

2023 Active Ransomware Attack Organizations Review

Antiy CERT

First published time: January 25, 2024

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

1 Overview

Ransomware is a highly destructive computer Trojan program. In recent years, it has become one of the major cybersecurity threats to organizations around the world, and has been used by threat actors as a criminal tool to make illegal economic gains. In order to increase the probability of victims paying the ransom and to raise the ransom amount, threat actors have evolved from maliciously encrypting data to a double extortion strategy of "stealing files+encrypting data". What's more, they have added DDoS attacks and harassment of third parties related to the victim on the basis of double extortion, evolving into "multiple extortion". Once attacked by ransomware, the normal operation of an organization will be seriously affected, which may lead to business interruption, data theft and malicious encryption. Threat actors threaten victims with data recovery and exposure and demand ransom. The data includes files in various formats such as documents, emails, databases and source code; the ransom can be in real currency or virtual currency (such as Bitcoin). Threat actors usually set a ransom payment deadline and increase the amount over time. Sometimes, even if the ransom is paid, the maliciously encrypted files cannot be fully restored.

In 2023, ransomware attacks occurred frequently. Threat actors carried out ransomware attacks in a wide-ranging non-directional mode and a targeted directional mode. One of the factors that caused the continued activity of ransomware attacks was the continuous updating of the Ransomware as a Service (RaaS) business model. RaaS is the infrastructure developed and operated by ransomware attack organizations, including customized destructive ransomware, stealing components, ransomware rhetoric, and toll channels. Various attack organizations and individuals can rent RaaS attack infrastructure and share the ransom with RaaS organizations after the attack. The rise and maturity of this business model has lowered the threshold for ransomware attacks, and threat actors can target targets without even having ransomware development skills. Another factor is the help of Initial Access Brokers (IABs). IABs make illegal profits by selling valid access credentials to threat actors without having to conduct attacks themselves. Threat actors use the obtained credentials to carry out targeted ransomware attacks on specific targets, and carry out subsequent malicious activities after establishing initial access, ultimately achieving ransomware

against the target.

Some ransomware attack organizations publish victim information on specific information sources, such as Tor websites or Telegram channels. Since 2019, according to incomplete statistics, there are about 115 organizations with different names that have published victim information. Due to resource integration, brand reshaping, or closure by law enforcement agencies, in 2023, a total of 68 organizations with different names have published victim information, involving about 5,500 organizations from different countries or regions in different industries. The actual number of victims may be higher, because threat actors may choose not to disclose or delete information for some reasons, such as reaching an agreement through negotiation or the victim paying the ransom.

Table 1-1 Organizations that released victim information in 2023

Organizations that released victim information in 2023				
0mega	8base	Abyss	Akira	Alphv/BlackCat
Arvinclub	AvosLocker	BianLian	Black Basta	BlackByte
BlackSuit	Cactus	CiphBit	Cloak	Clop
CrossLock	CryptNet	Cuba	Cyclops	Daixin
DarkPower	DarkRace	Donut	Dragonforce	Dunghill Leak
Everest	Hive	Hunters	INCransom	Karakurt
Knight	La Piovra	LockBit	Lorenz	LostTrust
Malas	MalekTeam	Mallox	Medusa	MedusaLocker
Meow	MetaEncryptor	MoneyMessage	Monti	NoEscape
Nokoyawa	Play	QiLin	RaGroup	RagnarLocker
RanStreet	Rancoz	RansomEXX	RansomHouse	Ransomedvc
Raznatovic	Rhysida	Royal	Siegedsec	Snatch
Stormous	Threeam	Toufan	Trigona	Unsafe
Vendetta	Vice Society	WereWolves		

At present, the mainstream threat form of ransomware attacks has evolved into a RaaS+ targeted attack mode with high ransoms. Globally, industries such as manufacturing, medical care, construction, energy, finance and public administration have frequently become targets of ransomware attacks, causing serious losses to global industrial output value.

2 Ransomware Attack Behavior Classification

There are three main types of active ransomware attacks in 2023 :

➤ **Encrypt files**

Threat actors that use this type of ransomware attack will use the ransomware executable to encrypt data files. The executable uses a combination of specific encryption algorithms (such as AES, RSA, ChaCha20 and Salsa20 , etc.) to encrypt files. Most of the encrypted files cannot be decrypted temporarily without the decryption tool with the corresponding key. Only a small number of victim files can be decrypted due to algorithmic logic errors in the ransomware executable.

➤ **Steal files**

Use this type of ransomware attack do not use the ransomware executable to encrypt data files. They only reside in the target system and steal data files. After the theft is completed, they notify the victim that the file has been stolen. If the ransom is not paid on time, the stolen data files will be made public or sold, putting pressure on the victim and forcing the victim to pay the ransom as soon as possible.

➤ **Steal files + encrypt files**

Before launching a ransomware attack, threat actors that use this type of ransomware attack will reside in the target system for a period of time, stealing data files during this period. After the theft is completed, they will drop a ransomware executable to encrypt 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 encrypted and unusable, but the stolen data files will also be made public or sold, putting pressure on the victim and forcing the victim to pay the ransom as soon as possible.

3 2023 Active Ransomware Attack Organizations Review


Reviewing the ransomware attacks that occurred in 2023 , this article takes stock of active ransomware attack organizations, including basic information of the organizations, organization overviews, and related cases, sorted in alphabetical order by the first letter of the organization name, in no particular order.

3.1 8Base

8Base ransomware was discovered in March 2022. The ransomware executable is a variant of Phobos ransomware. The attack organization behind it uses RaaS and double extortion modes. It is suspected to be a branch or rebranding of the Ransom House ransomware attack organization. It makes profits through RaaS and ransom sharing. The threat actors using this ransomware carry out ransom attacks in non-targeted and targeted modes. The ransomware attack organization mainly penetrates the target system through weaponized vulnerabilities, valid access credentials, and other malware. It often uses the Smoke Loader Trojan to achieve initial access to the target system. No public decryption tools have been found so far.

As of mid-2023, its victim information release and data leakage platform had published information on approximately 200 victims, and the actual number of victims may be higher.

3.1.1 Organization Overview

Organization name	8Base
Appearance time	March 2022
Typical penetration method	Valid access credentials, carrying other malware
Typical encryption suffixes	.8base
Decryption tool	No public decryption tools have been found yet.
Encrypt the target system	Windows
How it works	Ransomware as a service, ransomware and data trafficking
Intrusion mode	Encryption paralysis, stealing, publishing or selling data
Commonly targeted industries	Financial industry, manufacturing industry, service industry, medical industry, construction industry
Common countries/regions	United States, Brazil, United Kingdom, Canada, Australia, Germany, India
Ransom note	



3.1.2 Related Cases

- Indian medical company Clear Medical was listed as a victim by 8Base ransomware attack group

On July 3, the 8Base ransomware attack group listed ClearMedi as a victim, claiming to have stolen documents related to employees, patients, insurance, and finances, which have now been made public.

