Inventory of Active Ransomware Attack Groups in 2025

Antiy CERT

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Ransomware attacks have become one of the major cybersecurity threats to organizations worldwide, serving as a tool for victims to obtain illicit economic gains. To increase the likelihood of victims paying ransoms and to raise the ransom amount, attackers have evolved from simply maliciously encrypting data to employing a dual ransomware strategy of "stealing files + encrypting data". Even more egregiously, some attackers have added DDoS attacks and harassment of third parties related to the victim to this dual ransomware strategy, further evolving into "multi-layered ransomware attacks". In recent years, the mainstream threat model of ransomware attacks has gradually shifted from ransomware groups widely distributing ransomware to collect ransoms to a model of "RaaS (Ransomware as a Service) + targeted attacks" to collect high ransoms.

In 2025, the ransomware ecosystem underwent unprecedented fragmentation and reorganization. On the one hand, international law enforcement actions (such as Operation Cronos against Lockbit and the sudden shutdown of RansomHub) impacted large ransomware groups; on the other hand, new groups emerged rapidly, and existing groups continuously reorganized, renamed, or formed alliances, creating a more complex threat landscape. Code reuse was particularly prominent in 2025, with leaked source code from Conti, Lockbit, and others becoming the technological foundation for multiple emerging groups, leading to increasingly blurred boundaries between ransomware variants. Simultaneously, AI technology began to be used by ransomware groups for social engineering, data analysis, and ransomware strategy optimization, further increasing the complexity and success rate of attacks.

As defense systems continue to upgrade and attackers become increasingly sophisticated, the weaponization of vulnerabilities has become a core tactic in ransomware attacks. According to statistics from the US CISA, 245 vulnerabilities were used in cyberattacks in 2025, with 24 of them discovered for ransomware attacks, involving groups such as Akira, Clop, and QiLin. Incomplete statistics indicate that in 2025, at least 115 different ransomware groups released victim information through specific sources such as the Tor website or Telegram channels, with 37 new ransomware groups added. The victim information released by these groups involves approximately 7,300 organizations from different countries and regions worldwide, covering multiple industries. However, the actual number of victims may be far greater than this figure, because in some cases, attackers may choose not to disclose or delete information for various reasons, such as after reaching an agreement with the victim, or the victim paying a ransom for the removal of the information.

10 ransomware attack groups with high attack activity and a large number of victim information releases in 2025. These groups include Akira, Clop, DragonForce, INC, LockBit, Lynx, Medusa, Play, QiLin, and SafePay, listed alphabetically by their names in no particular order. For related ransomware and ransomware attack group information, please refer to the Computer Virus Classification and Naming Encyclopedia (https://www.virusview.net/).

Antiy Intelligent Endpoint Protection System (IEP) has specialized ransomware defense capabilities, providing a five-layer protection solution against ransomware attacks, including system hardening, perimeter defense, scanning and filtering, proactive defense, and file protection.

2 Ransomware Attack Behavior Classification

The main types of ransomware attacks active in 2025 can be categorized into the following four types:

- **Encrypting Files**

Attackers using this type of ransomware attack encrypt data files using ransomware executables. The executables use a combination of specific encryption algorithms (such as AES, RSA, Cha Cha 20, and Salsa 20) to encrypt the files. Most encrypted files cannot be decrypted without the corresponding decryption tool. Only a small number of victim files are decrypted due to algorithmic logic errors in the ransomware executables.

- **Stealing Files**

Attackers using this type of ransomware attack do not encrypt data files using ransomware executables. Instead, they reside on the target system and steal data files. After stealing the data, they notify the victim that the files have been stolen. If the ransom is not paid on time, the attackers will publish or sell the stolen data files, putting pressure on the victim and forcing them to pay the ransom as soon as possible.

- **Stealing Files + Encrypting Files (Double Extortion)**

Before launching a ransomware attack, attackers using this method will reside in the target system for a period of time, during which they will steal data files. After completing the theft, they will deploy the ransomware executable, encrypt the files in the system, and notify the victim that the files have been stolen. If the ransom is not paid on time, not only will the files in the existing network environment be unusable due to encryption, but the stolen data files will also be made public or sold, putting pressure on the victim and forcing them to pay the ransom as soon as possible.

- **Multiple Extortion**

Some groups are adding DDoS attacks or contacting victims' clients/partners to further pressure them on top of the double extortion. Groups like QiLin even offer "legal advice" as a form of intimidation, assessing the regulatory risks of data breaches for victims to increase the pressure to pay.

3 Inventory of Active Ransomware Attack Groups in 2025

This review summarizes ransomware attacks that occurred in 2025, identifying active ransomware groups based on attack activity and the number of victim reports released. The groups are listed alphabetically by their names, in no particular order.

