GLOBAL CYBER THREAT INTELLIGENCE

ANNUAL REPORT 2025

WITH FURTHER *2026* PREDICTIONS

Prepared by

Cyberthint Threat Hunters

This report was prepared using Cyberthint Unified Cyber Threat Intelligence & Digital Risk Protection Platform, Cyberthint's Dark Monitor, and analysis from Cyberthint Threat Hunters.

Prepared for

Community

Table of Contents

cyberthint

Unified CTI & DRP Platform

We know what information hackers have on you!

Cyberthint is an unified cyber threat intelligence & digital risk protection platform that allows you to take precautions against cyber threats that may affect your company and employees in cyberspace.

Be aware of cyber threats targeting your organization in advance with Cyberthint's advanced cyber threat intelligence technology!

Everything you need is on a single platform!

Observe and Prevent to Avoid Being Hunted

Cyberthint is an organization that protects your assets with an integrated digital vision with more than 15 years of experience in the cyber security world.

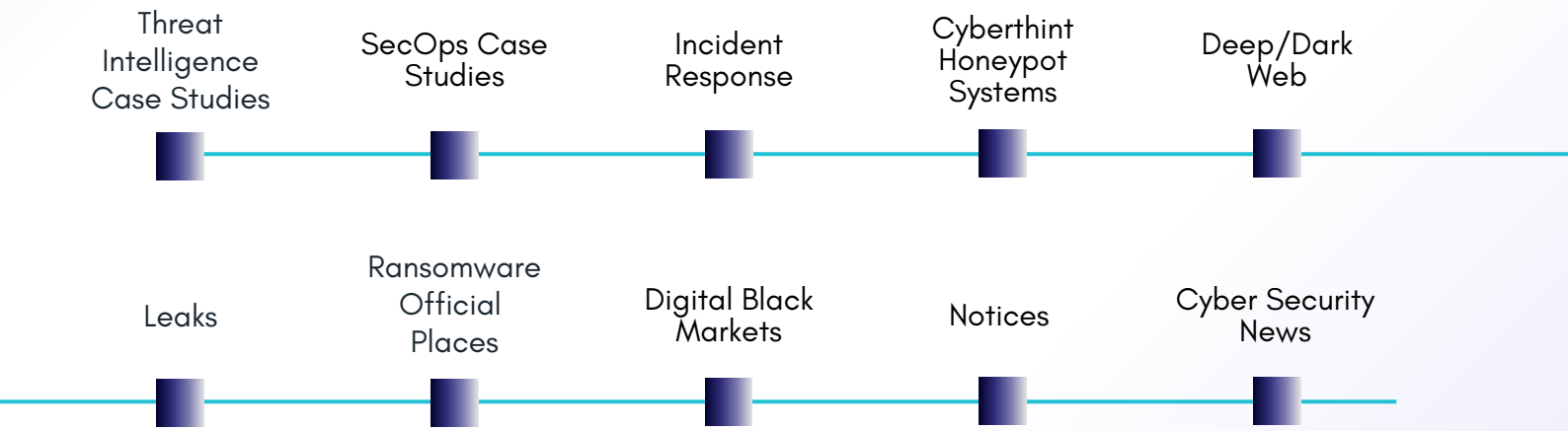
Improvised threats that fall outside the foreseen risks in workflows can be overlooked. As cybersecurity professionals, we have ambitiously realized the idea of early detection of behind-the-scenes movements that may pose a risk to organizations with an "automated cyber patrol approach".

Cyberthint provides ideal cyber threat intelligence and security solutions for your organization with its capabilities.
We can help you protect your brands and IT infrastructure with a preventive threat intelligence approach.

cyberthint

About the Report

This cyber threat intelligence report stats prepared by Cyberthint, which includes important cyber events that took place in 2025 at the global level, cases encountered by Cyberthint's & Seccops's teams, observations and analysis, also includes threat predictions for 2026.



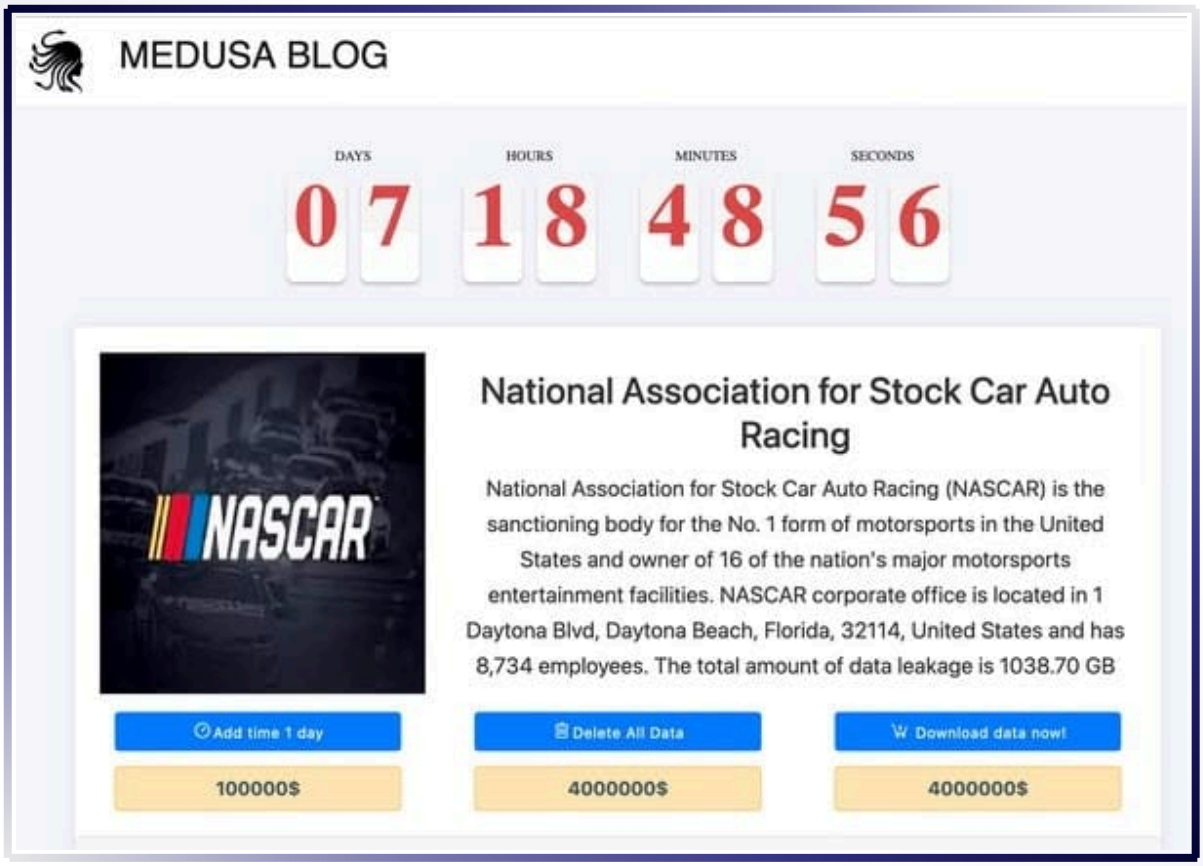
Ransomware Attacks/News

Section 1

Ransomware Incidents

NASCAR (National Association for Stock Car Auto Racing)

In April 2025, NASCAR, America's largest motor sports organization, became the target of the Medusa ransomware group. While the attack did not affect the organization's operational racing systems, it crippled its ticketing infrastructure and corporate network. It was determined that the attackers infiltrated the network by purchasing VPN access credentials for one of the organization's subcontractors (Vendor) from the Dark Web (via an Initial Access Broker).

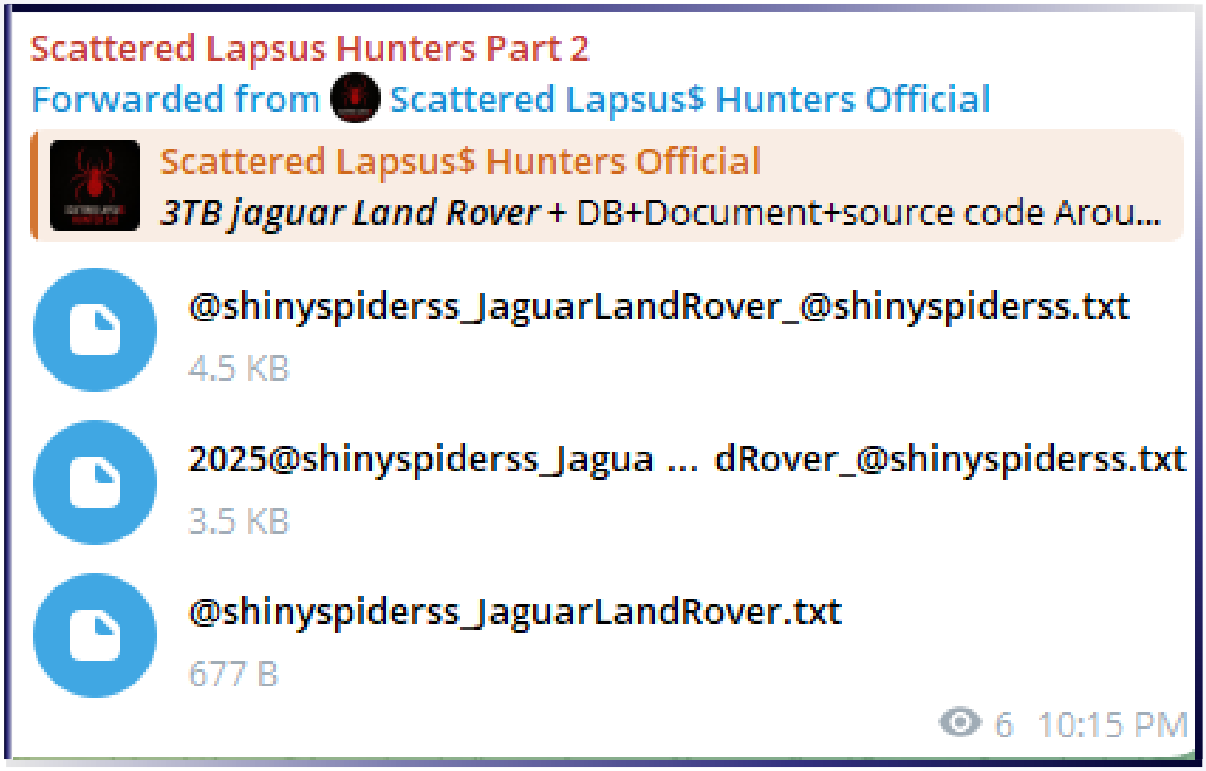


The Medusa group demanded $4 million in ransom from NASCAR. When their demands were rejected, the group adopted an extremely aggressive tactic: they began leaking data in batches, including personal information (names, addresses, credit card summaries) belonging to race fans and the social security numbers of NASCAR employees. Additionally, confidential documents related to the organization's sponsorship agreements were published on the leak site.

Ransomware Incidents

Jaguar Land Rover (JLR)

In September 2025, Jaguar Land Rover (JLR), the UK's largest automotive manufacturer, faced a catastrophic cyberattack that paralyzed its global operations. The incident forced the company to completely halt production at key facilities in Solihull, Wolverhampton, and Halewood for nearly four weeks. This disruption resulted in an estimated £1.9 billion loss to the UK economy and severed critical links in the global automotive supply chain, leaving thousands of vehicles unfinished.

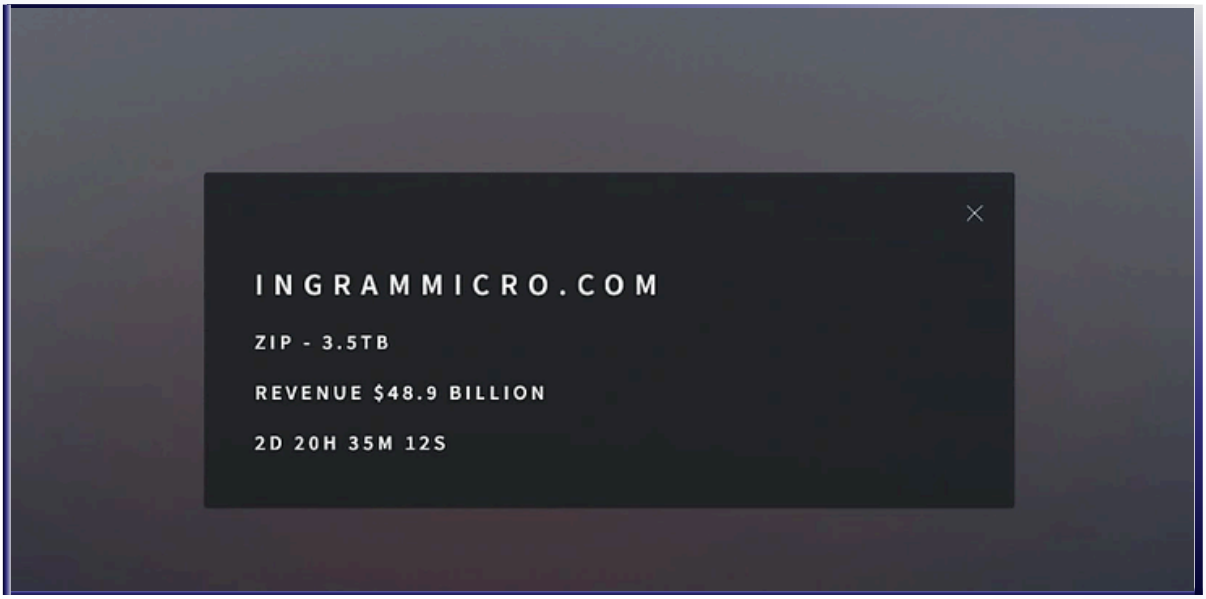


The attack was orchestrated by Scattered Lapsus$ Hunters, a coalition of sophisticated threat actors targeting industrial environments. Unlike typical encryption attacks, the group leveraged advanced social engineering and credential theft to bypass Multi-Factor Authentication (MFA), gaining front-door access to the Operational Technology (OT) network. They did not just steal sensitive vehicle schematics; they physically locked down the assembly line control systems. The group demanded a record-breaking ransom to restore the production grid, marking one of the most expensive operational disruption events in automotive history.

Ransomware Incidents

Ingram Micro

In July 2025, Ingram Micro, the world's largest technology distributor, fell victim to a massive ransomware attack that severed critical arteries of the global IT supply chain. The incident, which struck during the Fourth of July weekend, forced the company to shut down its core operational systems, including the AI-powered Xvantage platform. For nearly a week, thousands of resellers and vendors worldwide were unable to place orders or track shipments, causing an estimated revenue loss of $136 million per day during the outage.

