www.saptanglabs.com

SAPTANG

Proactive Threat Defence.

Monthly Threat Report

July 2025

3iHub
National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP
Microsoft for Startups
Founders Hub
NVIDIA.
INCEPTION PROGRAM

Table of Contents

Executive Summary

During the month of July 2025, the global cybersecurity landscape witnessed a notable escalation in malicious activity, primarily orchestrated by advanced persistent threat (APT) groups and sophisticated ransomware operators. A series of high-impact security incidents—including data breaches, and precision-targeted intrusions—affected key sectors such as government, insurance, and critical infrastructure. These attacks were observed across multiple geographic regions, notably the Middle East, Asia, Europe, and the Americas.

Adversaries leveraged both newly discovered zero-day vulnerabilities and previously known but unpatched flaws to infiltrate systems, disrupt operations, and exfiltrate sensitive information. The incidents underscore the rapid evolution of threat actor capabilities and tactics, techniques, and procedures (TTPs). This report presents a consolidated analysis of major cyber incidents, highlights commonly exploited vulnerabilities, and identifies emerging threat trends observed throughout the month. The insights provided aim to assist organizations in reinforcing their cybersecurity posture and mitigating risk in the face of an increasingly hostile threat environment.

Key Data Breaches

1. **DayTrans, Indonesia:** Breach by FLIRT exposed 941,000 user records including IDs, emails, billing info, and mobile numbers.

2. **Schrödinger, Germany:** Sentap leaked internal data of Schrödinger which includes financial invoices, legal contracts, and operational details and allegedly sold online.

3. **EH Bildu, Spain:** Cargo, a threat actor is selling unauthorized access to the private email system of EH Bildu, a political organization based in Spain.

4. **Crypto-Verified Database, USA:** Aisdata allegedly selling the database of US based crypto-verified database of 5.6M users for USD. 12,000 which includes personal data of individuals.

5. **MedLife SA, Romania:** Wieko exposed over 2K records of plain text user-password pairs of MedLife SA users for USD. 30 and included a Telegram-based negotiation.

Major Cyber Incidents

1. **Microsoft SharePoint – Zero-Day Exploited Globally:** On July 8, 2025, a Chinese-linked group exploited an unpatched SharePoint zero-day to compromise over 400 on-prem servers globally, including U.S. federal agencies like the National Nuclear Security Administration. Despite emergency patches, persistent access via backdoors remains a risk.

2. **ASI Group – Ransomware Attack by incransom:** Between July 21–22, 2025, Canadian marine services firm ASI Group (asi-group.com) was hit by the incransom gang, resulting in system encryption and theft of internal data.

3. **José Antonio Rodríguez & Advisors – Qilin Ransomware Leak:** On July 17, 2025, Qilin claimed an attack on joseantoniorodriguez.com, a Spanish legal advisory firm, leaking stolen legal and financial records.

4. **Media Broadcast Satellite – 870 GB Data Breach:** On July 17, 2025, Qilin breached German telecom integrator mb-satellite.com, exfiltrating 870 GB of data and posting samples as ransom pressure.

5. **Morrison Companies – Play Ransomware Attack:** On July 16, 2025, U.S.-based real estate services provider Morrison Companies (morrison-usa.com) was targeted by Play group, which encrypted and stole sensitive internal documents.

6. **Palmas del Ixcán – SafePay Ransomware Breach:** On July 16, 2025, Guatemalan agribusiness palmasdelixcan.com was attacked by SafePay ransomware, with threat actors warning of data leaks unless payment is made.

7. **USA – 3,000 Credit Cards on Dark Web:** As of June 30, 2025, a dark web listing advertised the sale of 3,000 stolen U.S. credit card records, indicating a possible recent compromise.

Key Threats

In July 2025, the global threat landscape remained highly volatile, with ransomware attacks, critical vulnerabilities, and data breaches affecting multiple sectors, including healthcare, finance, and critical infrastructure. Noteworthy vulnerabilities disclosed during the month included CVE-2025-5600 (TOTOLINK EX1200T allows remote attackers to take control of the device without needing to log in.), CVE-2025-20286 (Cisco Identity Services Engine (ISE) cloud setups on AWS, Azure, and OCI could let attackers access sensitive data or disrupt services without logging in.), CVE-2025-45854 (JEHC-BPM v2.0.1 allows attackers to upload malicious files and remotely run harmful code on the system.), and CVE-2025-4797 (The "Golo – City Travel Guide" WordPress theme (up to version 1.7.0) has a flaw that lets attackers gain full admin access without logging in, simply by knowing the victim's email address.). These flaws represent significant risks to enterprise environments and have the potential to facilitate unauthorized access, lateral movement, and service disruption if left unpatched.

