A Review of Popular Ransomware in 2021

Antiy CERT

First draft completed: December 30, 2021

First published: January 3, 2022

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

1 Overview

Ransomware has become a major cyber threat facing businesses and organizations worldwide. Infection with ransomware severely impacts their operations, including business interruptions and the theft and public sale of data and information. In 2021, global manufacturing, service industries, construction, finance, energy, healthcare, industrial control, and government organizations were frequently attacked by ransomware, causing significant losses to global industrial output.

In 2021 , Antiy CERT released multiple ransomware analysis reports and published more than 30 ransomware information in Antiy's "Weekly Typical Threat Analysis". Antiy Persistent Threat Analysis System product can accurately identify the behavior of ransomware, and Antiy Intelligent Endpoint Protection System (IEP for short) can accurately detect and kill ransomware, providing effective protection for user terminals.

Antiy CERT has sorted out the popular ransomware in 2021, formed a family overview, and shared it.

2 Ransomware Behavior Classification

Ransomware activities in 2021 mainly fall into the following four categories:

1. **Affect user systems**

By modifying the disk MBR or setting a lock screen program, users cannot use the computer normally. (For example, Petya, Ransom Locker, and Screen Locker)

2. **Destroy data**

This type of ransomware does not encrypt files but instead overwrites them with random characters, permanently destroying user data. However, after destroying the data, it will also demand a ransom. (For example, GermanWiper and Combo13 [1].[1]ransomware, etc.)

3. Encrypt files

This type of ransomware encrypts files using a combination of specific encryption algorithms (such as AES, RSA, DES, and RC4). Most ransomware cannot be decrypted without the corresponding decryption tool. Some ransomware has algorithmic logic errors that allow files to be decrypted. (For example, Cont [1].[2], and Cring [1].[3]ransomware.)

4. Steal files

This type of ransomware will reside in the victim's system for a period of time before launching a ransomware attack, during which time it steals data files. After the theft is completed, it will launch a ransomware attack, encrypt the files in the system, and notify the victim that the files have been stolen. If the ransom is not paid on time, the stolen data files will be made public to put pressure on the victim, forcing the victim to pay the ransom as soon as possible. (For example, DarkSide [1].[4], REvil [1].[5]and Avaddon ransomware, etc.)

3 Introduction to Popular Ransomware

3.1 Avaddon

The Avaddon ransomware was first discovered in February 2019. On June 2, 2020, the Avaddon group appeared on a Russian dark web forum. Besides developing the ransomware for their own use, they also sought external collaborations by offering ransomware-as-a-service (RaaS) services for greater profitability. After security researchers released a public decryptor in February 2021, the Avaddon group quickly organized its partners to update the decryptor. Since then, research has observed a surge in Avaddon activity, with its developers actively developing next-generation tools for this active RaaS platform.

According to the Avaddon organization, ransomware distribution is prohibited in CIS member states, including the Russian Federation, Belarus, Moldova, Armenia, Azerbaijan, Tajikistan, Kyrgyzstan, Kazakhstan, and Uzbekistan. Given that the Avaddon ransomware group only accepts Russian-speaking partners, it seems likely that the attackers are from Russian-speaking regions. Furthermore, the ransomware dashboard supports Chinese, indicating that China

is a key target of the group. It also supports English, German, French, Italian, Spanish, Portuguese, Japanese, and Korean.

Avaddon announced the closure of its ransomware operations in June 2021 and released a large number of decryption keys. Haron (also known as Midas) ransomware was discovered in July 2021. Since Avaddon shut down its operations in June, Haron is believed to be a successor to Avaddon due to similar ransomware formats and content, similar Tor website addresses, and similar data leakage platform pages. It spreads through phishing emails and vulnerability exploits, employing a dual extortion strategy of "threatening to expose corporate data and then ransomware-encrypting that data".

