tied the incident to the RansomHub group. The compromised data included PII and employment records, and the company engaged forensic and notification processes.
- **Kido nursery chain - theft of data for ~8,000 children**
  A multi-region nursery chain confirmed that images and personal details of roughly 8,000 enrolled children were stolen and leaked by threat actors. The chain notified affected families and regulators, and external forensics were engaged.
- **Rhysida gang claim against Maryland Transit Administration**
  Rhysida publicly claimed a ransomware breach of the Maryland Transit Administration and published sample documents (including PII) to support the claim. MTA acknowledged disruption and engaged incident response. While demands and actor claims are public, the sample leaks and operational impact are confirmed by agency statements and security reporting.
- **npm Supply Chain Attack - September 2025**
  A significant supply chain attack compromised over 180 npm packages, including widely used ones like chalk, debug, and ansi-styles, collectively accounting for billions of weekly downloads. The attack involved a self-replicating worm dubbed "Shai-Hulud," which harvested developer credentials and cloud secrets, then propagated through CI/CD pipelines by publishing malicious updates to other packages owned by the same maintainers. This breach underscores the critical need for enhanced security measures in the open-source ecosystem.
- **Cloudflare Mitigates Record-Breaking DDoS Attack**
  Cloudflare recently thwarted the largest DDoS attack ever recorded, peaking at 22.2 terabits per second and 10.6 billion packets per second. The attack lasted approximately 40 seconds and targeted its content delivery network (CDN). Despite its massive scale, Cloudflare's infrastructure successfully mitigated the assault without service disruption, highlighting the resilience of modern DDoS defence systems.

Data Breach Alerts

Executive summary

This reporting period saw a broad set of claimed data exposures spanning government, education, healthcare, financial services, e-commerce platforms, and cloud/app providers. Most incidents are actor-claimed postings on underground forums or social platforms and remain **unverified** at time of reporting.

Commonly exposed data fields include full PII (names, DOBs, contact details), employment and payroll identifiers, government IDs and health numbers, financial details (bank accounts; in one claim, partial payment card data), hashed/password fields, and in multiple cases source code or system metadata.

The pattern indicates opportunistic collection of publicly accessible misconfigurations, credential reuse/compromise, and forum resale of datasets rather than coordinated zeroday mass exploitation. However, the scale of several claims (hundreds of thousands to millions of records) warrants prioritized monitoring and rapid containment if validated.

Incident summaries

- **PT. Kawauso Teknologi Indonesia - Makassar, Indonesia (IT & Services) Claim:** Internal accounts (corporate emails) disclosed.
  Data reportedly exposed: user identifiers, full names, usernames, company emails, passwords, contact numbers, addresses, DOB, gender.
  Threat actor (claimed): kawauso
  Impact: Internal account compromise increases risk of lateral access, supplychain or partner-targeting, and targeted phishing.
- **Nestlé Indonesia - Indonesia (FMCG / Corporate HR) Claim:** ~18,000 records leaked.
  Data reportedly exposed: full name, position, joining date, employee ID, corporate email, phone, bank account number, tax/NPWP number, BPJS health/employment numbers, PTKP.
  Threat actor (claimed): Phenom
  Impact: High privacy and financial risk for employees; regulatory and reputational impact possible.
- **NCC Alumni Association (National Cadet Corps) - India (Government-linked association)**
  Claim: Enrollment records leaked.
  Data reportedly exposed: names, contact info, DOBs, blood groups, bank details, cadet Enrollment data.

Threat actor (claimed): purple0piod
Impact: Moderate; PII exposure can enable targeted scams and identity fraud for enrolled cadets.

