



# A Review of Active Ransomware Attack Organizations in 2024

Antiy CERT

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



First published at 17: 01 on 14 February 2025

This edition was updated at 17: 01 on 14 February 2025

Scan QR code for the latest  
version of the report

# Contents

---

<b>1.General</b> .....	<b>1</b>
<b>2.Classification of racketeering attack behavior</b> .....	<b>3</b>
<b>3.2024 Active Racketeering Attack Organization Inventory</b> .....	<b>4</b>
3.18base .....	5
3.2 Akira .....	6
3.3 Black Basta .....	8
3.4blacksuit .....	9
3.5 Hunters .....	10
3.6 INC .....	12
3.7lockbit .....	13
3.8 Medusa .....	14
3.9 Play .....	15
3.10 RansomHub.....	17
<b>4.Summary</b> .....	<b>18</b>
<b>Appendix I: Reference Link</b> .....	<b>20</b>
<b>Appendix II: About Antiy</b> .....	<b>21</b>

## 1 Overview

---

Extortion attacks have now become one of the major cyber security threats to organizations around the world, and have been used by attackers as a criminal tool for seeking illegal economic benefits. In order to increase the probability of the victim paying ransom and increase the amount of ransom, the attacker has evolved from a pure malicious encryption to a double blackmail strategy of "stealing files + encrypted data." What's more, on the basis of double blackmail, DDoS attacks and harassment of third parties related to the injured parties are added to further evolve into "multiple blackmail." In recent years, the mainstream threat form of blackmail attack has gradually transformed from the ransomware widespread dissemination of ransomware by ransomware gangs to the mode of "RaaS (ransomware as a service) + targeted attack" to collect high ransom. This mode is aimed at high-value targets, and affiliated members of RaaS improve their penetration capability and the success rate of landing blackmail loads by purchasing 0Day vulnerabilities, developing high-level malicious codes, and buying corporate insiders and intelligence. This combined chain of "targeted extortion + theft + exposure + sale" makes money by coercing victims to pay ransom. In order to effectively deal with that risk of blackmail, the defenders need to change their understanding of the threat of blackmail and understand the operation mechanism of targeted blackmail in order to construct an effective enemy scenario. Targeted improvements in defense and responsiveness.

In the middle of 2024, blackmail attacks occurred frequently, and the attackers carried out extortion attacks through the broad-cast, non-targeted mode and targeted targeting mode. One of the factors in the continued activity of ransomware attacks is the constant updating of the RaaS business model. RaaS is the infrastructure for ransomware attack organizations to develop and operate, including custom destructive ransomware, stealing components, ransomware, and toll channels. Various attack organizations and individuals can rent the RaaS attack infrastructure and share the spoils proportionally with the RaaS organization after the attack is completed. The rise and maturity of this business model has dramatically lowered the threshold for blackmail attacks, allowing attackers to target targets without even extorting software development skills. Another important factor is the assistance of Initial Access Broker (IAB). IAB achieves illegal profit by selling valid access credentials to the attacker without having to attack in person. The attackers make use of these credentials to carry out targeted blackmail attacks on specific targets, establish initial access and carry out subsequent malicious activities, and finally realize blackmail to the targets.

According to incomplete statistics, at least 90 extortion attack groups of different names have posted victim information through specific sources such as the Tor website or the Telegram channel in 2024. Of these, 21 of the 50 new extortion attack groups are linked to known groups. The victim information released by these organizations involves about 5,300 organizations from different countries or regions around the world, covering a wide range of industries. However, that actual number of victims may well exceed this figure, since in some cases an attacker may choose not to disclose or delete information for a variety of reasons, such as after reaching an agreement with the victim, or the victim pays a ransom in exchange for the removal of the information.

For information on ransomware and ransomware organizations, refer to the Computer Virus Encyclopedia (<https://www.virusview.net/>).

Table 11- Organizations Releasing Victim Information 2024 1-1

Extortionate attack group that published information about injured parties in 2024 (in alphabetical order)				
Omega	8base	Abyss	Akira	Apos
Apt73	Arcus Media	Argonauts	Bianlian	Black Basta
Blackbyte	Blackcat / ALPHV	Blacksuit	Blackout	Bluebox
Brain Cipher	Cactus	Chort	Cicada 3301	Ciphbit
Cloak	Clop	Cuba	Daixin	Dan0n
Dark Angel / Dunghill	Dark Vault	Donex	Donut	Dragonforce
El dorado	Embargo	Everest	Fsociety	Fog
Gookie	Hellcat	Helldown	Hunters	Inc
Insane	Interlock	Kairos	Kill Security	Knight
Lockbit	Lynx	Mad Liberator	Lorenz	Mallox
Medusa	Medusa Locker	Meow	Metacryptor	Money Message
Monti	Mydata	Nitrogen	Noname	Orca
Play	Playboy	Pryx	Qilin	Qiulong
Ra World	Ransomcortex	Ransomexx	Ransomhouse	Ransomhub
Red	Rhysida	Safepay	Sexi (APT INC)	Sarcoma
Sensayq	Slug	Catch	Spacebears	Stormous
Termite	Threem (3AM)	Trigona	Trinity	Trisec
Underground	Unsafe	Valencia	Vanir Group	Werewolves

