SAPTANG™
Proactive Threat Defence

Monthly Threat Report
AUGUST 2025

Executive Summary

During August 2025, the global cybersecurity landscape experienced a significant surge in malicious activity, driven by advanced persistent threat (APT) actors, hacktivist groups, and highly active ransomware operators. A wave of disruptive incidents including large-scale data breaches, DDoS campaigns, and targeted intrusions impacted critical sectors such as government, finance, healthcare, telecommunications, and manufacturing. These attacks spanned multiple regions, with notable activity across Europe, the Middle East, Asia-Pacific, and North America.

Adversaries exploited both zero-day vulnerabilities and widely deployed but unpatched enterprise platforms, enabling remote compromise, data exfiltration, and service disruption. Ransomware groups expanded their operations globally, while state-aligned campaigns such as China's Salt Typhoon underscored the growing role of cyber espionage in geopolitical conflict. The month also saw a sharp rise in incidents affecting India, ranging from healthcare data leaks and financial fraud to retaliatory cyber strikes.

This report consolidates key developments from August, highlights the most exploited vulnerabilities, and tracks emerging threat trends to help organizations strengthen defenses and mitigate escalating risks in an increasingly hostile cyber environment.

Key Threat Groups

- **Observed No Name** – Actively targeted European entities including Belgium, Spain, Germany, and the Czech Republic. Primary victims included banks, energy companies, telecom providers, and cyber agencies. Activity aligns with pro-Russian operations against EU nations.
- **Hider Nex** – Conducted attacks against Israel, Bahrain, and the United States. Targets included banks, ministries, hospitals, utilities, and transport regulators, suggesting access to sizeable botnet resources and broad targeting capability.
- **Keymous+** – Focused on high-profile and symbolic targets such as ministries of health, financial services, and international institutions (including the International Court of Justice). The goal appeared to be reputational impact rather than technical disruption.
- **Dark Storm** – Carried out opportunistic campaigns in Iraq, Syria, Japan, and the United States, impacting government entities, telecoms, universities, and public platforms. This group displayed less consistency in targeting but widespread opportunism.
- **Other regional actors** – Engaged in smaller-scale operations in the Philippines, Armenia, and Norway, typically against universities, energy firms, and local government services.

Targeted Regions and Sectors

Regions:

- Europe (Belgium, Spain, Germany, Czech Republic, Norway), Middle East (Israel, Bahrain, Iraq, Syria), Asia-Pacific (Japan, Taiwan, Philippines), and North America (USA).

Sectors Impacted:

- Government and municipal services
- Financial services and banking infrastructure
- Critical infrastructure (energy, utilities, telecom, and transport)
- Healthcare and education
- Private corporations including airlines, IT service providers, automotive, and retail
- Attack Characteristics

Type of attacks:

- Most incidents involved volumetric DDoS floods and application-layer attacks intended to overwhelm public-facing portals.

Duration and impact:

- Attacks typically caused short-lived service degradation or outages; however, no evidence of prolonged disruption was observed.

Tactics and infrastructure:

- Botnets and DDoS-for-hire platforms were leveraged extensively.
- Attacks were often launched in waves, targeting multiple organizations in parallel.
- Propaganda campaigns were used to amplify the perceived scale of operations, with responsibility claimed through Telegram channels, dark web forums, and social media.

Threat Actor Motivation

The primary motivation for driving these campaigns appears to be:

- Political alignment with ongoing geopolitical conflicts (e.g., pro-Russian activity against EU states, anti-Israel sentiment).
- Propaganda and visibility, with many groups exaggerating impact to gain recognition in hacktivist communities.
- Psychological operations, aiming to erode public trust in government and corporate resilience.

DDoS Activity Analysis

Overview

During the reporting period, several Distributed Denial-of-Service (DDoS) campaigns were observed across multiple regions like African, Asian and Middle East regions. Many of these attacks were carried out by hacktivist groups, often politically motivated and aligned with ongoing geopolitical tensions. The operations primarily targeted government services, financial institutions, critical infrastructure, and private organizations, aiming to disrupt services and generate media attention rather than causing long-term outages.