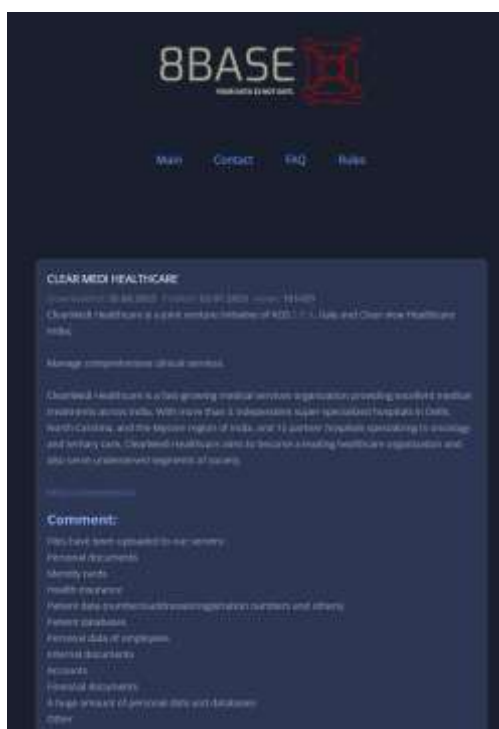


Figure 3-1 8Base ransomware group lists ClearMedia as a victim

- Toyota Lift Northeast, a US Toyota forklift dealer, was listed as a victim by the 8Base ransomware attack group

On August 23, the 8Base ransomware attack group listed ToyotaLift Northeast as a victim, claiming to have stolen documents related to communications, customers, finances, and confidential information, which have now been made public.

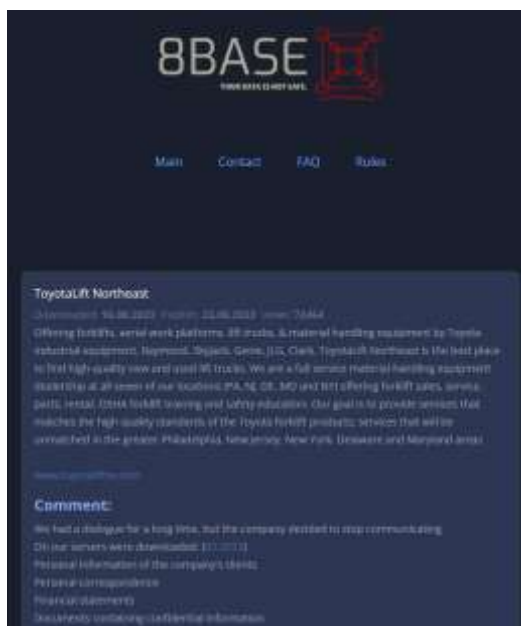


Figure 3-2 8Base ransomware group lists ToyotaLift Northeast as a victim

3.2 Akira

Akira⁰ransomware was discovered in March 2023. The attack organization behind it operates the ransomware through RaaS and double extortion modes, and makes profits through RaaS operation and ransom sharing. The ransom is used to decrypt encrypted files and delete stolen data. Threat actors using this ransomware carry out ransom attacks in non-targeted and targeted modes. The ransomware attack organization mainly penetrates the target system through valid access credentials, VPN accounts without multi-factor authentication (MFA) configured, and vulnerability weaponization. It has used Cisco VPN-related vulnerability CVE-2023-20269 to achieve initial access to the target system. After establishing initial access to the target system, it uses a variety of third-party tools as attack equipment to implement other malicious behaviors, such as using AnyDesk to remotely control computers and transfer files, using Power Tool to shut down processes related to antivirus software, using PChunter, Masscan, and Ad Find to obtain specific information, using Mimikatz to steal credentials, and using Rclone and FileZilla to steal data.

Akira ransomware has executables for target systems such as Windows, Linux, and VMware. In addition to the "stealing + encryption" behavior, there is also a mode of stealing without encryption. After stealing data from the victim system, the threat actor chooses not to release the ransomware executable, but to use the stolen data to threaten the victim for ransom. Avast, a foreign security vendor, discovered a vulnerability in Akira ransomware⁰ and released a decryption tool on June 29, but the tool is only applicable to the Akira ransomware executable version before June 29, because the Akira ransomware developers have since fixed the vulnerability.

The Akira ransomware group is suspected to be related to the Conti ransomware group that previously withdrew from the ransomware market, as reflected in some code segments of the ransomware executable and encrypted digital currency wallet addresses. In mid-2023, its victim information release and data leakage platform had published information on about 142 victims and stolen data, and the actual number of victims may be higher.

3.2.1 Organization Overview

Organization name	Akira
Appearance time	March 2023
Typical penetration method	Valid access credentials, accounts without multi-factor authentication configured, weaponized vulnerabilities
Typical encryption suffixes	.akira
Decryption tool	encrypted files before June 29 can be decrypted)
Encrypt the target system	Windows、Linux、VMware ESXi
How it works	Ransomware as a service, based on two parts: extortion of ransom (decryption of files and deletion of stolen data) and data trafficking
Intrusion mode	Encryption paralysis, stealing, publishing or selling data
Commonly targeted industries	Service industry, education industry, manufacturing industry, finance industry, medical industry, public administration
Common countries/regions	United States, France, United Kingdom, Canada, Australia, Netherlands
Ransom note	
Scan the QR code to view relevant information in the Computer Virus Encyclopedia	

3.2.2 Related Cases

- Akira ransomware group targets Cisco VPN users who don't configure multi-factor authentication

On August 24, Cisco released a bulletin⁰stating that the Akira ransomware group launched attacks against Cisco VPN users who did not configure multi-factor authentication. In attacks against VPNs, threat actors first exploited exposed services or applications to launch attacks against users whose VPN accounts did not configure multi-factor authentication and users with vulnerabilities in VPN software. Once threat actors have a clear understanding of the basic situation of the target network, they will attempt to extract credentials through the dump of LSASS (Local Security Authentication Subsystem Service) in order to further move and escalate privileges in the target network environment.

- Aquallectra, a government-owned water and electricity company on the Dutch island of Curacao, has been named a victim of the Akira ransomware attack group

December 6, the Akira ransomware group targeted Aquallectra, a government-owned water and electricity company on the Dutch island of Curacao, as a victim. The threat actor claimed that it would soon make public operational documents, business documents, and a large amount of payment information stolen from the company, which is expected to affect the privacy of 80,000 families and companies.