At present, the mainstream threat form of blackmail attack has evolved into the operation mode of RaaS + targeted attack charging high ransom. Globally, industries such as manufacturing, healthcare, construction, energy, finance and public administration are frequently targeted by extortion attacks, causing serious losses to the global industrial output. The active blackmail in 2024 is now sorted out to form an overview of the attack organizations for sharing.

## 2 Classification of extortion and attack

There are three main types of active extortion attacks in 2024.

### 1. Encrypted file

The attacker using this kind of blackmail attack method will use the ransomware executor to encrypt the data file, and the executor will use a combination of specific encryption algorithms (such as AES, RSA, ChaChaCha20 and Salsa20) to encrypt the file. Most of the encrypted files cannot be decrypted temporarily without the decryption tool corresponding to the key, and only a few of the damaged files can be decrypted due to the logic error of the algorithm of the ransomware executor.

## 2. Stealing documents

The attacker using this kind of blackmail attack method does not use the ransomware executor to encrypt the data file, but only stays in the target system and steals the data file, and notifies the victim that the file is stolen after the theft is completed. If the ransom is not paid on time, the stolen data files will be made public or sold, putting pressure on the victim to pay the ransom as soon as possible.


## 3. Theft of files + encrypted files (double blackmail)










The attacker using this kind of blackmail attack method will stay in the target system for a period of time before launching the blackmail attack, during which the data files will be stolen, and after the stealing work is completed, the ransomware executor will be launched. Encrypting the file in the system and notifying the victim that the file is stolen, if the ransom is not paid on time, not only the file in the existing network environment can not be used because it is encrypted, It also exposes or sells stolen data files, putting pressure on victims to pay ransoms sooner rather than later.

# 3 Stocktaking of active extortion attack organizations in 2024

Review the ransomware attacks that occurred in 2024 and take inventory of active ransomware attack organizations based on attack activity and the number of victim information releases. The inventory is sorted by the initials of the organization name, in no particular order.

Table 3-1 Overview of active extortion organizations, 2024 3-1

Organization name	Time of occurrence	Typical Suffix	Encryption	Detailed information on the organization's encyclopedia
8base	March 2022	.8base		


Akira	March 2023	.akira	
Black Basta	April 2022	Basta	
Blacksuit	May 2023	.blacksuit	
Hunters	October 2023	.locked	
Inc	July 2023	.inc	
Lockbit	September 2019	A 9-digit personal ID with a random combination of letters and numbers	
Medusa	Jun-21	.medusa	
Play	June 2022	.play	
Ransomhub	February 2024	Six digits of a random combination of letters and numbers	

### 3.1 8base

The 8Base ransomware, whose ransomware code is based on Phobos ransomware development, was first discovered in March 2022. The attack group behind the ransomware operates on a model of RaaS and double blackmail, suspected to be an offshoot or rebranding of the RansomHouse ransomware attack group. The organization attacks the target system mainly by means of vulnerability weaponization, effective access credentials and other malicious software, and often uses SmokeLoader Trojan horse to realize initial access to the target system. After establishing initial access to the target system, the organization utilizes a variety of tools as attack equipment to implement other malicious actions. For example, Mimikatz, LaZagne, VNCPassView and other tools are used to steal credentials in the system, PsExec is used to realize horizontal movement, and Rclone is used to return the stolen data. So far, no public decryption tools have been found.

In 2024, the 8Base victim information release and data breach platform releases information on about 150 victims, and the actual number of victims may be higher.

**Table 3-2 Overview of Base Organizations 3-2**

Organization name	8base
Time of occurrence	March 2022
Typical penetration mode	Valid access credentials loaded with other malware
Typical Encryption Suffix	.8base
Decryption tools	So far, no public decryption tools have been found
Encrypt the target system	Windows
Operation mode	RaaS, based on ransom and trafficking data
Patterns of victimization	Encryption causes paralysis, theft, disclosure or trafficking of data
Industry of common victims	Finance, manufacturing, services, health care, construction
Country / Region of Common Victims	Usa, Brazil, UK, Canada, India
Ransom note	