3.1.1 Family Overview

Table 1 Avaddon Family Overview

Family name	Avaddon
Appearance time	February 2019
Typical propagation methods (except phishing attacks)	Phorpiex botnet, RDP brute force attack
Encryption algorithm	AES+RSA
Typical encryption suffixes	.avdn
Decryption tool	Some versions can be decrypted
Encryption system	Windows
Attack mode	Non-directional
Common industries	Education industry, manufacturing industry
Common countries/regions	Chinese, English, German, Italian, French, Spanish, Portuguese, Japanese and Korean regions
Ransom payment method	Bitcoin
Is it double extortion?	Yes
Ransom note	

3.1.2 Key Cases

- **AXA Group branches in Thailand, Malaysia, Hong Kong, and the Philippines were attacked and 3 TB of sensitive data was stolen**

Insurance giant AXA Group's branches in Thailand, Malaysia, Hong Kong, and the Philippines were attacked by a ransomware cyberattack. According to media reports, the Avaddon ransomware group claimed on its leaked website that they had stolen 3TB of sensitive data from AXA's Asian operations. According to the group, the data

obtained by Avaddon included clients' medical reports, ID card copies, bank account statements, claim forms, payment records, contracts, etc. [1] [1].[6]

- **Mexican National Lottery website was attacked and data was stolen**

The Avaddon ransomware family said they successfully attacked "Pronosticos Deportivo", where they claim to have stolen data and then encrypted the devices. If negotiations do not begin within 240 hours, the ransomware gang threatens to release more files and DDoS the victim's website [1].[7]]

3.2 Babuk (Babyk)

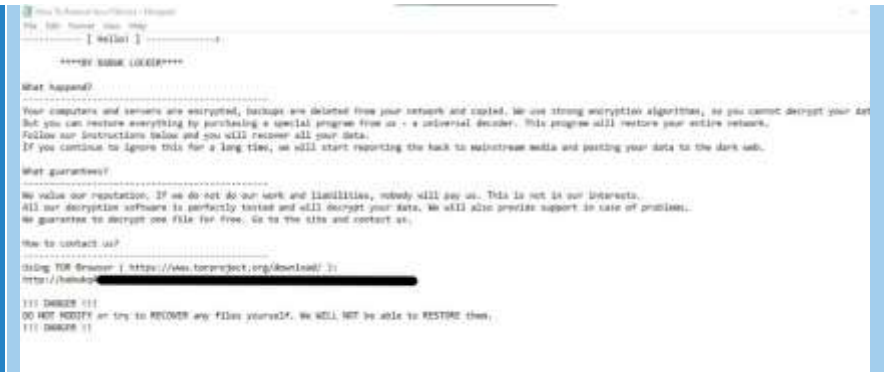
The Babuk ransomware family was discovered in early 2021 and spread through phishing emails and vulnerability exploits. It uses a double extortion strategy of "threatening to expose corporate data + encrypting data for ransom". It develops attack payloads for Windows, Linux, and VMware. In July, some data files of the Babuk ransomware were leaked by a member of the organization. The leaked source code also contained decryption keys. Researchers then used these keys to create free decryption tools for certain specific versions. The leaked content includes all the content needed to create the ransomware. In October, the new version used ProxyShell, a set of Microsoft The Exchange vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) can be chained together to bypass authentication and execute code as a privileged user.

3.2.1 Family Overview

Table 2 Babuk (Babyk) Family Overview

Family name	Babuk (Babyk)
Appearance time	Early 2021
Typical propagation methods (except phishing attacks)	Exploits
Encryption algorithm	ECDH+ HC-128
Typical encryption suffixes	. babyk
Decryption tool	Partially decryptable
Encryption system	Windows, Linux
Attack mode	Non-targeted attacks
Common industries	Large companies and organizations, FBI , CSA and other departments
Common countries/regions	United States, Spain, etc.
Ransom payment method	Bitcoin
Is it double extortion?	Yes

Ransom note



3.2.2 Key Cases

- **Attacked the District of Columbia Police Department and stole 250GB of confidential documents**

The Babuk locker gang posted on the dark web that they had breached the police department's network and stolen 250GB of unencrypted files. The group shared screenshots of various folders containing investigative reports, arrests, disciplinary actions, and other intelligence briefings. The attackers gave the police three days to meet their ransom demands and threatened to leak the data if they did not receive the ransom.[1].[8]]

- **Attacked the US NBA Houston Rockets and stole more than 550GB of data**

The Babuk cybercrime gang published a post on its ransomware website that exposed data and files allegedly from the Rockets' network system, but the post has now been deleted. The Babuk cybercrime gang claimed that they had deleted 500GB of data, including third-party contract companies, customers, employees and financial information [1].[9]