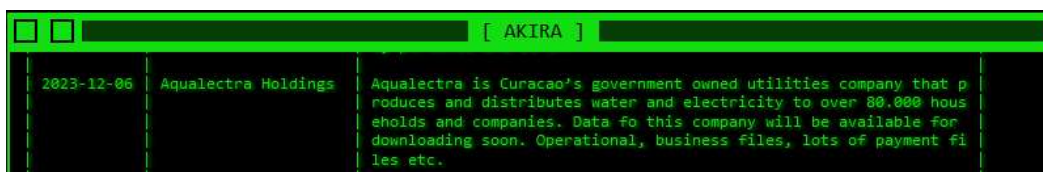


Figure 3-3Akira ransomware attack group lists Aquallectra as a victim

3.3 BianLian

BianLian ransomware was discovered in June 2022. The attack organization behind it operated the ransomware through RaaS and double extortion modes, and made profits through RaaS mode operation and ransom sharing. The threat actors using this ransomware carried out ransom attacks in non-targeted and targeted modes. The ransomware attack organization mainly penetrated the target system through effective access credentials and vulnerability weaponization. It used the CVE-2021-31207, CVE-2021-34473, and CVE-2021-34523 vulnerabilities of Sonic Wall VPN devices and Microsoft Exchange software to achieve initial access to the target system. After the threat actor used the penetration method to achieve initial access to the target system, it launched a backdoor Trojan compiled in Go language and installed remotely controlled third-party tools to implement subsequent malicious behaviors, such as Team Viewer, Splash Top, and Any Desk. In January 2023, the foreign security vendor A vast released a decryption tool for the BianLian ransomware ⁰. Subsequently, the BianLian ransomware attack organization changed its strategy,

abandoned the encryption executable, and only carried out ransomware attacks by stealing data files.

Currently, its victim information release and data leakage platform has published information of 223 victims and stolen data, and information of 143 victims was left in mid-2023. The actual number of victims may be higher.

3.3.1 Organization Overview

Organization name	BianLian
Appearance time	June 2022
Typical penetration method	Valid access credentials, weaponized vulnerabilities
Typical encryption suffixes	.bianlian
Decryption tool	Encrypted files can be decrypted before January 2023, and will only be used to steal secrets without encryption .
Encrypt the target system	Windows
How it works	Ransomware as a service , ransomware and data trafficking
Intrusion mode	Encryption paralysis, stealing, publishing or selling data
Commonly targeted industries	Medical industry, financial industry, manufacturing industry, education industry, service industry, public administration
Common countries/regions	United States, Australia, United Kingdom, Canada, Indonesia
Ransom note	
Scan the QR code to view relevant information in the Computer Virus Encyclopedia	

3.3.2 Related Cases

- Waynesboro, USA, was listed as a victim by the BianLian ransomware attack group

In March, the BianLian ransomware attack group listed the city of Waynesboro in the United States as a victim. The threat actor claimed to have stolen approximately 350 GB of data, including internal police department documents, personal and employee information, and business-related documents, which have now been made public.

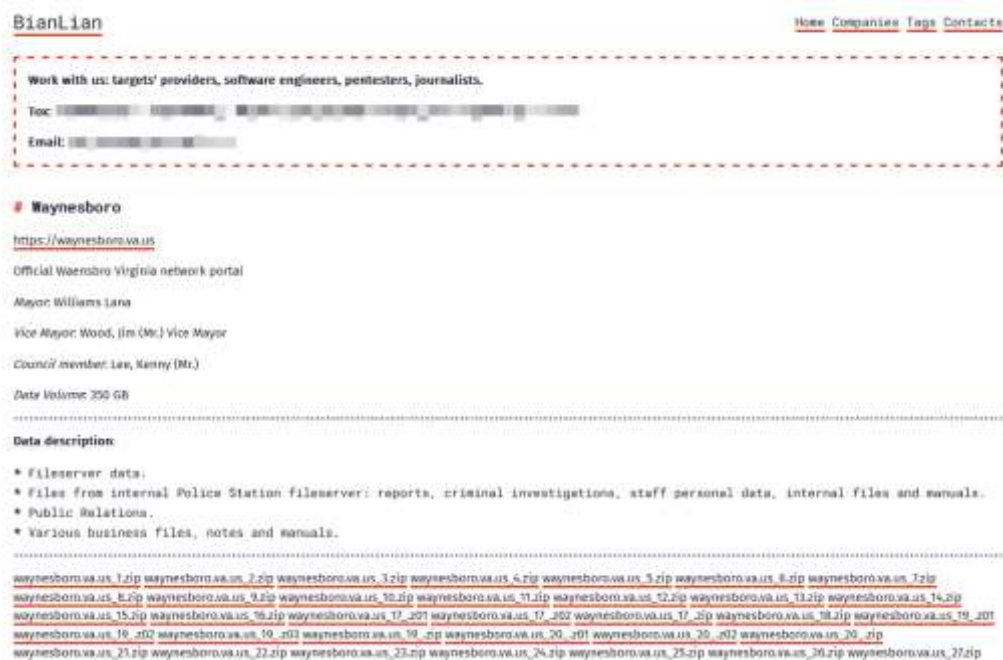


Figure 3-4BianLian ransomware attack group lists Wayneboro as a victim

- Indonesian telecom operator Smartfren Telecom was listed as a victim by the BianLian ransomware attack group

In September, the BianLian ransomware attack group targeted Indonesian telecom operator Smartfren Telecom as a victim. The threat actor claimed to have stolen approximately 1.2 TB of data, including personal data, financial and financial, business operations, emails, and confidentiality-related documents, which have now been made public.

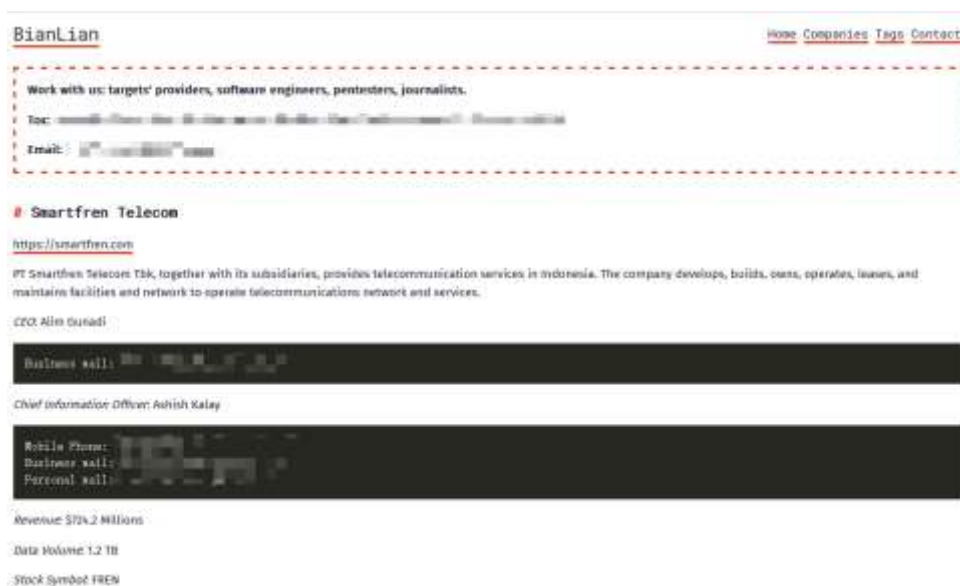


Figure 3-5BianLian ransomware attack group lists Smartfren Telecom as a victim

- Air Canada listed as victim of BianLian ransomware attack group

In October, the BianLian ransomware attack group targeted Air Canada as a victim, with the threat actor claiming to have stolen approximately 210 GB of data, including technical and operational data from 2008 to 2023, SQL database backup data, and employee personal information and other related files, which are now public.