## 3.2 Akira

The Akira [1] ransomware was discovered in March 2023, and the attack organization behind it operated the ransomware through RaaS and dual ransomware models, operating in the RaaS model and extorting ransom sharing to achieve illegal profits, Ransom is used to decrypt encrypted files and to delete stolen data two parts. The blackmail attack organization penetrated the target system mainly through effective access credentials, VPN accounts without multiple identity authentication (MFA) and weaponization of vulnerabilities. Cisco VPN-related vulnerabilities (CVE-2023-20269) were used to achieve initial access to the target system. After initial access to the target system is established, a variety of tools are used as attack equipment to implement other malicious actions, such as using AnyDesk to remotely control computers and transfer files, using PowerTool to close processes related to anti-virus



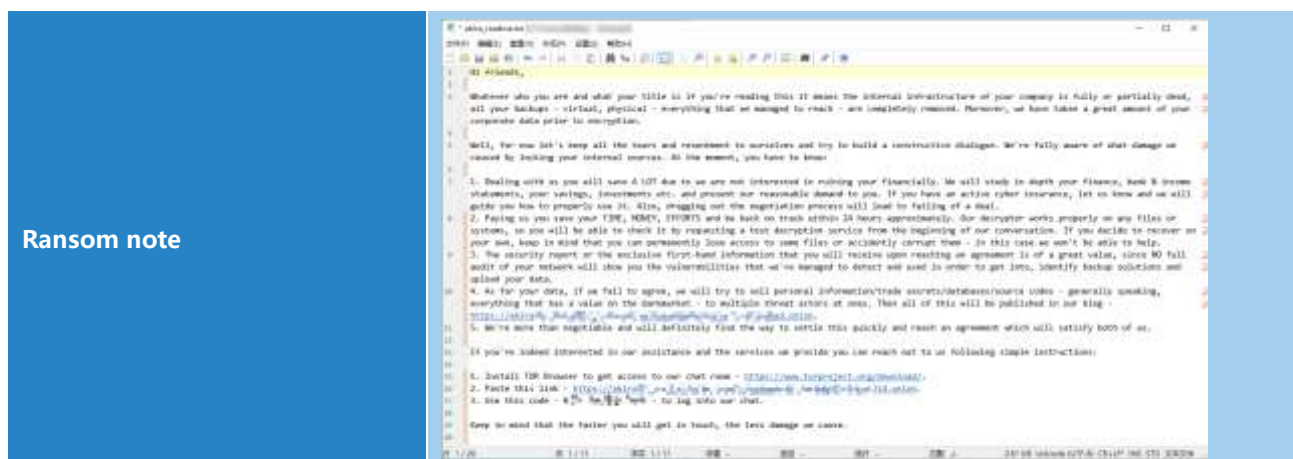
software, Use PCHunter, Masscan and AdFind to obtain specific information, use Mimikatz to steal credentials, and use Rclone and FileZilla to return stolen data.<sup>[1]</sup>

Akira has ransomware for target systems such as Windows, Linux and VMware. In addition to the behavior of "stealing and encrypting," there is a mode of only stealing and not encrypting, and after stealing the data of the victim system, the attacker chooses not to launch the ransomware. Instead, they threaten victims with blackmail through stolen data. Avast, a foreign security vendor, found vulnerability 0 in the Akira ransomware and released the decryption tool on June 29, 2023, but the tool is only applicable to the Akira ransomware executive version before June 29. Because the Akira ransomware developers have since fixed the vulnerability. The Akira ransomware attack group is suspected to be associated with Conti ransomware, which previously exited the ransomware market, in terms of code snippets of ransomware executors and addresses of encrypted digital currency wallets.<sup>0</sup>

In 2024, the Akira Victim Information Publishing and Data Breach Platform releases about 310 victim information and stolen data, and the actual number of victims may be much higher.

**Table 3-3 Overview of the Akira Organization 3-3**

<b>Organization name</b>	Akira
<b>Time of occurrence</b>	March 2023
<b>Typical penetration mode</b>	Valid access credentials, accounts not configured with multiple identity authentication, weaponization of vulnerabilities
<b>Typical Encryption Suffix</b>	.akira
<b>Decryption tools</b>	Some versions have public decryption tools (it is possible to decrypt the encrypted files before June 29, 23)
<b>Encrypt the target system</b>	Windows, Linux, VMware ESXi
<b>Operation mode</b>	Raas, based on two-part ransom (decryption of files and removal of stolen data) and data trafficking
<b>Patterns of victimization</b>	Encryption causes paralysis, theft, disclosure or trafficking of data
<b>Industry of common victims</b>	Services, education, manufacturing, finance, health care, public administration
<b>Country / Region of Common Victims</b>	United States, France, United Kingdom, Canada, Australia, Netherlands