- **Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) - Germany (Higher Education)**
  Claim: Student data and source code posted.
  Data reportedly exposed: user IDs, timestamps, names, associated records, and source code artifacts.
  Threat actor (claimed): karuhunters
  Impact: Academic records and source code leaks can enable IP theft, targeted phishing of staff/students, and exploitation if source code contains vulnerabilities.
- **PGS Database - (Country unspecified; actor claims ~47,000 rows)**
  Claim: 47,000+ user records posted.
  Data reportedly exposed: IDs, names, emails, account details, roles, school info, phone numbers, CNICs, hashed passwords.
  Threat actor (claimed): karuhunters
  Impact: Large user PII exposure; hashed passwords may be cracked if weak. Elevated risk for account takeover.
- **Solok District Court - Indonesia (Judicial / Public Service) Claim:** 3,718 violation/case records posted.
  Data reportedly exposed: violation IDs, names, fines, license plates, legal articles, addresses, case details.
  Threat actor (claimed): WASHD
  Impact: Sensitive legal and personally identifying case information exposed; privacy and operational implications for citizens.
- **Hamdard Pakistan - Pakistan (Pharmaceutical / Education) Claim:** ~6,000 records leaked.
  Data reportedly exposed: personal details (name, marital status), department, email, mobile number, etc.
  Threat actor (claimed): KaruHunters
  Impact: PII and contact data exposure; phishing and identity misuse risk.
- **Livelong Wealth - India (Financial Services, Bangalore) Claim:** 7,000 dehashed and 22,000 hashed records.
  Data reportedly exposed: account records with both plaintext and hashed credentials.
  Threat actor (claimed): x_JackTheRipper_x
  Impact: High - financial services data plus dehashed credentials represent an elevated fraud and takeover risk.
- **Nepal Ministry of Agriculture and Livestock Development - Nepal (Government) Claim:** 165 records leaked.
  Data reportedly exposed: names, emails, contact numbers, user types, statuses, roles.
  Threat actor (claimed): Purpl0pi0d
  Impact: Limited by number but still sensitive for government staff; could facilitate

targeted attacks.

- **Berkeley County Government - United States (Local Government)**
  Claim: Source code leak from a government web property.
  Data reportedly exposed: source code and associated repository artifacts.
  Threat actor (claimed): skra1a
  Impact: Source disclosures can reveal internal logic, credentials, or configuration leading to follow-on exploitation.
- **Republic Tax Relief - United States (Tax/Professional Services)**
  Claim: 3,040 user records leaked.
  Data reportedly exposed: full names, signatures, addresses, Social Security Numbers (SSNs), phone numbers, partial credit card details (last 4 digits, expiration dates, CVVs reported).
  Threat actor (claimed): harvardhan
  Impact: Very high - exposure of SSNs and payment data significantly increases identity theft and fraud risk.
- **Gobierno de San Juan - Argentina (Provincial Health System)**
  Claim: ~992,815 patient records leaked.
  Data reportedly exposed: provider, patient names, ID numbers, DOB, gender, province, department, locality.
  Threat actor (claimed): Z1k3n
  Impact: Very high - mass health data exposure with regulatory and patient privacy implications.
- **Liverpool Canoe Club - United Kingdom (Sports/Community)**
  Claim: Membership and payment records leaked.
  Data reportedly exposed: membership and payment records, transaction dates, fees, participant names, event details, membership emails.
  Threat actor (claimed): TERRORISM666
  Impact: Localized but sensitive membership and payment data; financial privacy and fraud risk for members.
- **Vercel - United States (Cloud / Application Platform)**
  Claim: Account and business data leaked.
  Data reportedly exposed: user and business account details and associated account data.
  Threat actor (claimed): purple0piod
  Impact: Platform-level disclosures can have cascading effects on hosted apps and customers if credentials or tokens are present.
- **ePardoseli - Romania (Design / Retail)**
  Claim: Company and client data leaked (detailed company/client information, addresses, and financial data). **Threat actor (claimed):** kaaruhunters
  Impact: Customer privacy and possible financial exposure; reputational and legal risk.
- **Shiprocket - India (eCommerce logistics/platform) Claim:** >8 million records exposed.
  Data reportedly exposed: sensitive information across large dataset (per actor

claim).
Threat actor (claimed): meoow
Impact: Very high scale: logistics platforms hold extensive customer, merchant, and transaction metadata - massive potential for fraud, targeted phishing, and operational disruption.

Observed trends & contextual analysis

- **Scope & sectors impacted:** Government (local and national), healthcare, education, financial services, cloud platform, logistics, and SMBs - indicating attackers target both high-value institutions and high-volume consumer platforms.
- **Data types recurrently exposed:** PII (names, DOB, contacts), government IDs and health IDs, employment/HR data, banking/tax identifiers, and in some cases source code and payment data.
- **Likely root causes:** A mix of misconfiguration and exposed backups, credential compromise (reused/weak passwords), opportunistic data scraping and forum resale. Several claims include hashed password dumps - password cracking risk should be assumed.
- **Actor behaviour:** Most reports are forum or social posts claiming data ownership; some actors attempt monetization via sales or ransom demands, consistent with underground marketplace behaviour.

