www.saptanglabs.com

SAPTANG

Proactive **Threat Defence**.

Monthly Threat Report

June 2025

National Centre of Excellence CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

Microsoft for Startups Founders Hub

NVIDIA INCEPTION PROGRAM

SAPTANG
Driving Excellence with Pinaca Group.

Executive Summary

In June 2025, the global cybersecurity landscape experienced a sharp rise in malicious activity driven by prominent APT groups and ransomware operators. High-profile data breaches and targeted attacks impacted organizations across sectors such as government and critical infrastructure, spanning regions including the Middle East, Asia, and the Americas. This report outlines key incidents, exploited vulnerabilities, and threat trends observed during the month.

Table of Contents

Key Data Breaches

1. **Claro, Peru:** Breach by DEDALE exposed 15.4M customer records including IDs, emails, billing info, and subscription data.

2. **Mercadona, Spain:** WhiteCoat exploited a zero-day in a third-party logistics system, leaking backend data linked to Mercadona's Hacendado brand.

3. **Ministry of Health, Peru:** Kitten_FBI_Nz leaked sensitive reproductive health data of women from government medical programs.

4. **Montgomery County, USA:** HIME666 leaked procurement data including names, emails, contact numbers, and contract details.

5. **Ministry of Labor, Iraq:** Shada007 exposed over 550K records including employment info, ID scans, passports, and family forms.

Major Cyber Incidents

1. **Gunra Ransomware Group – Colombia:** Claimed ransomware attack targeting the Military and Police Criminal Justice system of Colombia, with potential exposure of sensitive government records.

2. **Critical CVEs Exploits for Sale:** Multiple high-risk exploit kits for unpatched vulnerabilities were spotted on dark web marketplaces, being sold to threat actors for targeted attacks.

3. **Mashreq Bank – Dark Web Sale:** Stolen credit card records allegedly from Mashreq Bank customers were listed for sale on dark web forums, indicating a possible data compromise.

4. **Coinbase – Admin Panel Access for Sale:** Dark web sources revealed a listing offering unauthorized access to Coinbase's internal admin panel, suggesting a potential compromise or insider threat.

5. **Cisco ISE Zero-Day – Exploit on Sale:** A previously unknown (zero-day) vulnerability in Cisco Identity Services Engine (ISE) was advertised by actor skart7, increasing risk to enterprise networks.

6. **FortiGate API Exploit Tool:** A custom tool designed to exploit Fortinet FortiGate's API weaknesses was seen circulating in hacking forums, potentially allowing unauthorized access to network appliances.

7. **16 billion Leaked Credentials:** A compilation of over 16 billion credentials surfaced on underground forums, including previously breached and newly gathered login data, increasing credential stuffing threats.

8. **Handala Threat Actor – Israel:** Handala claimed to have exfiltrated the list of Israeli bomb shelters, publicly threatening Sara Netanyahu, raising concerns of targeted psychological operations and info warfare.

Key Threats

The key threats identified this month include critical vulnerabilities affecting widely used enterprise and networking platforms. These include a command injection flaw in multiple TP-Link products (CVE-2025-5600), an authentication bypass vulnerability in IBM QRadar SIEM (CVE-2025-20286), and a high-severity arbitrary file upload issue in Apache OFBiz (CVE-2025-45854). Additionally, remote code execution vulnerabilities in SolarWinds Platform (CVE-2025-4797) and Adobe ColdFusion (CVE-2025-47966) pose significant risks to confidentiality and system control, highlighting the urgent need for patching and layered defense strategies.

June 2025 saw a sharp rise in cyber threats, with ransomware campaigns and politically motivated attacks heavily targeting critical industries. Government agencies, law enforcement systems, aviation and airline services, financial institutions, telecommunications, and e-commerce platforms experienced significant disruptions due to data breaches and infrastructure attacks. The ongoing geopolitical cyber conflict in the Middle East also intensified, involving large-scale DDoS operations and data leaks.