### 3.3 Black Basta

Black Basta ransomware was discovered in April 2022 and the attack organisation behind it operated the ransomware through a model of RaaS and double blackmail, Since each ransomware executor used by Black Basta is hard-coded with a unique identifier, it is assumed that the group is only using targeted mode to conduct ransomware attacks. The blackmail attack organization is mainly through effective access credentials, other malicious software and vulnerability weaponization of the penetration of the target system. Members of the group, who post in underground forums seeking network access credentials for the organization, have used the QBot Trojan and PrintNightmare related vulnerability CVE-2021-34527 to achieve initial access to the target system. After initial access to the target system is established, various tools are used as attack equipment to implement other malicious actions, such as establishing a remote connection using AnyConnect and TeamViewer, executing commands using PsExec, scanning using Netcat, Use Mimikatz to dump credentials and use Rclone to return stolen data. In December 2023, Security Research, a foreign network security research institution, released a decryption tool named "Black Basta Buster" [3] to recover files encrypted by Black Basta ransomware. But the tool only works with some versions of the ransomware variant between November 2022 and December 2023.<sup>[3]</sup>

Black Basta ransomware attack group is suspected to be associated with BlackMatter and Conti ransomware attack groups that previously exited the ransomware market, as reflected in the ransomware executive part of the code segment, Victim information release and data leakage site design style, communication method and blackmail negotiation words and so on. So it is speculated that the Black Basta ransomware attack group may be an offshoot or rebranding of BlackMatter and Conti ransomware groups. In 2024, the Black Basta Victim Information Release and Data Breach platform released information on about 190 victims, and the actual number of victims may be higher.

### Table 3-4 Overview of Black Basta Organization 3-4

Organization name	Black Basta
Time of occurrence	April 2022
Typical penetration mode	Effective access credentials, loaded with other malware and weaponized vulnerabilities
Typical Encryption Suffix	Basta
Decryption tools	It is possible to decrypt some variant versions between November 2022 and December 2023
Encrypt the target system	Windows, Linux, VMware ESXi
Operation mode	Raas, based on ransom and trafficking data
Patterns of victimization	Encryption causes paralysis, theft, disclosure or trafficking of data
Industry of common victims	Manufacturing, health care, services, finance, public administration
Country / Region of Common Victims	United States, Canada, United Kingdom, Australia, Italy
Ransom note	 <p>Your network is encrypted by the Black Basta group. Instructions in the file readme.txt</p>

### 3.4 Blacksuit

The BlackSUIT ransomware was first discovered in May 2023 and the attack group behind it operated with a double blackmail strategy. The group has a more complex identity background and is considered a rebranding of Royal's ransomware. The Royal was renamed by the Zeon group, which is suspected to have been built by the original members of the Conti group. The Conti group was disbanded due to factors such as source code leakage, and the Conti group was considered the successor to Ryuk, with layers of complex relationship. The BlackSUIT organization has not yet been found to recruit affiliate members through the RaaS model. BlackSUIT has ransomware for target systems such as Windows, Linux and VMware. The organisation has mainly infiltrated target systems through the weaponization of vulnerabilities, effective access credentials and other malware such as SystemBC and GootLoader. After initial access to the target system is established, a variety of tools are used as attack equipment to implement

other malicious actions. For example, use tools such as AnyDesk, LogMeIn and AteraAgent to remotely control computers and transmit files, use Mimikatz and Nirsoft to steal credentials in the system, and use Rclone to return stolen data. So far, no public decryption tools have been found.

In 2024, the BlackSuit victim information release and data breach platform releases information on about 150 victims, and the actual number of victims may be higher.

**Table 3-5 Overview of BlackSuit Organizations 3-5**

Organization name	Blacksuit
Time of occurrence	May 2023
Typical penetration mode	Effective access credentials, loaded with other malware and weaponized vulnerabilities
Typical Encryption Suffix	.blacksuit
Decryption tools	So far, no public decryption tools have been found
Encrypt the target system	Windows, Linux, VMware ESXi
Operation mode	Based on ransom and trafficking data
Patterns of victimization	Encryption causes paralysis, theft, disclosure or trafficking of data
Industry of common victims	Manufacturing, health care, education, finance, public administration
Country / Region of Common Victims	United States, United Kingdom, Japan, Netherlands, Canada
Ransom note	<pre> Good whatever time of day it is!Your safety service did a really poor job of protecting your files against ourprofessionals. Extortioner named BlackSuit has attacked your system.As a result all your essential files were encrypted and saved at a securaserverfor further useand publishing on the Web into the public realm.Now we have all your files like: financial reports, intellectual property,accounting,law actionsand complaints,personal filesand so onand soforth. We are able to solve this problem in one touch.We (BlackSuit)are ready to give you an opportunity to get all the things backif you agree to makea deal with us.You have a chance to get rid of all possible financial, legal, insurance andmany others risks and problems for aYou can have a safety review of your systems.All your files will be decrypted, your data will be reset, your systems willstay in safe.Contact us through TOR browser using the link: </pre>