Table 3-1 2

Group Name	Time of Appearance	Typical Encrypted Suffix	Development Trends in 2025
Akira	2023	.akira	Encryption on the Nutanix AHV platform, employing "intermittent encryption" technology, has led to a significant increase in attacks on the financial industry.
Clop	2019	.clop	This type of ransomware attack employs a data theft-only model, exploiting vulnerabilities to achieve a "supply chain" ransomware attack, such as the Cleo MFT and Oracle EBS vulnerabilities.
DragonForce	2023	Rename to random characters + ".dragonforce_encrypted"	They formed a cartel extortion alliance, allied with multiple attack groups, and attacked critical infrastructure in several countries.
INC	2023	.INC	Frequent exploitation of Citrix NetScaler vulnerabilities to update encryption features and strengthen VMware ESXi encryption capabilities.
LockBit	2019	A 16-character personal ID consisting of a random combination of letters and numbers	Released version 5.0 after enforcement action, specifically optimized attack modules targeting industrial control systems such as SCADA and DCS, and allied with DragonForce and QiLin.

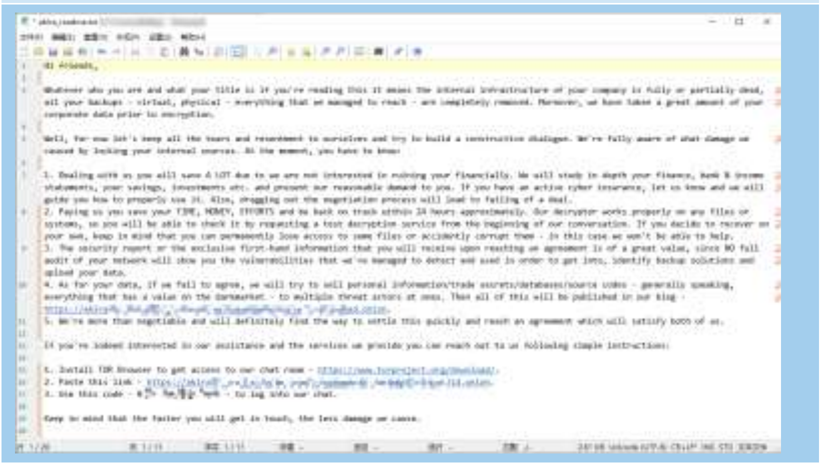
Lynx	2024	.lynx	The new version has been released, optimizing the attack chain, enhancing the backup destruction function, and integrating AI phishing tools, resulting in a significant increase in the number of victims.
Medusa	2021	.MEDUSA	They are adept at using remote monitoring and management (RMM) tools and weaponizing vulnerabilities to carry out ransomware attacks, and have been found to be collaborating with APT groups.
Play	2022	.PLAY	The code and its associated members were inherited by DragonForce, leading to a significant increase in the number of victims.
QiLin	2022	Random combinations of ten letters	In alliance with LockBit and DragonForce, they launched a large-scale attack exploiting the Fortinet vulnerability, resulting in a significant increase in the number of victims.
SafePay	2024	.SafePay	The attack scope continues to expand, with the addition of a payment system database encryption module.

3.1 Akira

Akira[1]ransomware group first emerged in 2023 and quickly grew into one of the most destructive ransomware groups in the world. Akira made significant evolutions in 2025, expanding its attack vectors from traditional Cisco VPN vulnerabilities (CVE-2020-3259, CVE-2023-20269) to large-scale exploitation of SonicWall firewall vulnerabilities (CVE-2024-40766, CVE-2024-53704), bypassing multi-factor authentication to gain initial access by hijacking VPN sessions or stealing credentials. In June, it successfully encrypted Nutanix AHV virtual machine disk files for the first time, marking its expansion from VMware ESXi to a diversified virtualization platform. At the same time, it distributed Bumblebee malware as an initial access tool through SEO poisoning strategies, tricking users into downloading trojanized installers.

In terms of attack tactics, Akira demonstrates strong stealth and persistence, utilizing RDP, SSH, and SMB protocols for lateral movement and employing "ClickFix" social engineering techniques (faking CAPTCHA verification) to trick users into downloading remote control trojans. Akira's Rust cipher is used in parallel with earlier C++ versions, flexibly selected based on the target environment, reflecting its pragmatic strategy of balancing operational efficiency with technological adaptability.

3.1.1 Group Overview

Group Name	Akira
Time of Appearance	2023
Typical Penetration Methods	Valid access credentials, accounts without multi-factor authentication, weaponization of vulnerabilities.
Typical Encrypted Suffix	.akira
Decryption Tools	Some versions have publicly available decryption tools (files encrypted before June 29, 2023 may be decryptable).
Attack Target System	Windows、Linux、VMware ESXi、Nutanix AHV
Operating Methods	RaaS, based on a two-part ransom demand (decrypting files and deleting stolen data) and the sale of data.
Infringement Mode	Encryption-based denial-of-service attacks, data theft, and the disclosure or sale of data.
Ransom Note	

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at once. Then all of this will be published in our blog - [illegible]
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - [illegible]
2. Paste this link - [illegible]
3. Use this code - [illegible] - to log into our chat.