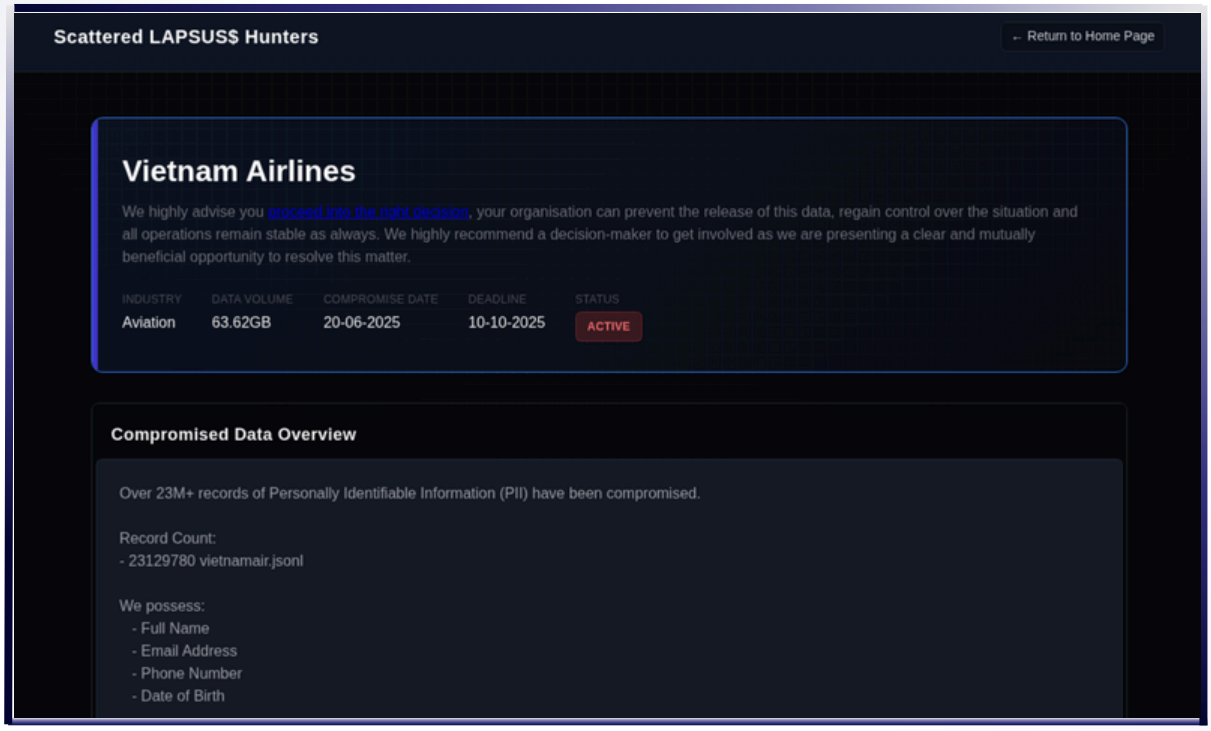


The attack was claimed by SafePay, a rapidly emerging threat group that surfaced in late 2024. Leveraging compromised credentials to breach the company's GlobalProtect VPN, the attackers exfiltrated 3.5 terabytes of sensitive corporate data and subsequently encrypted the network. SafePay utilized a Double Extortion tactic, threatening to leak employee SSNs and proprietary vendor contracts if their demands were not met. This incident served as a wake-up call for the industry, demonstrating how a single point of failure in a distributor can trigger a cascading paralysis across the entire global technology market.

Ransomware Incidents

Vietnam Airlines

In June 2025, Vietnam Airlines suffered a massive data breach affecting over 23 million passengers. The attack compromised a critical database containing personally identifiable information (PII), exposing the personal details of nearly a quarter of the country's population. This incident stands as one of the largest data leaks in the aviation industry's history, raising severe concerns about the privacy and safety of travelers across Southeast Asia.

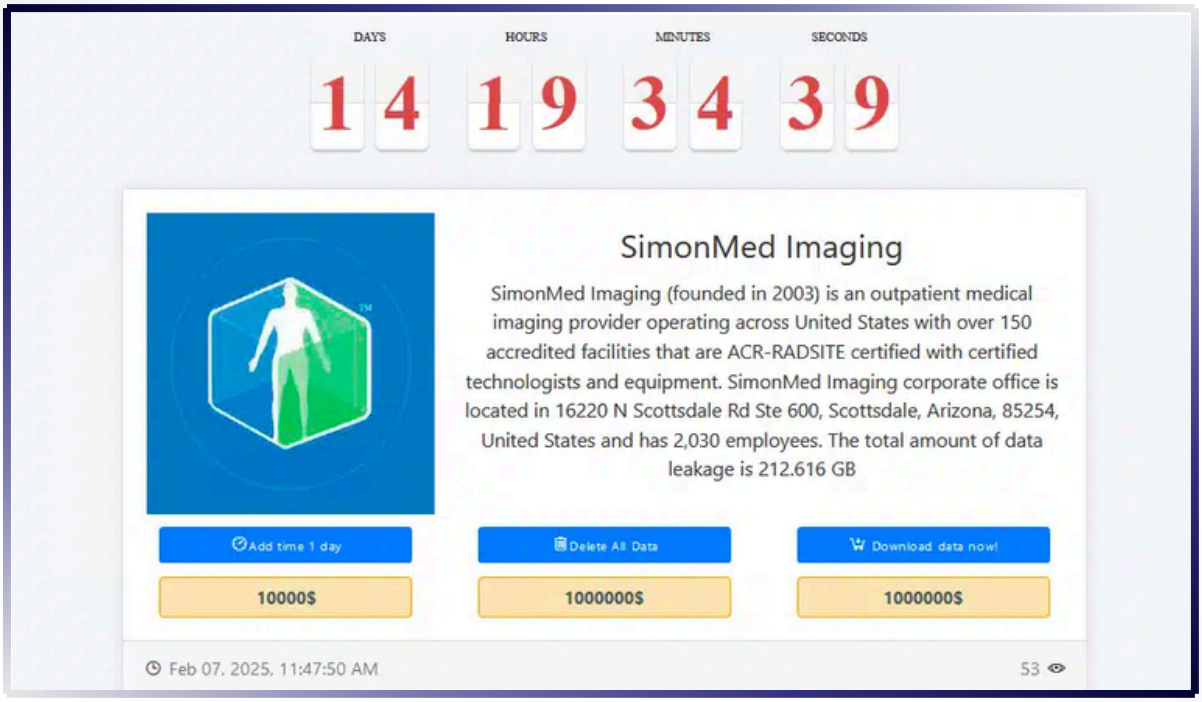


The attack was claimed by the threat group "Scattered LAPSUS$ Hunters," which listed the airline on their leak site with an "ACTIVE" status. According to the group's dashboard, they exfiltrated 63.62 GB of data, specifically a file named vietnamair.jsonl containing 23,129,780 records. The compromised fields included Full Names, Email Addresses, Phone Numbers, and Dates of Birth. The group set a deadline of October 10, 2025, threatening to release the full dataset if their demands were not met.

Ransomware Incidents

SimonMed Imaging

Early in 2025, SimonMed Imaging, one of the largest outpatient imaging providers in the US, was rocked by a major data breach and ransomware attack. The attack exposed the highly sensitive medical records (MRI results, X-rays, insurance information, and ID copies) of approximately 1.2 million patients.

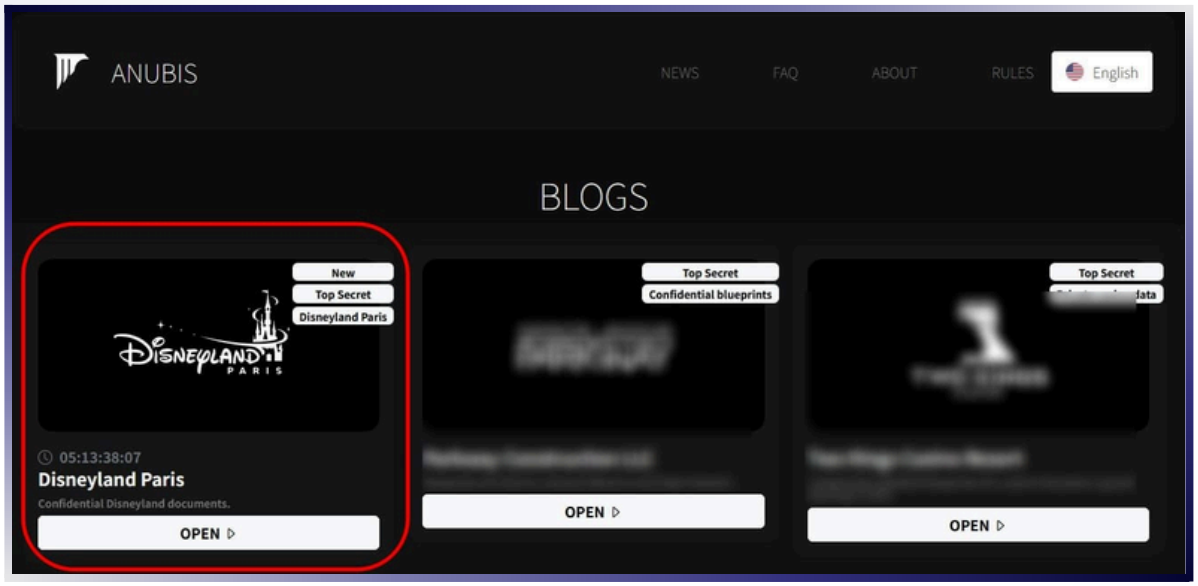


The Medusa group, which claimed responsibility for the attack, exploited configuration errors in the company's firewalls. The attackers remained on the network for weeks (dwell time) before encrypting the data, leaking it externally. The most frightening part was the group's blackmail tactic: they contacted not only the company but also the patients whose data had been stolen, individually calling or emailing them with the threat, “We will publish your data on the internet.”

Ransomware Incidents

Disneyland Paris

In early August 2025, Disneyland Paris was targeted by the Anubis group, a player that has surprised the cybersecurity world. Previously known for mobile banking fraud and Android-based malware, the group prooved that they have elevated their capabilities advancement to enterprise ransomware with this attack. The attack locked servers controlling the park's theme management, hotel reservations, and most importantly, the “Disney Premier Access” (FastPass) system.



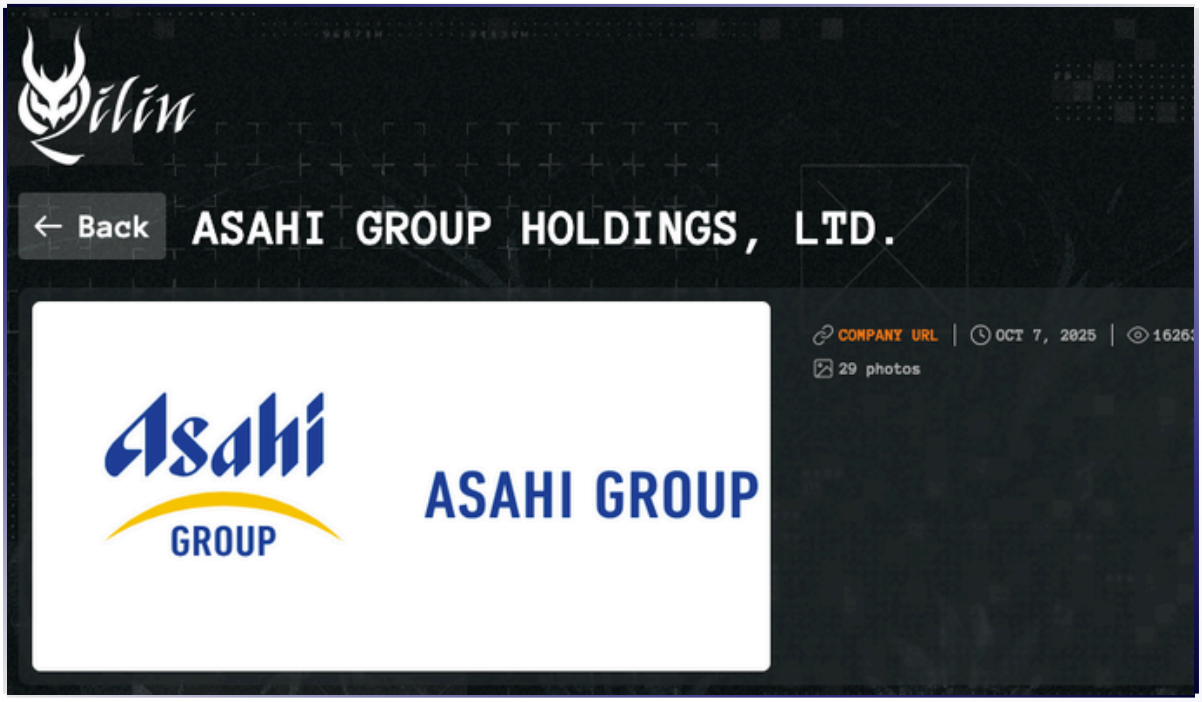
The Anubis group employed an unusual method in the attack. Instead of classic RDP or VPN attacks, they jumped to the internal network via an advanced Android “dropper” that they infiltrated into the park employees' corporate mobile devices. This “Mobile-to-Endpoint” lateral movement technique allowed them to bypass traditional firewalls and EDR solutions. As a result of the attack, the park's digital payment points and ticketing counters were rendered inoperable for 48 hours, forcing visitors to resort to physical cash.

The group demanded 15 million euros in exchange for the encrypted data. When their demands were rejected, Anubis leaked the park's VIP customer database and drafts of Disneyland's new theme park projects (Blueprint) planned for the next 5 years. Disneyland Paris management confirmed that the incident stemmed from a “Mobile Security Vulnerability” and switched to a zero trust policy on all employee devices.

Ransomware Incidents

Asahi Group Holdings

In September 2025, Asahi Group Holdings, Japan's largest beverage manufacturer, suffered a crippling ransomware attack that paralyzed its domestic production and logistics network. The incident forced the company to suspend operations at multiple factories and distribution centers, leading to a nationwide shortage of its flagship "Super Dry" beer. For weeks, the company had to revert to manual processes, accepting orders via telephone and fax, as digital inventory systems remained offline.

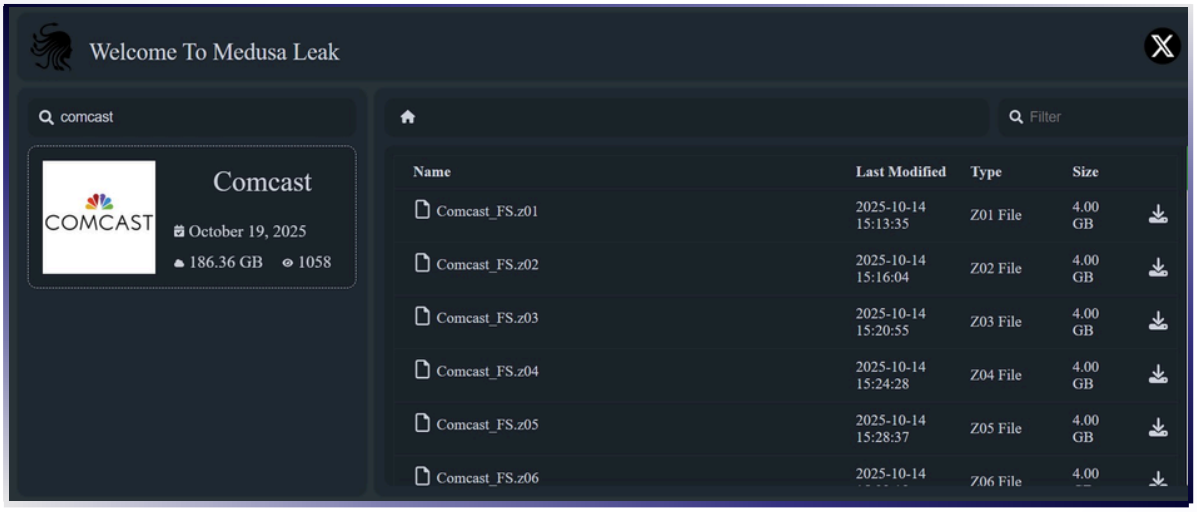


The attack was attributed to the Qilin ransomware cartel, known for targeting high-value industrial sectors with customized "Rust-based" payloads. The breach compromised the personal data of nearly 2 million individuals, including customers, employees, and business partners. While Asahi refused to pay the ransom, the operational disruption caused a 40% plunge in soft drink sales and significant financial losses during the critical recovery period, highlighting the fragility of "Just-in-Time" manufacturing against modern cyber threats.