## 3.5 Hunters

The Hunters (aka Hunters International) ransomware was first discovered in October 2023, and the attack organisation behind it operated the ransomware using a model of RaaS and double blackmail. The ransomware code used by the group is highly similar in technical architecture and operational strategies to Hive, which has been targeted by law enforcement agencies. That similarity led security researchers to suspect that Hunters could be an offshoot or rebrand of Hive. However, the Hunters organisation denied having a direct relationship with Hive, claiming they simply bought Hive's source code and network infrastructure and, on that basis, optimised using the Rust language

to create a standalone brand. The Hunters Group has penetrated the target system mainly through the weaponization of vulnerabilities, effective access credentials and other malicious software. The organization often uses SharpRhino Trojans disguised as Angry IP Scanner network scanners to achieve initial access to the target system. After initial access to the target system is established, a variety of tools are used as attack equipment to implement other malicious actions. Use tools such as Pink, AnyDesk, TeamViewer to remotely control computers, transfer files and move horizontally, and transfer stolen data to the MEGA cloud platform. So far, no public decryption tools have been found.

In 2024, the Hunters victim information release and data breach platform releases information on about 230 victims, and the actual number of victims may be higher.

**Table 3-6 Overview of Hunters Organization 3-6**

<b>Organization name</b>	Hunters (aka Hunters International)
<b>Time of occurrence</b>	October 2023
<b>Typical penetration mode</b>	Effective access credentials, weaponization of vulnerabilities, and other malware
<b>Typical Encryption Suffix</b>	.locked
<b>Decryption tools</b>	So far, no public decryption tools have been found
<b>Encrypt the target system</b>	Windows, Linux, VMware ESXi
<b>Operation mode</b>	Raas, based on ransom and trafficking data
<b>Patterns of victimization</b>	Encryption causes paralysis, theft, disclosure or trafficking of data
<b>Industry of common victims</b>	Manufacturing, services, finance, health care, education, public administration
<b>Country / Region of Common Victims</b>	United States, United Kingdom, Canada, France, China
<b>Sample Letter of Blackmail</b>	

### 3.6 Inc

The attack group behind the INC ransomware, which was first discovered in July 2023, operated with a double blackmail strategy. This blackmail attack organization mainly uses the vulnerability of NetScaler product CVE-2023-3519 to penetrate the target system by means of vulnerability weaponization, effective access credentials and other malicious software. After initial access to the target system is established, a variety of tools are used as attack equipment to implement other malicious actions. For example, using tools such as AnyDesk, TightVNC, and PuTTY to implement remote control, transmission tools and horizontal movement, and using tools such as NetScan, Advanced IP Scanner, and Mimikatz to implement network scanning and credential theft, transferring stolen data to the MEGA cloud platform. So far, no public decryption tools have been found.

In March 2024, the INC group sold the source code for its ransomware and network infrastructure on hacking forums for \$300,000 and limited the number of potential buyers to three. In July, the newly emerging Lynx Ransomware group used ransomware and network infrastructure for ransomware attacks similar to the INC group, and the subsequent Lynx group claimed to have purchased the INC group's source code. In 2024, the INC victim information release and data breach platform releases information on about 160 victims, and the actual number of victims may be higher.

**Table 3- Overview of INC Organization 3-7**

<b>Organization name</b>	Inc
<b>Time of occurrence</b>	July 2023
<b>Typical penetration mode</b>	Effective access credentials, weaponization of vulnerabilities, and other malware
<b>Typical Encryption Suffix</b>	.inc
<b>Decryption tools</b>	So far, no public decryption tools have been found
<b>Encrypt the target system</b>	Windows, Linux, VMware ESXi
<b>Operation mode</b>	Based on ransom and trafficking data
<b>Patterns of victimization</b>	Encryption causes paralysis, theft, disclosure or trafficking of data
<b>Industry of common victims</b>	Manufacturing, services, finance, health care, education, public administration
<b>Country / Region of Common Victims</b>	Usa, UK, Germany, Canada, Australia



## 3.7 Lockbit


The LockBit ransomware [4] was first discovered in September 2019, initially known as ABCD ransomware because of its encrypted filename suffix of .abcd. The attack organization behind it operates the ransomware through RaaS and multi-ransomware models, and profits mainly from RaaS and ransom sharing. Threat actors using the ransomware carry out ransomware attacks in both non-targeted and targeted modes. The group released ransomware version 2.0 in June 2021, adding the ability to remove disk shadow and log files, along with the release of a proprietary data theft tool, StealBit. A "threat to expose (sell) corporate data + encrypted data" double blackmail strategy was used. In August 2021, the group's attack infrastructure spectrum increased support for DDoS attacks. In June 2022, the ransomware was updated to version 3.0, which is also known as LockBit Black due to the fact that part of the code of version 3.0 overlaps with the BlackMatter ransomware code, This reflects the possibility of personnel flow and capability exchange among different blackmail attack organizations. On February 20, 2024, Operation Cronos, a coalition of multinational law enforcement agencies, successfully dealt a blow to the LockBit extortion attack group, with law enforcement agencies taking over the cyber infrastructure used by the group for attacks, And provides the victim with a key for decryption. The operation did not wipe out LockBit, which resumed its extortion campaign after a lull and announced on December 19, 2024 that it planned to launch a version of LockBit 4.0 in February 2025. The LockBit organization primarily achieves initial access to the target system through effective access credentials, weaponization of vulnerabilities and other malware. So far, no public decryption tools have been found.[4]