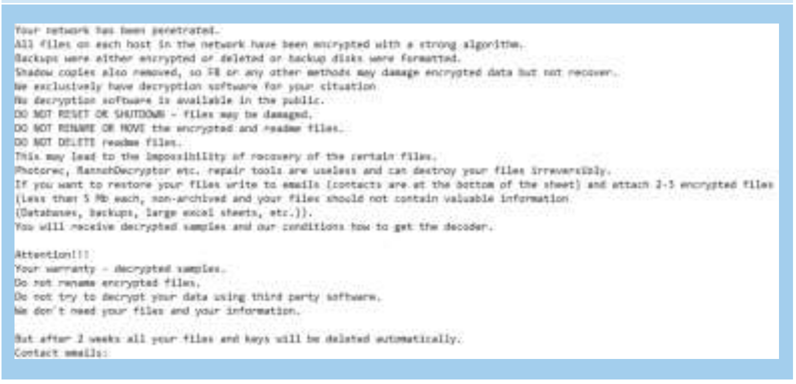
Keep in mind that the faster you will get in touch, the less damage we cause.

3.2 Clop

Clop (also known as Cl0p/CL0P) is an established ransomware group associated with the TA505 group and active since 2019. It initially operated as a RaaS service, but gradually shifted to a pure data ransomware model after 2023. In 2025, this group firmly established itself as one of the world's most destructive ransomware groups. Throughout the year, it became a key driver of the global increase in ransomware attacks, relying on its core strategy of "zero-day vulnerability-driven + large-scale data extortion". Completely abandoning traditional file encryption processes, it focused entirely on the theft and leakage of sensitive data to exert pressure. Employing a supply chain attack model of single-point breakthrough and overall data harvesting, it rapidly exploited zero-day vulnerabilities to achieve large-scale data theft. It independently controlled its vulnerability discovery and exploitation capabilities, reducing its reliance on the RaaS model and specializing in high-risk zero-day vulnerabilities in enterprise-level general software. In Q1, it exploited a vulnerability in the Cleo file transfer system to disclose 115 victims (expected to eventually reach 500). In Q3-Q4, it launched a surprise attack on over 100 well-known institutions, including

Harvard University, Envoy Aviation, and Logitech, using a high-risk vulnerability (CVE-2025-61882) in the Oracle EBS ERP system. At the end of Q4, it leveraged Gladinet... The CentreStack file server vulnerability (CVE-2025-11371, etc.) targets publicly exposed storage devices, focusing on medium and large-sized institutions in industries such as manufacturing, transportation, education, and media throughout the year. It has not only forced global enterprises to strengthen supply chain security management and patch common software vulnerabilities, but also promoted the popularization of pure data theft ransomware, making it one of the most representative supply chain ransomware attack groups in 2025.

3.2.1 Group Overview

Group Name	Clop (also known as Cl0p/CL0P)
Time of Appearance	2019
Typical Penetration Methods	Weaponizing vulnerabilities and obtaining valid access credentials through illegal means.
Typical Encrypted Suffix	.clop
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi
Operating Methods	Based on ransom demands and sales data.
Infringement Mode	Encryption-based disruption, theft of confidential information, and the disclosure and sale of stolen data.
Ransom Note	 Your network has been penetrated. All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted. Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover. We exclusively have decryption software for your situation No decryption software is available in the public. DO NOT RESET OR SHUTDOWN - files may be damaged. DO NOT RENAME OR MOVE the encrypted and readme files. DO NOT DELETE readme files. This may lead to the impossibility of recovery of the certain files. Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly. If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files (Less than 5 Mb each, non-archived and your files should not contain valuable information (Databases, backups, large excel sheets, etc.)). You will receive decrypted samples and our conditions how to get the decoder. Attention!!! Your warranty - decrypted samples. Do not rename encrypted files. Do not try to decrypt your data using third party software. We don't need your files and your information. But after 2 weeks all your files and keys will be deleted automatically. Contact emails:

3.3 DragonForce

DragonForce ransomware group was discovered in 2023 and quickly evolved into a hybrid threat actor. In 2025, DragonForce ransomware group completed a major transformation from a RaaS platform to a "ransomware cartel", becoming one of the most aggressive emerging forces in the ransomware ecosystem. The group officially announced its transformation into a "cartel" model on March 19, allowing affiliates to launch attacks using their own brand while sharing DragonForce's infrastructure and tools. This strategy enabled it to quickly absorb the resources of

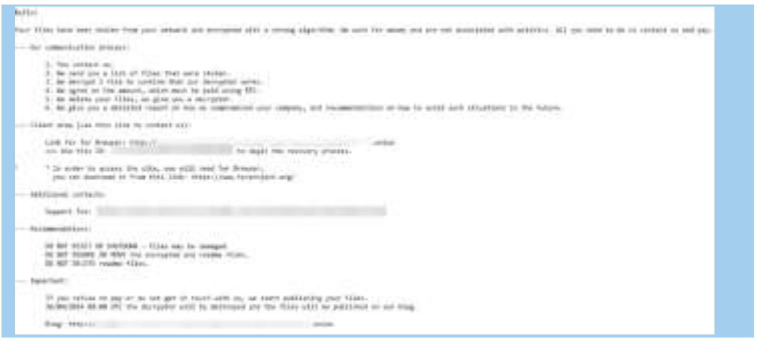
RansomHub[0]after it shut down in April, and it claimed that RansomHub had decided to migrate to its infrastructure and invited the group to consider its cooperation proposal.