3.3 Clop

The Clop ransomware family, a variant of CryptoMix, was discovered in February 2019. Encrypted files have the suffix ".clop". The attackers behind the Clop ransomware family claim that their targets are not individual users but businesses. In March 2020, the Clop ransomware family first launched a data leak site on the dark web, distributing victim information for double ransomware attacks. The site remains active and has subsequently leaked large amounts of stolen data from victim organizations, causing significant data breaches globally. In the first half of 2021, Clop became one of the most active ransomware groups. After being attacked by this family, they deploy lateral movement and remote access tools to penetrate the target's intranet and infect more machines. This ransomware is used in targeted attacks, spreading through phishing emails, vulnerability exploits, or brute-force attacks using the Remote Desktop Protocol (RDP). It employs a double ransomware strategy: exposing enterprise data and then

extorting encrypted data.

3.3.1 Family Overview

Table 3 Clop Family Overview

Family name	Clop
Appearance time	2019
Typical propagation methods (except phishing attacks)	Vulnerability exploitation, RDP brute force cracking
Encryption algorithm	AES+RSA
Typical encryption suffixes	. clop
Decryption tool	No decryption tool yet
Encryption system	Windows
Attack mode	Non-directional
Common industries	Large Enterprises
Common countries/regions	The United States, Germany, Canada, etc.
Ransom payment method	Bitcoin
Is it double extortion?	Yes
Ransom note	

3.3.2 Key Cases

- **Hack on UK police steals 13 million messages and records**

In October 2021, the Clop ransomware gained access to data managed by Dacoll Limited and stole the personal information and records of 13 million people. The stolen files included images of drivers, footage stolen from the national Automatic Number Plate Recognition (ANPR) system, and close-up images of the faces of drivers who had committed traffic violations [1].[10]]

- **Attacked German software company Software AG , stole data, and demanded a $20 million ransom**

In October 2021, the Clop ransomware operators attacked Software AG, one of Germany's largest software companies, and demanded a ransom of $20 million. After the first negotiations failed due to price and security concerns, the Clop gang published screenshots showing Software AG's data on a leak website, including employee ID scans, employee emails, financial documents and directories. [1] [1].[11]

3.4 Conti

The Conti ransomware family was discovered in 2019. The attack organization behind it operated as a RaaS (Ransomware as a Service) on underground forums and widely recruited affiliated members. Since May 2020, the attack activities have gradually increased and remain active to this day. The ransomware is mainly spread through phishing emails, other malware, vulnerability exploits, and Remote Desktop Protocol (RDP) brute force attacks. It uses a combination of various tools to achieve lateral movement within the intranet. After the Log4j vulnerability (CVE-2021-44228) was exposed in December 2021, the Conti ransomware operators began to use VMWare vCenter, which has a Log4j vulnerability, to move laterally. In July 2020, they used the anonymous Tor to establish a ransom payment and data leakage platform, adopting a double extortion strategy of "threatening to expose corporate data + ransom encrypted data".

Antiy CERT discovered through correlation analysis that this group has a connection with Grim Spider, a branch of the Wizard Spider group that operates the Ryuk ransomware. Considering the declining activity of Ryuk ransomware attacks, the fact that both groups share some of the same attack tools and payload code, and that both groups have previously spread using Trojans such as TrickBot, Emotet , IcedID, and BazarLoader, Antiy CERT speculates that Conti ransomware will be the successor to Ryuk ransomware.

Conti ransomware uses Tor to establish a website to publish victim information and stolen data files. Since the first victim information was released on July 29, 2020, as of December 15, 2021, a total of 631 victim information has been released, of which more than 470 organizations were affected worldwide in 2021. According to statistics from Antiy CERT, from November 1 to December 15, 2021, the number of victims disclosed was 90, and there may be undisclosed victims. The victims' countries of origin are mainly concentrated in the United States, Italy, Germany, Australia and France, and their industries include manufacturing, services, construction, finance, energy, medical care and government organizations. There are also victims disclosed in China. [1].[2]

3.4.1 Family Overview

Table 4 Conti Family Overview

Family name	Conti
Appearance time	2019
Typical propagation methods (except phishing attacks)	Leverage other malware, exploits, and RDP brute force
Encryption algorithm	AES
Typical encryption suffixes	.CONTI
Decryption tool	No public decryption tool has been found yet