In October 2023, Boeing was named as a victim by the LockBit blackmail attack group, Antiy CERT has analyzed the attack process recovery, the list of attack tools, the mechanism of extorting samples, the multi-party response after the attack effect, the loss assessment, and the process visual repeat. It also analyzes the defense-side problem exposed



in the incident and the mode of RaaS + directed blackmail, and puts forward suggestions on defense and governance [5]. In 2024, the LockBit victim information release and data breach platform releases information and stolen data about 520 victims, and the actual number of victims may be much higher.<sup>[5]</sup>

**Table 3-8 Overview of the LockBit Organization 3-8**

Organization name	Lockbit
Time of occurrence	September 2019
Typical penetration mode	Effective access credentials, weaponization of vulnerabilities, and other malware
Typical Encryption Suffix	A 9-digit personal ID with a random combination of letters and numbers
Decryption tools	So far, no public decryption tools have been found
Encrypt the target system	Windows, Linux, macOS, VMware ESXi
Operation mode	Raas, based on ransom and trafficking data
Patterns of victimization	Encryption leads to paralysis, theft, disclosure or sale of data, DDoS interference
Industry of common victims	Finance, services, construction, education, manufacturing, public administration
Country / Region of Common Victims	Usa, UK, Germany, Canada, India, Japan
Sample Letter of Blackmail	 <p>LockBit 3.0 the world's fastest and most stable ransomware from 2019</p> <p>&gt;&gt;&gt;&gt; Your data is stolen and encrypted. If you don't pay the ransom, the data will be published on our TOR darkest sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.</p> <p>For Browser Links:</p> <p>http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted]</p> <p>links for manual browser:</p> <p>http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted] http://lockbitag: [redacted]</p> <p>&gt;&gt;&gt;&gt; What guarantee is there that we won't cheat you? We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you</p>

## 3.8 Medusa


The Medusa ransomware was first detected in June 2021, unrelated to the Medusa Locker ransomware that emerged in 2019. The organization attacks target systems mainly by means of weaponization of vulnerabilities, effective access credentials and brute force cracking of Remote Desktop Protocol (RDP). The Fortinet-related vulnerability (CVE-2023-48788) was used to achieve initial access to the target system. After initial access to the target system is



established, a variety of tools are used as attack equipment to implement other malicious actions. For example, use ConnectWise, PDQ Deploy, AnyDesk and other tools to remotely control computers and transfer files, and use NetScan to find other targets that can be attacked. So far, no public decryption tools have been found.

In 2024, its victim information release and data breach platform has about 210 published victim information, and the actual number of victims may be higher.

**Table 3-9 Medusa Organization overview 3-9**

Organization name	Medusa
Time of occurrence	Jun-21
Typical penetration mode	Weaponization of vulnerabilities, effective access credentials, RDP brute force cracking
Typical Encryption Suffix	.medusa
Decryption tools	So far, no public decryption tools have been found
Encrypt the target system	Windows, Linux
Operation mode	Raas, based on ransom and trafficking data
Patterns of victimization	Encryption leads to paralysis, theft, DDoS interference, disclosure and sale of stolen data
Industry of common victims	Manufacturing, education, services, finance, construction, public administration
Country / Region of Common Victims	Usa, UK, Canada, India, Australia, Italy
Ransom note	


## 3.9 Play

Play (aka PlayCrypt) ransomware [6] was first discovered in June 2022, with the attack organisation behind it operating the ransomware through a model of double blackmail and claiming not to operate through a RaaS model, Attackers using the ransomware carry out ransomware attacks in both non-targeted and targeted modes. In that

method, the blackmail attack organization penetrate the target system mainly through effective access credentials and weaponization of vulnerability, Initial access to the target system has been achieved using Fortinet (CVE-2018-13379, CVE-2020-12812) and Microsoft Exchange Server (CVE-2022-41040, CVE-2022-41082) related vulnerabilities. After initial access to the target system is established, a variety of tools are used as attack equipment to implement other malicious actions. For example, use AdFind to discover information related to Active Directory, use Grixba to steal specific information, use tools such as GMER, Iobit and PowerTool to disable anti-virus software and delete log files, and use SystemBC to implement horizontal movement. The credentials in the system are stolen using Mimikatz, and the files to be stolen are packed using WinRAR and sent back through WinSCP. So far, no public decryption tools have been found.<sup>[6]</sup>

Play ransomware attacks are suspected to be associated with Conti, Royal, Hive and Nokoyawa ransomware attacks in terms of infrastructure used for attacks and techniques and tactics used in ransomware attacks. In 2024, its victim information release and data breach platform has about 350 published victim information, and the actual number of victims may be higher.