Technically, DragonForce underwent a significant upgrade in 2025. Its latest variant employs BYOVD (Born with a Vulnerable Driver) technology, exploiting vulnerable drivers such as truesight.sys and rentdrv2.sys to terminate the EDR security software process. After the Akira encryption vulnerability was publicly disclosed, it proactively strengthened its own encryption scheme to avoid similar vulnerabilities. The attack scope covers Windows, Linux, ESXi, and NAS platforms. Through cooperation with Scattered Spider, it leverages Scattered Spider's "disk swapping" technology in VMware ESXi environments to extract critical databases. The group established a deep partnership with Scattered Spider, which used advanced social engineering techniques (such as help desk spoofing and MFA bypass) to gain initial access before DragonForce deployed the ransomware. This "access-as-a-service" model caused severe disruptions to e-commerce and customer data breaches in the large-scale attacks targeting the UK retail industry from April to June 2025.

In August 2025, DragonForce further launched its "Data Analytics Service", providing customized ransomware (including ransom call scripts, draft management letters, and fake legal analysis reports) to companies with annual revenue exceeding $15 million during attacks, for a fee ranging from 0% to 23% of the ransom payment. The sophistication of its attack tactics and its close collaboration with hacker groups made it one of the most threatening ransomware attack groups in 2025.

3.3.1 Group Overview

Group Name	DragonForce
Time of Appearance	2023
Typical Penetration Methods	Valid access credentials, weaponization of vulnerabilities.
Typical Encrypted Suffix	Rename to random characters + ".dragonforce_encrypted"
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi
Operating Methods	Based on ransom demands and sales data.
Infringement Mode	Encryption-based disruption, theft of confidential information, and the disclosure and sale of stolen data.

Ransom Note	

```
Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics. All you need is to contact us and pay.

--- Our communication process:

    1. You contact us.
    2. We send you a list of files that were stolen.
    3. We decrypt 1 file to confirm that our decryptor works.
    4. We agree on the amount, which must be paid using BTC.
    5. We delete your files, we give you a decryptor.
    6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

--- Client area (use this site to contact us):

    Link for Tor Browser: http://[redacted].onion
    >>> Use this ID: [redacted] to begin the recovery process.

    * In order to access the site, you will need Tor Browser,
      you can download it from this link: https://www.torproject.org/

--- Additional contacts:

    Support Tox: [redacted]

--- Recommendations:

    DO NOT RESET OR SHUTDOWN - files may be damaged.
    DO NOT RENAME OR MOVE the encrypted and readme files.
    DO NOT DELETE readme files.

--- Important:

    If you refuse to pay or do not get in touch with us, we start publishing your files.
    30/04/2024 00:00 UTC the decryptor will be destroyed and the files will be published on our blog.

    Blog: http://[redacted].onion
```

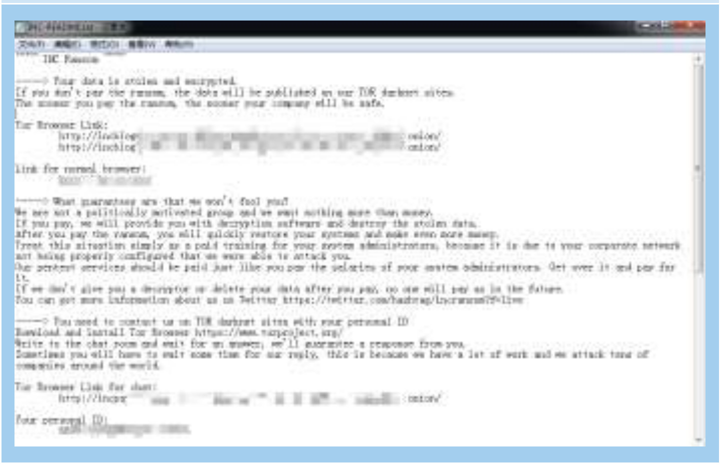
3.4 INC

INC ransomware group was first discovered in 2023, operating with a dual ransomware strategy. In March 2024, INC sold the source code of its ransomware and network infrastructure on hacker forums. In July, the newly emerged Lynx ransomware group used ransomware and network infrastructure similar to INC's, and Lynx later claimed to have purchased INC's source code. In 2025, INC continued to expand, becoming a major threat in the cybersecurity field. The group's activity increased significantly throughout the year, with attacks primarily targeting the industrial sector in the third quarter, reflecting the results of its expansion by absorbing affiliates from other collapsed RaaS projects. INC employs a dual ransomware model, focusing on automotive, chemical, equipment manufacturing, construction, and government entities, while the healthcare industry has become a key target.

On the technical front, INC continues to advance its multi-platform strategy. Its Linux and Windows versions are highly configurable, employing embedded JSON configuration files to drive runtime behavior. It supports three encryption modes (fast/medium/slow), selective file encryption, and advanced features such as secure mode startup. It evades detection by terminating critical processes and services and clearing event logs. Meanwhile, it steals data by relying on cloud storage channels such as MEGAsync and Rclone, demonstrating mature anti-forensic capabilities. It performs volume shadow copy deletion, Windows backup clearing, and event log clearing, completely destroying the evidence chain for recovery. Its self-deletion mechanism uses PowerShell and fsutil to overwrite file content with null bytes.