Ransomware Incidents

Comcast

In September 2025, the telecommunications giant Comcast was targeted by the Medusa ransomware gang in a high-profile extortion attempt. The attackers claimed to have breached the company's internal servers, exfiltrating over 834 GB of sensitive corporate data. The group demanded a ransom of $1.2 million to prevent the leak, marking one of the most significant direct challenges to a major US service provider in 2025.



Following Comcast's refusal to negotiate, Medusa carried out their threat in October 2025, publishing the stolen dataset on their leak site. The dump included critical internal documents such as actuarial reports, insurance modeling scripts, and employee information. The incident compounded a challenging year for Comcast, which had already faced a $1.5 million FCC fine in November related to a separate third-party vendor breach, highlighting the mounting regulatory and operational pressures on the telecom sector.

Ransomware Incidents

Volkswagen Group (France)

In early October 2025, the French operations of global automotive giant Volkswagen Group suffered a cyberattack by the Qilin ransomware group, known for targeting Linux and virtualised systems (ESXi). The attack paralysed critical databases and dealer communication infrastructure within Volkswagen Group France's internal networks.

The Qilin group went beyond conventional encryption tactics, announcing that it had exfiltrated 150 GB of highly sensitive data from the network during the attack. To strengthen their ransom demands, the group released samples from the leaked dataset. This data included highly critical documents such as photocopies of French customers' IDs, vehicle registration information, technical service histories, and financing agreements with dealers.

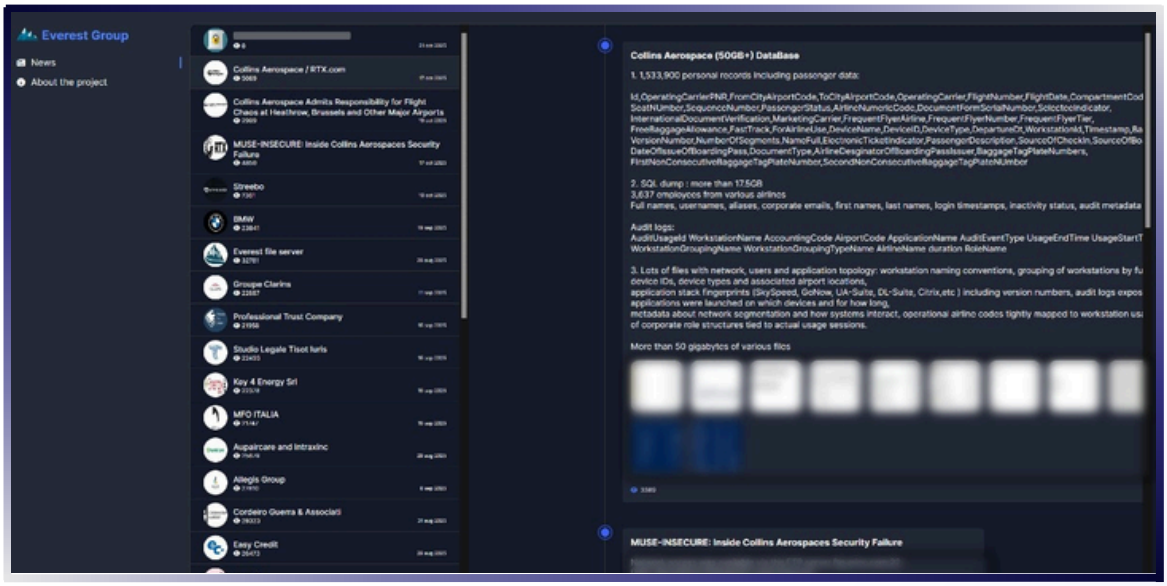
Following the incident, Volkswagen Group France confirmed that it had contacted the relevant cyber security authorities and data protection agencies. When the Qilin group failed to reach an agreement, they subsequently published a significant portion of the stolen data on a Dark Web leak site as publicly available. This situation left the company facing not only an operational disruption but also substantial fines under the European Union's strict GDPR regulations and significant reputational damage among its customers.

Ransomware Incidents

Collins Aerospace

IIn the final quarter of 2025, Collins Aerospace, RTX Corporation's most critical subsidiary and the backbone of the global aerospace defence industry, became the target of the Everest Ransomware group. This attack went down in history as one of the most dangerous national security breaches of the year, not only because of the encrypted files but also due to the group's aggressive 'access trading' tactic.

In an announcement on its dark web leak site, the Everest group claimed to have gained full administrator (Domain Admin) access to Collins Aerospace's systems. The group took an unusual approach to corner the company during ransom negotiations: instead of publicly releasing the data, they put the 'backdoor' access to the company's internal network up for sale to foreign intelligence agencies and rival defence industry spies.



The leaked sample files included military aircraft cockpit modernisation projects, space suit designs jointly developed with NASA, and US Air Force technical schematics subject to ITAR (International Traffic in Arms Regulations) restrictions. The Everest group's threat to 'sell access to the highest bidder' triggered a red alert at the Pentagon and NATO.
Collins Aerospace announced that it had shut down all external network gateways and switched to 'Offline Mode' following the attack, and that it was cooperating with federal authorities.

Ransomware Incidents

Lee Enterprises

In June 2025, Lee Enterprises, publisher of more than 70 daily newspapers across the United States (including the St. Louis Post-Dispatch and The Buffalo News), was attacked by the Qilin ransomware group, one of the most aggressive actors in the cybercrime world. The attack targeted not only corporate offices but also the company's printing facilities and digital publishing infrastructure (CMS), blocking access to news for millions of readers.

The Qilin group used its signature 'Rust-based ESXi Encryption' technique in this attack. The attackers infiltrated the company's virtualised server infrastructure and locked hundreds of virtual machines within minutes, where newspaper layouts were created, advertisements were managed, and subscriber data was stored. This led to many local newspapers were unable to print the next day or to reduce the number of pages and produce an 'Emergency Edition'.

Shortly after the attack, Qilin listed Lee Enterprises on a leak site on the dark web and threatened to publish 600 GB of data stolen from the company. The leaked data included payment details for hundreds of thousands of subscribers, employees' social security numbers and, more importantly, journalists' confidential notes about their news sources. When the ransom demand was not met, Qilin began leaking this data in 'batches'.
Lee Enterprises underwent a weeks-long 'Incident Response' process to clean up its systems and get operations back up and running. This incident became the most symbolic attack of 2025, demonstrating that cyberattacks are not only a commercial loss but also a direct threat to 'Freedom of the Press and the Public's Right to Know'.

Ransomware Operation

8BASE Ransomware Operation

In February 2025, the 8Base ransomware group was officially dismantled through "Operation Phobos Aetor," a joint effort by Europol, the FBI, and German authorities. The operation successfully seized the group's dark web infrastructure, replacing their data leak sites with law enforcement banners and effectively ending one of the most persistent threats to small and medium-sized businesses.

The operation's physical enforcement took place in Phuket, Thailand, where local police arrested four Russian nationals identified as the group's leadership. These individuals were responsible for managing the global distribution of Phobos ransomware variants. Their arrest and subsequent extradition proceedings sent a clear message that cybercriminals can no longer rely on geographic distance for immunity.

Following the seizure of 8Base's servers, authorities recovered thousands of decryption keys and distributed them freely to victims through the "No More Ransom" initiative. This allowed hundreds of companies to restore their data without paying a dime. Additionally, law enforcement froze the group's cryptocurrency assets, permanently cutting off the financial resources needed to rebuild their network.

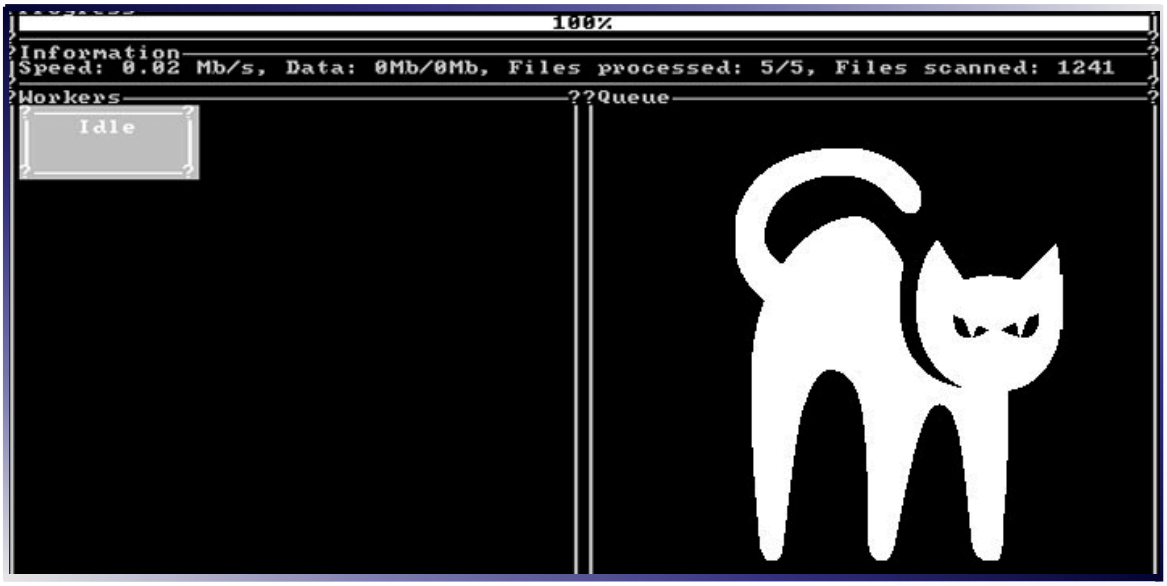
The collapse of 8Base was a strategic victory for cybersecurity in 2025, as the group was the primary driver of the Phobos ecosystem. In the months following the takedown, analysts recorded a 60% drop in ransomware incidents targeting the manufacturing sector, proving the effectiveness of coordinating physical arrests with digital infrastructure seizures.

Ransomware Operation

US Nationals Convicted in ALPHV (BlackCat) Scheme

On December 30, 2025, a significant legal victory was achieved against the ALPHV (BlackCat) ransomware ecosystem with the guilty pleas of two U.S. nationals, Ryan Goldberg and Kevin Martin. Unlike the typical profile of state-sponsored foreign actors, these defendants were cybersecurity professionals who leveraged their technical training to attack American infrastructure. Operating as "Affiliates" in the Ransomware-as-a-Service (RaaS) model, they targeted over 1,000 victims, agreeing to a revenue split where they retained 80% of the extortion proceeds while remitting 20% to the BlackCat administrators.

The investigation, led by the FBI Miami Field Office, revealed the lucrative nature of their operations, including a single successful extortion of approximately $1.2 million in Bitcoin.



The Department of Justice emphasized that ransomware is not just a foreign threat but can originate from within U.S. borders. The convictions follow the FBI's strategic disruption in late 2023, where decryption keys were released to save victims nearly $99 million.

The prosecution of Goldberg and Martin marks a turning point in attribution capabilities in 2025. It demonstrates that law enforcement can successfully pierce the anonymity of Tor-based networks and hold domestic cybercriminals accountable. Scheduled for sentencing in March 2026, the defendants face up to 20 years in prison, sending a clear message that the "Affiliate" model offers no immunity from prosecution, regardless of geographic location or technical sophistication.

Ransomware Statistics

Section 2

Ransomware Statistics

Ransomware has evolved significantly in 2025, moving beyond traditional encryption to 'extortion-only' and 'data theft' strategies. This year, threat actors have increasingly targeted backups and leveraged regulatory fines (GDPR) to pressure victims. Operators have shifted towards a more agile, cell-based structure, making detection and attribution more challenging than ever.

Cyberthint threat hunters have been closely monitoring these shifting tactics throughout the year, meticulously collecting data from dark web leak sites and private negotiation channels. This data was provided by Cyberthint's Dark Monitor and threat intelligence analyst team for the purpose of analyzing the global threat landscape.

Summary

- In 2025 compared to 2024, the volume of high impact ransomware attacks increased by 35%
- There were more than 7,200 publicly reported ransomware victims in 2025.
- 24 new major ransomware groups were detected, filling the void left by dismantled cartels.
- RansomHub has become the ransomware group with the highest number of attacks in 2025, dethroning previous leaders with its aggressive affiliate model.
- In 2025, the USA remained the most targeted country, followed by the UK and Germany.

Ransomware groups emerging in 2025:

- Eldorado
- Volcano Demon
- Cicada3301
- InterLock
- Embargo
- ShrinkLocker
- Yurei
- Global Group
- Kraken
- Ailock
- Babuk V2
- VanHelsing
- Dire Wolf
- Warlock
- Sinobi
- The Gentlemen
- Nova (RaLord)
- Gunra
- Silent
- CrazyHunter
- NightSpire

New Ransomware Groups

Eldorado

This group, which appeared on cybersecurity radars in early 2025, stands out from others by developing its own unique encryption infrastructure rather than using leaked code found on the market. Targeting VMware ESXi virtual servers and Windows systems in particular, Eldorado bypasses EDR (Endpoint Detection and Response) solutions by leveraging drivers that directly interact with the system kernel rather than relying on PowerShell, locking virtual machines within minutes.

Volcano Demon

This group, which has completely abandoned the classic 'Dark Web Leak Site' method, is known for encrypting systems with 'LukaLocker' and then blackmailing company executives and IT managers by calling them directly on their personal phones. Their strategy, based on leaving no trace and keeping negotiations secret, makes it difficult for intelligence agencies to track the group while increasing the psychological pressure on the victims.

Cicada3301

This group, named after the famous cryptographic internet puzzle, uses an extremely sophisticated ransomware written in the Rust programming language, reminiscent of the technical legacy of the ALPHV (BlackCat) group. Capable of operating on both Windows and Linux/NAS devices, the group stands out for its cross-platform capabilities, aggressive attacks targeting critical infrastructure in 2025, and the extremely short payment deadlines it imposes on its victims.

New Ransomware Groups

InterLock

This new entity, which has entered the sector as the 'Big Game Hunter,' targets only large corporations and healthcare organisations with high turnover, rather than small businesses. After lying dormant within the network for weeks (dwell time), the group first destroys backup systems, then locks down systems and demands astronomical ransoms, making it one of the groups with the highest average ransom demands in 2025.

Embargo

Emerging in mid-2025, this group is known for its specially coded 'Process Killer' tools designed to disable sophisticated EDR/XDR security solutions. Thanks to their Rust-based infrastructure, the group can simultaneously target Windows and Linux systems. To increase pressure, they not only leave ransom notes digitally but also force physical printouts from all printers on the network, creating chaos in the office environment.

ShrinkLocker

This is an extremely cunning group that exploits Windows' legitimate disk encryption tool, 'BitLocker,' instead of using its own proprietary encryption software (Living-off-the-Land). Since security software recognises BitLocker as a legitimate Windows component, it does not raise an alarm. The group deletes the system's recovery keys and locks the disk, carrying out attacks that are particularly difficult to detect in the public and energy sectors.

New Ransomware Groups

Yurei

The most distinctive feature of this group, known as Ghost Ransomware(has also entered the literature under this name) since late 2025, operates entirely in memory (RAM), built no files on the system (fileless) and shows no disk activity until the encryption process is complete. By injecting itself into legitimate Windows processes (svchost.exe), this structure completely blinds traditional antivirus and static analysis tools. Targeting financial institutions, particularly in the Asia Pacific region, the group makes forensic processes nearly impossible due to its trace free nature.