**Table 3-10 Play Organization Overview 3-10**

<b>Organization name</b>	Play (aka PlayCrypt)
<b>Time of occurrence</b>	June 2022
<b>Typical penetration mode</b>	Effective access credentials and weaponization of vulnerabilities
<b>Typical Encryption Suffix</b>	.play
<b>Decryption tools</b>	So far, no public decryption tools have been found
<b>Encrypt the target system</b>	Windows, Linux, VMware ESXi
<b>Operation mode</b>	Based on ransom and trafficking data
<b>Patterns of victimization</b>	Encryption leads to paralysis, theft, DDoS interference, disclosure and sale of stolen data
<b>Industry of common victims</b>	Telecommunications, health care, services, finance, education
<b>Country / Region of Common Victims</b>	United States, Germany, Canada, Sweden, Netherlands
<b>Ransom note</b>	

### 3.10 Ransomhub

Ransomhub ransomware [7] was first discovered in February 2024, and the attack organisation behind it operated the ransomware through a model of RaaS and double blackmail. The ransomware attack organization is mainly through vulnerability weaponization, effective access credentials and other malicious software to penetrate the target system. After initial access to the target system is established, a variety of tools are used as attack equipment to implement other malicious actions. It has used Confluence (CVE-2023-22515), Citrix (CVE-2023-3519), Fortinet (CVE-2023-27997) related vulnerabilities to achieve initial access to the target system. After successful access, the user account is created to realize persistence, EDRKillShifter is used to disable and close the security protection tools, and then Angry IP Scanner, Nmap, NetScan and other tools are used to scan and discover other attackable targets. Mimikatz, LaZagne and other tools are used to collect credentials in the system, PsExec, AnyDesk, Connectwise and other tools are used to realize remote access and horizontal movement, and PuTTY, Rclone and other tools are used to return stolen data. So far, no public decryption tools have been found.<sup>[7]</sup>

The ransomhub blackmail attack group uses ransomware payloads and techniques and tactics that bear similarities to the Knight group and are suspected of being a rebranding or successor to the Knight group. In 2024, the RansomHub victim information release and data breach platform releases information on about 530 victims, and the actual number of victims may be higher.

**Table 3-11 Overview of the RansomHub Organization 3-11**

<b>Organization name</b>	Ransomhub
<b>Time of occurrence</b>	February 2024
<b>Typical penetration mode</b>	Effective access credentials, weaponization of vulnerabilities, and other malware
<b>Typical Encryption Suffix</b>	Six digits of a random combination of letters and numbers
<b>Decryption tools</b>	So far, no public decryption tools have been found
<b>Encrypt the target system</b>	Windows, Linux, VMware ESXi
<b>Operation mode</b>	RaaS, based on ransom and trafficking data
<b>Patterns of victimization</b>	Encryption causes paralysis, theft, disclosure or trafficking of data
<b>Industry of common victims</b>	Finance, services, construction, education, manufacturing, public administration
<b>Country / Region of Common Victims</b>	Usa, UK, Canada, Italy, India, Brazil

## Sample Letter of Blackmail

```

Hello!

Visit our Blog:

For browser links:
http://ransom[REDACTED]...anion/

Links for normal browser:
http://ransom[REDACTED]...anion.jp/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data
appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The
sooner you pay the ransom, the safer your company will be safe.

>>> If you have an external or cloud backup; what happens if you don't agree with us?

- All countries have their own GDPR (Personal Data Protection Law) regulations. In the event that you do not agree
with us, information pertaining to your companies and the data of your company's customers will be published on the
Internet, and the respective country's personal data usage authority will be informed. Moreover, confidential data
related to your company will be shared with potential competitors through email and social media. You can be sure that
you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.

>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse. They will try to prevent you from negotiating with us, because
the regulations will make them look incompetent. After the incident report is handed over to the government
department, you will be fined (this will be a huge amount, read more about the GDPR
legislation: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation). The government uses your fine to reward
them. And you will not get anything, and except you and your company, the rest of the people will forget what
happened!!!!