Ransomware activity continued at a concerning pace, with actors such as PLAY and Safepay executing targeted attacks. Notably, Safepay reportedly compromised APPS Northwest, a healthcare organization in the United States, resulting in potential exposure of sensitive internal documents. Though the extent of data leakage remains unconfirmed, the incident highlights the persistent threat to healthcare infrastructure. In another incident, INC Ransom leaked 12GB of internal data from Community Care Resources (CCR) Wisconsin, a non-profit focused on trauma-informed foster care, and 150GB from Academic Urology & Urogynecology of Arizona, including sensitive patient records. These breaches raise serious concerns regarding patient confidentiality, HIPAA compliance, and ethical risks associated with exposed personal and operational data.

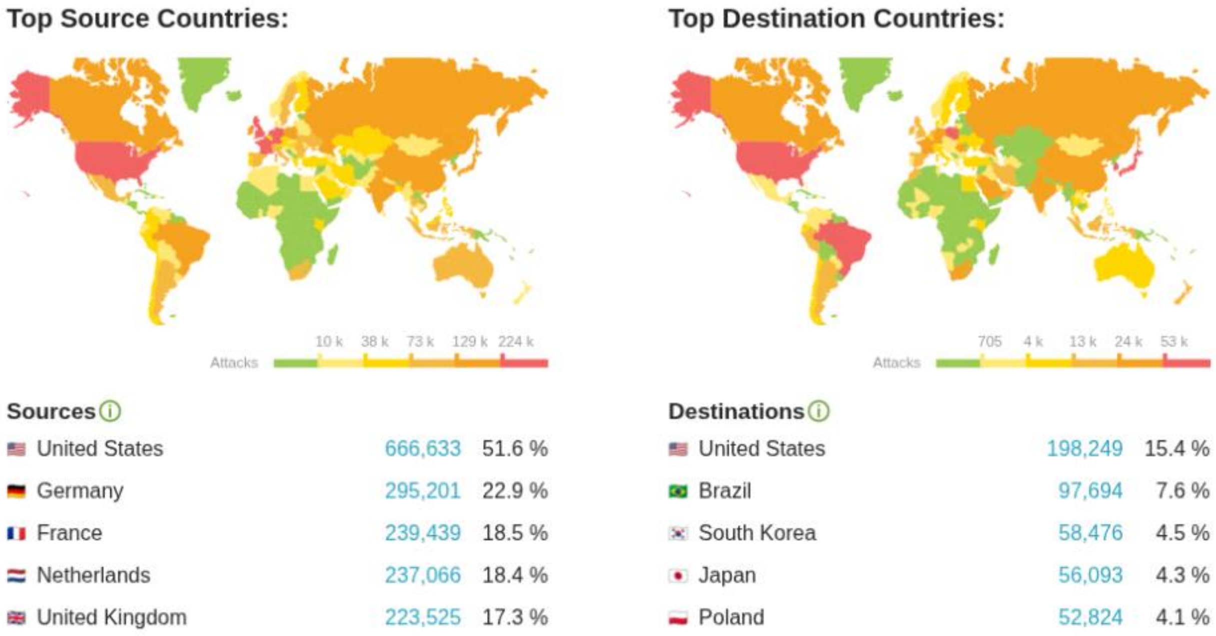
Additionally, underground forums witnessed heightened activity involving the trade of stolen credentials, RDP access, and zero-day exploit kits. Several indicators pointed to increased reconnaissance and initial access attempts across telecommunications and aviation sectors. Concurrently, disruption campaigns—including DDoS attacks and targeted service outages—impacted public-facing services, reaffirming the need for continuous monitoring and threat detection capabilities.

The events of July 2025 emphasize the urgent need for proactive security strategies, including timely vulnerability remediation, ransomware resilience planning, and continuous intelligence-led defense postures.

Threat landscape

Ransomware attacks are happening more often and causing more trouble, while mobile malware takes advantage of how many people use smartphones and tablets. Both threats show that there is an urgent need to improve security measures.

DDoS Activity



Sources		
United States	666,633	51.6 %
Germany	295,201	22.9 %
France	239,439	18.5 %
Netherlands	237,066	18.4 %
United Kingdom	223,525	17.3 %

Destinations		
United States	198,249	15.4 %
Brazil	97,694	7.6 %
South Korea	58,476	4.5 %
Japan	56,093	4.3 %
Poland	52,824	4.1 %

Underground Findings

The findings listed below are among the critical datasets discovered on underground forums in July 2025. Additionally, several threat actors are noted based on their prominent activities during this period.