Global Group

Emerging from the ashes of the former BlackLock and Mamona ransomware operations, this group pioneered the "AI-Powered RaaS" model in 2025. Global Group has increased its operational speed to levels unattainable by human operators by using specially trained Large Language Models (LLMs) in pre-attack reconnaissance processes and negotiations with victims. The group uses an autonomous "Data Management Module" that automatically classifies sensitive data within compromised networks and leaks it in the most damaging way possible (e.g., to rival companies or regulatory agencies) if the ransom is not paid.

Kraken

This is an extremely cunning group that exploits Windows' legitimate disk encryption tool, 'BitLocker,' instead of using its own proprietary encryption software (Living-off-the-Land). Since security software recognises BitLocker as a legitimate Windows component, it does not raise an alarm. The group deletes the system's recovery keys and locks the disk, carrying out attacks that are particularly difficult to detect in the public and energy sectors.

New Ransomware Groups

Ailock

This group, which claims to have the fastest encryption engine of 2025, bypasses security sensors by perfecting the intermittent encryption technique. Instead of encrypting entire files, Ailock encrypts every 16th byte, thereby locking gigabytes of data in seconds without creating anomalies in the system's I/O (input/output) traffic. Targeting healthcare and e-commerce systems where time is critical, the group is known for completing operations without giving victims a chance to intervene.

Babuk V2

This is an extremely dangerous variant built on the original Babuk source code leaked years ago, but rewritten according to 2025 modern defense mechanisms. This group targets companies' backup and restore capabilities, focusing particularly on ESXi virtualization platforms and NAS (Network Attached Storage) devices. Babuk V2 exploits authorization vulnerabilities in Linux based systems to encrypt the storage layer that Windows based security software cannot protect, making it impossible to recover data without paying the ransom.

VanHelsing

It is a low-cost yet highly aggressive RaaS (Ransomware-as-a-Service) model that lowers the entry barrier in the market. Ironically named after a monster hunter, this group focuses on hunting down antivirus and EDR (Endpoint Detection and Response) solutions. Using specially developed scripts, VanHelsing disables popular security software by launching it in “Safe Mode,” offering an “automated attack kit” that allows even affiliates with low technical skills to compromise complex corporate networks.

New Ransomware Groups

Dire Wolf

It is not just a ransomware group motivated solely by financial gain, but also a hybrid structure that acts like an APT actor. After infiltrating the system, Dire Wolf does not immediately initiate the encryption process; it remains silently on the network for an average of 25 days (dwell time), mapping backup routines, administrator habits, and the location of critical data. Using social engineering techniques to pose as IT personnel, this group gains the victim's trust and infiltrates the system through legitimate means, then locks it down using privileged access from within, making detection extremely difficult.

Warlock

This is an extremely opportunistic group that uses corporate collaboration platforms as an attack vector. Warlock infiltrates networks by targeting unpatched vulnerabilities on Microsoft SharePoint servers. Instead of encrypting files, it pulls critical documents to its own servers and then applies the Double Extortion tactic. The group bypasses SharePoint's authorization mechanism, creating shadow accounts that are difficult even for administrators to detect, thereby ensuring persistence on the network.

Sinobi

This group poses a silent threat targeting technology companies in Japan and East Asia. Sinobi keeps network traffic so low during an attack that even if data exfiltration takes weeks, it does not trigger IDS alarms. During the encryption phase, it silently disables the system's Volume Shadow Copy services, eliminating any chance of recovery. They operate under the motto “Silent Infiltration, Certain Destruction.”

New Ransomware Groups

The Gentlemen

The Gentlemen use an extremely professional and corporate language in their negotiations with victims. Their customer service departments even provide victims with free advice on how to close security vulnerabilities. However, this politeness is deceptive; the group targets law firms and financial advisory firms in particular, threatening to violate customer confidentiality and, if the ransom is not paid, sending the data directly to rival firms via email rather than posting it on the Dark Web.

Nova (RaLord)

Nova is an aggressive group based on the RaLord ransomware variant, but transformed into a modern RaaS platform. Nova boasts Fast Encryption technology; instead of encrypting all files on the system, it only corrupts file headers. This method allows them to render a 10 TB database unusable in minutes. Targeting the gaming industry and companies that process high volumes of data, Nova leaves defense teams no response time with its operational speed.

Gunra

It is a dangerous group with cross-platform attack capabilities, specifically targeting Linux servers. Unlike Windows-based ransomware, Gunra uses binary files written in the Go (Golang) language that can directly encrypt ESXi hypervisors and Docker containers. When infiltrating cloud infrastructures, they prioritize backup servers as their primary targets. They ruthlessly exploit security vulnerabilities in companies Cloud Native transformations.

New Ransomware Groups

Silent

True to its name, this group leaves no ransom note on the system and does not change the desktop wallpaper. Silent encrypts files and changes file extensions to random characters. Victims realize they have been attacked when their applications stop working. They use a hidden portal on the Tor network for communication, and the address of this portal is hidden in the metadata of the encrypted files. This hide and seek tactic is designed to confuse automated analysis tools.

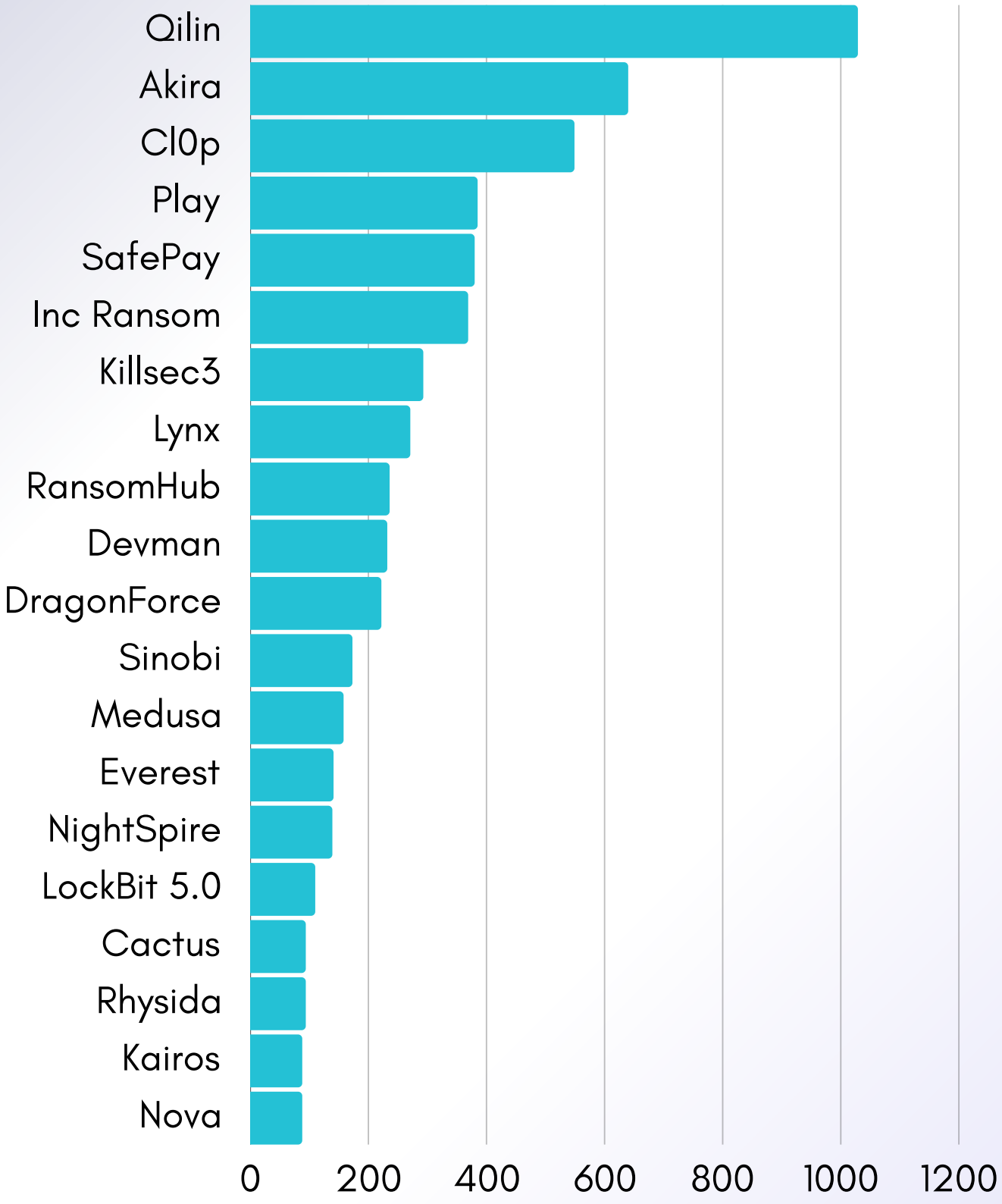
CrazyHunter

This group, which is the nightmare of database administrators (DBAs), focuses primarily on SQL, Oracle, and MongoDB servers. Instead of encrypting databases, CrazyHunter deletes tables using the Drop Table command, but copies the data to their own servers before deletion. They send their victims a message stating, "Your data has not been encrypted; we have it. Pay up if you want it back." This method eliminates the risk of dealing with a decryption key and allows them to present the process entirely as a "Data Recovery Service."

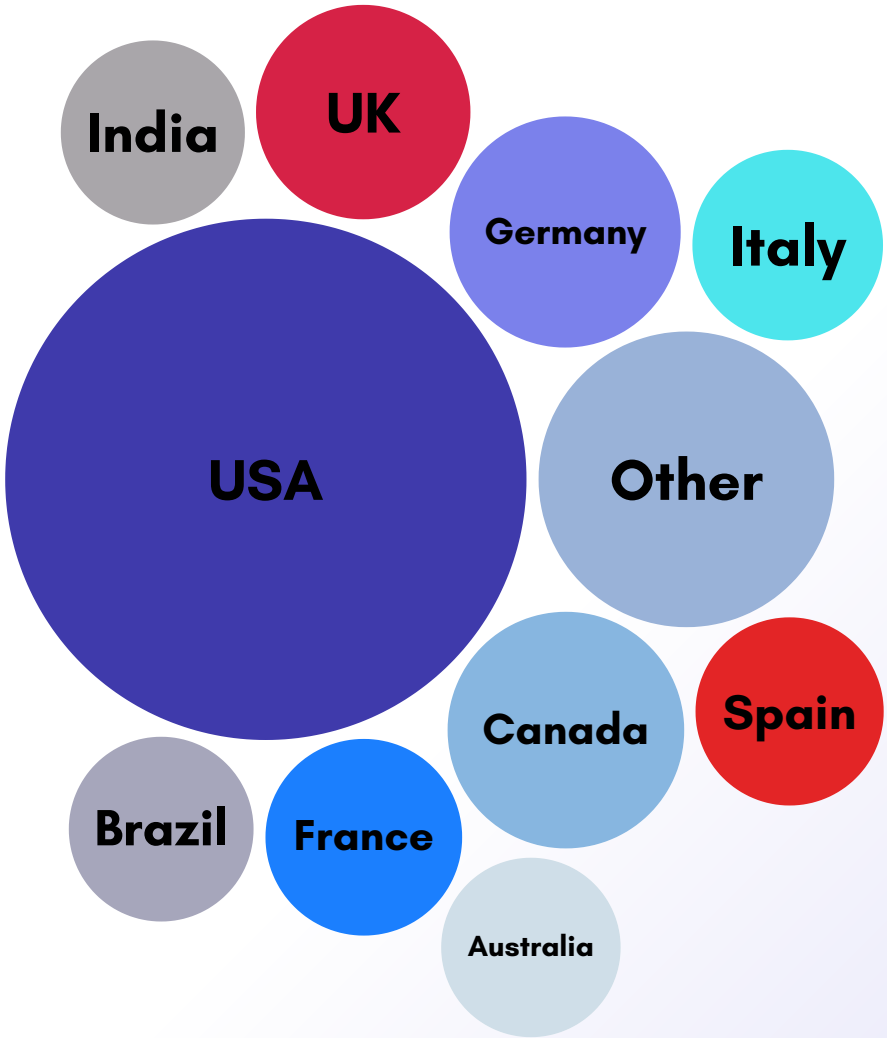
NightSpire

It is a ransomware group focused on espionage that targets corporate secrets rather than operational data. NightSpire can lie dormant in the system for months after infiltrating it. During this time, it steals patent applications, merger/acquisition (M&A) documents, and R&D data. It only uses encryption as a smoke screen in the final stage of the operation to cover the tracks of the stolen data and stall incident response teams.