Figure 3-6 BianLian ransomware attack group lists Air Canada as a victim



3.4 Black Basta

Black Basta ransomware was discovered in April 2022. The attack organization behind it operates the ransomware through RaaS and double extortion modes. Since each ransomware executable used by Black Basta has a hard-coded unique identification code, it is speculated that the organization only uses a targeted mode to carry out ransomware attacks. The ransomware attack organization mainly penetrates the target system through effective access credentials, carrying other malware, and weaponizing vulnerabilities. Members of the organization posted on underground forums seeking network access credentials for organizations, and used the QBot Trojan and PrintNightmare-related vulnerability CVE-2021-34527 to achieve initial access to the target system. After establishing initial access to the target system, a variety of third-party tools are used as attack equipment to achieve other malicious behaviors, such as using AnyConnect and TeamViewer to establish remote links, using PsExec to execute commands, using Netcat for scanning, using Mimikatz to dump credentials, and using Rclone to steal data. In December 2023, the foreign cybersecurity research organization Security Research released a decryption tool called "Black Basta Buster" ⁰ to recover files encrypted by the Black Basta ransomware, but the tool is only applicable to some ransomware variants from November 2022 to December 2023.

The Black Basta ransomware attack group is suspected to be related to the Black Matter and Conti ransomware

attack groups that have previously withdrawn from the ransomware market, which is reflected in some code segments of the ransomware executable body, the design style of the victim information release and data leakage site, the communication method and the ransom negotiation language. Therefore, it is speculated that the Black Basta ransomware attack group may be a branch or rebranding of the BlackMatter and Conti ransomware organizations. In 2023 , its victim information release and data leakage platform has left information on about 150 victims, and the actual number of victims may be more.

3.4.1 Organization Overview

Organization name	Black Basta
Appearance time	April 2022
Typical penetration method	Valid access credentials, weaponization of other malware vulnerabilities
Typical encryption suffixes	.basta
Decryption tool	Some variants may be decrypted between November 2022 and December 2023
Encrypt the target system	Windows、Linux、VMware ESXi
How it works	Ransomware as a service , ransomware and data trafficking
Intrusion mode	Encryption paralysis, stealing, publishing or selling data
Commonly targeted industries	Manufacturing, medical, construction, service, finance, public administration
Common countries/regions	United States, Canada, United Kingdom, Australia, New Zealand, Germany
Ransom note	
Scan the QR code to view relevant information in the Computer Virus Encyclopedia	

3.4.2 Related Cases

- American Virgin Coca-Cola Bottling Company Named Victim of Black Basta Ransomware Attack

In May, the Black Basta ransomware attack group listed the American Viking Coca-Cola Bottling Company as a victim. The threat actor publicly displayed examples of stolen data files, including employee information sheets, ID cards, passport application records, confidentiality agreements, and payment records, which are now public.

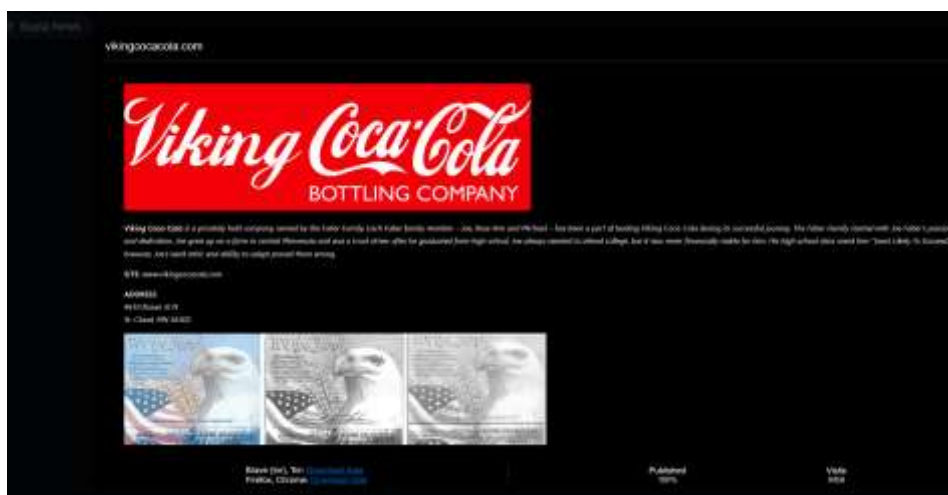


Figure 3-7 Black Basta ransomware group lists Viking Cocoa as a victim

- German defense industry Rheinmetall Group listed as victim by Black Basta ransomware attack group

In May, the Black Basta ransomware attack group listed the German defense industry Rheinmetall Group as a victim. The threat actor publicly displayed examples of stolen data files, including employee personal information, confidentiality agreements, authorization letters, design drawings and procurement contracts, which are now public.



Figure 3-8 Black Basta ransomware group lists Rheinmetall as victim

- Volex, a manufacturer of electronic and electrical cables, was listed as a victim by the Black Basta ransomware attack group

In October, the Black Basta ransomware group targeted Volex, a UK-based manufacturer of electronic and electrical wiring harnesses, as a victim. The threat actor publicly displayed examples of stolen data files, including employee ID cards, medical records, offer letters, nondisclosure agreements, and product drawings, which are now publicly available.