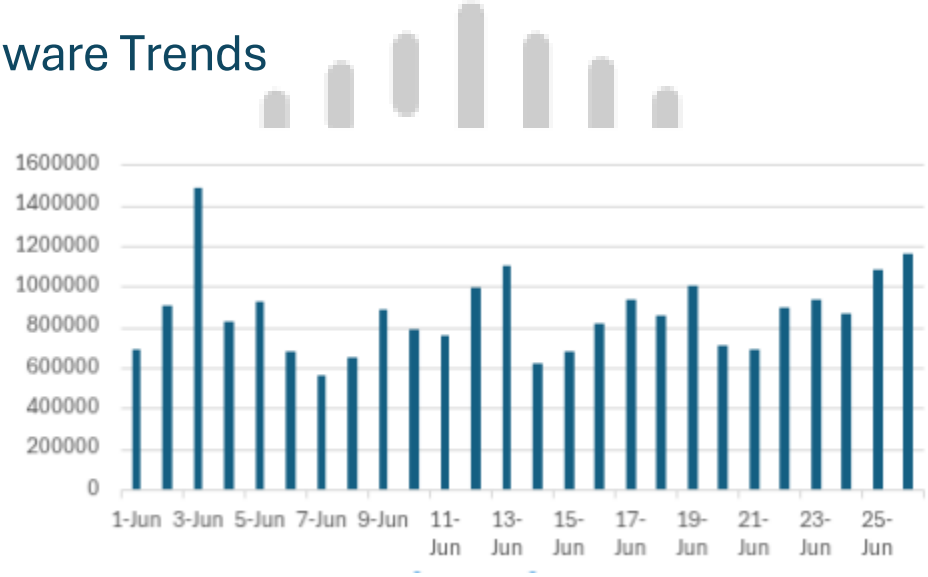
Furthermore, dark web forums saw increased activity related to the sale of zero-day

vulnerabilities, administrator-level access to cloud services, and compromised financial data. A major internet-wide disruption affected several high-profile digital services across cloud, communication, and productivity platforms — raising concerns over systemic dependencies in global IT infrastructure. Collectively, these incidents emphasize the urgent need for enhanced threat monitoring, proactive patching, and resilience-building across sectors.

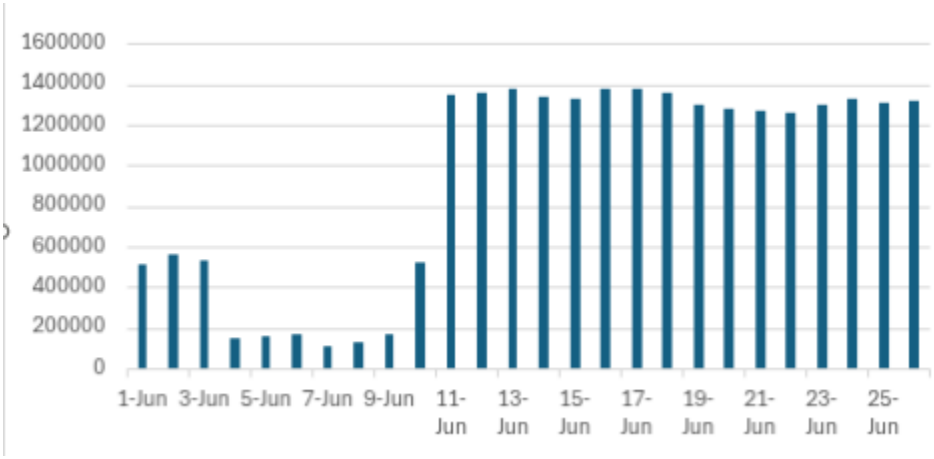
Threat landscape

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.