Encryption system	Windows
Attack mode	There are cases of targeted attacks
Common industries	Manufacturing, services, construction, finance, energy, healthcare and government organizations
Common countries/regions	United States, Italy, Germany, Australia and France
Ransom payment method	Bitcoin
Is it double extortion?	Yes
Ransom note	

3.4.2 Key Cases

- **Hack on the Irish Health Service Executive steals 700GB of sensitive files**

On May 14, 2021, the Irish Health Service Executive (HSE) was attacked by the Conti ransomware, resulting in the cancellation and interruption of services at several hospitals. The Conti ransomware attackers claimed to have stolen 700GB of unencrypted files from the HSE, including patient and employee information, contracts, financial statements, payrolls, etc. The Irish Prime Minister stated that they refused to pay the $20 million ransom demanded by the attack group behind the Conti ransomware [1].[12]]

- **Attack on Tulsa , Oklahoma, USA , stealing over 18,000 sensitive documents**

Tulsa, Oklahoma, was attacked by the Conti ransomware in May, which disrupted the city's online bill payment system, utility billing system, and email system. The group behind the Conti ransomware claimed responsibility and said it had publicly released 18,938 stolen files. [1].[13]]

- **Japanese electronics supplier hacked and 1.5TB of data stolen**

JVC Kenwood, a multinational electronics supplier headquartered in Japan, was attacked by the Conti ransomware. The attackers claimed to have stolen 1.5TB of data and demanded a ransom of US$7 million. [1].[14]]

- **Attack on high-end jewelers in London, UK and stealing data files of celebrities, politicians and heads of state**

Graff, a high-end jeweler based in London, UK, was attacked by Conti ransomware in October. The stolen files included data files of many celebrities, politicians and heads of state.[1].[15]The attacking organization in this incident

published tens of thousands of files on its Tor website. Under political pressure, the organization issued a statement on November 4th that any information related to family members of Saudi Arabia, the United Arab Emirates and Qatar would be deleted, and apologized to His Royal Highness Prince Mohammed bin Salman and all other members of the royal family.[1].[16]]

3.5 Dark Side (Renamed Black Matter)

The DarkSide group first appeared in August 2020. It employs a RaaS (Ransomware as a Service) model, meaning that in addition to DarkSide's own operations, it also operates through cooperative organizations. DarkSide uses multi-threaded encryption techniques, making it faster than other ransomware, meaning it takes less time to encrypt the same file. It uses the RSA1024+Salsa20 algorithm to encrypt files and can infect both Windows and Linux systems. The group is very active on dark web forums. DarkSide uses a combination of "stealth and ransomware" attacks against victims, meaning attackers not only encrypt user data but also steal it and threaten to release it publicly if a ransom is not paid. On August 10, 2020, the DarkSide group stated on its dark web forum that, in accordance with its principles, it will not attack the following targets: the medical and funeral services, the education sector, non-profit organizations, and government agencies.

By collecting information about victims and analyzing data from DarkSide ransomware victims, the average ransom demand is approximately $6.5 million, with an average business downtime of five days. DarkSide ransomware attackers have exploited CDN servers to store and deliver stolen data from victims. Once leaked, the data is uploaded to servers within their CDN, which are used as ransomware tools by the attackers. Data leaked publicly on the dark web by the DarkSide organization since August 2020 indicates that 82 companies have been targeted by this ransomware family to date, including those in the legal, financial, construction, healthcare, and energy sectors. On average, leaked data from more than a dozen companies is released each month.

3.5.1 Family Overview

Table 5 Dark Side Family Overview

Family name	Dark Side (Renamed Black Matter)
Appearance time	August 2020
Typical propagation methods (except phishing attacks)	RDP brute force cracking, vulnerability exploitation
Encryption algorithm	RSA1024+Salsa20
Typical encryption suffixes	An 8-digit personal ID consisting of a random combination of letters and numbers
Decryption tool	Some versions can be decrypted
Encryption system	Windows + Linux
Attack mode	There are cases of targeted attacks
Common industries	Legal, financial, construction, medical, energy and other industries

Common countries/regions	English-speaking countries and regions
Ransom payment method	Bitcoin and Monero
Is it double extortion?	Yes
Ransom note	

3.5.2 Key Cases

- **Attacked Colonial Pipeline, a US refined oil pipeline operator, and stole data**