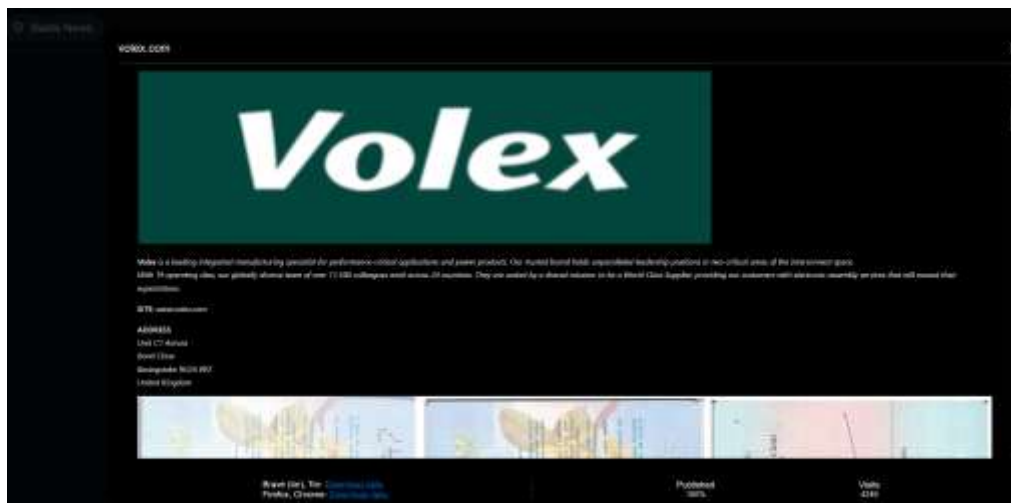


Figure 3-9 Black Basta ransomware group lists Volex as victim

3.5 BlackCat

BlackCat (also known as ALPHV or Noborus) ransomware ⁰was discovered in November 2021. The attack organization behind it operates the ransomware through RaaS and multi-ransom models, mainly making profits through RaaS operations and ransom sharing. Threat actors using this ransomware carry out ransom attacks in non-targeted and targeted modes. The organization released version 2.0 called "Sphynx" on February 21, 2023. The ransomware attack organization mainly penetrates the target system through weaponized vulnerabilities and valid access credentials. The BlackCat ransomware attack organization uses a variety of means to force victims to pay ransom, including reporting to the victim's supervisory unit, DDoS attacks, and harassing relevant personnel of the victim unit. In December 2023, the FBI cooperated with multiple law enforcement agencies to successfully investigate and deal with the infrastructure used by the BlackCat organization for ransomware attacks, shut down the website that published victim information, and provided the key to decrypt the victim's encrypted files, which is expected to help more than 500 victims recover their files ⁰.

BlackCat ransomware is related to REvil, Dark Side, and Black Matter ransomware, which have already withdrawn from the ransomware market. It is the first ransomware to use the Rust programming language to develop a cross-platform attack payload. Its payload supports execution on Windows, Linux, and VMware ESXi systems. Its victim information release and data leakage platform has successively released victim information and stolen data. In 2023, the information of about 410 victims was released, and the actual number of victims may be higher.

3.5.1 Organization Overview

Organization name	BlackCat (also known as ALPHV or Noborus)
Appearance time	November 2021
Typical penetration method	Weaponized vulnerabilities, valid access credentials
Typical encryption suffixes	. (6-7 digits + letters are randomly combined)
Decryption tool	Victims need to contact the FBI (more than 500 victims' keys were seized)
Encrypt the target system	Windows、Linux、VMware ESXi
How it works	Ransomware as a service, based on extortion and data trafficking
Intrusion mode	Encryption paralysis, stealing secrets, disclosing or selling data, DDoS interference, harassment of third parties involved
Commonly targeted industries	Manufacturing, service, education, medical, finance, public administration
Common countries/regions	United States, Australia, India, Indonesia, United Kingdom, Mexico
Ransom note	<pre> >> Introduction Important files on your system was ENCRYPTED and now they have have "xxxxxxx" extension. In order to recover your files you need to follow instructions below. >> Sensitive Data Sensitive data on your system was downloaded and it will be PUBLISHED if you refuse to cooperate. Data Includes: - Employees personal data, CVs, DL, SSN. - Complete network map including credentials for local and remote services. - Financial information including clients data, bills, budges, annual reports, bank statements. - Complete datagrams/schemas/drawing for manufacturing in solidworks format - And more... >> CAUTION DO NOT MODIFY FILES YOURSELF. DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA. YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS. YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY. >> Recovery procedure Follow these simple steps to get in touch and recover your data: 1) Download and install Tor Browser from: https://torproject.org/ 2) Navigate to: {REMOVED TOR URL} </pre>
Scan the QR code to view relevant information in the Computer Virus Encyclopedia	

3.5.2 Related Cases

- Mexican beverage company Coca-Cola FEMSA named victim of BlackCat ransomware attack

In June, the BlackCat ransomware attack group listed the Mexican beverage company Coca-Cola FEMSA as a victim. The threat actor publicly displayed examples of stolen data files. The example images contained order information, transaction contracts, profit-sharing contracts and other documents between Coca-Cola FEMSA and its partner companies, which have now been made public.



Figure 3-10 BlackCat ransomware group names Coca-Cola FEMSA as victim

- US social news site Reddit listed as a victim by BlackCat ransomware attack group

In June, the BlackCat ransomware group listed the American social news website Reddit as a victim. The threat actor claimed that it had hacked into Reddit's system on February 5. The incident was caused by a targeted phishing attack on Reddit employees. The threat actor stole 80GB of compressed data. The threat actor wanted \$4.5 million as a ransom and asked Reddit to withdraw its decision to increase the price of the API .



Figure 3-11 BlackCat ransomware group lists Reddit as victim

➤ MGM Resorts International suffered BlackCat attack

In September, the BlackCat ransomware attack organization listed MGM Resorts International as a victim. In this incident, the hotel and casino operating facilities in Las Vegas were attacked by BlackCat ransomware, which made the hotel accommodation system and casino entertainment facility system inoperable, forcing guests to wait for hours to check in, and paralyzed electronic payment, digital key cards, slot machines, ATMs and paid parking systems.



Figure 3-12 BlackCat ransomware group names MGM Resorts International as victim

3.6 Clop

The Clop (also known as Cl0p) ransomware was discovered in February 2019. The attack organization behind

it operates the ransomware through RaaS and double extortion modes , and mainly makes profits through RaaS operations and ransom sharing. The threat actors using this ransomware carry out ransom attacks in non-targeted and targeted modes, and in some attacks, they only steal data files to achieve ransom attacks. The ransomware attack organization mainly penetrates the target system through effective access credentials and vulnerability weaponization. It has used related vulnerabilities of Accellion (now Kiteworks) file transfer equipment (FTA) , SolarWinds Serv-U managed file transfer (MFT) , Fortra 's GoAnywhere MFT and Progress 's MOVE it MFT products to achieve initial access to the target system. After establishing initial access to the target system, it uses a variety of third-party tools as attack equipment to achieve other malicious behaviors. SentinelLabs found that some Linux variants of Clop ransomware can support decryption⁰ due to defects in the encryption algorithm of the ransomware executable. No public decryption tools have been found for other variants.