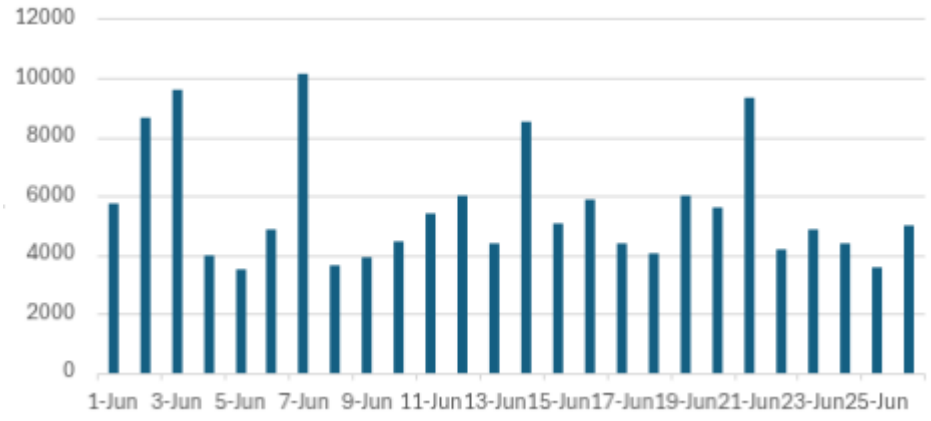
Ransomware Trends



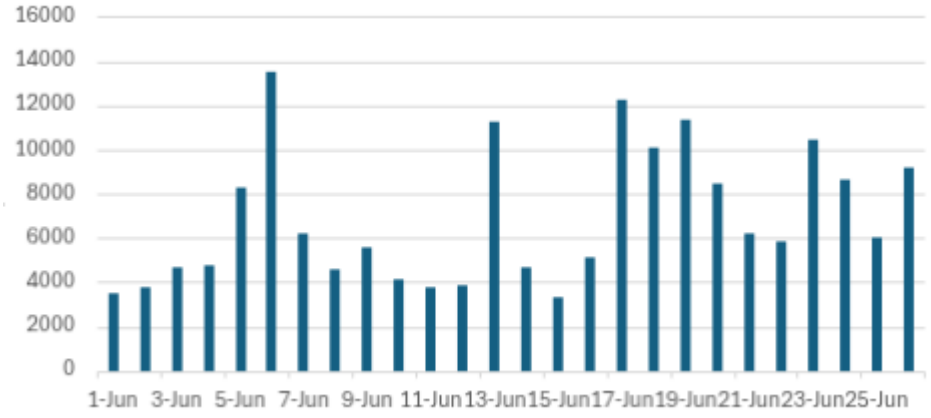
MALWARE



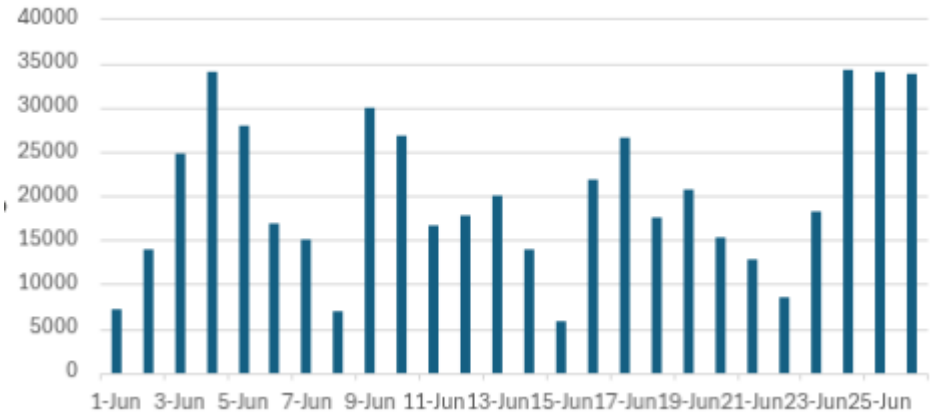
SCRIPT MALWARE



MOBILE THREAT



COIN MINER



EXPLOITS

DDoS Activity

Top Source Countries:

Sources		
United States	698,974	50.8 %
Germany	302,299	22 %
Netherlands	248,256	18.1 %
France	247,230	18 %
United Kingdom	236,657	17.2 %

Top Destination Countries:

Destinations		
United States	216,903	15.8 %
Brazil	108,148	7.9 %
Poland	65,157	4.7 %
South Korea	54,879	4 %
Japan	54,129	3.9 %

Underground Findings

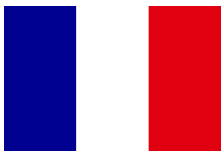
The findings listed below are among the critical datasets discovered on underground forums in June 2025. Additionally, several threat actors are noted based on their prominent activities during this period.

Global Data Breaches and Leaks

Region	Organization	Significant Data
	Revolut	A high-severity data exposure incident has been identified involving a verified Revolut Business account allegedly registered in the Czech Republic and listed for sale by a threat actor operating under the alias "Ivan-bro." Revolut, a major global fintech company serving over 40 million customers across more than 35 countries, is the target of this breach. The compromised account reportedly has a turnover of approximately €2,000 and includes access to the associated email, phone number (active for 46 more days), and is offered with web-only access through cookies, proxy, and login credentials, suggesting session hijacking. The package also involves support from a cooperating dropper, pointing to the use of malware for persistence. This raises significant concerns about unauthorized access to verified financial platforms, potential money laundering, and reputational harm. The root cause is likely poor session control and lack of robust threat detection, leading to potential regulatory exposure and operational disruption for both the victim business and Revolut's platform integrity.
	Claro	A major data breach has impacted Claro Peru, a subsidiary of the South American telecom giant Claro, following an intrusion by the threat actor known as DEDALE. The attacker claims to have