On May 7, 2021, Colonial Pipeline, the largest refined oil pipeline operator in the United States, was attacked by the Conti ransomware, which knocked offline pipelines transporting oil and gas to major cities along the East Coast. The day before the Dark Side group lost access to its servers via SSH, US President Biden declared at a White House press conference that he would pursue the group. According to a post by a user named U NKN on the Exploit darknet forum, Dark Side has lost access to its data exfiltration servers, ransom payment servers, and CDN servers due to law enforcement action. Since its emergence in July 2021, the renamed Dark Side ransomware has targeted multiple US critical infrastructure entities, including two US food and agriculture sector organizations, demanding ransoms ranging from $80,000 to $15 million in Bitcoin and Monero. The ransomware group issued a notice in November, stating that it had ceased operations due to pressure from authorities and unresolved issues.

3.6 DoppelPalmer (Renamed Grief)

The DoppelPaymer ransomware group has been active since June 2019 and has been involved in a series of malicious ransomware campaigns, including attacks on the city of Edecouche, Texas, and the Ministry of Agriculture in Chile. However, early versions of DoppelPaymer were released in April 2019. Compared to later versions, these early versions lack many new features, so it is not clear whether these versions were constructed simply for testing. In fact, as early as November of last year, the Microsoft Security Response Center (MSRC) issued an announcement to alert customers to the threat of DoppelPaymer ransomware and provided useful information about the related threats. According to relevant security research experts, another unnamed security company once mentioned that the headquarters of the DoppelPaymer ransomware operator is located in Russia.

DoppelPaymer is actually a new variant of the BitPaymer ransomware, dubbed DoppelPaymer. While DoppelPaymer shares much of its code with BitPaymer, there are also many differences. BitPaymer was previously operated by the INDRIK SPIDER group. This shift may indicate that a member of the group has defected and independently integrated the Dridex banking trojan with BitPaymer, forging their own unique criminal enterprise.

DoppelPaymer, the successor to BitPaymer ransomware, has undergone a rebranding after a period of near-inactivity, now known as Grief. Starting in February 2020, the malicious actors behind DoppelPaymer launched a data leak site. As part of their ransomware extortion scheme, they threatened victims by publishing stolen files on the data leak site. An early Grief ransomware sample was discovered on May 17, 2021. It contained the Grief ransomware code and a ransom note, but the link in the ransom note led to a DoppelPaymer ransom portal.

3.6.1 Indrik Spider Origins

INDRIK SPIDER is a sophisticated cybercriminal group that has been operating the Dridex banking trojan since June 2014. In 2015 and 2016, Dridex was one of the most profitable banking trojans worldwide. Since 2014, INDRIK SPIDER has reaped millions of dollars in illicit profits from this trojan. Over the years, Dridex has undergone multiple updates, becoming more sophisticated and specialized, while also incorporating new anti-analysis capabilities.

Over time, INDRIK SPIDER's core business of wire fraud became less successful. In 2015, INDRIK SPIDER, using the alias "Smilex", was arrested. Following this, UK law enforcement launched an operation aimed at dismantling INDRIK SPIDER's money laundering network through Dridex. A UK bank employee who had helped set up the fake accounts was also arrested and imprisoned.

Due to these setbacks, INDRIK SPIDER changed their operations in 2017, focusing on smaller-scale Dridex distribution campaigns. In August 2017, the group introduced the BitPaymer ransomware and began focusing on this type of high-payout ransomware.

3.6.2 BitPaymer Origins

BitPaymer was first discovered in August 2017. The first version of the ransom note contained a ransom demand and a link to a TOR-based payment website, with the title "Bitpaymer", user ID, Bitcoin (BTC) wallet, and contact email address. Less than a month later, the ransom note no longer contained the ransom amount. By July 2018, the link to the payment website was also deleted. Since then, only two contact email addresses for negotiation remain in the ransom note.

In addition to the aforementioned changes, BitPaymer has also been updated to use AES-256 in CBC (Cipher Block Chaining) mode, along with a randomly generated key and a NULL initialization vector for encryption (previous versions of BitPaymer used 128-bit RC4).

Because AES is a block cipher, data must be padded if it is not a multiple of the block size, usually by adding zeros or n times of padding. However, INDRIK SPIDER chooses to pad with randomly generated n bytes, which means that these random padding bytes must be known to correctly decrypt the last data block of the file. This is reflected in the new field TAIL in the ransom note, which contains the Base64-encoded TAIL and the encrypted AES KEY.