As of mid-2023, its victim information release and data leakage platform had published information on approximately 353 victims, and the actual number of victims may be higher.

3.6.1 Organization Overview

Organization name	Clop (also known as Cl0p)
Appearance time	February 2019
Typical penetration method	Weaponized vulnerabilities, valid access credentials
Typical encryption suffixes	.cl0p
Decryption tool	Some ransomware executable variants under Linux can be decrypted
Encrypt the target system	Windows、Linux、 VMware ESXi
How it works	Ransomware as a service , ransomware and data trafficking
Intrusion mode	Encryption paralysis, stealing, publishing or selling data
Commonly targeted industries	Finance, service, medical, education, public administration
Common countries/regions	United States, Canada, India, United Kingdom, Netherlands
Ransom note	<pre> 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 if you 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 REMOVE OR MOVE the encrypted and ransom files. DO NOT DELETE ransom files. This may lead to the impossibility of recovery of the certain files. Photores, RansomwareCryptor 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 reuse 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: </pre>



3.6.2 Related Cases

- Clop ransomware group uses MOVE it -related vulnerabilities to launch large-scale ransomware attacks

The Clop ransomware attack organization exploited vulnerabilities related to the MOVE it product to launch ransomware attacks on users of the product. In this incident, the threat actor mostly adopted the strategy of stealing secrets without encryption. It claimed that the victims included Ernst&Young (EY), Deloitte (DTT), PricewaterhouseCoopers (PwC), Aon Group in the insurance industry, Estee Lauder Group in the cosmetics industry, etc. The stolen data has been publicly downloaded.



Figure 3-13Clop ransomware attack group lists multiple victims

3.7 LockBit

The LockBit ransomware⁰ was discovered in September 2019. Initially, it was called ABCD ransomware because its encrypted file name suffix was .abcd. The attack organization behind it operated the ransomware through RaaS and multi-ransom models, mainly making profits through RaaS and ransom sharing. The threat actors using this ransomware carried out ransom attacks in non-targeted and targeted modes. The organization released version 2.0 of the ransomware in June 2021, adding the function of deleting disk shadows and log files, and at the same time released a dedicated data stealing tool StealBit, adopting a double ransom strategy. In August 2021, the organization's attack infrastructure spectrum added support for DDoS attacks. In June 2022, the ransomware was updated to version 3.0. Since part of the code of version 3.0 overlaps with the code of BlackMatter ransomware, LockBit 3.0 is also called LockBit Black, which reflects the possible personnel flow and capability exchange between different ransomware

attack organizations. Organizations that use LockBit RaaS to carry out attacks have conducted a large number of attacks, achieving initial access to target systems through effective access credentials, vulnerability weaponization, and other malware. LockBit ransomware only encrypts the first 4K of data in the encrypted file header, so the encryption speed is significantly faster than other ransomware that encrypts the entire file. Since the corresponding sectors of the original file are overwritten, victims cannot restore the plaintext data before encryption through data recovery. No public decryption tools have been found so far.

In October 2023, Boeing was listed as a victim by the LockBit ransomware attack organization. Antiy CERT conducted analysis work from the aspects of attack process restoration, attack tool list sorting, ransomware sample mechanism, multi-party response after the attack was successful, loss assessment, process visualization review, etc., and analyzed the defense-side problems exposed in the incident and the RaaS+targeted ransomware model, and put forward defense and governance suggestions⁰. In 2023, its victim information release and data leakage platform released information on about 1,030 victims and stolen data, and the actual number of victims may be higher.

3.7.1 Organization Overview

Organization name	LockBit
Appearance time	September 2019
Typical penetration method	Valid access credentials, weaponized vulnerabilities, and other malware
Typical encryption suffixes	9-digit personal ID with random combination of letters and numbers
Decryption tool	No public decryption tools have been found yet.
Encrypt the target system	Windows, Linux, macOS, VMware ESXi
How it works	Ransomware as a service, ransomware and data trafficking
Intrusion mode	Encryption paralysis, stealing secrets, disclosing or selling data, DDoS interference
Commonly targeted industries	Finance, service, construction, education, manufacturing
Common countries/regions	United States, United Kingdom, Germany, Canada , India, Japan

<p>Ransom note</p>	
<p>Scan the QR code to view relevant information in the Computer Virus Encyclopedia</p>	

3.7.2 Related Cases

- Royal Mail named as victim of LockBit ransomware attack

In February, the LockBit ransomware group listed the British Royal Mail as a victim. The ransomware attack occurred in January. This incident caused the British Royal Mail's international export services to be disrupted, and it was temporarily unable to deliver items to overseas destinations. The threat actor disclosed the negotiation records with the British Royal Mail and indicated that the final ransom was 40 million US dollars to restore the encrypted files and delete the stolen data. Due to the failure to pay the ransom on time, about 44.4 GiB of stolen data has been made public. The organization uses GiB data measurement units on its data leakage platform , and 1 GiB is approximately equal to 1.07 GB.

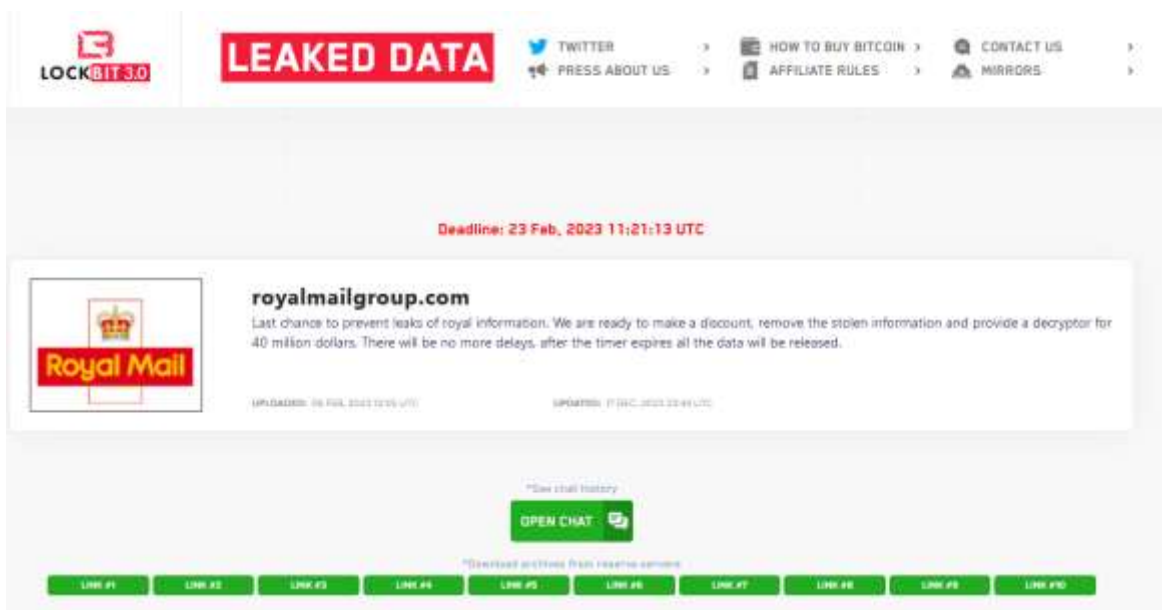


Figure 3-14 LockBit ransomware attack group lists the British Royal Mail as a victim