		accessed and exfiltrated sensitive data belonging to over 15.4 million customers, including full names, email addresses, national ID numbers, billing information, and subscription metadata. As one of the largest telecommunications providers in the region, Claro's compromise poses a serious threat to customer privacy and trust. The scale and sensitivity of the exposed data raise concerns about potential identity theft, financial fraud, and long-term reputational damage for the company. This breach underscores significant weaknesses in the organization's data protection infrastructure and highlights the need for enhanced threat monitoring and response capabilities.
	Mercadona	Mercadona, one of Spain's largest supermarket chains with over 1,600 stores and extensive backend logistics, suffered a breach attributed to the threat actor group WhiteCoat. The attacker exploited a zero-day vulnerability in a third-party logistics and inventory system linked to Mercadona’s private-label brand, Hacendado. As a result, sensitive operational data—such as inventory movements, order metadata, and potentially customer fulfillment records—may have been exposed. This incident highlights critical vulnerabilities in the company’s supply chain infrastructure and could lead to operational disruptions, increased logistical risks, and potential regulatory scrutiny over data handling practices.

	Odoo Inc	A significant cybersecurity incident affected Odoo S.A., a large Belgium-based ERP software provider serving thousands of enterprise clients globally. The incident was attributed to the threat group HAXORTeams, who claimed to have compromised Odoo's internal infrastructure with alleged assistance from an insider. As a result of the breach, the attackers exfiltrated a 63.4MB internal employee database, which they listed for sale on underground forums for $25,000 in Bitcoin or Monero. The data, purportedly updated to version 1.6.25, includes sensitive employee information and may potentially expose Odoo to regulatory scrutiny, reputational damage, and internal operational risks. The breach underscores the critical threat posed by insider involvement and highlights the need for enhanced internal access controls, employee activity monitoring, and zero-trust architecture to mitigate such risks in enterprise environments.
	Ministry of Health. Peru	A major data breach targeting Peru's Ministry of Health (Ministerio de Salud - MINSA) was claimed by the threat actor known as Kitten_FBI_Nz. The breach led to the unauthorized exposure of highly sensitive medical data pertaining to women enrolled in national family planning and pregnancy-related programs. The leaked information includes personal identifiers, diagnostic records, contraception methods, contact details, and detailed medical histories. The attacker publicly shared screenshots and download links, confirming the legitimacy and

		scope of the compromised records. This breach represents a severe violation of patient confidentiality and poses significant risks to the privacy and safety of affected individuals. The incident also exposes the Ministry to reputational damage, potential legal consequences, and a loss of public trust in digital health services.
	SNCF (National Railway Company)	The French national railway company SNCF, a major European transportation provider serving millions of passengers annually, experienced a significant data breach attributed to the threat actor Zoldyck. The attacker claimed to have exfiltrated over 5 million records involving both customers and employees. The compromised data includes personal identifiers, contact information, and account-related details, all of which could be leveraged for phishing attacks, identity theft, and unauthorized access to SNCF travel services. This breach presents a high risk to customer privacy and operational integrity and may result in substantial reputational damage and regulatory consequences for SNCF.
	Montgomery County, Maryland	Montgomery County, Maryland, one of the largest and most populous counties in the United States, suffered a targeted cyberattack on its government procurement systems. The incident, attributed to the threat actor HIME666, resulted in the unauthorized access and exfiltration of sensitive procurement records. Exposed data includes contract numbers, procurement metadata, names

		and contact details of staff, departmental affiliations, and critical scheduling information. This information was subsequently posted on a dark web forum, significantly elevating the risk of procurement fraud, impersonation of officials, and manipulation of vendor relationships, and raising broader concerns about the security and integrity of local government infrastructure.
	Ministry of Labor and Social Affairs	The Iraq Ministry of Labor and Social Affairs experienced a significant data breach executed by the threat actor Shada007. The breach led to the exposure of a vast dataset comprising over 100,000 employment records and more than 450,000 additional entries, including scanned national identity cards, passports, family documents, and other sensitive personal information. This incident constitutes a high-impact compromise with severe implications for identity theft, administrative fraud, and national data security, directly affecting both Iraqi citizens and the operational integrity of a key government institution.
	Bezeq	Bezeq, Israel's largest telecommunications provider, was reportedly breached by the threat actor HAXORTeams. The attacker claims to have gained deep access to critical infrastructure, including the fiber-optic backbone, core servers, cloud environments, and 5G systems. If the extent of the compromise is confirmed, this incident constitutes a strategic-level breach with potentially severe implications for national communications

		integrity, operational continuity, and sensitive data confidentiality. Such access could enable long-term surveillance, service disruption, or manipulation of Israel's telecom backbone, posing a serious risk to both civilian and governmental digital infrastructure.
	Military Depot Mount Chaâbanbi	A sensitive Israeli military depot situated at Mount Chaâbanbi was compromised by the threat actor known as mrdump. The breach resulted in the unauthorized exposure of highly classified materials, including thermal surveillance imagery, internal government schematics, and detailed inventory blueprints associated with critical military infrastructure. The nature and content of the leaked files present a serious national security threat, as this information could be exploited by hostile entities to assess vulnerabilities, plan targeted operations, or disrupt defense logistics. The incident underscores a significant failure in safeguarding strategic military data and raises concerns about the broader cybersecurity posture of defense assets.