Outlook of Attack

a. DDoS attacks will likely continue to serve as a **low-cost, high-visibility tactic** for hacktivist groups.
b. European and Middle Eastern organizations are expected to remain primary targets due to their political alignments.
c. Campaigns may evolve into **multi-vector operations**, combining DDoS with website defacements, data-leak claims, or credential dumps to maximize reputational damage

Most Exploited Vulnerabilities – August 2025

During August 2025, several high-impact vulnerabilities were actively exploited in the wild, with attackers focusing on widely deployed enterprise platforms such as Citrix, Trend Micro, SAP, Microsoft Office, and cloud services. The following table highlights the top exploited CVEs this month, their severity, and key technical context. These flaws were observed in both targeted intrusions and opportunistic mass exploitation campaigns.

Key Observed CVEs

- **CVE-2025-7775 (Citrix NetScaler ADC/Gateway, CVSS 9.2)**

  Heap/stack memory-overflow in request processing allows unauthenticated attackers to trigger **remote code execution (RCE) or denial-of-service** on exposed appliances. Widely targeted in external attack surfaces.

- **CVE-2025-5777 ("Citrix Bleed-2", CVSS 9.3)**

  Insufficient input validation leading to **out-of-bounds reads/writes**. When chained with other flaws, this results in **RCE or sensitive information disclosure**. Confirmed as a key focus for threat actors.

- ## CVE-2025-48384 (Git Server, CVSS 8.0)

  Specially crafted repository metadata or hooks can cause arbitrary **command execution** during repo operations. Exploitation depends on configuration but poses significant risk for DevOps pipelines.

- ## CVE-2025-8875 & CVE-2025-8876 (N-able N-Central, CVSS 9.4 each)

  Insecure deserialization and command injection flaws in the N-central management platform, allowing **unauthenticated remote command execution**. Added to CISA's Known Exploited Vulnerabilities (KEV) catalog in August.

- ## CVE-2025-54948 & CVE-2025-54987 (Trend Micro Apex One / Management Console, CVSS 9.8)

  Pre-auth OS command injection and authentication bypass in Trend Micro's on- prem management interfaces. These flaws are being **exploited in the wild**, leading to full product compromise.

- ## CVE-2025-31324 & CVE-2025-42999 (SAP NetWeaver, CVSS 10.0 & 9.1)

  Combination of **unrestricted file upload** and **insecure deserialization** vulnerabilities allows RCE on SAP NetWeaver servers. Public exploit code exists, and active exploitation has been confirmed.

- ## CVE-2025-43300 (Apple Image I/O, CVSS 8.8)

  Out-of-bounds write when parsing crafted images, leading to **memory corruption and arbitrary code execution**. Exploited as a **zero-day in targeted campaigns** before Apple's emergency patch release.

- ## CVE-2025-53767 (Azure OpenAI, CVSS 10.0)

  A critical **Elevation of Privilege (EoP)** vulnerability in **Azure OpenAI services**, caused by **Server-Side Request Forgery (SSRF)** (CWE-918), which could allow attackers to escalate privileges.

- **CVE-2025-53733, CVE-2025-53740, CVE-2025-53784 (Microsoft Word/Office, CVSS 8.4 each)**

  Multiple **memory corruption and use-after-free vulnerabilities** in Word and Office documents allow attackers to execute arbitrary code when victims open malicious attachments. All three were **exploited in the wild**, driving urgent patch adoption.

- **CVE-2025-34028 (Commvault Command Center, CVSS 10.0)**

  Path traversal during archive extraction allows attackers to drop web shells and achieve **pre-auth RCE**. PoC code is publicly available, and exploitation has been reported.

Assessment

The trend this month indicates:

- **Citrix and Trend Micro** remain prime targets for exploitation due to their wide deployment in enterprise environments.
- **Cloud services (Azure OpenAI)** are increasingly being targeted, highlighting adversaries' interest in tenant-level privilege escalation and data exfiltration.
- **SAP NetWeaver and Commvault** flaws represent highly critical pre-authentication RCE vectors with public exploits available.
- **Microsoft Office vulnerabilities** continue to be leveraged in phishing and email-borne attack chains.
- Exploits are heavily focused on **remote command execution**, **authentication bypass**, and **deserialization flaws**, which offer attackers broad post-exploitation opportunities.