Global Data Breaches and Leaks

Region	Organization	Significant Data
Vietnam	Vietnamese Health Insurance	A threat actor identified as “show_more” claimed to have breached Vietnam’s Health Insurance system, offering the stolen data for $1000 on Telegram. The exposed dataset reportedly includes sensitive personal information such as full names, email addresses, dates of birth, residential addresses, insurance card and policy

		details, phone numbers, and occupational data. To prove the legitimacy of the breach, the actor shared sample records containing real individuals' information. This incident poses serious risks of identity theft, financial fraud, and privacy violations, significantly impacting the healthcare and insurance sectors. The breach underscores the growing threat of data exploitation by cybercriminals targeting critical national infrastructure.
USA	Cryptocurrency Platforms	A threat actor identified as "btcokiz" advertised unauthorized access to U.S.-based cryptocurrency user accounts, claiming the data was sourced from compromised email inboxes. The exposed information is linked to major platforms such as Coinbase, Kraken, KuCoin, and ByBit, with samples revealing sensitive personal and financial details, including wallet balances ranging from $10,000 to over $2 million USD. The actor further asserted persistent access to these accounts, along with supporting materials such as ID documents, transaction histories, and private communications. This incident underscores a severe compromise within the crypto sector, demonstrating the growing sophistication of financially motivated cybercriminals and the urgent need for enhanced user and platform-level email security controls.
Nigeria	Chartered Institute of	A threat actor known as "Golia" advertised Remote Desktop Protocol (RDP) access for sale to a

	Bankers of Nigeria	Windows Server 2019 instance allegedly belonging to The Chartered Institute of Bankers of Nigeria (CIBN). The actor claims the access provides full administrative privileges, with connectivity to portal.cibn.org and related subdomains. The compromised server is reportedly hosted in France and is said to contain sensitive financial and personal information linked to Nigerian banking professionals. The access was listed for $330, with room for negotiation. This poses a serious threat to institutional integrity, with potential implications for data confidentiality, financial systems, and insider access within the Nigerian banking sector.
Italy	doValue S.p.A.	A cybercriminal identified as “data block” alleged the theft of more than 16 terabytes of data from doValue S.p.A., a leading financial services provider in Italy, along with its affiliated entities. The attacker claims the intrusion affected several interconnected domains, leading to the compromise of database and file servers integrated with Active Directory. The leaked content is said to encompass a wide array of internal corporate files and highly sensitive financial records. This breach, targeting a core player in the financial industry, underscores the increasing risk landscape for European financial institutions and reinforces the urgency for strengthened network segmentation and access control mechanisms.
Malaysia	Malaysian	a threat actor identified as Arikos listed for sale a

	Government Websites	24GB dataset allegedly exfiltrated from two key Malaysian government portals — spa.gov.my (Public Service Commission) and doe.gov.my (Department of Environment). Priced at $1,000 USD for exclusive access, the dump is said to contain over 2.2 million user records, including full names, birthdates, emails, phone numbers, and hashed passwords. Arikos claims the breach exposes multiple structured database tables containing detailed personal and administrative records of Malaysian citizens. If authentic, the incident signifies a severe compromise of national identity data, raising significant concerns around public sector cybersecurity posture and citizen data integrity.
UK / Europe	Baxter Kelly Ltd.	A threat actor using the alias _Sentap advertised a 24GB data leak allegedly sourced from the internal systems of Baxter Kelly Ltd, a UK-based contractor prominent in the home energy retrofit sector. The dataset, priced at $2,000 USD, is being offered for sale on a dark web forum, with communication directed through an email address. The exposed data reportedly contains highly sensitive information, including personally identifiable information (PII) of customers, technical project documents, regulatory compliance files, energy retrofit materials details, and staff certifications such as Gas Safe IDs. Notably, this breach affects a firm accredited under TrustMark, BBA, and CIGA, with operational involvement in the UK

		government's ECO4 and Great British Insulation Scheme initiatives.
USA	Tradeify	Zagoramiy200, a threat actor listed for sale a database allegedly exfiltrated from Tradeify, a U.S.-based financial services provider, on the Exploit.in marketplace. The actor claims the stolen data—originally acquired on June 6 and now reportedly shared among multiple threat actors—contains 40,000 complete user records. The exposed dataset includes sensitive personally identifiable information (PII) and transactional metadata, such as full names, billing addresses, contact numbers, email IDs, states, and order-related details. With an initial bid set at $30,000 and a near price of $40,000, the breach represents a serious threat to affected customers and poses significant reputational and regulatory risk to the financial firm.
Global	Crypto Verified Data	A threat actor operating under the handle "aisdata" advertised a massive database for sale on a cybercrime forum, allegedly containing over 21 million verified cryptocurrency user records from across the globe. The dataset, described as "Crypto Verified," reportedly includes names, email addresses, phone numbers, country codes, and verification timestamps, with validations as recent as June 29, 2024. Sample entries provided in the listing display full user details alongside their verification status and timestamp. The actor has priced the leak at $20,000, offering escrow to