Indian Cyber Incidents and Data Breaches

Organization	Significant Data
Aditya Birla Capital	Aditya Birla Capital—a major Indian financial services company with over 25 million customers—suffered a targeted cyberattack on its Digital mobile app, resulting in the unauthorized theft of approximately ₹1.95 crore worth of digital gold from 435 customer

	accounts. The breach exploited critical flaws in the app's transaction validation logic, allowing attackers to manipulate account balances and execute unauthorized gold conversions. Although swift detection led to account freezes and limited further losses, the incident underscores serious vulnerabilities in fintech platforms handling high-value digital assets. It highlights the urgent need for robust backend security controls, secure transaction workflows, and real-time anomaly detection to defend against business logic abuse and sophisticated financial fraud.
Zoomcar	Zoomcar, India's leading peer-to-peer car-sharing platform with millions of active users, suffered a significant data breach that exposed the personal information of approximately 8.4 million users. The compromised data included names, phone numbers, email addresses, home addresses, and vehicle registration numbers—although financial details and passwords remained unaffected. This breach poses a serious risk of phishing, identity theft, and social engineering attacks, given the nature of the leaked information. In response, Zoomcar activated its incident response protocols, brought in external cybersecurity experts, and intensified system monitoring efforts to contain the breach and strengthen its data protection measures.
Sant Parmanand Hospital, North Delhi	Sant Parmanand Hospital in North Delhi experienced a severe ransomware attack that crippled its core IT infrastructure, disrupting critical services such as Electronic Medical Records (EMR), patient admissions, diagnostics, and billing operations. The attack, attributed to the threat actor group 0rbitalStealer, resulted in a complete digital outage and the exfiltration of sensitive patient data, including personal identifiers, medical histories, Aadhaar-linked records, and partial payment information. The attackers publicly posted evidence of the stolen data on the dark web,

	accompanied by ransom threats. The breach significantly impacted healthcare service delivery for nearly 48 hours until recovery processes were initiated using offline backups, highlighting the urgent need for cybersecurity resilience in the healthcare sector.
NKS Super Specialty Hospital, Delhi	NKS Super Speciality Hospital, a prominent private healthcare provider in North Delhi, was compromised in a cyberattack orchestrated by the DragonForce threat actor group. Exploiting a vulnerability in a third-party vendor portal, the attackers gained admin-level access to backend servers and swiftly exfiltrated a wide range of sensitive data, including employee records, internal communications, OPD/IPD logs, insurance databases, radiology images, prescriptions, and doctor-patient communication logs. The hospital's website was briefly defaced with DragonForce's digital signature, publicly confirming their involvement. The breach disrupted operations and forced the hospital to initiate emergency IT recovery protocols. A sample of the stolen data was later published on a ransomware leak site, accompanied by threats of further exposure, underscoring the critical risks associated with third-party access and inadequate vendor security controls in the healthcare sector.
Sun Direct	Sun Direct, one of India's leading direct-to-home (DTH) service providers with a nationwide customer base, fell victim to a major ransomware attack carried out by the Medusa group. The attackers infiltrated internal servers, encrypting critical infrastructure and exfiltrating a substantial volume of sensitive customer and operational data. Leaked information includes Aadhaar-linked subscriber details, service activation records, call logs, CRM exports, recharge histories, vendor communications, and support ticket logs. Medusa listed Sun Direct on its dark web leak site, publishing screenshots of stolen data and issuing ransom demands

	to prevent further exposure. The breach caused temporary disruptions to customer service operations and exposed significant risks related to personal data privacy and operational continuity in the telecom sector.
UHBVNL	Uttar Haryana Bijli Vitran Nigam Ltd (UHBVNL), a key state-run electricity distribution provider in North India, suffered a coordinated cyberattack that disrupted its official website and digital service portals, leaving critical operations offline for nearly 72 hours. Although no ransomware group publicly claimed responsibility, security analysts linked the breach to a data extortion campaign that exploited exposed admin panels and API misconfigurations. The attack stalled over 50,000 pending electricity connection applications and compromised sensitive data, including consumer IDs, addresses, billing records, internal emails, and maintenance logs. While no ransom demand was disclosed, the exfiltrated data is suspected to be intended for future monetization on dark web markets, underscoring the growing threat to critical infrastructure from opportunistic and financially motivated threat actors.