3.4.1 Group Overview

Group Name	INC
Time of Appearance	2023
Typical Penetration Methods	Valid access credentials, weaponization of vulnerabilities, and the integration of other malicious software.
Typical Encrypted Suffix	.INC
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi

Operating Methods	Based on ransom demands and sales data.
Infringement Mode	Encryption-based denial-of-service attacks, data theft, and the disclosure or sale of data.
Ransom Note	 INC Ransom -----> Your data is stolen and encrypted. If you don't pay the ransom, the data will be published on our TOR darknet sites. The sooner you pay the ransom, the sooner your company will be safe. Tor Browser Links: http://incblog[redacted].onion/ http://incblog[redacted].onion/ Link for normal browser: [redacted] -----> What guarantees are that we won't fool you? We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly restore your systems and make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Twitter https://twitter.com/hashtag/incransom?f=live -----> You need to contact us on TOR darknet sites with your personal ID Download and Install Tor Browser https://www.torproject.org/ Write to the chat room and wait for an answer, we'll guarantee a response from you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack tons of companies around the world. Tor Browser Link for chat: http://incpay[redacted].onion/ Your personal ID: [redacted]

3.5 LockBit

LockBit ransomware[0]was first discovered in September 2019. Initially, it was called ABCD ransomware because the encrypted file name had the suffix .abcd. The attack group behind it operates the ransomware through RaaS and multi-ransomware modes, mainly profiting from RaaS and ransom revenue sharing. Threat actors using the ransomware carry out ransomware attacks in both non-targeted and targeted modes. In June 2021, the group released ransomware version 2.0, which added the function of deleting disk volume shadows and log files. At the same time, it released a dedicated data theft tool StealBit, which adopts a dual ransomware strategy of "threat exposure (sale) of enterprise data + encrypted data". In August 2021, the group's attack infrastructure spectrum added support for DDoS attacks. In June 2022, the ransomware was updated to version 3.0. Because some code of version 3.0 overlapped with the code of BlackMatter ransomware, LockBit 3.0 was also called LockBit Black. This reflects the possible personnel flow and capability exchange between different ransomware attack groups. In October 2023, Boeing was listed as a victim by the LockBit ransomware attack group. Antiy CERT conducted analysis on the attack process reconstruction, attack tool list sorting, ransomware sample mechanism, multi-party reactions after the attack, loss assessment, process visualization review, and analyzed the defense side problems exposed in the incident and the RaaS + targeted ransomware mode, and put forward suggestions on defense and governance[0].

In February 2024, Operation Cronos, a joint operation by law enforcement agencies from multiple countries, successfully dealt a blow to the LockBit ransomware attack group. Law enforcement agencies seized control of the group's network infrastructure used for attacks and provided victims with decryption keys. This operation did not completely eradicate the LockBit group; after a period of inactivity, the group resumed its ransomware attacks and announced in December 2024 plans to release LockBit version 4.0 and its corresponding RaaS service in February 2025. However, this version failed to be deployed on a large scale due to the law enforcement operation. LockBit version 5.0 was officially released in September 2025, marking the group 's strong comeback after suffering a major blow from law enforcement in 2024 and an internal database leak in May 2025. In September 2025, DragonForce group issued a public statement announcing a "cartel alliance" with the LockBit and QiLin ransomware groups. LockBit version 5.0 employs a two-stage execution model in its technical architecture, separating the loader from the payload. It evades security tools through advanced anti-detection techniques such as control flow obfuscation, API dehooking, ETW patching, and DLL reflection loading. For the first time, it achieves coverage of Windows, Linux, VMware ESXi, and Proxmox platforms, using a strengthened encryption scheme and 16-character random file extensions. It also supports a stealth operation mode (no extension, no ransom note, and retains the timestamp) to hide its tracks. By 2025, LockBit had completed a comprehensive evolution from a single version to cross-platform compatibility, and from independent operation to an attempt at alliance building. Although the actual integration of this alliance is limited, it still reflects the adaptive evolution of the ransomware ecosystem under high-pressure law enforcement, posing a serious challenge to the cybersecurity defense systems of enterprises worldwide.

3.5.1 Group Overview

Group Name	LockBit
Time of Appearance	2019
Typical Penetration Methods	Valid access credentials, weaponization of vulnerabilities, and the integration of other malicious software.
Typical Encrypted Suffix	A 16-character personal ID consisting of a random combination of letters and numbers.
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、macOS、VMware ESXi、Proxmox
Operating Methods	RaaS, based on ransom demands and data sales.
Infringement Mode	Encryption-based denial-of-service attacks, data theft, disclosure or sale of data, DDoS attacks, reporting to regulatory authorities.