		facilitate transactions. This exposure poses a potential risk to user privacy, particularly in the context of identity fraud and targeted phishing within the crypto ecosystem.
USA	Ticketmaster	The threat actor auden_greyfall advertised a dataset containing over 11 million Ticketmaster e-ticket and customer records, allegedly sourced from a breach of the U.S.-based online ticketing platform Ticketmaster. The exposed data includes full names, email addresses, phone numbers, residential addresses, event details, ticket barcode metadata, and partial payment card information. The actor claimed the breach originated from compromised credentials linked to a third-party cloud storage provider—reportedly Snowflake—with improperly secured access controls and no multi-factor authentication. The scale and sensitivity of the breach poses major risks of ticket fraud, phishing attacks, and identity theft, and reflects the growing threats targeting cloud-integrated service providers in the event management industry.
Singapore	Style Theory	A cyber threat actor operating under the alias “menksoa” publicly advertised unauthorized access to the administrative panel and database of Style Theory, a prominent Singapore-based fashion e-commerce and subscription platform. The actor asserts full backend control of styletheory.co, claiming access to personal records of over 218,000 users and upwards of 2

		million product reviews. The compromised data allegedly contains users' full names, email addresses, contact numbers, and precise physical measurements utilized for tailored deliveries. Moreover, backend privileges for managing inventory, user accounts, reservations, and content moderation were also highlighted, indicating a significant breach with potential operational and reputational consequences for the targeted organization.

Indian Cyber Incidents and Data Breaches

Organization	Significant Data
ShareKhan Ltd.	A dark web actor identified as "RareData" disclosed a significant data breach targeting ShareKhan Ltd., a major Indian investment and brokerage platform. The actor claims to have exfiltrated over 3.4 million sensitive PAN-linked customer records, allegedly sourced from ShareKhan's back-office systems. The leaked dataset reportedly includes personally identifiable information (PII) such as full names, PAN numbers, family references, account types, internal references, email IDs, phone numbers, dates of birth, holding patterns, transaction histories, and branch-level segmentation data. The actor has listed the breach under an exclusive "one buyer only" sale, indicating the potentially high value of this financial intelligence trove. The exposure poses a serious risk of identity theft, targeted fraud, and financial exploitation across India's retail investment sector.
ICAR	The Indian Council of Agricultural Research (ICAR)—India's premier agricultural research institution—suffered a major cyber incident

	that wiped out critical data across its primary data center in Delhi and the disaster recovery replica at NAARM in Hyderabad. The breach resulted in the loss of key records related to recruitment (from Technical Officers up to Deputy Director General), scientist-submitted research projects, financial documentation, internal email communications, and administrative data. The affected entities included the Agricultural Scientists Recruitment Board (ASRB), Indian Agricultural Statistics Research Institute (IASRI), and NAARM. In response, a six-member panel has been appointed to investigate the root causes of the data center failure and develop enhanced security and recovery mechanisms by July 31, 2025. This breach raises serious concerns over operational continuity, institutional transparency, and the protection of national research infrastructure.
CoinDCX	CoinDCX, a prominent Mumbai-based cryptocurrency exchange, suffered a major security breach that resulted in the theft of approximately $44.2 million worth of digital assets. The attack specifically targeted the exchange's hot wallets—wallets connected to the internet for liquidity and operational needs—leading to a significant fund drain. CoinDCX has confirmed that customer assets stored in segregated cold wallets remained unaffected, as those wallets were not connected to the compromised infrastructure. The breach highlights ongoing threats to digital asset exchanges operating in high-risk environments and emphasizes the need for stronger wallet segmentation, real-time monitoring, and incident response capabilities. An investigation is currently underway to identify the exploit vector and mitigate further risk.
Namasthe Telangana	The ransomware group W.A. claimed responsibility for an attack targeting Namasthe Telangana, a private entity functioning within India's Communication Services sector. The specifics surrounding