Ransomware Activity – August 2025

Ransomware remained one of the most disruptive cyber threats throughout August 2025. The month witnessed **a significant surge in victim disclosures**, with over **300 confirmed cases across more than 40 distinct ransomware operations**. This demonstrates both the resilience of established groups and the increasing fragmentation of the ransomware ecosystem, where smaller or rebranded groups seek to capitalize on the profitability of extortion-driven attacks. The landscape this month was defined by a **dual dynamic**, highly active, **well-established gangs** like **Akira, Qilin, Beast, Everest, Play, and Black Byte**, which collectively accounted for the majority of reported victims. A growing number of **emerging or opportunistic groups** such as **Brain Cipher, Direwolf, Cloak, and Flocker**, showing that the ransomware-as-a-service (RaaS) model continues to lower the barrier for entry.

1. Ransomware Ecosystem Activity

- **Victim Volume:** Over **300 organizations** publicly listed across leak sites.
- **Most Active Gangs: Akira, Qilin, Beast, Everest, Incransom, Play and Safepay**.
- **Sectoral Impact:** Healthcare, education, law firms, finance, industrial manufacturing, and SaaS/cloud platforms were disproportionately affected.
- **Global Reach:** Victims spanned **North America, Europe, Asia, and Latin America**, reflecting a broad targeting strategy unconstrained by geography.

2. Detailed Breakdown of Major Groups

• Akira – Opportunistic Expansion

- **Victim Count:** 50+ confirmed victims.
- **Victim Profile:** Diverse – law firms, architectural firms, engineering consultancies, logistics companies, IT service providers, and manufacturers.
- **Notable Victims:** Insero & Co. CPAs (US), Cevital (Algeria), GWU-Umwelttechnik GmbH (Germany), Sweetener Supply (US).
- **Tactics:** Akira continues its **opportunistic compromise strategy**, relying on vulnerabilities in **VPNs, remote services, and unpatched enterprise applications**. Its victim spread indicates **no sectoral boundaries**, targeting both large and small entities.

• Qilin – Large-Scale Industrial & Education Targeting

- **Victim Count:** 60 victims, one of the highest this month.
- **Victim Profile:** Heavy concentration in **manufacturing, education, healthcare, and logistics**.
- **Notable Victims:** St Thomas More Catholic High School (UK), Haeger & Schmidt Logistics (Germany), CIMEXSTEEL (Czech Republic), Uganda Electricity Transmission Co. Ltd.
- **Tactics:** Qilin's campaigns reveal **a systematic approach** – combining **network penetration and lateral movement** with selective double-extortion tactics (data exfiltration + encryption). Its focus on **supply-chain entities and public institutions** highlights its goal of high-impact disruption.

• Beast – Public Services & Community Targets

- **Victim Count:** 30 victims.

- **Victim Profile:** School districts, hospitals, legal services, SMEs.
- **Notable Victims:** Huron Regional Medical Center (US), Winner School District (US), Grand Rapids Metrology (US).
- **Tactics:** Beast's campaigns are notable for **targeting mid-tier organizations** that may lack mature defenses but handle sensitive community or healthcare data, making them highly susceptible to ransom demands.

• Everest – High-Value, High-Visibility Attacks

- **Victim Count:** 15.
- **High-Profile Victims:** Mailchimp, Grayscale Investments, Crumbl, Pacific HealthWorks. **Assessment:** Everest distinguishes itself by going after **brand-recognizable and reputationally sensitive organizations**, using public pressure as leverage.
- This reflects a trend toward **reputation-driven extortion** beyond financial theft.

• Play – Consistent Global Campaigns

- **Victim Count:** 20+ organizations.
- **Victim Profile:** Aerospace, engineering, logistics, IT services, and manufacturers.
- **Notable Victims:** Quartus Engineering, Jamco Aerospace, Travancore Analytics.
- **Assessment:** Play continues to act as a **persistent threat actor**, balancing volume with high-value industrial targets. Its operations often exploit **unpatched VPN and RDP exposures**.