Threat Actors

1. Qilin

In June 2025, the Qilin ransomware group launched one of its most disruptive attacks against a European logistics conglomerate with a footprint in over 30 countries. The incident resulted in the encryption of over 2,000 devices and the exfiltration of 1.6 TB of critical logistics documentation, shipment tracking data, and internal communications. This breach halted global cargo movement for several days, causing downstream delays across manufacturing and retail sectors. Qilin's leak site previewed internal warehouse control systems and sensitive export licenses to pressure the victim into ransom negotiations.

2. Akira

The Akira group continued its aggressive global campaigns in June by breaching ALFA Testing in Turkey. The attack led to a massive leak of 300 GB of sensitive testing data, HR records, and industrial client contracts. Akira published screenshots showing active domain control and a complete file directory of test protocols used by prominent construction and environmental organizations. The breach has drawn attention from Turkey's data protection authority due to the regulatory risks posed by the leaked information.

3. 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.

4. INC Ransom

Incransom made headlines this month after compromising a healthcare group in Latin America. The attack resulted in the leak of over 40 GB of patient records, insurance documentation, and government audit reports. With leveraging access gained through misconfigured RDP services, the group deployed its ransomware payload across clinical systems, temporarily disabling medical scheduling and billing operations. The incident raised alarms across regional hospitals due to the sensitive nature of exposed patient data and the potential for follow-on extortion.

5. DragonForce

The politically motivated DragonForce group played a central role in the ongoing Iran-Israel cyber conflict in June. DragonForce targeted municipal infrastructure in Haifa, Israel, leaking evacuation maps and emergency communication plans of Israeli civil defense networks. Additionally, the group exploited exposed Jenkins dashboards used in city service coordination, exfiltrating credentials and real-time sensor data. Their actions were coordinated alongside

over 35 other pro-Iran threat groups during this month's cyber escalation, intensifying tensions in the region.

6. Lynx

Lynx ransomware operators attacked Falavinha Contábil, a prominent financial consulting firm in Brazil, exfiltrating 68 GB of confidential documents. The leak included tax records, payroll files, and accounting reports from high-profile clients. Screenshots of tax return forms and internal audit communications were shared publicly, putting pressure on the company and triggering local legal action. The breach marked Lynx's continued focus on targeting finance and regulatory firms for high ransom yields.

7. Play

Play ransomware group executed a disruptive attack on a Southeast Asian e-commerce firm, encrypting web infrastructure and leaking 220 GB of customer data. This breach included order histories, delivery addresses, payment confirmations, and vendor account credentials. The firm's website and mobile application were down for over 48 hours, affecting thousands of users. Play released a portion of the data on their dark web site to demonstrate the extent of the breach and prompt negotiations.

8. Handala

Handala engaged in a cyber-psychological operation in June by leaking the full list of Israeli emergency shelters, including geo-coordinates and facility photos. The threat actor group claimed the attack was part of its retaliatory campaign and threatened further leaks involving high-ranking Israeli officials. The incident is being treated as a national security threat in Israel due to its implications for public safety, particularly amid rising regional tensions.

9. Warlock

Warlock launched a targeted ransomware campaign against a Middle Eastern petrochemical processing company. The group encrypted engineering diagrams, refinery configuration files, and SCADA system backups. Approximately 750 GB of sensitive documents were stolen, and screenshots of production dashboards and control panel code were shared on their blog. The attack briefly halted the company's export operations and drew international attention due to

the energy sector's critical infrastructure vulnerabilities.

10. WorldLeaks

Warlock launched a targeted ransomware campaign against a Middle Eastern petrochemical processing company. The group encrypted engineering diagrams, refinery configuration files, and SCADA system backups. Approximately 750 GB of sensitive documents were stolen, and screenshots of production dashboards and control panel code were shared on their blog. The attack briefly halted the company's export operations and drew international attention due to the energy sector's critical infrastructure vulnerabilities.

Threat Analysis

Notable Incidents

1. **Iran–Israel Cyber Crisis Escalates Involving 35+ Threat Groups**

   The ongoing cyber conflict between Iran and Israel intensified throughout June 2025, with over 35 distinct threat groups reported to be involved. The campaign includes large-scale DDoS attacks, data breaches, and infrastructure targeting. Both public and private entities across government, defense, healthcare, and critical utilities were affected. Israeli sources reported over 244 cyberattacks in one week alone, showing the campaign's scale and sophistication.