	the incident remain limited, with no public confirmation regarding data exposure or financial impact. The group's motives and the method of intrusion have not been disclosed, and as of now, no sample data has surfaced to validate the breach. This incident adds to the growing list of cyber threats aimed at Indian media and communication infrastructures, reinforcing concerns about the sector's resilience against targeted ransomware campaigns.
Rattan India Power Ltd.	In July 2025, the threat actor World Leaks reportedly published over 651 GB of data allegedly exfiltrated from RattanIndia Power Limited, a public entity in India's Utilities sector. The leaked archive comprises approximately 476,000 files and includes directories labeled with sensitive classifications such as HR_DATA, IT_SUPPORT, Govt_Correspondence, Direct_Tax, and Bank Power, indicating the potential exposure of confidential personnel records, internal financial documents, government communications, and IT infrastructure details. While the full impact remains under assessment, the scale and nature of the disclosed data suggest significant operational and reputational risks for the organization.
OPaL	World Leaks reportedly published internal data allegedly belonging to ONGC Petro Additions Ltd. (OPaL), a public sector organization operating in India's materials industry. The leaked material appears to include a wide range of administrative and technical documentation, suggesting unauthorized access to internal resources. While the authenticity and impact of the exposure are yet to be officially confirmed, the incident raises concerns about potential data confidentiality risks and the organization's overall cybersecurity posture.
Usha Martin Ltd	The ransomware group W.A. claimed responsibility for an attack on Usha Martin Limited, an Indian multinational manufacturer, and

	published evidence of the breach on its dark web leak site. The threat actor alleged access to sensitive internal information, including network architecture diagrams, asset credentials, NTLM hashes, personnel records, and DNS configurations. Accompanying the post were multiple download links and an archive password, indicating that a data leak had occurred. While the exact volume of data exfiltrated remains unspecified, the exposure of such critical assets poses a substantial security risk to the organization.

Threat Actors

1. INC Ransom

The ransomware group INC Ransom has claimed responsibility for data breaches affecting two U.S. healthcare organizations: Community Care Resources (CCR) Wisconsin and Academic Urology & Urogynecology of Arizona. CCR Wisconsin, a non-profit focused on trauma-informed foster care, suffered a leak exceeding 12GB, potentially compromising sensitive information about foster children, families, and internal processes—posing significant ethical and legal risks. Meanwhile, Academic Urology & Urogynecology of Arizona faced a larger breach of 150GB, which may have exposed data on hundreds of patients. The attackers publicly criticized the organization's inaction, highlighting concerns over patient privacy, HIPAA violations, and regulatory consequences. Both incidents underline serious threats to data security, patient trust, and compliance in the healthcare sector.

2. Safepay

Safepay claimed responsibility for a ransomware incident targeting India-based Planet IT Services. The attackers reportedly compromised internal systems using the Raccoon Infostealer malware, leading to a breach of privileged user accounts and sensitive operational data. A public leak page showed screenshots of backend consoles and internal file servers, sparking concerns about supply chain threats linked to Indian technology firms. Safepay's operations in June marked an intensification of attacks on infrastructure and mid-sized service providers in South Asia.

3. Akira

The ransomware group Akira reportedly targeted Druni, S.A., a Spanish company in the Consumer Discretionary sector known for selling perfumes, makeup, and cosmetics. The attackers claimed to possess over 40 GB of sensitive corporate data, including employee identification documents (like DNI), financial records, project data, customer information, and contracts with major brands such as L'Oréal, Dior, and Chanel. While the breach was publicly listed, it remains unclear whether the data was ultimately leaked or if the organization suffered any confirmed material losses.

4. PLAY

The ransomware group PLAY publicly leaked a portion of sensitive data stolen from CyberlinkASP, a U.S.-based business services and IT provider. The breach involves highly confidential and private information, including client documents, payroll data, tax records, budgets, financial information, and personally identifiable data such as IDs—posing a serious threat to both CyberlinkASP and its clients. The attackers have published this data on multiple dark web sites, warning that the full data dump will be released if there is no response, indicating a clear extortion attempt. Given the nature of the data exposed, the incident is extremely severe, risking regulatory violations, financial losses, reputational damage, and significant disruption for clients relying on CyberlinkASP's services.

5. DragonForce

The threat actor group Dragon Force published a massive 629.1 GB data leak from the official website of the City of Keene, New Hampshire (www.keene.nh.us). This breach affects critical municipal infrastructure and potentially exposes sensitive records such as internal communications, resident data, public service documents, and administrative files. As Keene serves as the county seat and hosts institutions like Keene State College and Antioch University New England, the breach could impact not just city operations but also educational and civic institutions. The exposure of such a large volume of municipal data raises serious concerns regarding privacy, operational disruption, and potential exploitation by other malicious actors. Given the increasing frequency of cyberattacks on local governments, this incident highlights the urgent need for stronger cybersecurity resilience across public sector entities.