• Incransom – Focus on Nonprofits & SMBs

- **Victim Count:** 25+.
- **Victim Profile:** Religious organizations, schools, healthcare, and small businesses.
- **Notable Victims:** Radford City Schools (US), Louis Tieu DDS MD (US), Netstar (South Africa).
- **Assessment:** Incransom reflects the **long-tail threat of ransomware** – smaller gangs targeting community institutions that often lack incident response resources, ensuring quick payouts.

- **Medusa – Low Volume, High Impact**
    - **Victim Count:** 5, but in **high-value sectors**.
    - **Notable Victims:** Franklin Pierce Schools (US), White Coffee Corporation (US), PANSARD & ASSOCIES (France).
    - **Assessment:** Medusa maintains a **selective victimology**, focusing on
    - **strategically chosen organizations** where disruption ensures leverage.

3. Sectoral & Geographic Impact

- **Healthcare & Education:**
  Examples: Cookeville Regional Medical Center, Radford City Schools, Franklin Pierce Schools.
  Healthcare remains an attractive target due to the **criticality of patient data and service continuity**, while schools often lack adequate defenses.
- **Financial & Legal Services:**
  Examples: Vinson & Elkins LLP, Insero & Co. CPAs, Philadelphia Investment Partners, Grayscale Investments.
- Ransomware groups recognize that **financial/legal firms are both data- rich and reputation-sensitive**, ensuring extortion leverage.
- **Manufacturing & Industrial Supply Chains:**
  Examples: MGM Transformer, Hytrol, Geotec, Haeger & Schmidt Logistics.
  Manufacturing disruptions ripple across supply chains, amplifying pressure on victims.
- **Cloud & SaaS Providers:**
  Example: Mailchimp compromise (Everest).
  The inclusion of **cloud and SaaS companies** in victim lists highlights attackers' strategic shift to **ecosystem-level disruption**.
- **Public Sector & Communities:**
  Examples: Winner School District, multiple local governments, nonprofits.
  Smaller community organizations continue to suffer **disproportionately high targeting rates** due to underfunded cybersecurity postures.

4. Trends & Strategic Assessment

- **Fragmented Ecosystem:** The sheer diversity of active gangs shows the ransomware economy is **splintering into multiple smaller actors**, many of whom imitate the methods of larger groups.
- **Cloud & SaaS in Crosshairs:** Attacks on **Mailchimp** and financial SaaS services point to a **pivot toward service providers**, where one breach can impact multiple downstream clients.

- **Healthcare & Education Remain Vulnerable:** These sectors face **sustained targeting**, highlighting the need for urgent investment in resilience.
- **RCE Exploitation:** Multiple ransomware gangs are **leveraging critical CVEs** (Citrix Bleed-2, Commvault RCE, SAP NetWeaver file upload) as **initial access vectors**, underscoring the convergence of vulnerability exploitation and extortion operations.
- **Future Outlook:** Expect ransomware operators to further adopt **opportunistic "spray-and-pray" exploitation campaigns** of newly disclosed CVEs, while continuing to selectively target **cloud services, healthcare, and financial sectors** for maximum leverage.

Indian Cyber Incidents – August 2025

August 2025 witnessed a surge of cyber activity impacting Indian government agencies, financial institutions, healthcare providers, and civilian users. Threat actors ranging from **Pakistan-based APTs** to **hacktivist collectives** orchestrated espionage, fraud, ransomware attempts, and large-scale data leaks. Below is a consolidated overview of the major incidents observed during the month.

1. Nationwide Targeting of Govt, BFSI, and Healthcare

CERT-In reported **1.5 million cyberattacks**, with around **150 successful intrusions**, against Indian government, banking, and healthcare institutions. Seven APT groups from Pakistan, Bangladesh, Indonesia, and the Middle East coordinated the offensive after the **Pahalgam attack**, leveraging phishing campaigns, DDoS strikes, and exploitation of known vulnerabilities.

Impact: Heightened cyber alert posture across critical sectors; multiple IOCs shared by CERT-In.

2. Spyware Campaign: 'Dance of the Hillary'

Indian civilians and officials were targeted by a large-scale malware campaign dubbed **'Dance of the Hillary'**, spreading through phishing links and compromised social media platforms. Attributed to **Pakistan-based operators**, the spyware harvested personal data, credentials, and sensitive communications.