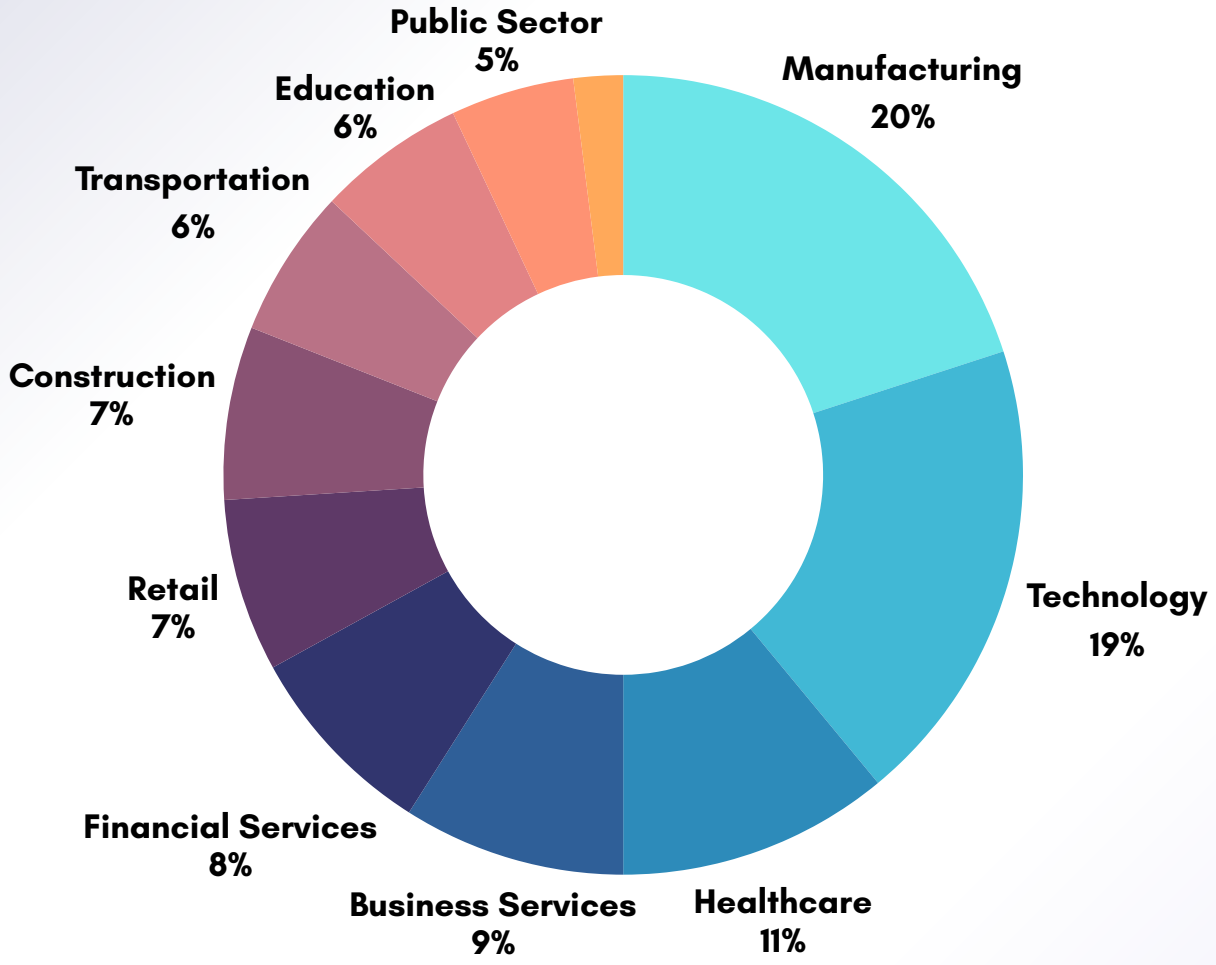
Top Ransomware Groups 2025



Top Affected Countries by Ransomware Attacks



Top Affected Industries by Ransomware Attacks



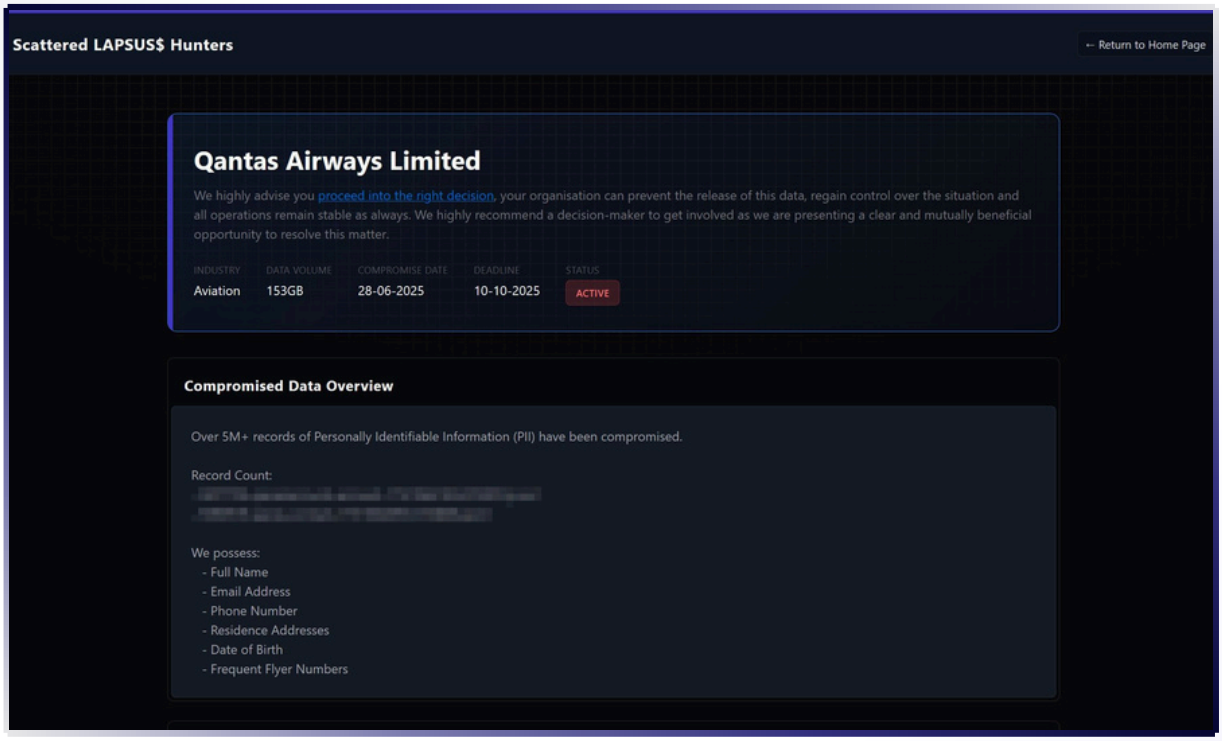
Data Exposure Analysis

Section 3

Qantas Airways Data Leak

In June 2025, Australia's largest airline, Qantas Airways, suffered a significant data breach affecting nearly six million customers. The breach, part of a larger campaign targeting Salesforce instances, was orchestrated by the cybercriminal collective known as Scattered Lapsus$ Hunters (SLSH).

The attackers gained access the system by impersonating IT support staff in a sophisticated voice phishing campaign targeting a third-party call center in the Philippines. This allowed them to infiltrate Qantas' Salesforce environment and exfiltrate 153 GB of sensitive customer data.



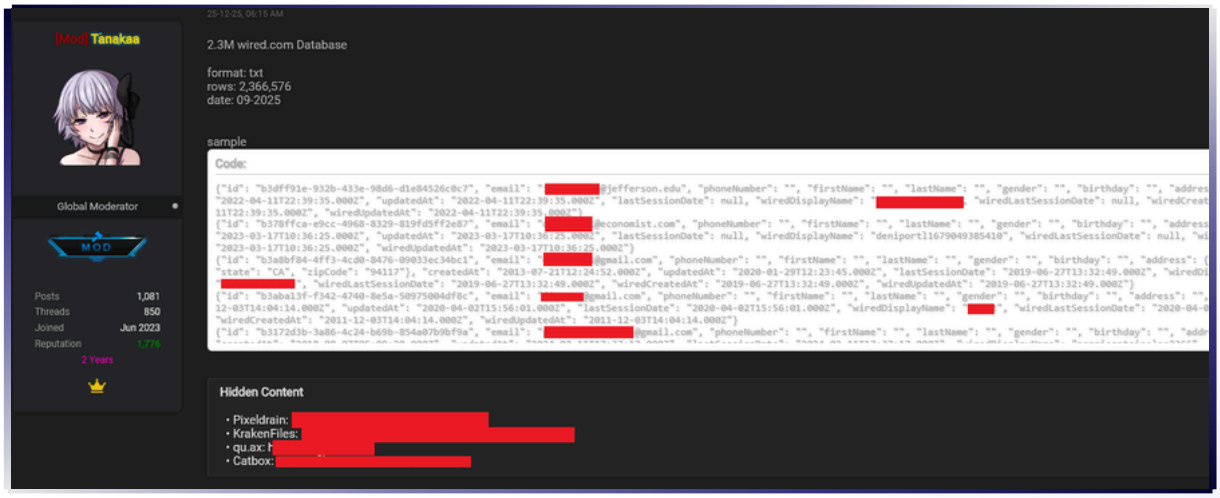
The compromised data includes customer names, email addresses, phone numbers, dates of birth, and Qantas Frequent Flyer numbers. While Qantas obtained a court injunction to prevent the data's publication , SLSH threatened to release the data publicly if a ransom was not paid by October 10.

The collective also launched a harassment campaign, offering bounties to followers who spammed and threatened company executives. Salesforce denied any platform vulnerability, attributing the incident to social engineering tactics used against third-party vendors.

WIRED Data Leak

In late 2025, the cybersecurity world was rocked by a massive data breach targeting media giant Condé Nast and technology publication WIRED. On December 25, 2025, an actor named “Tanakas” posted a database containing 2.3 million user records belonging to WIRED.com on hacking forums. This leak included up-to-date data dating back to September 2025 and exposed critical personal information such as email addresses, usernames, phone numbers, birth dates, and physical addresses to the public.

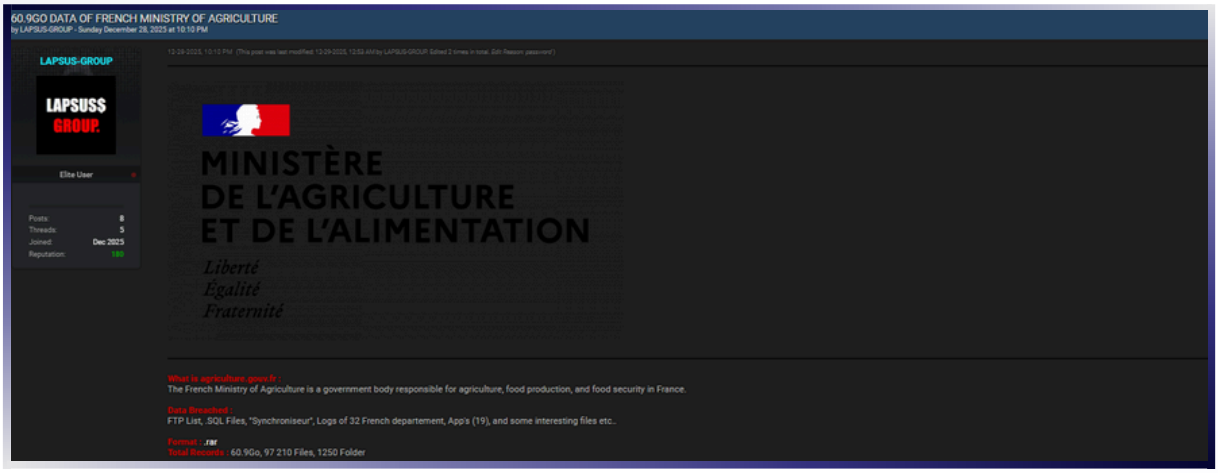
The leak began with a sophisticated social engineering operation carried out by an attacker codenamed “Lovely,” who posed as an ethical researcher. The attacker manipulated cybersecurity researchers by claiming to have discovered six different security vulnerabilities affecting 33 million accounts in Condé Nast systems, allowing profile information to be viewed or passwords to be changed. It was later revealed that the actor, who initially claimed to only want to report the vulnerabilities, had actually quietly leaked the entire database and used third parties to reach the company for their own benefit.



Following the incident, cybersecurity experts and the Have I Been Pwned platform quickly verified the authenticity and currency of the WIRED data. The leaked 2.3 million WIRED dataset is considered only a subset of the total 33 million Condé Nast data pool that the attacker claims to possess. This breach once again highlighted how devastating identity theft risks can be in the 2025 threat landscape and exposed the structural weaknesses of major media platforms in protecting user data.

French MASA Data Leak

On December 28, 2025, a sensitive database allegedly belonging to the French Ministry of Agriculture, totaling 60 GB in size, was leaked to the public via “Breachforums.bf” by the threat actor known as LAPSUS-GROUP. This leak is not just a simple data dump; it is a comprehensive operational dataset containing FTP lists, .SQL files, a synchronization tool called “Synchroniseur,” 19 different applications, and log records belonging to 32 French departments. The fact that the attackers obtained not only structured data but also tools and application files that manage internal data flows indicates that the leak provides deep insight into the organization's internal operations.



The content of the leak poses multidimensional risks to public institutions and citizens. While SQL files contain structured sensitive records, log records covering 32 departments expose internal IP addresses, user behavior, and system architecture. In particular, the compromise of synchronization tools and application binaries carries the risk that these systems could be reverse engineered, paving the way for more destructive attacks in the future. Considering LAPSUS-GROUP's high-profile leaks in the past, this action is assessed as aiming not only to steal data but also to undermine public trust and exert reputational pressure on the institution.

This case has once again highlighted how critical Dark Web visibility is in public sector cybersecurity. Rapid detection of the breach is the only way to ensure timely intervention steps such as password resets, communication strategies, and system shutdowns. The French Ministry of Agriculture case stands as one of the most symbolic public sector breaches of 2025, illustrating how legacy systems, broad access privileges, and inadequate underground monitoring activities can lead to catastrophe.

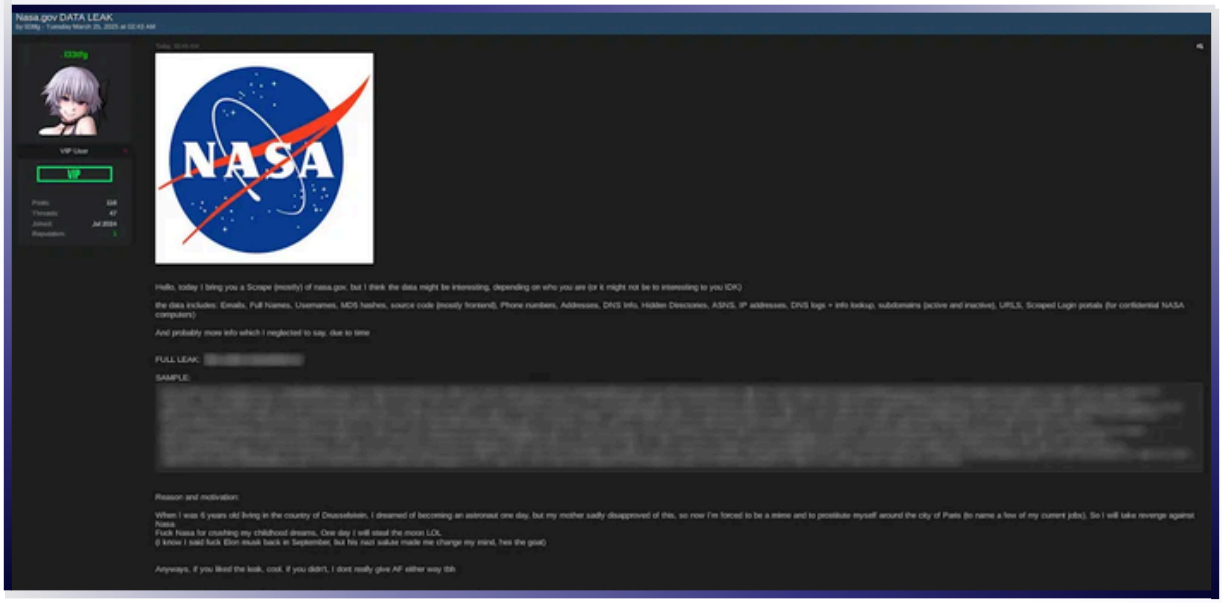
Mango Data Leak

In May 2025, the global fashion giant Mango became the target of a sophisticated cyber extortion campaign that disrupted its operations across 110 countries. While physical stores remained open, the attack crippled the company's internal logistics systems and design platforms. The breach exposed sensitive corporate data, including financial reports and employee contracts, forcing the retailer to temporarily suspend its global e-commerce shipments to prevent further compromise.

The attack was claimed by RansomHouse, a group known for presenting themselves not as hackers but as security auditors. Unlike traditional ransomware groups, they did not encrypt Mango's files; instead, they exfiltrated 4 terabytes of proprietary data and demanded payment solely to prevent its release. In a mocking statement published on their dark web blog, the group ridiculed Mango's cybersecurity posture, claiming they had access to the network for months due to a simple unpatched vulnerability in the company's VPN gateway.

NASA Data Leak

On December 28, 2025, a sensitive database allegedly belonging to the French Ministry of Agriculture, totaling 60 GB in size, was leaked to the public via “Breachforums.bf” by the threat actor known as LAPSUS-GROUP. This leak is not just a simple data dump; it is a comprehensive operational dataset containing FTP lists, .SQL files, a synchronization tool called “Synchroniseur,” 19 different applications, and log records belonging to 32 French departments. The fact that the attackers obtained not only structured data but also tools and application files that manage internal data flows indicates that the leak provides deep insight into the organization's internal operations.