➤ Nagoya Port hit by LockBit ransomware group

In July, the Port of Nagoya in Japan was attacked by the LockBit ransomware group⁰. This incident affected the Nagoya Port Unified Terminal System, which is the central system that controls all container terminals in the port. As a result, container handling work could not be carried out and five terminals in the port were shut down for nearly three days, affecting approximately 20,000 containers entering and leaving the port and 260 related companies. Toyota Motors mainly transports goods through this port. During this period, some containers containing imported and exported parts could not be loaded and unloaded.

➤ Boeing hit by LockBit ransomware attack group

In October, the victim information release platform to which LockBit belongs posted a message claiming that a large amount of sensitive data from Boeing had been stolen, and threatened Boeing to release the stolen sensitive data if it did not contact the LockBit organization before November 2, 2023. After that, perhaps due to the failure of negotiations between the two parties, the LockBit organization publicly released the 21.6 GiB of data stolen from Boeing.

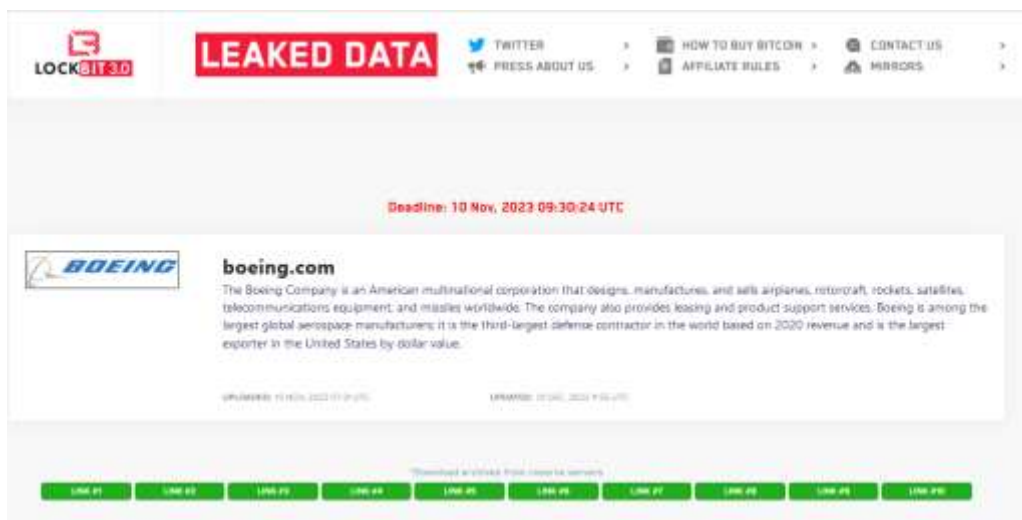


Figure 3-15 LockBit ransomware attack group lists Boeing as a victim

3.8 Medusa

The Medusa ransomware was discovered in June 2021. It is unrelated to the MedusaLocker ransomware that appeared in 2019. The attack organization behind it uses RaaS and double extortion modes to operate, mainly through RaaS and ransom sharing. The threat actors using this ransomware carry out ransom attacks in non-targeted and targeted modes. The ransomware attack organization mainly penetrates the target system through weaponized vulnerabilities, valid access credentials, and remote desktop protocol brute force cracking. No public decryption tools have been found so far.

As of mid-2023, its victim information release and data leakage platform had published information on approximately 140 victims, and the actual number of victims may be higher.

3.8.1 Organization Overview

Organization name	Medusa
Appearance time	June 2021
Typical penetration method	Weaponized vulnerabilities, valid access credentials
Typical encryption suffixes	. MEDUSA
Decryption tool	No public decryption tools have been found yet .
Encrypt the target system	Windows
How it works	Ransomware as a service , ransomware and data trafficking
Intrusion mode	Encryption paralysis, stealing secrets, DDoS interference, publicizing and selling stolen data

Commonly targeted industries	Manufacturing, education, service, finance, construction, public administration
Common countries/regions	United States, United Kingdom, Canada, India, Türkiye, Australia, Tonga, Italy
Ransom note	
Scan the QR code to view relevant information in the Computer Virus Encyclopedia	

3.8.2 Related Cases

- Tonga Telecom listed as victim of Medusa ransomware attack

In February, the Medusa ransomware group targeted Tonga Telecom as a victim, with the threat actor publicly displaying examples of stolen data files, including employee ID cards, business contacts and confidentiality agreements, which are now public.



Figure 3-16 Medusa ransomware group names Tonga telecom as victim

- Italian water supplier Alto Calore Servizi S.p.A named victim of Medusa ransomware attack

In May, the Medusa ransomware group targeted Italian water supplier Alto Calore Servizi S.p.A., with the threat actor publicly displaying examples of stolen data files, including personnel information, water supply line information, construction drawings and construction plans, and other documents, which are now public.



Figure 3-17 Medusa ransomware group names Alto Calore Servizi S.p.A as victim

- Toyota Financial listed as victim of Medusa ransomware attack

In November, the Medusa ransomware group targeted Toyota Financial Services as a victim, with the threat actor publicly displaying examples of stolen data files, including employee ID cards, company financial statements, vehicle assessment information, and business contracts, which are now public.



Figure 3-18 Medusa ransomware group lists Toyota Financial as a victim



3.9 Play

Play (also known as PlayCrypt) ransomware⁰ was discovered in June 2022. The attack organization behind it operated the ransomware in a double extortion mode and claimed that it did not operate in a RaaS mode. The threat

actors using this ransomware carried out ransom attacks in non-targeted and targeted modes. The ransomware attack organization mainly penetrated the target system through effective access credentials and vulnerability weaponization. It once used ProxyNotShell, Microsoft Exchange Server and FortiOS related vulnerabilities to achieve initial access to the target system. No public decryption tools have been found so far.

The Play ransomware group is suspected to be related to the Conti, Royal, Hive, and Nokoyawa ransomware groups, as reflected in the infrastructure used for the attacks and the techniques and tactics used in the ransomware attacks. In 2023, its victim information release and data leakage platform had published information on about 213 victims, and the actual number of victims may be higher.