6. Payoutsking

Cybercriminal group payoutsking claimed responsibility for leaking a massive 2.5TB of data from Schlemmer Holding GmbH, a German-based automotive and industrial supplier with an estimated annual revenue of $655 million. Although specific contents of the leak remain undisclosed, the scale alone suggests a significant compromise, likely involving sensitive internal documentation, business contracts, technical designs, or employee and client data. This type of breach can have far-reaching consequences, including potential disruption to manufacturing and supply chain operations, reputational damage, legal liabilities, and loss of trust from global automotive partners. As Schlemmer operates in a highly competitive and precision-driven industry, safeguarding intellectual property and confidential business information is critical—and any exposure could severely impact its strategic positioning.

7. WorldLeaks

Dell Technologies, a global leader in computer hardware, software, and IT services, was listed as a victim of a data breach, with confidential information reportedly published online. While the specific nature of the compromised data has not been fully disclosed, the public exposure of internal company materials could have serious implications for Dell’s operations, particularly in its enterprise and government service sectors. As a company heavily involved in digital transformation and cloud computing across critical industries like healthcare and education, any breach undermines customer trust and could potentially expose strategic vulnerabilities. Given Dell's scale—with over 108,000 employees and $95.6 billion in annual revenue—the incident may lead to reputational damage, increased regulatory scrutiny, and a potential loss of business partnerships.

8. Lynx

Nactarome, a leading Italian manufacturer of natural flavors, colors, and functional ingredients for the food and beverage industry, was targeted in a cyberattack that resulted in the unauthorized publication of confidential company documents. The leaked material, published under the title "nactarome_full," is categorized as proof of compromise and labeled confidential, suggesting the exposure of sensitive internal information. Although no personally identifiable information has been publicly confirmed, the breach of proprietary data related to product formulations, research, or strategic operations can severely impact Nactarome's competitive standing in the global market. With over 3,000 views already recorded, the leak poses significant reputational and financial risks to the organization.

9. Everest

The Everest ransomware group launched a cyberattack against Best Price Financial Services, a UK-based financial organization, resulting in the leak of over 7,370 lines of highly sensitive client data. The compromised information includes personally identifiable details such as full names, dates of birth, gender, email addresses, cities, counties, full home addresses (including postcode), telephone numbers, and alternative contact numbers. Such data is not only highly sensitive but also extremely valuable to cybercriminals, as it can be used for identity theft, financial fraud, phishing attacks, and other forms of exploitation. The attackers posted a countdown on their dark web leak site and urged the company to contact them before time ran out, indicating the possibility of further escalation or data exposure if ignored. Given the nature of the financial sector and the volume of personal data involved, this breach poses a serious threat to the privacy and financial security of thousands of clients and could potentially trigger legal consequences and regulatory investigations under data protection laws such as the UK GDPR.

10. Devman

The Devman ransomware group reportedly targeted the Ministry of Labour of the Kingdom of Thailand in a major cyberattack. According to the group's leak site, approximately 300 GB of data was exfiltrated, with the attackers demanding a ransom of 15 million USD. The threat actors also published references to "bigdata.mol.go.th" and "mol.go.th/devman," suggesting the compromise may involve sensitive government datasets. While the exact contents of the leak remain unclear, the public exposure of such a volume of data could have severe implications for national operations, including risks to internal communications, labor-related personal records, and regulatory documents. At the time of reporting, it is unknown whether the Thai government has initiated negotiations, paid the ransom, or taken significant countermeasures to contain the impact. The situation underscores the growing threat of ransomware groups targeting government institutions with large-scale data theft and extortion tactics.

Threat Analysis

Notable Incidents

1. **National Nuclear Security Administration exploited through Microsoft SharePoint Server Vulnerability**

   The National Nuclear Security Administration (NNSA), a U.S. government agency, was impacted by a security breach attributed to the exploitation of a zero-day vulnerability in Microsoft SharePoint Server. While technical indicators suggest unauthorized access may have occurred, there is currently no public confirmation of data exfiltration or material loss resulting from the incident. The situation highlights the critical risks posed by unpatched enterprise software in sensitive government environments.