Impact: Widespread infections, espionage potential against public and private entities.

3. Star Health Breach – 7.24 TB of Data Leaked

A hacker operating under the alias **'xenZen'** leaked **7.24 TB of sensitive health data**, affecting **31 million customers** of **Star Health Insurance**. The stolen information included medical records and PII, disseminated via **Telegram chatbots and dark web sites**. Executives received direct threats, compounding the breach's severity.

Impact: One of India's largest healthcare data exposures; reputational damage and regulatory scrutiny.

4. Financial Sector on Alert – BSE Advisory

The **Bombay Stock Exchange (BSE)** issued a security advisory after CERT-In flagged potential threats against financial institutions. Risks included **ransomware, DDoS, and supply-chain intrusions** aimed at banks, stock exchanges, and NBFCs.

Impact: Sector-wide defensive hardening and rapid patch rollouts.

5. Fraud Networks Across Bihar and Telangana

Bihar Cyber Fraud Gang: Over **200 bank accounts** tied to Pakistan-linked operatives were used for large-scale fraud. Busted under **Operation Sindoor**, the network exploited single-use mule accounts.

Telangana Cybercrime Network: The **TGCSB** arrested 20 members, including a bank manager, seizing **27 mule accounts** linked to **515+ fraud cases**. Fake job offers, trading apps, and insider collusion enabled the scams.

Impact: Exposure of deep-rooted financial fraud ecosystems with international ties.

6. Hacktivist-Driven DDoS Campaigns

Hacktivist groups from Southeast Asia disrupted over **100 Indian organizations**, primarily targeting **government portals, financial services, and telecom providers**. While service availability was temporarily affected, no confirmed data breaches were reported.

Impact: Highlighted the geopolitical dimension of cyber disruptions.

7. Defacements & Service Disruptions

Ulhasnagar Municipal Corporation website was defaced with religious propaganda, forcing temporary shutdown.

Nippon Life India Asset Management suffered a cyberattack disrupting its web and mobile services on April 9 (disclosed this month), with investigations ongoing.

Impact: Erosion of public trust in municipal and financial digital services.

8. Indian Cyber Force Retaliation

Following the Pahalgam incident, the **Indian Cyber Force(ICF)** conducted retaliatory cyber strikes against **Pakistani institutions**, including Habib Bank, Euro Oil, Federal Board of Revenue, and several universities. Attacks involved **DDoS, breaches, and defacements**.

Impact: Visible escalation in bilateral cyber hostilities.

9. Crypto Sector Under Fire

North Korea's **Lazarus Group** successfully breached **WazirX**, exploiting smart

contract flaws in its wallet infrastructure. Unauthorized withdrawals and service disruptions were reported, raising alarms across the Indian crypto ecosystem.

Impact: Financial losses and reduced trust in Indian exchanges; regulatory focus on crypto security.

Summary

August 2025 reflected **high-intensity cyber conflict** involving **foreign APT groups, fraud syndicates, and hacktivists**, alongside **retaliatory operations by Indian forces**. The month underscored vulnerabilities across **healthcare, finance, defense, identity services, and critical infrastructure**. Data theft, espionage, and financial fraud remain persistent risks, reinforcing the need for **multi-layered defense strategies and rapid incident response mechanisms**.

Global Data Breaches – August 2025

August 2025 saw a **wave of high-profile breaches** impacting defense contractors, government institutions, healthcare providers, and global corporations. Threat actors leveraged exposed directories, misconfigured services, insider compromise, and underground forum sales to exfiltrate massive datasets. Below is a consolidated overview of the top reported breaches this month.

1. Northrop Grumman (USA – Defense & Space)

On **August 4, 2025**, a forum user advertised alleged leaks of **sensitive defense project data** spanning 2015–2019. The actor claims to have compromised a **senior developer's account**, exfiltrating targeting pod configurations (LITENING ATP

data), aircraft deployment forms, training reports, and location-specific documentation tied to multiple U.S. bases.

Impact: Potential exposure of classified defense project information; authenticity still unverified.