3.9.1 Organization Overview

Organization name	Play (also known as Play Crypto)
Appearance time	June 2022
Typical penetration method	Valid access credentials, weaponized vulnerabilities
Typical encryption suffixes	.play
Decryption tool	No public decryption tools have been found yet.
Encrypt the target system	Windows
How it works	Claims not to use RaaS , based on ransom and data trafficking
Intrusion mode	Encryption paralysis, stealing secrets, DDoS interference, publicizing and selling stolen data
Commonly targeted industries	Telecommunications, medical, service, finance, education, real estate
Common countries/regions	Germany, United States, United Kingdom, Australia, Portugal, Switzerland
Ransom note	
Scan the QR code to view relevant information in the Computer Virus Encyclopedia	

3.9.2 Related Cases

- Swiss media company CHMedia listed as victim of Play ransomware attack

In April, the Play ransomware group targeted Swiss media company CHMedia as a victim, with the threat actor claiming to have stolen 500 GB of data files, including confidential information, project engineering, employee

salaries and employee information, which have now been made public.



Figure 3-19 Play ransomware group lists CHMedia as a victim

- Swiss IT service provider Xplain listed as a victim of Play ransomware attack group

In May , the Play ransomware group listed Swiss IT service provider Xplain as a victim, and the threat actor claimed to have stolen 907 GB of data files. In June, the Swiss police began investigating the incident because the company provided services to multiple federal and state government departments, the military, customs and police departments, and multiple units were indirectly affected by the incident.



Figure 3-20 Play ransomware group lists Xplain as victim

- Dallas City Named Victim of Play Ransomware Attack

In October , the Play ransomware group targeted the city of Dallas, USA, with the threat actor claiming to have stolen 400 GB of data files, which were private files of the city and have now been made public.



Figure 3-21 Play ransomware group lists Dallas as victim

3.10 Rhysida

Rhysida ransomware was discovered in May 2023. The attack organization behind it operates the ransomware through RaaS and double extortion modes, and makes profits through RaaS mode operation and ransom sharing. The threat actors using this ransomware carry out ransom attacks in non-targeted and targeted modes. The ransomware attack organization mainly penetrates the target system through effective access credentials and vulnerability weaponization, and has used the Microsoft Netlogon vulnerability CVE-2020-1472 to achieve initial access to the target system. No public decryption tools have been found so far.

The Rhysida ransomware group is related to the Vice Society ransomware group. It is speculated that Rhysida may be a branch or rebranding of Vice Society. In mid-2023, its victim information release and data leakage platform had published information on about 76 victims, and the actual number of victims may be higher.

3.10.1 Organization Overview

Organization name	Rhysida
Appearance time	May 2023
Typical penetration method	Valid access credentials, weaponized vulnerabilities
Typical encryption suffixes	.rhysida
Decryption tool	No public decryption tools have been found yet.
Encrypt the target system	Windows、Linux、VMware ESXi
How it works	Ransomware as a service, ransomware and data trafficking
Intrusion mode	Encryption paralysis, stealing, publishing and selling stolen data
Commonly targeted industries	Manufacturing, medical, manufacturing, education, service, public administration
Common countries/regions	United States, United Kingdom, Indonesia, Germany, Brazil, Chile

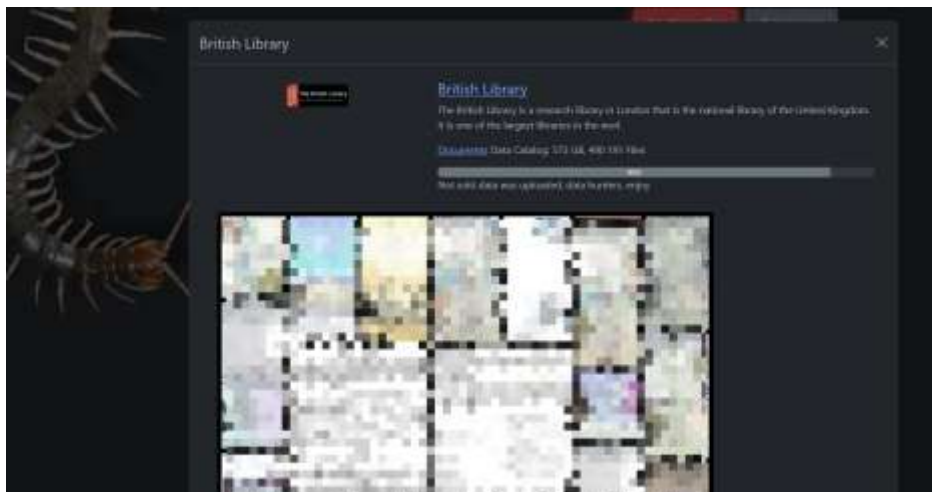


Figure 3-23The Rhysida ransomware attack group lists British Library as a victim

Reference Links

[1] Antiy. Analysis of Akira Ransomware Suspected of Using Targeted Attack Mode [R/OL]. (2023-05-30)

https://www.antiy.cn/research/notice&report/research_report/Akira_Ransomware_Analysis.html

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

<https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/>

[3] Cisco. Akira Ransomware Targeting VPNs without Multi-Factor Authentication [R/OL]. (2023-08-24)

<https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication>

[4] Avast. Decrypted: BianLian Ransomware [R/OL]. (2023-01-16)

<https://decoded.avast.io/threatresearch/decrypted-bianlian-ransomware/>

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

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

[6] Antiy. Beware of Data Leakage Caused by BlackCat Ransomware [R/OL]. (2023-07-03)

https://www.antiy.cn/research/notice&report/research_report/BlackCat_Analysis.html

[7] U.S. Department of Justice. Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant [R/OL]. (2023-12-19)

<https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant>

[8] SentinelLabs. Cl0p Ransomware Targets Linux Systems with Flawed Encryption | Decryptor Available [R/OL]. (2023-02-07)

<https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor->

available/

[9] Antiy. Analysis of Lockbit Ransomware Samples and Defense Against Targeted Ransomware [R/OL]. (2023-11-17)

https://www.antiy.cn/research/notice&report/research_report/LockBit.html

[10] Antiy. Boeing Ransomware Attack Analysis and Review - Threat Trend Analysis and Defense Thinking of Targeted Ransomware [R/OL]. (2023-12-30)

https://www.antiy.cn/research/notice&report/research_report/BoeingReport.html

[11] CSO. Japan's Nagoya Port Resumes Operations After Ransomware Attack [R/OL]. (2023-07-06)

<https://www.csoonline.com/article/644765/japans-nagoya-port-resumes-operations-after-ransomware-attack.html>

[12] Antiy. PLAY Ransomware Analysis[R/OL]. (2023-10-20)

https://www.antiy.cn/research/notice&report/research_report/PlayCrypt_Analysis.html

Appendix: 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.