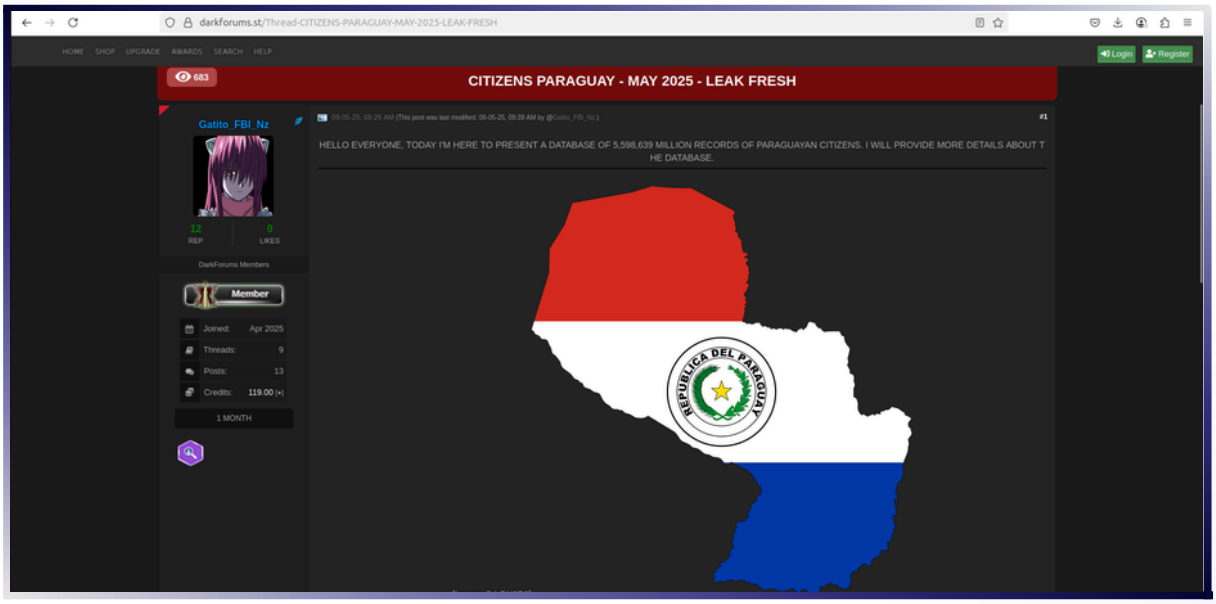
On March 25, 2025, a threat actor using the alias l33tfg on cybercrime forums posted a claim stating they had leaked a large dataset belonging to the United States National Aeronautics and Space Administration (NASA.gov). This incident was carried out not through a direct cyber intrusion into the agency's internal systems, but rather through intensive scraping of NASA's public infrastructure, entry portals, and inactive subdomains. The threat actor emphasized that the systems were not directly hacked, but rather that public data was professionally collected to create an institutional roadmap.

The leaked dataset contains critical technical and personal information about the organization's digital footprint. The alleged contents include NASA employees' email addresses, full names, and usernames, as well as password hashes in MD5 format. More critically, the leak exposes the organization's internal system entry portals, secret directories, IP/DNS configurations, and frontend source code. While such data may not directly cause a system catastrophe, it provides attackers with a unique intelligence base for future spear-phishing attacks and attempts to infiltrate corporate networks.

Paraguay Citizen Records Leak

In May 2025, an actor using the alias “Gatito_FBI_NZ” in the cybercrime world claimed to have put a massive dataset belonging to Paraguayan citizens up for sale on a popular hacking forum. This leak, containing the personal records of approximately 5.59 million Paraguayan citizens, has the potential to directly affect a large portion of the country's total population. Sample data and partial CSV files shared on the forum supported the authenticity of the leak.

The leaked dataset contains highly sensitive personal data such as full names, national ID numbers, contact information, dates of birth, and parental information. The threat actor aimed to quickly monetize the data by demanding a relatively low price of $400 for full access to this database.

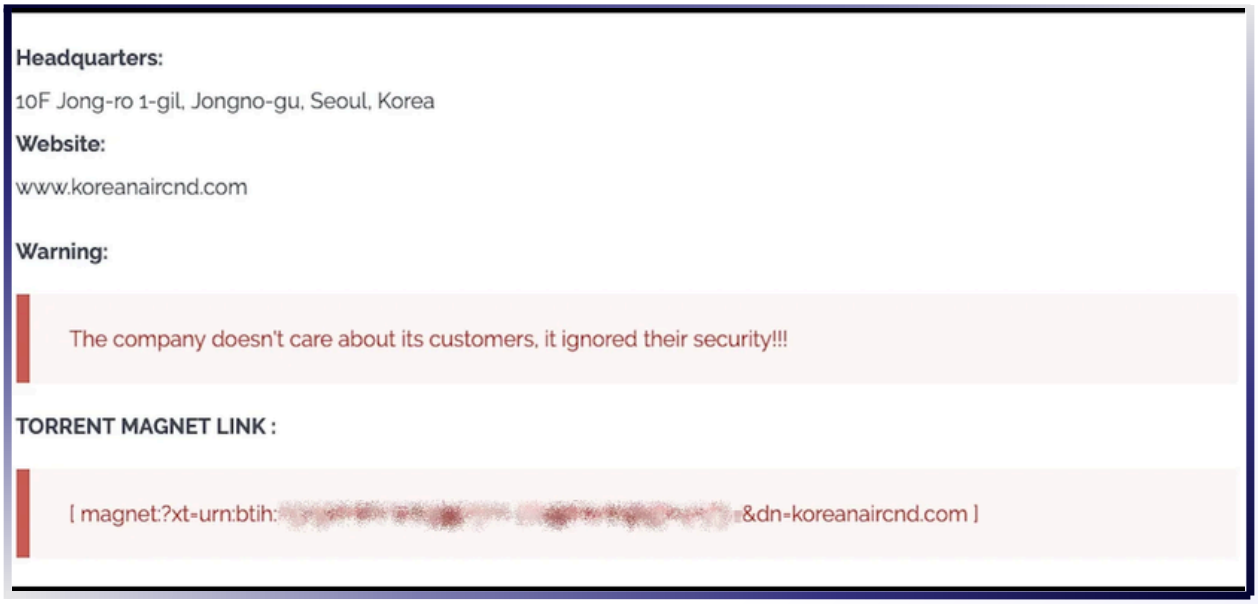


The Paraguay case reinforces the trend that public sector data will become a low-cost, high-volume commodity in underground markets by 2025. Part of the multi-country mega breaches trend, this incident demonstrates how governments' failure to protect citizen data translates into a national security risk. Such large-scale breaches not only undermine individual security but also erode long-term digital trust in government institutions.

Korean Air Data Leak

By the end of December 2025, Korean Air, South Korea's flag carrier airline, announced that it had experienced a serious data breach originating from a third-party supplier, affecting approximately 30,000 employees. The breach occurred as a result of a cyberattack targeting the systems of Korean Air Catering & Duty-Free (KC&D), a company that Korean Air spun off in 2020 but which continued to operate as its catering and duty-free supplier. In this incident, which took place in November 2025 and was claimed by the Clop ransomware group, the stolen data was publicly shared via Torrent on the group's dark web leak site.

The technical details of the attack reveal that this breach is part of a broader series of attacks carried out by the Clop group throughout 2025, targeting Oracle EBS (E-Business Suite) instances worldwide. The compromise of KC&D's ERP (Enterprise Resource Planning) systems resulted in the exposure of critical financial and identity information, such as the full names and bank account numbers of Korean Air employees. This case is considered one of the largest "enterprise application exploits" of 2025, alongside other major organizations targeted in the same campaign, such as Logitech, Harvard University, and The Washington Post.

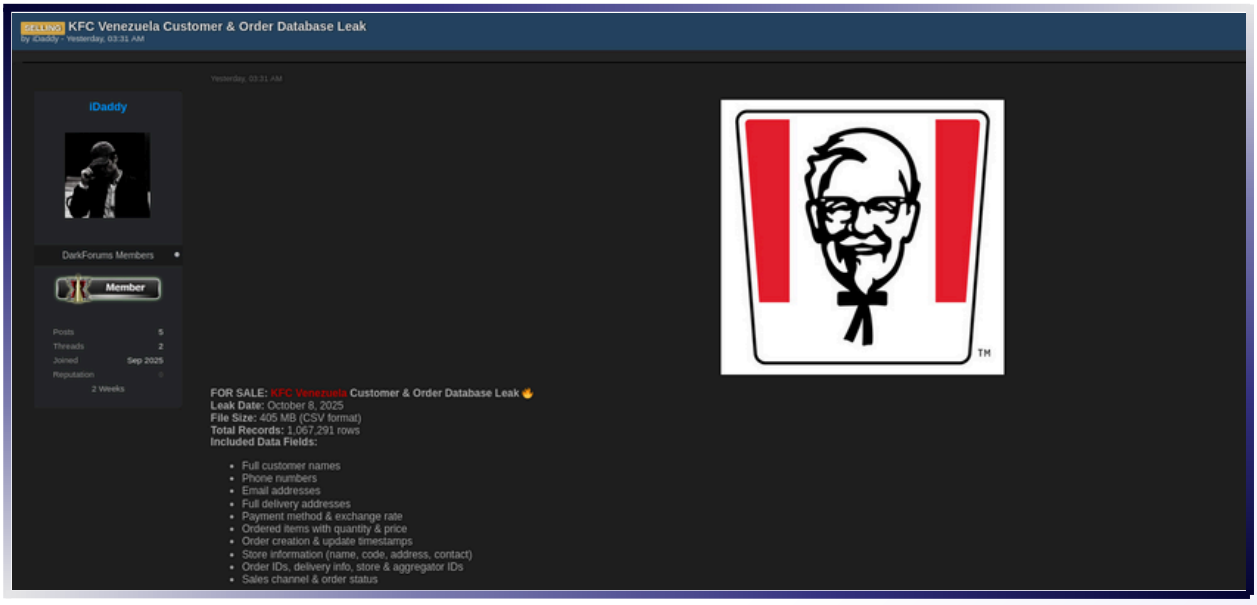


The Korean Air case is the most concrete example of the "Supply Chain and Spun-Off Affiliate Risks" trend. Companies' failure to adequately monitor data sharing processes and digital trust relationships with their former affiliates, from which they have operationally separated, serves as a weak link for attackers to infiltrate critical systems. The post-breach warning to employees about sophisticated vishing/phishing attacks impersonating the company and the US State Department's reiteration of its $10 million reward pledge against the Clop group reflect the seriousness of the global fight against the cybercrime economy at the end of 2025.

KFC Venezuela Customer Data Leak

In October 2025, a massive customer dataset belonging to fast-food giant KFC's Venezuelan operations was leaked on underground forums. The breach, detected during real-time monitoring operations on October 8, 2025, was shared on the popular underground marketplace Darkforums by an actor known as "iDaddy." This leak, containing approximately 1,067,291 customer records, includes fresh data obtained from the company's online order and delivery management platform.

The leaked database consists of over 1 million lines containing customers' full names, phone numbers, email addresses, and physical delivery addresses, as well as payment methods used, exchange rates, and detailed order histories. Although credit card numbers were not directly leaked, the disclosure of order details and physical addresses has heightened the risks of identity theft, targeted phishing/smishing, and location-based fraud. Furthermore, the leak of store codes and order tracking numbers indicated that third-party delivery operators and affiliates working with KFC were also indirectly at risk.

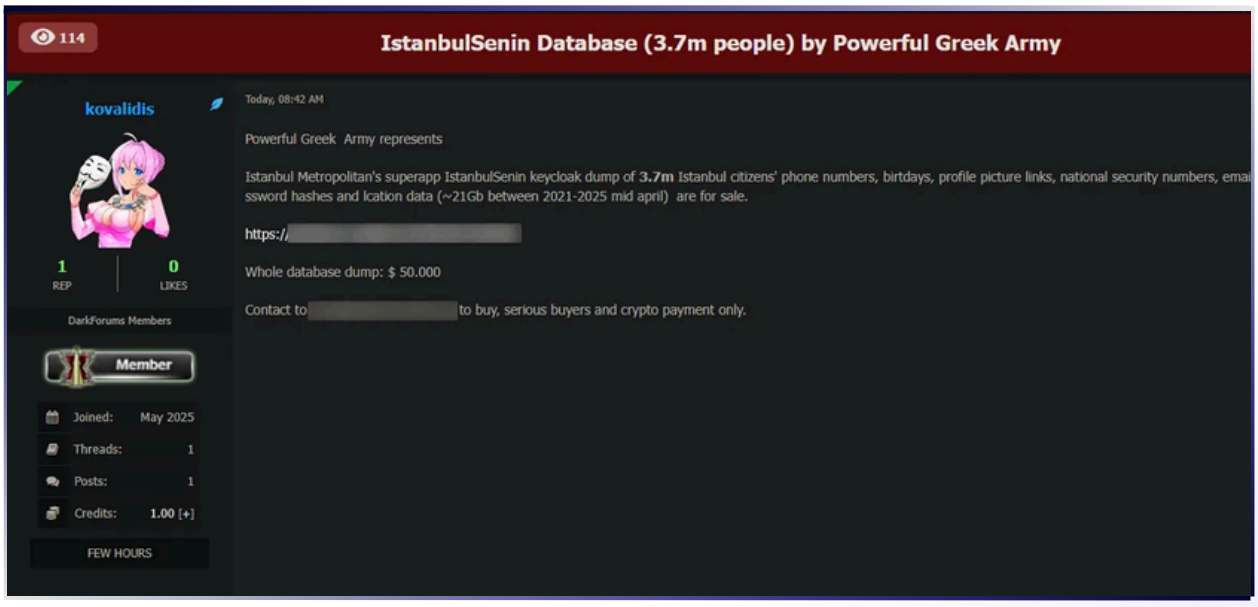


The KFC Venezuela case is one of the most critical examples of the frequently highlighted trend of "Increasing Threats to Retail and Food Distribution Ecosystems" in Latin America. Food delivery platforms, which generally have lower security controls compared to financial institutions, have become easy targets for cybercriminals in terms of behavioral and personal data mining. This breach once again demonstrates the urgent need for proactive dark web monitoring strategies that go beyond traditional firewalls and enable the detection of leaked data before it is weaponized.

Istanbul Senin Data Leak

On May 26, 2025, a threat actor using the alias “kovalidis” on the cybercrime forum DarkForums announced that they had put the database of the Istanbul Metropolitan Municipality's (İBB) digital assistant application “İstanbul Senin” up for sale. The data set, which allegedly contains the personal data of approximately 3.7 million citizens (name, surname, Turkish ID number, mobile phone number, and location coordinates), was offered for $50,000. Although the attacker claimed to have shared the announcement on behalf of the Powerful Greek Army group, the lack of confirmation from the group's official channels raised suspicions that the incident could be a false flag operation. However, it remained a serious matter when it resurfaced in the public eye in November 2025.

The investigations conducted have proven that the sample data is not a mixed set compiled from previous large data leaks or infostealer logs, but rather current records specific to the application (UUID/GUID, record dates, etc.). Cross-verifications conducted through platforms such as Youthside and direct communication established with victims confirmed the timeliness and accuracy of the data, formalizing one of the most notable local government leaks of 2025.



This case highlights the vulnerability of Smart Cities and Public Service Applications in the 2025 cyber threat landscape. Comprehensive applications such as Istanbul Senin, which combine citizens' daily needs such as transportation, payments, and social services on a single platform, have become strategic targets for attackers, providing them with access to sensitive data belonging to millions of people from a single point.

Most Important Vulnerabilities in 2025

Section 4

Vulnerabilities in 2025

CVE-2025-55182 CVSS Score: 10

React2Shell, this is a critical Remote Code Execution (RCE) vulnerability affecting React Server Components (RSC) and the Next.js framework. It originates from an insecure deserialization flaw in the React "Flight" protocol, allowing unauthenticated attackers to execute arbitrary code via a single malformed HTTP request. Throughout late 2025, it was aggressively exploited by China-nexus threat actors to deploy crypto-miners and harvest cloud credentials from compromised servers.

CVE-2025-0282 CVSS Score: 9.0

A critical stack-based buffer overflow vulnerability affecting Ivanti Connect Secure, Policy Secure, and Neurons for ZTA gateways. It allows remote, unauthenticated attackers to execute arbitrary code (RCE) by manipulating the IFT-TLS interface. Exploited in the wild since early 2025, threat actors leveraged this zero-day to bypass authentication and harvest credentials from edge devices before moving laterally into corporate networks.