2. SANIPES (Peru – Fisheries Regulator)

Threat actor **Gatito_FBI_Nz** leaked over **4,200 internal documents** from

SANIPES, Peru's fisheries regulatory body, on **August 5, 2025**. The breach, allegedly due to an **exposed directory**, contained payment records, audit reports, and internal correspondence in PDF/DOCX/PNG formats.

Impact: Exposure of regulatory and financial records; reputational damage for government transparency.

3. Legiit.com (USA – Outsourcing/Offshoring)

On **August 4, 2025**, actor **Jurak** advertised a **database of 330,000 users** from Legiit.com. The dataset allegedly includes **full PII of buyers and sellers** along with financial transaction histories. The database was listed for **$500 via escrow**.

Impact: Significant PII and financial data exposure for freelancers and outsourcing professionals.

4. Critical Sector Targeting

Defence Sector: APT36 used spear-phishing emails to spread **Crimson RAT**, targeting defense contractors and government personnel.

ICICI Bank: A malware implant via a **compromised vendor portal** was detected through SIEM anomaly analytics; no major breach reported.

UIDAI (Aadhaar Services): Brief **DDoS attack** disrupted authentication, mitigated quickly without data loss.

DigiLocker: CERT-In identified an API token validation flaw exposing limited user documents, which was patched promptly.

DRDO: Phishing emails with malicious PDFs attempted to compromise researcher accounts for espionage; blocked before execution.

Central Bank of India: Attackers cloned domains to harvest customer credentials, exploiting DNS misconfigurations.

AIIMS Delhi: A ransomware attempt—linked to 2022 attackers—was thwarted before encryption of patient systems.

India Critical Infrastructure (SCADA/OT): CERT-In flagged **Operation Bunyān al-Marsūs**, targeting energy, transport, and government IT systems via malware and phishing vectors.

Impact: Demonstrates persistent targeting of

India's most critical assets by state-aligned APTs.

5. Ministry of Health (Sri Lanka – Government Sector)

DarkForums user **Kazu** offered **398,769 records in JSON format**, allegedly stolen from Sri Lanka's Ministry of Health, on **August 11, 2025**. The data was listed at

$300, with a **$3,000 ransom demand** attached.

Impact: Compromise of national healthcare records, highlighting persistent gaps in government cyber defense.

6. Guitar Zoom (USA – E-Learning)

Actor **N1KA** leaked a database containing **23,869 customer records** from Guitar Zoom on **August 10, 2025**. Exposed data includes emails, product identifiers, purchase totals, and metadata.

Impact: Loss of customer trust in online education platforms.

7. UseRH (Brazil – Human Resources)

On **August 11, 2025**, actor **NemeaLocker** claimed responsibility for breaching UseRH, exposing **10,419 HR platform records** with names, emails, and user details.

Impact: HR-related personal data leakage, affecting employee security and compliance risks.

8. Archinect (USA – Architecture & Planning)

Actor **NemeaLocker** also claimed a **full breach of Archinect**, leaking **373,000 records** on **August 10, 2025**. Data includes user contact information and account metadata.

Impact: Substantial community-wide exposure of professional networking data.

9. Digo SA (Saudi Arabia – Marketing & Sales)

Actor **N1KA** leaked **11,621 records** from **Digo SA** on **August 18, 2025**, including CVs, job applications, and sensitive personal/professional information.

Impact: Exposure of candidate and employee records in a competitive corporate sector.

10. FACO PARIS (France – Education)

Threat actor **ghidra** advertised a breach of **FACO PARIS**, leaking highly sensitive student data on **August 18, 2025**. The breach reportedly includes:

- **1,248 student pictures**
- **5,448 ID/banking documents (IDs, passports, IBANs)**
- **3,212 course records**
- **1,957 student records with 1,000 IBANs**

Impact: Severe exposure of student identities and financial details; high potential for fraud.

11. German Manufacturing Company (Germany – Manufacturing)

On **August 13, 2025**, actor **betway** advertised **188,000 records** from a German manufacturer, including **101,000 phone numbers and 102,000 emails** along with names, addresses, and account data.

Impact: Corporate and personal contact data exposure; risk of industrial espionage.