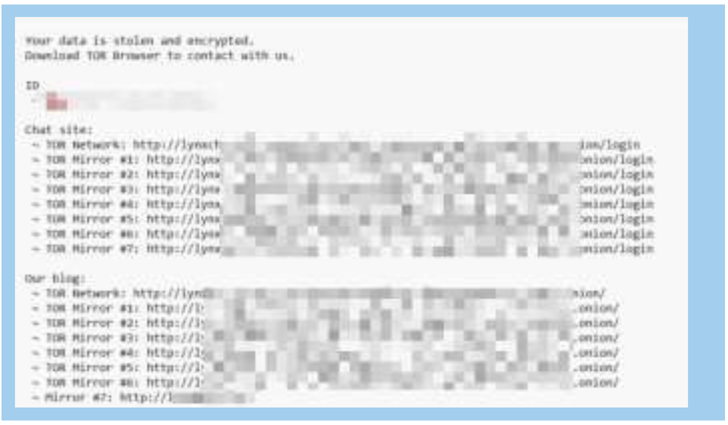
Ransom Note	[illegible]

3.6 Lynx

Lynx ransomware attack group was discovered in 2024. Developed using source code from INC ransomware attack group's infrastructure, it entered a period of rapid expansion in 2025, firmly establishing itself as a leading global ransomware threat. It employs a classic dual-track ransomware model, focusing on three main intrusion paths: credential theft, phishing attacks, and the purchase of initial access privileges. It further strengthens its deterrent by employing tactics such as terminating backup services, deleting volume shadow copies, and cleaning up virtual machine snapshots. Encrypted files have the .lynx extension, and it supports cross-platform attacks on Windows, Linux, and VMware ESXi. While claiming to evade healthcare and government agencies, it still frequently infiltrates global markets, primarily in Europe and the United States, targeting high-value industries such as manufacturing, technology, transportation, energy, and legal services. It uses a high- revenue-sharing system to attract affiliated members. Leveraging its mature RaaS architecture, stable attack pipeline, and the technological foundation inherited from INC, it became one of the most representative derivative ransomware threats of 2025.

3.6.1 Group Overview

Group Name	Lynx
Time of Appearance	2024
Typical Penetration Methods	Valid access credentials, weaponization of vulnerabilities.
Typical Encrypted Suffix	.lynx
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi
Operating Methods	Based on ransom demands and sales data.
Infringement Mode	Encryption-based denial-of-service attacks, data theft, and the disclosure and sale of stolen data.

Ransom Note	 Your data is stolen and encrypted. Download TOR Browser to contact with us. ID - [redacted] Chat site: - TOR Network: http://lynxc[redacted]ion/login - TOR Mirror #1: http://lynx[redacted]onion/login - TOR Mirror #2: http://lynx[redacted]onion/login - TOR Mirror #3: http://lynx[redacted]onion/login - TOR Mirror #4: http://lynx[redacted]onion/login - TOR Mirror #5: http://lynx[redacted]onion/login - TOR Mirror #6: http://lynx[redacted]onion/login - TOR Mirror #7: http://lynx[redacted]onion/login Our blog: - TOR Network: http://lynx[redacted]nion/ - TOR Mirror #1: http://l[redacted].onion/ - TOR Mirror #2: http://l[redacted].onion/ - TOR Mirror #3: http://l[redacted].onion/ - TOR Mirror #4: http://l[redacted].onion/ - TOR Mirror #5: http://l[redacted].onion/ - TOR Mirror #6: http://l[redacted].onion/ - Mirror #7: http://l[redacted]

3.7 Medusa

Medusa ransomware was discovered in 2021, operated by the Spearwing hacking group as a RaaS (Ragnarok Online Service). Initially operating as a closed group, it gradually expanded into an affiliated group model. Medusa is unrelated to earlier variants of MedusaLocker, the Medusa botnet, and the Medusa mobile malware. Its attack methods are complex, exploiting unpatched vulnerabilities in Microsoft Exchange, ScreenConnect, Fortinet EMS, and GoAnywhere MFT to gain initial access; deploying RMM tools such as SimpleHelp and AnyDesk to maintain persistence; employing BYOVD technology to disable security software; and using legitimate tools such as PDQ Deploy and Rclone for lateral movement and data theft, implementing double or even triple ransomware tactics. In April 2025, researchers breached its Tor anonymity to reveal its real IP address, and the FBI and other agencies warned that it had affected numerous critical infrastructure organizations. Medusa has overlapping affiliations with groups such as Play and BianLian, and shares tools with RansomHub.

3.7.1 Group Overview

Group Name	Medusa
Time of Appearance	2021
Typical Penetration Methods	Weaponizing vulnerabilities, valid access credentials, and brute-force attacks using RDP.
Typical Encrypted Suffix	.MEDUSA
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi
Operating Methods	RaaS, based on ransom demands and data sales.
Infringement Mode	Encryption-based denial-of-service attacks, data theft, disclosure and sale of stolen data, DDoS attacks, and contacting third parties to exert pressure.