2. **Major Financial Cyberattack Targets C&M Software, Exposes PIX Network Vulnerabilities**

   C&M Software (CMSW), a Brazil-based financial technology provider, suffered a major cyberattack in which threat actors reportedly used compromised client credentials—allegedly obtained from an insider—to gain unauthorized access to systems connected to the Central Bank's PIX instant payment network. This breach led to large-scale fraudulent transfers from reserve accounts of at least six financial institutions, with estimated losses ranging between R$400 million and R$1 billion. While no individual customer accounts were affected, the incident is considered one of Brazil's most significant financial cyberattacks to date, prompting regulatory investigations and heightened security measures across the sector.

3. **MercadoLibre Suffers Reported DDoS Attack by CyberTeam**

In July 2025, the hacker group CyberTeam reportedly launched a distributed denial of service (DDoS) attack targeting MercadoLibre, Inc., a publicly listed e-commerce and fintech company based in Uruguay and operating in the Consumer Discretionary sector. While the attack allegedly disrupted the platform's accessibility, there is no confirmed evidence of data leakage or disclosure of financial losses resulting from the incident. The organization has not released an official statement regarding the impact or scope of the attack.

4. **RedCuba Targeted in Alleged DDoS Attack by Anonymous**

The hacktivist collective Anonymous reportedly carried out a distributed denial of service (DDoS) attack against RedCuba, a government-affiliated organization in Cuba operating within the Information Technology sector. While the incident was claimed to have disrupted online services, there has been no official confirmation of data compromise or financial losses associated with the attack. The full extent of the impact remains unverified.

5. **Ransomware Attack Reported at Oregon Specialty Group**

An unidentified threat actor reportedly launched a ransomware attack against Oregon Specialty Group, a private organization in the Health Care sector in the United States. The breach resulted in the exposure of sensitive personal data, including patients' first and last names as well as protected health information. Affected individuals were formally notified by the organization on July 18, 2025. While the data compromise has been acknowledged, the extent of financial or operational impact remains undetermined.

6. **Software Design Consulting Group Targeted by DragonForce**

The hacktivist group DragonForce reportedly launched a ransomware attack against Software Design Consulting Group, a private organization based in Lebanon operating in the Information Technology sector. The incident led to the unauthorized encryption of internal systems and possible data compromise. Although the extent of data exposure has not been officially confirmed, the attackers have claimed responsibility and threatened further disclosures. It remains unclear whether any material losses were incurred due to the incident.

7. **Ransomware Attack on Helical Auto Technology by Akira Group**

The ransomware group Akira reportedly launched a cyberattack against Helical Auto Technology India Private Limited, a private organization operating within India's industrial sector. While the nature of the attack suggests potential data encryption and service disruption, there is currently no confirmed evidence of data exfiltration or material financial losses resulting from the incident.

8. **Ransomware Attack on Adrian Kenya by Lynx Group**

The ransomware group Lynx reportedly targeted Adrian Kenya, Ltd., a private organization in Kenya's Information Technology sector, with a ransomware attack. The incident is believed to have compromised sensitive business data and personal information, including names, bank account numbers, and email addresses. However, it remains uncertain whether any material losses were suffered as a result of the breach.

9. Dire Wolf Ransomware Attack Targets Anadolu Hastaneleri

The ransomware group Dire Wolf reportedly carried out an attack against Anadolu Hastaneleri, a private health care organization based in Turkey. While the details of the breach remain limited, it is currently unclear whether any data was exfiltrated or if the organization suffered any material losses as a result of the incident.

Prominent Vulnerabilities

CVE ID	Description	CVSS
CVE-2025-5777	A critical memory overread vulnerability (dubbed *CitrixBleed 2*) in **Citrix NetScaler ADC and Gateway** appliances, affecting systems configured as Gateway or AAA virtual servers. The flaw stems from insufficient input validation, allowing attackers to leak uninitialized memory containing sensitive session or credential data. It was observed being actively exploited prior to public disclosure.	9.3
CVE-2025-53770	A zero-day remote code execution vulnerability in **on-premises Microsoft SharePoint Server**, caused by unsafe deserialization of untrusted data. An unauthenticated remote attacker can execute arbitrary code over the network. Microsoft confirmed exploitation in the wild and issued temporary mitigations while a patch is under development.	9.8
CVE-2025-53771	A path traversal vulnerability in **Microsoft Office SharePoint** enables unauthorized attackers to spoof content by accessing restricted directories. Exploitation occurs via network-based attacks, affecting server integrity and user trust.	6.5
CVE-2025-49704	A code injection vulnerability in **Microsoft Office**	8.8