12. ProtectHealth (Malaysia – Healthcare)

Actor **stepbro** listed a **2.56M patient record dataset** from ProtectHealth on

August 21, 2025. Data includes full identities, DOBs, ID numbers, program details, and account balances. Sold for **$800 (full DB)**, with **sample packs available for** $100.

Impact: Large-scale patient data breach, one of Malaysia's biggest in recent years.

13. Telefónica (Spain – Telecommunications)

Threat actor **Zmata** claimed a **106 GB breach of Telefónica** on **August 20, 2025**. Exploiting a **Jira misconfiguration**, the actor exfiltrated **385,311 files** in 12 hours, including customer identities, employee details, source code, contracts, HR files, and invoices.

Impact: Critical breach of telco infrastructure with both corporate and customer fallout.

14. Ministry of Public Health (Ecuador – Government)

On **August 26, 2025**, actor **Gatito_FBI_Nz** leaked sensitive data from Ecuador's Ministry of Public Health — including **national IDs, clinical records, procurement contracts, and government documentation**. Notably, this is the **second breach of the agency in 2025**.

Impact: Repeated compromise of government health data; systemic security weaknesses exposed.

15. Civil Service Commission (Philippines – Government)

Actor **888** leaked a **76,718-record dataset** from the Civil Service Commission (CSC) on **August 27, 2025**. Records include IDs, names, roles, contact details, and organizational information.

Impact: Exposure of government employee data; insider and phishing risks amplified.

16. Ferplast World (UK – E-commerce)

Actor **N1KA** leaked **11,000 customer records and 13,000 addresses** from Ferplast World on **August 26, 2025**. Exposed data includes names, emails, phone numbers, physical addresses, and login credentials (hashed & salted).

Impact: E-commerce consumer data breach, affecting customer privacy and trust.

Summary

This month's breaches highlight **recurring weaknesses across multiple industries**:

- **Government & Public Health:** (Sri Lanka, Ecuador, Philippines, Malaysia) – critical datasets exposed, risking citizen data.
- **Defense & Manufacturing:** (Northrop Grumman, German manufacturer) – targeting sensitive industrial and military information.
- **Corporate Platforms:** (Legiit, Archinect, Ferplast) – mass PII theft from global user communities.
- **Telecommunications & Critical Services:** (Telefónica, Protect Health) – large- scale breaches with national-level implications.

Overall, August 2025 reinforces the **expanding global attack surface**, with **APT-linked actors, financially motivated hackers, and hacktivists** actively exploiting systemic flaws to monetize or weaponize stolen data.

Global Cyber Incident Highlights – August 2025

August 2025 witnessed a surge in **global cyber threats**: from state-sponsored espionage campaigns like **Salt Typhoon**—now spanning 80+ countries and multiple critical sectors—to widespread ransomware, data leaks, and phishing attacks targeting government, healthcare, finance, and telecom sectors. The volume and scale of these breaches emphasize the escalating complexity of cyber threats and underline the urgent need for **coordinated defenseframeworks**, rapid threat intelligence sharing, and robust incident response across borders.

1. Salt Typhoon: Escalating Global Chinese Cyber Espionage

- In a joint advisory dated **August 27, 2025**, the **FBI**, along with intelligence agencies from Five Eyes members and other nations—including Finland, Germany, Poland, the Netherlands, and the Czech Republic—revealed the dramatic expansion of the Chinese state-aligned **Salt Typhoon** hacking campaign. Originally focused on U.S. telecommunications providers, the campaign

now affects over **80 countries** and **200 U.S. organizations**, spanning telecom, government, transportation, lodging, and military infrastructure sectors.

- The attackers exploited vulnerabilities in network infrastructure, particularly in routers to exfiltrate over **1 million call records**, sensitive law enforcement communication systems, and GPS metadata. The operation, tied to Chinese
- intelligence agencies and supported by firms such as Sichuan Juxinhe (already sanctioned by the U.S.), is being called one of the most pervasive espionage campaigns in recent memory—far exceeding traditional norms.
- Detailed technical guidance, vulnerability indicators, and detection strategies have been shared via an extensive advisory by CISA/NSA/FBI and partners to aid global defenders.