Strategic Assessment

Key Findings

September 2025 demonstrated a threat landscape characterized by:

1. **Aggressive ransomware ecosystem expansion** with 433 confirmed victims representing a substantial increase in targeting breadth and operational tempo
2. **Rapid vulnerability weaponization**, particularly the SharePoint ToolShell cluster, which became a primary initial access vector within days of disclosure
3. **Sustained politically motivated DDoS campaigns** leveraging low-cost botnets for propaganda-driven disruption
4. **Widespread data exposure incidents** affecting millions of records, primarily through misconfiguration exploitation and credential compromise
5. **Supply chain vulnerabilities** producing cascading operational impacts across aviation, manufacturing, and service provider ecosystems

Threat Landscape Evolution

The convergence of ransomware operations with critical vulnerability exploitation demonstrates an increasingly efficient adversary ecosystem. The SharePoint ToolShell cluster's rapid adoption across multiple ransomware groups illustrates how shared intelligence and tooling accelerate threat actor capabilities. Healthcare, education, and public sector organizations continue to bear disproportionate impact due to limited cyber resilience investment combined with high-value data holdings and operational criticality.

The targeting of cloud and SaaS providers signals a strategic shift toward ecosystem-level compromise, where a single breach can cascade across hundreds of downstream clients. Hacktivist DDoS operations, while producing limited technical disruption, demonstrate sustained coordination and propaganda effectiveness. The pairing of DDoS with defacement and false data-leak claims suggests evolution toward multi-vector psychological operations.

Forward-Looking Threat Projections

Ransomware Operations:

- Continued dual-strategy approach combining opportunistic mass exploitation with targeted high-value campaigns
- Increased focus on cloud service providers and managed service providers for downstream ecosystem leverage
- Further fragmentation with emergence of new RaaS operations lowering entry barriers

Vulnerability Exploitation:

- Accelerating weaponization timelines requiring near-immediate patch deployment
- Continued targeting of authentication bypass and deserialization flaws in enterprise platforms
- Increased exploitation of supply chain and third-party vendor vulnerabilities

Hacktivist Activity:

- Sustained DDoS campaigns aligned with geopolitical developments, particularly in Europe and Middle East.
- Evolution toward multi-vector operations combining DDoS, defacement, and information operations.

Data Exposure:

- Persistent exploitation of misconfigured cloud storage, exposed repositories, and weak authentication
- Growing underground marketplace for PII and credential databases
- Increased targeting of healthcare, government, and financial sector datasets for maximum monetization potential

Adversary Simulation Services from Saptang Labs

The threat landscape outlined in this report makes one reality clear: cyberattacks are no longer limited to opportunistic exploits or isolated incidents. From DDoS campaigns and ransomware operations to advanced espionage and supply-chain intrusions, adversaries are continuously evolving their tactics. Organizations and their vendors face the same exposure, as attackers increasingly exploit third-party connections to bypass strong defenses.

At Saptang Labs, we help enterprises build resilience through adversary simulation services. Our approach goes beyond traditional penetration testing to realistically replicate the tactics, techniques, and procedures (TTPs) of nation-state actors, ransomware gangs, and hacktivist groups. By doing so, we enable organizations to understand how real adversaries would attempt to compromise their infrastructure, data, and people.

What We Deliver

- **Realistic Threat Testing** – Simulate live attack scenarios including DDoS floods, lateral movement, and exploitation of current CVEs
- **Supply-Chain Validation** – Test vendor ecosystems and third-party integrations before attackers exploit them
- **Maximum Kill Chain Coverage** – From reconnaissance to data exfiltration, identify critical gaps across your entire attack surface
- **Actionable Intelligence** – Prioritized remediation roadmaps mapped to MITRE ATT&CK and NIST frameworks
- **Executive Assurance** – Demonstrate measurable security readiness to leadership and stakeholders

Ready to test your defense

Contact: sales@saptanglabs.com