Ransom Note	[illegible]

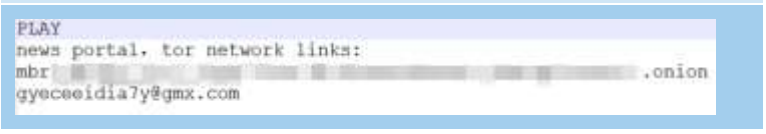
3.8 Play

Play (also known as PlayCrypt, Balloonfly)[0]is a long-established double ransomware attack group that emerged in June 2022 and operates in a closed manner. The group has distinctive technical characteristics. Each attack recompiles and customizes the malicious sample to avoid detection. It uses AES-RSA hybrid encryption technology, encrypts files with the suffix .PLAY, and supports cross-platform attacks on Windows and VMware ESXi. The intrusion path is diversified. It mainly obtains initial access by purchasing dark web credentials, brute-forcing RDP/VPN, and exploiting high-risk vulnerabilities such as FortiOS SSL VPN, Microsoft Exchange, and SimpleHelp. Then, it strengthens its deterrence and covers its tracks by disabling security software, clearing logs, and deleting shadow copies.

In terms of ransomware attacks, in addition to threatening to leak data on the dark web, Play group also directly calls victims' customer service and front desk staff to psychologically coerce them into paying ransoms. The scale of attacks surged in 2025, firmly establishing itself as one of the top five most active ransomware threats globally. With its highly secretive, closed operations, extremely strong anti-detection capabilities (its self-developed Grixba data theft tool), and aggressive telephone pressure tactics, the Play group became a difficult ransomware threat to defend against in 2025.

3.8.1 Group Overview

Group Name	Play (also known as Play Crypt, Balloonfly)
Time of Appearance	2022
Typical Penetration Methods	Valid access credentials, weaponization of vulnerabilities.
Typical Encrypted Suffix	.PLAY
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi
Operating Methods	Based on ransom demands and sales data.

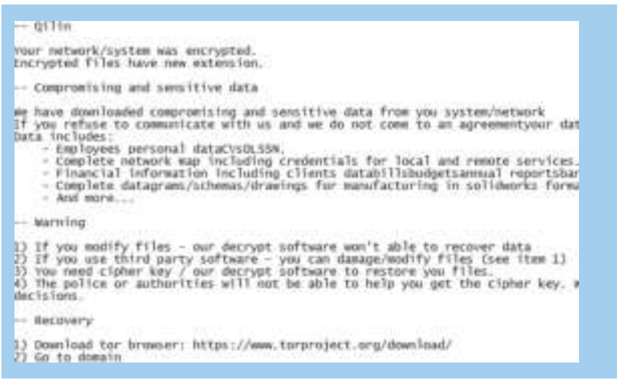
Infringement Mode	Encryption-based disruption, theft of confidential information, disclosure and sale of stolen data, and contacting third parties to exert pressure.
Ransom Note	 PLAY news portal, tor network links: mbr[redacted].onion gyeceeidia7y@gmx.com

3.9 QiLin

QiLin (also known as Agenda) was discovered in 2022. Operating on a RaaS model, it refactored its code from Golang to Rust in December 2022 to improve encryption speed and anti-detection capabilities. In 2025, it experienced explosive growth due to the absorption of a large number of affiliates following the collapse of RansomHub, resulting in a surge in attacks and surpassing RansomHub to become the world's most active ransomware group. This group employs a dual ransomware and multi-dimensional pressure strategy. In addition to data theft and AES-RSA hybrid encryption, it innovatively introduced legal threat functionality and DDoS attack capabilities, and abused the Windows Subsystem for Linux (WSL) to run Linux encryptors to bypass security detection, supporting cross-platform attacks on Windows and VMware ESXi. The intrusion paths included phishing emails (using disguised RMM tools to intercept MFA), exploitation of high-risk vulnerabilities such as FortiGate/SAP NetWeaver, brute-force attacks on RDP, and supply chain attacks. The attacks primarily targeted industries with high downtime costs, such as manufacturing, healthcare, government, and critical infrastructure in North America, Europe, and Australia. Victims included Synnovis, a pathology service provider in the UK, Asahi Group in Japan, and Malaysia Airports Holdings Berhad.

3.9.1 Group Overview

Group Name	QiLin (also known as Agenda)
Time of Appearance	2022
Typical Penetration Methods	Valid access credentials, weaponization of vulnerabilities.
Typical Encrypted Suffix	.qilin
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi
Operating Methods	Based on ransom demands and sales data.
Infringement Mode	Encryption-based disruption, data theft, DDoS attacks, disclosure and sale of stolen data, contacting third parties to exert pressure, and reporting to regulatory authorities.

Ransom Note	

```
-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreementyour dat
Data includes:
    - Employees personal dataCVsDLSSN.
    - Complete network map including credentials for local and remote services.
    - Financial information including clients databillsbudgetsannual reportsbar
    - Complete datagrams/schemas/drawings for manufacturing in solidworks forma
    - And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. W
decisions.

-- Recovery

1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
```

3.10SafePay

SafePay ransomware attack group was first discovered in 2024. Operating in a closed, independent manner, it refused to accept RaaS partners, with its core team controlling the entire attack process. Known for its ultra-fast attack chain, the group saw a continuous increase in victims throughout the year, becoming one of the most widespread cybercrime activities globally. Technically, it was developed based on leaked LockBit 3.0 code, and is suspected to include members of the disbanded Conti group. It uses the ChaCha20 algorithm (a unique key per file) for encryption and adds the .SafePay suffix. Its defenses were strengthened by disabling security software, clearing shadow copies of volumes, and event logs. Attack methods included purchasing dark web credentials, brute-forcing VPN gateways and RDP, exploiting misconfigured firewalls, and social engineering, with a focus on amplifying the impact on supply chain hubs. Major victims in 2025 included Conduent (who stole 8.5TB of data, affecting approximately 1.6 million people) and Ingram Micro (who paralyzed its global IT distribution system). With its high-frequency attacks, precise supply chain attacks, and stringent operational security, it became one of the most threatening ransomware groups in 2025.