```

## 4 Summary

While law enforcement agencies in various countries have stepped up efforts to crack down on extortion attacks, the number of cases of extortion is still on the rise. There are many factors that lead to the increase in the activity of blackmail attacks: The attackers can quickly exploit new vulnerabilities, and the vulnerability of telecommuting increases. The application of new technologies provides more attack opportunities for ransomware; IAB profits by selling access credentials, which attackers use to carry out targeted attacks; and the development of artificial intelligence technologies has both enhanced defense capabilities. It is also used by attackers to improve the efficiency of attacks, the mutual use of techniques and tactics between organizations of extortion attacks, and the frequent occurrence of supply chain-style extortion attacks, all of which make the number of victims increasing. In the face of the increasingly severe situation of blackmail attacks, law enforcement agencies and cyber security agencies have taken many measures to strengthen their defense and crackdown efforts. But the complexity and diversity of extortion attacks still pose a huge challenge to global cybersecurity.

In order to effectively deal with that risk of blackmail, the defenders need to change their understanding of the threat of blackmail and understand the operation mechanism of targeted blackmail in order to construct an effective enemy scenario. Targeted improvements in defense and responsiveness. In the report [5], Antiy said that "correct perception is the basis for effective defense improvement" in the analysis of the blackmail attack on Boeing. At present, the domestic protection against blackmail attacks usually stays at the stage of the original ransomware. Many people do not realize that extortion attacks have been committed by persistent targeted intrusions, stealing data, disabling encrypted data systems, extorting money, mining data-related value for secondary use, selling data and reporting to regulators. The public theft of data constitutes a value infringement chain, and has formed an extremely large-scale

criminal industry. In such a context, the risk of being blackmailed is no longer simply a form of consequence of data loss and business suspension, but a series of chain risks that all data stolen will be trafficked and made public.<sup>[5]</sup>

Facing the systematic attack operation mode of the attacker, the defender should establish the systematic defense mechanism and operation strategy to deal with the threat of blackmail attack. For systematic attacks, it is necessary to move forward the gateway, forward deployment, form a deep, closed-loop operation. Increases the ability of the attacker to detect fire and advance to the outside. reduces the possibility of the attacker entering the core. Improving the manageability of networks and assets is the basis of the work: Actively shaping and reinforcing the security environment, strengthening the constraint and management of exposed and attack-able surfaces, and strengthening the control of upstream entry points of the supply chain. Initiate a comprehensive log audit analysis and monitoring operation. Build the depth of defense from topology to system side, build layers of defense against attacker detection, launch, exploit vulnerabilities, code operation, persistence, horizontal movement and other behaviors, and especially build host system side protection. Take it as the last line of defense and the cornerstone of defense, and build the fine-grained governance capability around the identification and control of enforcement entities. Finally, based on the defense system to realize the perception, interference, blocking the directional attack killing chain of the actual combat operation results.

## Appendix I: Link for reference

---

[1]. Antiy.akira ransomware analysis suspected of using targeted attack patterns [R / OL]. (2023-05-30)

[https://www.antiy.cn/research/notice&report/research\\_report/Akira\\_Ransomware\\_Analysis.html](https://www.antiy.cn/research/notice&report/research_report/Akira_Ransomware_Analysis.html)

[2]. Avest.dectyped: Akira Ransomware [R / OL]. (2023-06-29)

<https://decided.avast.io/threatresearch/decipted-akira-ransomware/>

[3]. Security Research Lab. Black Basta Buster [R / OL]. (2023-12-30)

<https://github.com/srlabs/black-basta-buster>

[4]. Sample Analysis and Defense Thinking on Targeted Blackmail [R / OL]. (2023-11-17)

[https://www.antiy.cn/research/notice&report/research\\_report/LockBit.html](https://www.antiy.cn/research/notice&report/research_report/LockBit.html)

[5]. Antiy.boeing Encountered with Blackmail Attack Analysis and Resuming - Threat Trend Analysis and Defense Thinking of Targeted Blackmail [R / OL]. (2023-12-30)

[https://www.antiy.cn/research/notice&report/research\\_report/BoeingReport.html](https://www.antiy.cn/research/notice&report/research_report/BoeingReport.html)

[6]. Antiy.play ransomware analysis [R / OL]. (2023-10-20)

[https://www.antiy.cn/research/notice&report/research\\_report/PlayCrypt\\_Analysis.html](https://www.antiy.cn/research/notice&report/research_report/PlayCrypt_Analysis.html)

[7]. Antiy.analysis of the Active RansomHub Ransomware Attack Group [R / OL]. (2024-09-12)

[https://www.antiy.cn/research/notice&report/research\\_report/RansomHub\\_Analysis.html](https://www.antiy.cn/research/notice&report/research_report/RansomHub_Analysis.html)

## Appendix II: About Antiy

---

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP), etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat

detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as “Code Red”, “Dvldr”, “Heartbleed”, “Bash Shellcode” and “WannaCry”. Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspace threat actors (APT groups) such as “Equation”, “White Elephant”, “Lotus” and “Greenspot” and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.