2. **Gunra Ransomware Targets Colombian Military and Police Criminal Justice**

   A ransomware group operating under the name Gunra has claimed responsibility for a severe breach targeting the Military and Police Criminal Justice system of Colombia. The attack encrypted sensitive law enforcement and judicial data, disrupting operations and raising national security concerns. The group allegedly exfiltrated internal documents, criminal case files, and sensitive communications. The breach is seen as a politically motivated strike on Colombian institutions.

3. **Sun Direct Data Breach by Medusa Ransomware Group (India)**

Indian DTH service provider Sun Direct suffered a significant data breach carried out by the Medusa ransomware group. The attackers published data samples to a leak site, claiming the exfiltration of customer databases, billing records, and internal operational documents. The breach is under active investigation, and customers have been advised to monitor their accounts for unusual activity or phishing attempts.

4. **Thai Airways Suffers Confirmed Data Breach**

   National carrier Thai Airways confirmed a cyber incident where unauthorized access led to the compromise of passenger data and internal records. The breach is suspected of involving third-party supply chain vulnerabilities. Exposed information reportedly includes names, travel itineraries, passport numbers, and email addresses of both domestic and international passengers. The airline is working with regulators and forensic investigators to contain the fallout.

5. **CNPC USA Breached by Rhysida Ransomware Group**

   The Rhysida ransomware group listed China National Petroleum Corporation (CNPC) USA as a victim in early June. The breach allegedly involved terabytes of internal data, including engineering schematics, financial reports, and employee credentials. The leak was shown on a ransom portal with screenshots of sensitive documents. CNPC has yet to issue a formal response, but infrastructure partners have been alerted.

6. **Massive Multi-Service Outage Hits Cloud Giants and Global Platforms**

   On June 20, 2025, a widespread outage crippled multiple major services, including AWS, Microsoft Azure, Google Cloud, OpenAI, Cloudflare, Gmail, YouTube, and more than 50 other global platforms. The incident was initially suspected to be linked to upstream network provider failures or coordinated infrastructure-level cyberattacks. Services were gradually restored, but the event demonstrated global dependence on centralized cloud infrastructure.

7. **NightSpire Executes 300GB Ransomware Attack on ALFA Testing (Turkey)**

   The NightSpire threat actor launched a 300GB ransomware attack against ALFA Testing, a Turkish industrial and lab testing firm. The attackers claimed to have stolen

sensitive certifications, test reports, intellectual property, and customer lists. The stolen data could pose significant risks to downstream clients in sectors such as oil and gas, pharmaceuticals, and automotive manufacturing.

8. **Dark Web Sees Surge in Exploit and Data Sales – Cisco, Fortinet, Coinbase, Banks**

   Underground cybercrime forums saw a surge in exploit and credential sales in June. Notably, a zero-day vulnerability in Cisco ISE was offered by a seller named "skart7," along with exploit tools targeting FortiGate firewalls. Additionally, admin panel access for Coinbase and credit card data linked to Mashreq Bank were listed for sale, revealing a vibrant ecosystem for high-value cyber exploits.

9. **APT28 Uses Signal for Malware Delivery in Ukraine Campaigns**

   The Russian state-aligned group APT28 was observed exploiting Signal messaging platforms to deliver malware payloads to Ukrainian targets. The campaign utilized shortened URLs and Signal's encrypted channels to distribute malicious documents and gather user metadata. Targets included journalists, diplomats, and civil society members. The TTPs (tactics, techniques, and procedures) mark a shift toward encrypted C2 channels in nation-state attacks.

10. **Anonymous-linked Actors Breach GlobalX – Deportation Flight Data Exposed**

    Hacktivist-linked actors, potentially aligned with Anonymous, breached U.S.-based GlobalX charter airline, known for executing deportation flights. Attackers defaced a subdomain and leaked flight logs, passenger lists, and government contracts related to deportation operations. The attackers claimed access via a compromised AWS developer token. The incident has stirred public and legal debate over privacy, data handling, and governmental accountability.

Prominent Vulnerabilities

1. **CVE-2025-49113 – Roundcube Webmail Remote Code Execution via PHP Object Deserialization**

   CVSS: **9.9**

Roundcube Webmail versions prior to 1.5.10 and 1.6.11 suffer from a critical PHP object deserialization flaw in the upload.php endpoint due to the unsanitized _from parameter. This vulnerability enables authenticated users to inject crafted objects that result in remote code execution. It severely impacts webmail systems where user privileges can be escalated, leading to complete compromise of email infrastructure.