CVE-2025-5777 CVSS Score: 9.3

CVE-2023-37580 was discovered by Google TAG (Threat Analysis Group) as a zeroday vulnerability affecting Zimbra Collabration email servers. CVE-2023-37580 is an XSS vulnerability. There have been 4 cyber attack campaigns organized by exploiting this vulnerability.

Vulnerabilities in 2025

CVE-2025-59718 CVSS Score: 9.8

A critical Improper Verification of Cryptographic Signature vulnerability affecting FortiOS, FortiProxy, and FortiSwitchManager. It allows unauthenticated remote attackers to bypass FortiCloud Single Sign-On (SSO) authentication by sending a specially crafted SAML response message. Disclosed in December 2025 and immediately added to the CISA KEV catalog, this zero-day was actively exploited to gain administrative access to corporate firewalls without credentials.

CVE-2025-53770 CVSS Score: 9.8

Dubbed ToolShell, this is a critical Remote Code Execution (RCE) vulnerability affecting on-premise Microsoft SharePoint Servers. It originates from unsafe deserialization of untrusted data in the ToolPane.aspx endpoint, allowing unauthenticated attackers to execute arbitrary commands as the system user. Active exploitation began in July 2025, with threat groups like Storm-2603 and Warlock ransomware using it to breach corporate networks and establish persistence.

CVE-2025-66430 CVSS Score: 9.1

A critical Incorrect Access Control vulnerability affecting Plesk for Linux servers. It allows authenticated users to exploit the "Password-Protected Directories" feature to gain root-level access, effectively taking over the entire server infrastructure. Disclosed in December 2025, this vulnerability became a primary target for attackers targeting shared hosting environments, enabling them to bypass isolation and compromise thousands of websites simultaneously.

Vulnerabilities in 2025

CVE-2025-55754 CVSS Score: 9.6

A critical "Relative Path Traversal" vulnerability affecting Apache Tomcat versions 9.x, 10.x, and 11.x. It originates from a regression in the "RewriteValve" component where URL normalization occurs before decoding. This flaw allows attackers to bypass security constraints and access sensitive directories like /WEB-INF/. In configurations where HTTP PUT is enabled, this vulnerability escalates to Remote Code Execution (RCE), allowing attackers to upload malicious JSP files and take full control of the server.

CVE-2025-59230 CVSS Score: 7.8

A critical "Improper Access Control" vulnerability affecting the Windows Remote Access Connection Manager (RasMan) service. This vulnerability allows authenticated local attackers to escalate their privileges to SYSTEM level through manipulation of the RPC interface. Disclosed in October 2025 and immediately added to the CISA KEV catalog, this zero-day was actively exploited in the wild by threat actors to gain full control over compromised endpoints after achieving initial access.

CVE-2025-11001 CVSS Score: 7.8

A critical "Directory Traversal" vulnerability affecting the widespread 7-Zip file archiver (versions prior to 25.00). It originates from improper handling of symbolic links (symlinks) within crafted ZIP files. Attackers can exploit this by tricking a user into extracting a malicious archive, which then writes files to sensitive system directories outside the intended folder. While requiring user interaction, this vulnerability allows for Remote Code Execution (RCE) and was widely targeted in late 2025 via phishing campaigns aimed at IT administrators.

Vulnerabilities in 2025

CVE-2025-61882 CVSS Score: 9.8

A critical Pre-authentication Remote Code Execution (RCE) vulnerability affecting Oracle E-Business Suite (EBS) versions 12.2.3 through 12.2.14. This complex "exploit chain" combines Server-Side Request Forgery (SSRF), CRLF Injection, and unsafe XSLT processing to allow unauthenticated attackers to execute arbitrary code on the server. Disclosed in October 2025, this vulnerability is actively exploited in the wild by the Cl0p ransomware gang to breach corporate ERP systems and exfiltrate sensitive financial data.

ORACLE
E-BUSINESS SUITE

CVE-2025-59230 CVSS Score: 9.8

A critical Command Injection vulnerability affecting Fortra's GoAnywhere MFT solution. It allows unauthenticated remote attackers to execute arbitrary operating system commands via a specially crafted HTTP request to the administrative web interface. Reminiscent of the 2023 Clop attacks, this zero-day was weaponized in early 2025 by data extortion groups to gain initial access, deploy web shells, and mass-exfiltrate sensitive files from secure environments.

CVE-2025-53690 CVSS Score: 9.8

A critical Insecure Deserialization vulnerability affecting Sitecore Experience Platform (XP) and Experience Manager (XM). It arises from improper validation of the ASP.NET ViewState parameter when specific configurations are enabled. Attackers can inject malicious serialized objects into the ViewState to execute arbitrary code (RCE) on the IIS server without authentication. Active exploitation was observed in mid-2025, with attackers using it to hijack corporate marketing sites and inject SEO poisoning scripts.

Malwares in 2025

Section 5

Malwares in 2025

Cyberthint threat hunters conducted research on malware in 2025 to identify the most commonly employed methods by threat actors for malware delivery. These findings were obtained through the Cyberthint Unified Cyber Threat Intelligence Platform and the research efforts of Cyberthint threat hunters.

Summary

- Infostealers were the most infected malware type.
- The use of AI driven Ghost Sites increased in malware delivery.
- Deepfake generated content on social media emerged as a top vector for malware distribution.

Malware Infection via AI Generated Ghost Sites

Threat actors have evolved beyond simple typosquatting. In 2025, they utilized Generative AI to create thousands of "Ghost Sites"—highly convincing replicas of legitimate software pages—in seconds. They manipulated Search Engine Optimization (SEO) and purchased legitimate ad space (Google/Bing Ads) to appear at the very top of search results. Users searching for AI tools (like ChatGPT wrappers, Midjourney, Sora) or remote work software (AnyDesk, Zoom, Slack) were the primary victims. Upon visiting these sites, users were infected with modern "Stealer" malwares such as LummaC2 (v4.0), Rhadamanthys, and Latrodectus. In 2025, these campaigns specifically targeted creative professionals and developers, spoofing software like Adobe Creative Cloud, CapCut Pro, VSCode, and Python libraries.

Malware Infection via AI Crack & Pirated Software

With the rise of subscription based AI services, threat actors targeted users looking for Free versions of paid AI tools. Instead of traditional game cracks, 2025 saw a surge in malware hidden inside AI Model Unlocking scripts and Free GPU Access tools. When users executed these files, they unknowingly installed Loader type malware. Cyberthint threat hunters observed that Pikabot and DarkGate were frequently delivered this way. These malwares not only steal data but also turn the victim's device into a Residential Proxy node, selling the user's internet bandwidth to other cybercriminals for conducting DDoS attacks or scraping data.

Malwares in 2025

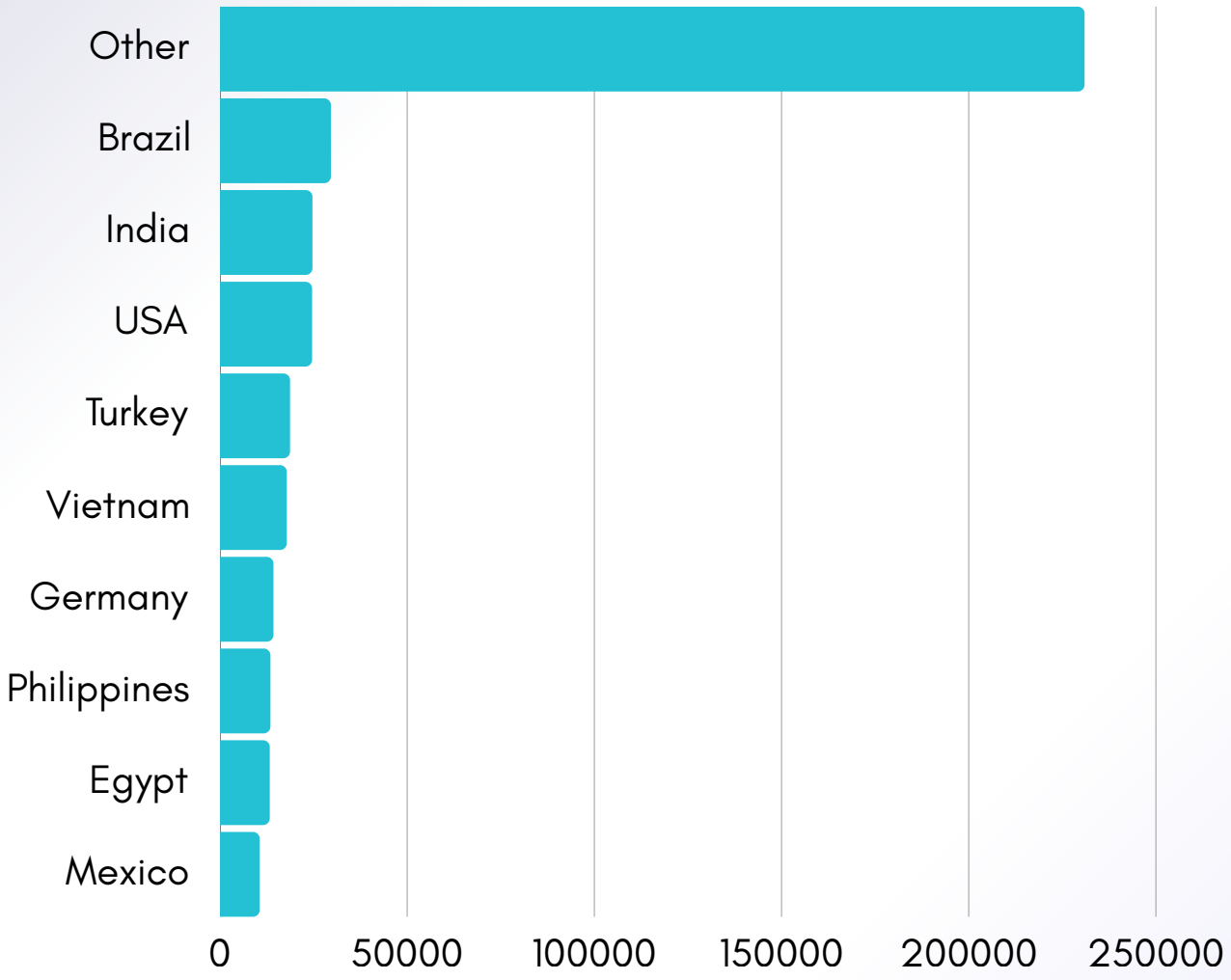
Malware Infection via Deepfake & Streaming Streams

In 2025, the YouTube Video Description attack method evolved into Deepfake Live Streams. Threat actors used real-time AI avatars of famous tech figures (e.g., Elon Musk, Sam Altman, Jensen Huang) on platforms like YouTube, TikTok, and Twitch. These AI avatars hosted fake Giveaways or promoted Exclusive Beta Access to new software. Viewers, trusting the realistic visuals and voice, scanned QR codes or clicked links in the bio/chat. These links directed users to download malicious mobile apps (APK) containing Anatsa banking trojan or desktop installers infected with Atomic Stealer (macOS). Cyberthint threat hunters identified that 60% of Gen-Z malware infections in 2025 originated from short-form video content (Shorts/Reels).

Malware Infection by Exploiting Cloud Misconfigurations

Instead of just targeting individual PCs, threat actors in 2025 focused on infecting Cloud Workspaces. By exploiting leaked API keys found in public code repositories, attackers deployed malware directly into corporate cloud containers (Docker/Kubernetes). Cyberthint research found that Cloud Native Cryptominers were often installed within minutes of a repository leak, silently consuming the victim's cloud budget while mining cryptocurrency.

Top Countries Most Affected by Malware Attacks



APT Activities in 2025

Section 6

APT Activities in 2025

Volt Typhoon's Pre Positioning in Critical Infrastructure

In the first half of 2025, the China-nexus group Volt Typhoon was detected deeply embedded within critical infrastructure networks across the US and Europe. Unlike traditional espionage, this campaign focused on pre-positioning maintaining silent access to operational technology (OT) in energy, water, and transportation sectors for potential future disruption. They utilized "Living off the Land" (LotL) techniques, abusing legitimate tools to evade EDR detection. Cyberthint analysts observed that the group heavily exploited the Ivanti Connect Secure Zero-Day (CVE-2025-0282) to gain initial access before pivoting to internal OT networks.

Midnight Blizzard's Cloud Identity Theft

The Russian state-sponsored actor Midnight Blizzard (APT29) shifted its focus in 2025 from malware deployment to sophisticated cloud identity attacks. Targeting government entities and NGOs, the group conducted high-volume OAuth Abuse attacks. By compromising legacy test tenants and creating malicious OAuth applications, they were able to exfiltrate email inboxes without triggering MFA alerts. This campaign demonstrated a strategic shift towards abusing cloud trust relationships rather than relying solely on endpoint compromises, making remediation significantly harder for victim organizations.

Lazarus Group's AI-Powered Crypto Heists

North Korea's Lazarus Group revolutionized their social engineering tactics in 2025 by integrating Generative AI into their operations. The group was observed using AI-generated code snippets and deepfake video personas to conduct fake job interviews with developers at cryptocurrency firms. Once trust was established, victims were tricked into downloading a malicious NPM package disguised as a coding assessment tool. This "Operation AI-Recruit" led to the theft of over $400 million in digital assets across three major DeFi platforms in Q3 2025 alone.

APT28 Targeting Diplomatic Cables

Phishing Campaign Against NATO Member States The Russian GRU-linked group APT28 launched a renewed spear phishing campaign targeting diplomatic entities in Eastern Europe. Leveraging the geopolitical tension, they used weaponized PDF documents disguised as "Strategic Briefings." These documents exploited a zero-day in a popular PDF reader to deploy the "HeadLace" backdoor, aimed specifically at intercepting classified diplomatic cables regarding defense spending.

APT Activities in 2025

Charming Kitten's Ghost LinkedIn Operation

APT42 Targets Dissidents via Professional Networks The Iranian threat actor APT42 (Charming Kitten) expanded its surveillance operations by creating elaborate fake personas on LinkedIn and X (formerly Twitter). Posing as recruiters for think tanks, they targeted Israeli and US-based researchers. Unlike previous years, APT42 utilized a new custom Android spyware dubbed "SultanRAT," delivered via a seemingly harmless webinar registration app. This allowed them to record calls and track the location of high-value targets in real time.

Mustang Panda's USB Ferry Campaign

APT31 Targets Logistics in the South China Sea Mustang Panda, a China-linked group, launched a massive campaign targeting shipping and logistics companies in Southeast Asia. The operation, dubbed USB Ferry 2.0, relied on infected USB drives distributed at maritime conferences. When plugged into air gapped systems on cargo ships, the malware automatically collected shipping manifests and navigation data. This campaign highlights the group's continued reliance on physical media to bridge the air gap in secure operational environments.