2. UNC6384 Delivers Malware via Fake Captive Portals

- Researchers at **Google Threat Intelligence Group** reported that **UNC6384**, a Chinese state-aligned threat group, has been distributing malware families such as **CANONSTAGER** and **SOGU.SEC** via **fake captive portal updates**. These deceptive updates, masquerading as legitimate network logins, specifically target diplomats and sensitive entities.

3. Colt Technology Services Hit by Warlock Ransomware

- UK-based telecom provider **Colt Technology Services** suffered a **Warlock ransomware** attack on **August 12, 2025**. Exploiting a SharePoint vulnerability (**CVE-2025-53770**), attackers stole hundreds of gigabytes of data, including employee salaries, contracts, and financial records, while disrupting customer portals and causing widespread service interruptions.

4. iiNet Breach Exposes ~280,000 Customers (Australia)

- Australian ISP **iiNet** disclosed that unauthorized third-party access to its order management system compromised roughly **280,000 customer records**—including email addresses, landline numbers, usernames, setup passwords, and home addresses—for both current and former customers.

5. UK MoD Contractor Breach—Afghan Refugee Data Compromised

- The outsourcing firm **Inflite The Jet Centre Ltd**, linked to the UK Ministry of Defence, was breached, exposing personal information of approximately **3,700 Afghan refugees** involved in relocation programs.

6. Farmers Insurance Vendor Breach Impacts 1.1 Million

- A third-party vendor breach impacted **Farmers Insurance**, exposing sensitive personal data of **1.07 million customers**, including names, dates of birth, driver's license numbers, and partial Social Security numbers.

7. Inotiv Pharma Hit by Qilin Ransomware

- **Inotiv**, a U.S. pharmaceutical firm, endured a **Qilin ransomware** attack that encrypted critical systems and resulted in the theft of **176 GB** of data (around 162,000 files), including proprietary research and internal documentation.

8. Orange Belgium Breach Affects ~850,000 Customers

- Telecom provider **Orange Belgium** experienced a cyber breach affecting **850,000 customers**, exposing names, phone numbers, SIM, and PUK codes. While financial and password data remained secure, the incident raised significant privacy concerns.

9. Data I/O Ransomware Disrupts Electronics Manufacturing

- **Data I/O**, a U.S.-based electronics firm, was hit by an operational ransomware attack, severely disrupting shipping and manufacturing workflows. Financial losses are expected to be substantial.

10. ShinyHunters Campaign Hits Google, Air France & Bouygues

- **Google**: Exposed 2.55 million business contact records from Salesforce.
- **Air France**: Customer data leakage including names, emails, phone numbers, and Frequent Flyer information.
- **Bouygues Telecom**: **6.4 million** customer accounts breached.

11. Workday Vendor Breach via ShinyHunters

- A third-party vendor connected to **Workday** was compromised by ShinyHunters, exposing customer contact details—names, emails, and phone numbers—linked to organizations using the service.

12. ManpowerGroup Leak by RansomHub

- **RansomHub** ransomware actors breached **ManpowerGroup**, exfiltrating approximately **500 GB** of data covering **144,000 individuals**, including SSNs, addresses, and sensitive corporate documents.

13. Canadian House of Commons Internal Data Breach

- A cyber intrusion exploited a vulnerability in IT systems, exposing internal data of parliamentary staff—including names, job titles, office locations, and emails.

14. CIRO Data Exposure

- The **Canadian Investment Regulatory Organization (CIRO)** suffered a cyberattack, resulting in exposure of employee and member firm data. Remediation and alerts are currently underway.

15. HCK Capital (Malaysia) Hit by Dire Wolf Ransomware

- **HCK Capital Group** fell victim to a **Dire Wolf** double-extortion ransomware attack, leaking **173 GB** of sensitive data, including legal, financial, customer details, and passport records.

16. Global Phishing Campaign "UpCrypter" & Pro-Ukraine Hacktivist Activity

- **UpCrypter**: A widespread phishing campaign distributing multiple RATs across sectors such as manufacturing, tech, healthcare, construction, and retail.
- **Cyber Anarchy Squad**: A pro-Ukraine hacktivist group disrupted a Russian investment platform, leaking internal files.

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 defenses?

Contact: sales@saptanglabs.com