	SharePoint allows authorized users to execute arbitrary code remotely. Exploiting this flaw may grant attackers elevated privileges and potential control over application components or backend infrastructure.	
CVE-2025-49706	**Microsoft SharePoint** suffers from an improper authentication flaw that enables spoofing by unauthorized users over a network. Exploitation could compromise the legitimacy of system interactions or impersonate valid users.	6.5
CVE-2025-20282	A critical vulnerability in **Cisco ISE and ISE-PIC** internal APIs allows unauthenticated remote attackers to upload and execute arbitrary files as root on the underlying OS. Caused by inadequate file validation, this flaw enables complete device takeover and privilege escalation.	10.0
CVE-2025-25257	An unauthenticated **SQL injection** vulnerability in **Fortinet FortiWeb** (versions 7.6.0–7.6.3, 7.4.x, 7.2.x, ≤7.0.10) enables attackers to execute unauthorized SQL commands via malicious HTTP/HTTPS requests. This flaw compromises database integrity and application logic.	9.8
CVE-2025-54309	A remote code execution vulnerability in **CrushFTP** (before 10.8.5 and 11.3.4_23) affects systems not using the DMZ proxy. Improper AS2 validation allows attackers to gain administrative access via HTTPS. The issue was actively exploited in the wild during July 2025.	9.8
CVE-2025-6558	**Google Chrome** (prior to version 138.0.7204.157) contains a sandbox escape vulnerability in ANGLE and GPU subsystems. A remote attacker can craft malicious HTML to bypass the browser sandbox, leading to arbitrary code execution.	8.8

CVE-2025-47172	An **SQL injection** vulnerability in **Microsoft SharePoint** allows authenticated users to execute unauthorized database commands over a network. This flaw threatens data integrity and could lead to privilege escalation or data exposure.	8.8

Top Initial Access ATT&CK TTPs

1. **Phishing:** ATT&CK Technique: **T1566**, Tactic: **TA0001** (Initial Access) Phishing tricks victims into revealing sensitive information or installing malware. It includes:

   T1566.001 - Spear phishing Attachment: Targeted emails with malicious attachments or links.

   T1566.002 - Spear phishing Link: Links to fake sites designed to steal credentials.
   T1566.003 - Spear phishing via Service: Deceptive messages on social media.
   T1566.004 – Spear phishing Voice: Highly targeted attacks on high-profile individuals.
2. **Exploit Public-Facing Application:** ATT&CK Technique: **T1190**, Tactic: **TA0001** (Initial Access)

   Adversaries exploit vulnerabilities in Internet-facing systems, such as web servers, databases, or cloud applications, to gain initial network access. They may also target edge devices with weak defenses or misconfigurations. Exploits can lead to broader access through compromised infrastructure or weak access controls.
3. **Supply Chain Compromise:** ATT&CK Technique: **T1195**, Tactics: **TA0001** (Initial Access) Supply chain compromise involves manipulating products or their delivery mechanisms to achieve data or system compromise. This can occur at various stages, including software and hardware, by manipulating development tools, source code, or distribution channels.

   Sub-techniques:

   T1195.001 - Compromise Software Dependencies and Development Tools
   T1195.002 - Compromise Software Supply Chain
   T1195.003 - Compromise Hardware Supply Chain

4. **Trusted relationship:** ATT&CK Technique: **T1199**, Tactic: **TA0001** (Initial Access) Malicious actors often infiltrate an organization by targeting its partners and contractors. If a partner is compromised, attackers can use their access points and tools to breach the organization. In practice, they frequently target IT subcontractors (like MSPs, authentication providers, and technical support specialists) who have administrative access to the organization's systems.
5. **Valid Accounts:** ATT&CK Technique: **T1078**, Tactic: **TA0001** (Initial Access) It involves attackers using stolen or compromised credentials to gain initial access to systems or networks. They may obtain these accounts through methods like phishing or credential dumping, allowing them to bypass security controls and move laterally within the network.

Appendix

Glossary

DDoS	Distributed Denial of Service
VM	Virtual Machine
POC	Proof of Concept
TIDE	Think-Tank for Information Decision and Execution Superiority
CVE	Common Vulnerabilities and Exposures
ATT&CK TTPs	Adversarial Tactics, Techniques, and Common Knowledge's Tactics, Techniques, and Procedures
IOC	Indicators of Compromise
NATO	North Atlantic Treaty Organization
USAID	United States Agency for International Development
SSH	Secure Shell
SNMP	Simple Network Management Protocol

M: +91 72919 38347
E: sales@saptanglabs.com
W: www.saptang.com

SAPTANG
Driving Excellence with **Pinaca Group.**

C3iHub

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

Microsoft for Startups
Founders Hub

NVIDIA.
INCEPTION PROGRAM