Kimsuky's Academic Espionage

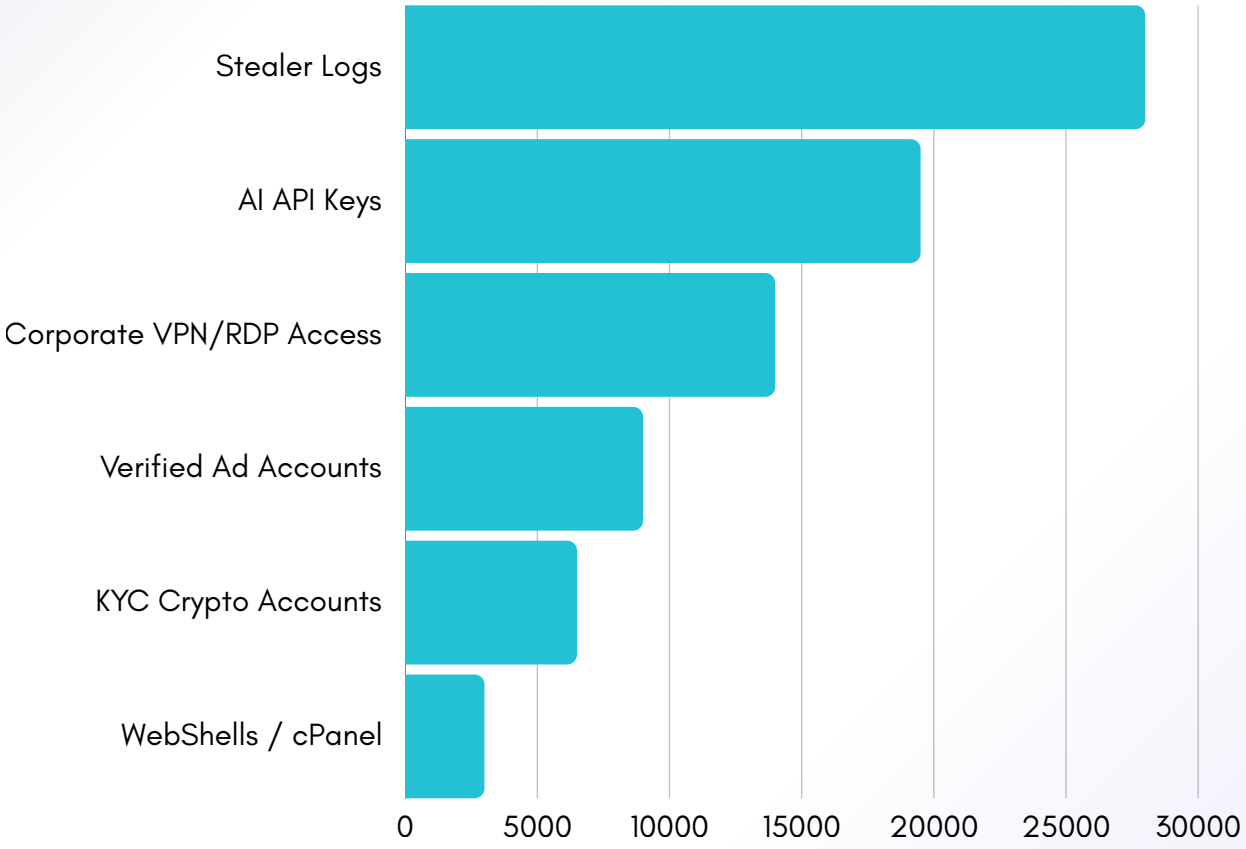
APT43 Hijacks Research Portals for Nuclear Intelligence Kimsuky (APT43), known for gathering intelligence for North Korea's weapons program, compromised several academic research portals in South Korea and Japan. By exploiting the Apache Tomcat vulnerability (CVE-2025-55752), they injected malicious scripts into login pages to harvest credentials of nuclear policy experts. The stolen credentials were used to access non-public research papers and draft policies regarding regional missile defense systems.

Black Markets in 2025

Section 7

Black Markets in 2025

In 2025, the underground economy underwent a paradigm shift from trading static credentials (username/password) to selling Session Artifacts and Machine Identities. With the widespread adoption of Multi Factor Authentication (MFA), threat actors turned to black markets to purchase active Session Cookies harvested by Infostealers, allowing them to bypass login challenges entirely. Cyberthint threat hunters also observed a massive surge in the sale of API Keys for generative AI services, which criminals use to automate phishing and malware development. The following data highlights the most traded assets in 2025's dark web marketplaces.



Dark Web Trends

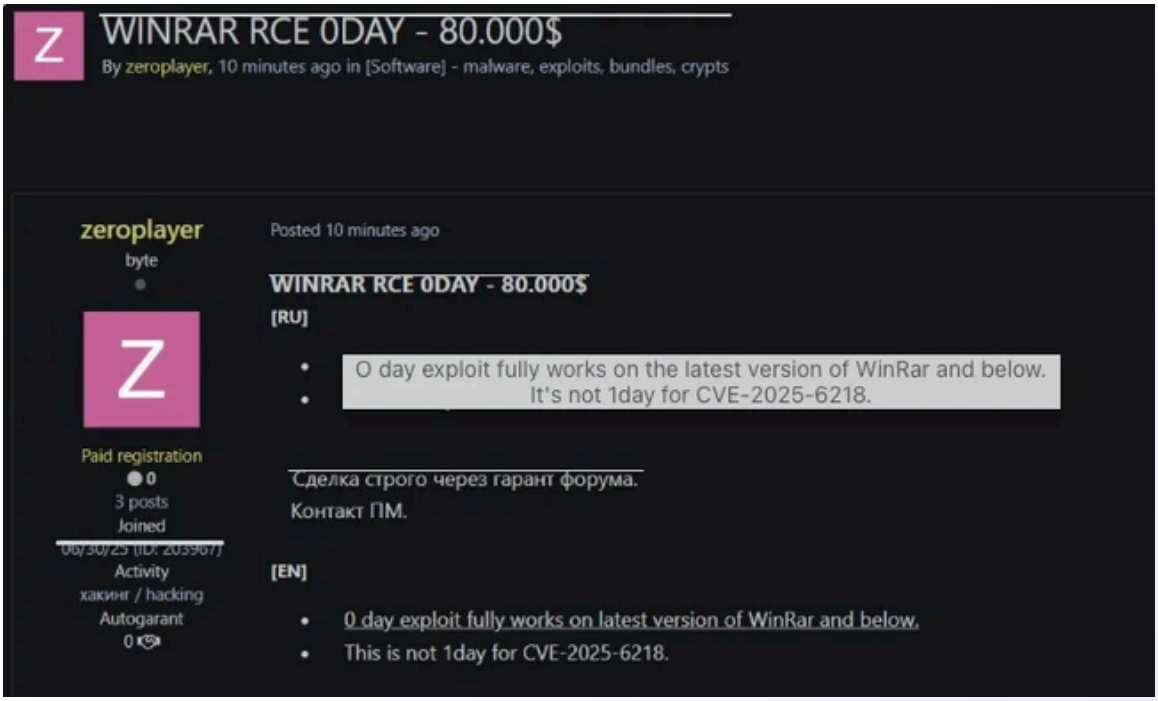
Section 8

Platforms on the DarkWeb Increase Their Security

Cyberthint threat hunters have detected a massive shift towards isolationism in underground forums. To combat AI-powered scrapers and law enforcement crawlers, major marketplaces have implemented Anti Bot challenges that require complex human interaction (e.g., solving logic puzzles) rather than simple CAPTCHAs. Furthermore, entry into high-tier marketplaces now strictly operates on a Vouch Only or High-Deposit system (often exceeding $1,000). This eliminates tourists and junior researchers, creating smaller but highly trusted circles where sophisticated tools like Zero-Day exploits are traded securely via private Telegram or Session channels.

The Zero-Day Brokerage Boom

In 2025, the trade of Zero-Day vulnerabilities moved from public auctions to exclusive, high-stakes Exploit Brokerage models. Instead of selling raw code to random buyers, specialized Access Brokers now act as intermediaries, connecting exploit developers directly with elite Ransomware-as-a-Service (RaaS) groups. These brokers offer Exploit-as-a-Service, providing not just the vulnerability (e.g., for VPNs or Cloud Gateways) but also the documentation and support needed to weaponize it. This industrialized supply chain has drastically reduced the time between a vulnerability's discovery and its mass exploitation, with prices for a critical RCE reaching upwards of $200,000 in private auctions.



2026 Predictions

Section 9

2026 Predictions

The Rise of Autonomous AI Attack Agents

While 2025 saw attackers using AI to assist in coding, 2026 is expected to be the year of Fully Autonomous Attack Agents. These AI driven malwares will not just follow a script but will be capable of reasoning. They will scan networks, identify vulnerabilities, and adapt their exploitation techniques in real-time without human intervention. Cyberthint analysts predict that these agents will significantly reduce the Mean Time to Compromise (MTTC), making speed of defense more critical than ever.

Shadow AI and Model Poisoning

As organizations rush to adopt private LLMs, the attack surface will shift to the data itself. We anticipate a surge in Data Poisoning attacks, where threat actors subtly manipulate training datasets to introduce hidden backdoors or bias into corporate AI models. Additionally, Shadow AI employees using unauthorized, unvetted AI tools will become the primary vector for data leakage, surpassing traditional phishing in severity.

Biometric Authentication Crisis (Deepfake 2.0)

The reliability of voice and facial recognition will face a critical test in 2026. With the perfection of real-time deepfake technology, Liveness Checks used by banks and remote access systems will be bypassed routinely. Threat actors will utilize Synthetic Identity Injection to spoof video calls and biometric scanners, forcing the cybersecurity industry to move towards hardware-based authentication keys (FIDO2) as the only trusted standard.

Cloud Native Ransomware & Extortion

Ransomware groups will evolve from encrypting files to locking resources. In 2026, attacks will focus on the cloud control plane. Attackers will not waste time downloading data; instead, they will exploit misconfigurations to change access policies, lock companies out of their own AWS/Azure tenants, and threaten to delete entire cloud infrastructures (snapshots and backups) unless a ransom is paid.

2026 Predictions

Post Quantum Cryptography (PQC) Urgency

With quantum computing advancements accelerating, the "Harvest Now, Decrypt Later" strategy will become a tangible threat. Nation-state actors are expected to aggressively hoard encrypted sensitive traffic in 2026, anticipating the ability to break current encryption standards (RSA/ECC) in the near future. Organizations will be forced to begin the migration to Post Quantum Cryptography (PQC) algorithms to protect long-term secrets.

Supply Chain Attacks on the AI Pipeline

The software supply chain attacks of the past will morph into Model Supply Chain attacks. Attackers will target public repositories like Hugging Face and PyTorch. By compromising a single popular pre-trained model or a foundational library, threat actors could instantly infect thousands of downstream applications that rely on these components, creating a cascading failure across industries.

Edge Computing & IoT Weaponization

As 5G networks mature and Smart Cities expand, the attack edge will move to IoT devices. In 2026, we predict the emergence of Killware targeting Operational Technology (OT) in critical infrastructure specifically targeting water treatment, traffic control, and power grids. These attacks will aim for kinetic (physical) damage rather than just financial gain, blurring the lines between cybercrime and cyberterrorism.

Disinformation-as-a-Service (DaaS) Automation

Influence operations will become fully automated and commoditized. Disinformation-as-a-Service platforms on the dark web will allow buyers to launch targeted smear campaigns or market manipulation efforts using armies of indistinguishable AI bots. These campaigns will be used not just for political interference, but increasingly for corporate sabotage, aiming to crash stock prices or ruin brand reputation within hours.

2026 Predictions

The Shift to Decision-Making AI (AI-SOC)

2026 will mark a pivot in Security Operations Centers (SOC) from interpretation to autonomous decision-making. We will move beyond AI that simply analyzes data to "AI-SOC" structures that execute actions based on those analyses. The industry will prioritize systems capable of operating independently of human intervention, acting solely on strategic directives. Those who can architect these decision-centric AI models rather than just interpretative ones will lead the global cybersecurity defense landscape.

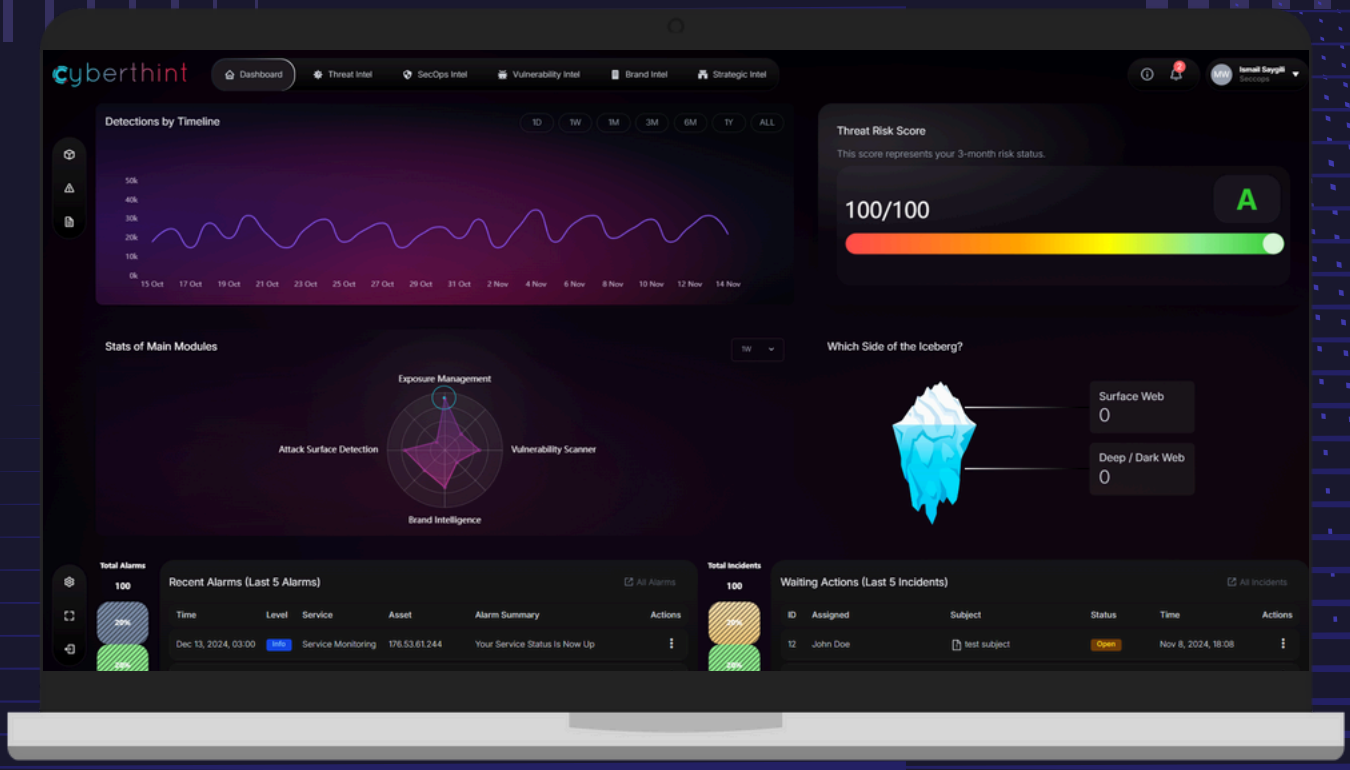
Automated Offensive Operations & Pentesting

On the offensive side, operations are becoming faster and more aggressive. Attack vectors such as Phishing, Malware, OAD, and Password Spraying will become significantly more sophisticated and effective through AI coordination. We predict that traditional Penetration Testing (Pentest) processes will be taken over by AI agents capable of continuously scanning, exploiting, and reporting vulnerabilities, turning static security testing into a dynamic, 24/7 autonomous operation.

AI vs. AI: The New Purple Team

The classic Purple Team approach (Red vs. Blue) is evolving into an "AI to AI" dynamic. In 2026, we will witness defense algorithms battling offense algorithms in real-time, with minimal human interference. As the speed of attacks surpasses human reaction times, integrating AI into every layer of security will shift from being an advantage to an absolute necessity. Everyone in the ecosystem will essentially be managing or combating AI-driven entities.

We know what information hackers have on you!



cyberthint

See Cyberthint Unified CTI & DRP Platform in action!

FREE TRIAL REQUEST

Website
cyberthint.io

X
@cyberthint

Telegram
t.me/cyberthint

Linkedin
Cyberthint

Email Address
info@cyberthint.io

Address
71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