2. **CVE-2025-24016 – Wazuh Untrusted Deserialization Leading to Remote Code Execution**

   CVSS: 9.9

   Wazuh, a widely used security monitoring platform, contains a deserialization vulnerability that allows attackers to remotely execute arbitrary code. The issue arises from the unsafe deserialization of untrusted data, impacting core components of the server. Successful exploitation could allow attackers to take full control of Wazuh instances, manipulate detection rules, or pivot to other connected infrastructure in SOC environments.

3. **CVE-2024-12987 – DrayTek Vigor Routers OS Command Injection via APM Config Upload**

   CVSS: 9.8

   This OS command injection vulnerability in the /cgi-bin/mainfunction.cgi/apmcfgupload endpoint affects DrayTek Vigor2960, Vigor300B, and Vigor3900 routers. Attackers can remotely inject system commands without authentication. Since these routers are often deployed in enterprise networks, exploitation could lead to lateral movement, man-in-the-middle attacks, or complete network compromise through backdoors or malware delivery.

4. **CVE-2021-32030 – ASUS Router Improper Authentication**

CVSS: 9.8

ASUS Lyra Mini and GT-AC2900 routers have an authentication bypass vulnerability allowing attackers to access the administrative interface without proper credentials. These models, now end-of-life, are still in use across consumer and SMB networks. Attackers could reconfigure devices, disable encryption, or hijack connected systems. Given the lack of updates, mitigation depends entirely on device decommissioning.

5. **CVE-2023-39780 – ASUS RT-AX55 Command Injection Vulnerability**

CVSS: 8.8

In ASUS RT-AX55 routers, authenticated attackers can exploit the command injection flaw to run arbitrary system commands. This vulnerability can be abused in botnet creation or to intercept and redirect network traffic. It remains under active exploitation, especially in IoT botnet campaigns, targeting users who fail to update firmware or change default credentials.

6. **CVE-2023-33538 – TP-Link Routers Command Injection via WLAN RPM**

CVSS: 8.8

Several legacy TP-Link routers such as TL-WR940N, TL-WR841N, and TL-WR740N are affected by a command injection vulnerability through the /userRpm/WlanNetworkRpm component. Attackers can craft payloads to execute system commands remotely. As these devices are end-of-life, they no longer receive patches. Exploits are available publicly, and they are widely targeted in automated botnet scans.

7. **CVE-2024-56145 – Craft CMS Remote Code Execution through Improper Input Sanitization**

CVSS: 9.3

Craft CMS versions with register_argc_argv enabled in php.ini are vulnerable to a remote

code execution vulnerability caused by improper sanitization of input. This allows attackers to inject and execute malicious PHP code via manipulated requests. The flaw could be used to compromise entire websites, escalate privileges, and steal sensitive information from backend databases or user sessions.

8. **CVE-2024-42009 – Roundcube Cross-Site Scripting in Mail Viewer**
   CVSS: 9.3
   This XSS vulnerability in Roundcube Webmail allows remote attackers to craft malicious emails that abuse desanitization issues in the message_body() function within show.php. When victims open these emails, their sessions can be hijacked, and their entire mailbox contents could be silently forwarded to the attacker. It's actively exploited in targeted phishing and espionage campaigns.

9. **CVE-2023-0386 – Linux Kernel OverlayFS Privilege Escalation**
   CVSS: 7.8
   A flaw in OverlayFS in the Linux kernel allows a user to copy a capable file from a nosuid mount, bypassing standard UID controls. This can result in local privilege escalation, especially in container environments or systems running multiple users. Exploitation can lead to full root access, making this vulnerability valuable in post-exploitation stages.

10. **CVE-2023-38950 – ZKTeco BioTime Path Traversal via iClock API**
    CVSS: 7.5

    ZKTeco’s BioTime v8.5.5 is vulnerable to a path traversal issue in its iClock API, enabling unauthenticated attackers to access arbitrary files on the server. Sensitive system configurations, user logs, and credential files are at risk. This flaw is critical for environments relying on ZKTeco for biometric attendance or access control, exposing

identity management infrastructure.

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 - Spearphishing Attachment: Targeted emails with malicious attachments or links.
   T1566.002 - Spearphishing Link: Links to fake sites designed to steal credentials.
   T1566.003 - Spearphishing via Service: Deceptive messages on social media.
   T1566.004 – Spearphishing 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