3.10.1 Group Overview

Group Name	SafePay
Time of Appearance	2024
Typical Penetration Methods	Illegal means of obtaining valid access credentials, weaponization of vulnerabilities, brute-force attacks.
Typical Encrypted Suffix	.SafePay
Decryption Tools	No publicly available decryption tools have been found yet.
Attack Target System	Windows、Linux、VMware ESXi
Operating Methods	Based on ransom demands and sales data.
Infringement Mode	Encryption-based denial-of-service attacks, data theft, and the disclosure and sale of stolen data.

Ransom Note	[illegible]

Summary

Despite intensified efforts by law enforcement agencies worldwide to combat ransomware attacks, the number of ransomware incidents continues to rise. Numerous factors contribute to this increasing activity: attackers can quickly exploit new vulnerabilities; the vulnerability of remote work increases; the application of new technologies provides ransomware with more opportunities to attack; IAB profits by selling access credentials, which attackers use to launch targeted attacks; the development of artificial intelligence technology, while enhancing defenses, is also being used by attackers to improve attack efficiency; the mutual exploitation of techniques and tactics among ransomware groups; and the frequent occurrence of supply chain ransomware attacks all contribute to the increasing number of victims. Faced with the increasingly severe ransomware attack situation, although law enforcement and cybersecurity agencies worldwide have taken numerous measures to strengthen defenses and combat attacks, the complexity and diversity of ransomware attacks continue to pose a significant challenge to global cybersecurity.

In order to effectively deal with the risk of ransomware, defenders need to change their perception of the threat of ransomware attacks and gain a deeper understanding of the operating mechanism of targeted ransomware attacks in order to build effective enemy situation scenarios and improve defense and response capabilities in a targeted manner. Antiy once 0**"correct perception is the foundation for effectively improving defense capabilities"**. At present, the prevention of ransomware attacks in China is often still at the stage of the original ransomware. Many people have not realized that ransomware attacks are a value infringement chain consisting of continuous targeted intrusion, data theft, data encryption to paralyze the system, extortion, mining data correlation value for secondary use, data selling, reporting to regulatory agencies, and public disclosure of stolen data. Moreover, it has formed a criminal industry of extremely large scale. In this context, the risk of encountering ransomware attacks is no longer simply the result of data loss and business suspension, but rather the risk that all stolen data will be sold and made public.

Faced with systematic attack methods, defenders should establish systematic defense mechanisms and operational strategies to counter ransomware threats. For systematic attacks, it is essential to prioritize forward deployment, creating depth and a closed-loop operation. This involves enhancing attacker reconnaissance capabilities and the ability to detect their advance into peripheral areas, reducing the likelihood of attackers reaching the core. Improving network and asset manageability is fundamental: proactively shaping and hardening the security environment, strengthening constraints and management of exposed and vulnerable surfaces, enhancing control over upstream entry points in the supply chain, and initiating comprehensive log auditing, analysis, and monitoring. A defense depth should be built from topology to the system level, employing layered defenses against attacker probing, deployment, exploitation, code execution, persistence, and lateral movement. Particular emphasis should be placed on host system-level protection, treating it as the last line of defense and the cornerstone of defense, and building fine-grained governance capabilities around the identification and control of executors. Ultimately, the goal is to achieve practical operational effectiveness in sensing, interfering with, and blocking the targeted attack kill chain based on the defense system.

References

[1] Antiy. Analysis of Akira Ransomware Suspected of Using Targeted Attack Tactics [R/OL]. (2023-05-30)
https://www.antiy.cn/research/notice&report/research_report/Akira_Ransomware_Analysis.html

[2] Antiy. Analysis of the Active RansomHub Ransomware Group [R/OL]. (2024-09-12)
https://www.antiy.cn/research/notice&report/research_report/RansomHub_Analysis.html

[3] Antiy. Analysis of LockBit Ransomware Samples and Considerations on Defenses Against Targeted Ransomware [R/OL]. (2023-11-17)
https://www.antiy.cn/research/notice&report/research_report/LockBit.html

[4] Antiy. Analysis and Review of the Boeing Ransomware Attack Incident—Analysis of Targeted Ransomware Threat Trends and Defense Strategies [R/OL]. (2023-12-30)
https://www.antiy.cn/research/notice&report/research_report/BoeingReport.html

[5] Antiy. PLAY Ransomware Analysis [R/OL]. (2023-10-20)
https://www.antiy.cn/research/notice&report/research_report/PlayCrypt_Analysis.html