3.6.3 Family Overview

Table 6 Doppel Palmer Family Overview

Family name	Doppel Palmer (Renamed Grief)
Appearance time	2019
Typical propagation methods (except phishing attacks)	Vulnerability exploitation, RDP brute force cracking
Encryption algorithm	AES+RSA
Typical encryption suffixes	. locked
Decryption tool	No decryption tool has been found yet
Encryption system	Windows
Attack mode	There are cases of targeted attacks
Common industries	Government, retail/wholesale, manufacturing, finance, insurance, transportation/logistics, high-tech, healthcare, real estate
Common countries/regions	United States, Canada, Mexico, South Africa, Belgium, Italy, Norway, Germany
Ransom payment method	Bitcoin
Is it double extortion?	Yes
Ransom note	

3.6.4 Key Cases

- **Attack on New York Rehabilitation Support Services (RSS) and steal sensitive data**

On September 10, 2021, Rehabilitation Support Services, Inc. (RSS) issued a statement saying that the June attack may have affected the information of some current and former employees, and that information such as names,

addresses, dates of birth, social security numbers, health insurance information, medical diagnoses and treatments may have been accessed without authorization, and a leak is suspected to have occurred. [1].[17]]

- **Attack on the National Rifle Association and steal sensitive data**

In October 2021, the National Rifle Association (NRA) was attacked by the Grief ransomware, and the organization displayed screenshots of Excel spreadsheets containing US tax information and investment amounts on its leaked website, including the NRA's grant application. [1].[18]]

3.7 Lock Bit 2.0

The LockBit ransomware family was discovered in September 2019 and released version 2.0 in June 2021. It spreads through phishing emails, other malware, vulnerability exploits, and Remote Desktop Protocol (RDP) brute force attacks. Members of the group claim that Lockbit 2.0 ransomware and the Stealbit information stealer are the fastest on the market today at encrypting files and stealing data. Compared to the 2019 version of LockBit, LockBit 2.0 adds the ability to automatically encrypt devices across Windows domains using Active Directory (AD) Group Policies. LockBit 2.0 is a new ransomware strain that utilizes a Ransomware-as-a-Service (RaaS) model. Currently, this malware has been used in ransomware attacks targeting multiple industries worldwide. It employs a dual ransomware strategy of exposing enterprise data and encrypting data for ransom. In August 2021, it added a DDoS attack threat, creating a triple ransomware attack.

3.7.1 Family Overview

Table 7 Lock Bit 2.0 Family Overview

Family name	LockBit 2.0
Appearance time	2019
Typical propagation methods (except phishing attacks)	Leverage other malware, exploits, and RDP brute force
Encryption algorithm	AES+RSA
Typical encryption suffixes	.lockbit
Decryption tool	No decryption tool has been found yet
Encryption system	Windows
Attack mode	There are cases of targeted attacks
Common industries	Important enterprises and governments
Common countries/regions	China, India, Indonesia, Ukraine, United Kingdom, France, Germany, etc.
Ransom payment method	Bitcoin
Is it double extortion?	Yes
Ransom note	

3.7.2 Key Cases

- **Bangkok Airways hacked and stole 200GB of data**

In August 2021, the LockBit ransomware group stole more than 200GB of Bangkok Airways data and posted a message on its leak website, threatening to leak the stolen data if Bangkok Airways did not pay the ransom. The message also indicated that they had more data to leak. Investigations showed that the leaked data may include passenger names, surnames, nationalities, genders, phone numbers, emails, addresses, contact information, passport information, historical travel information, partial credit card information, and special meal information. [1].[19]]

- **Attack on Irish IT consulting firm Accenture and steal over 6TB of data**

In August 2021, Accenture, a global IT consulting giant, was attacked by the LockBit group. In the Accenture incident, the LockBit ransomware group claimed to have stolen more than 6TB of Accenture data and demanded that Accenture pay $50 million (about 320 million RMB) as a ransom. After the countdown ended, the ransomware group immediately released a small portion of the stolen data, consisting of 2,384 items. The leaked files included PDF files allegedly stolen from the company, which appeared as general marketing materials .[1].[20]]

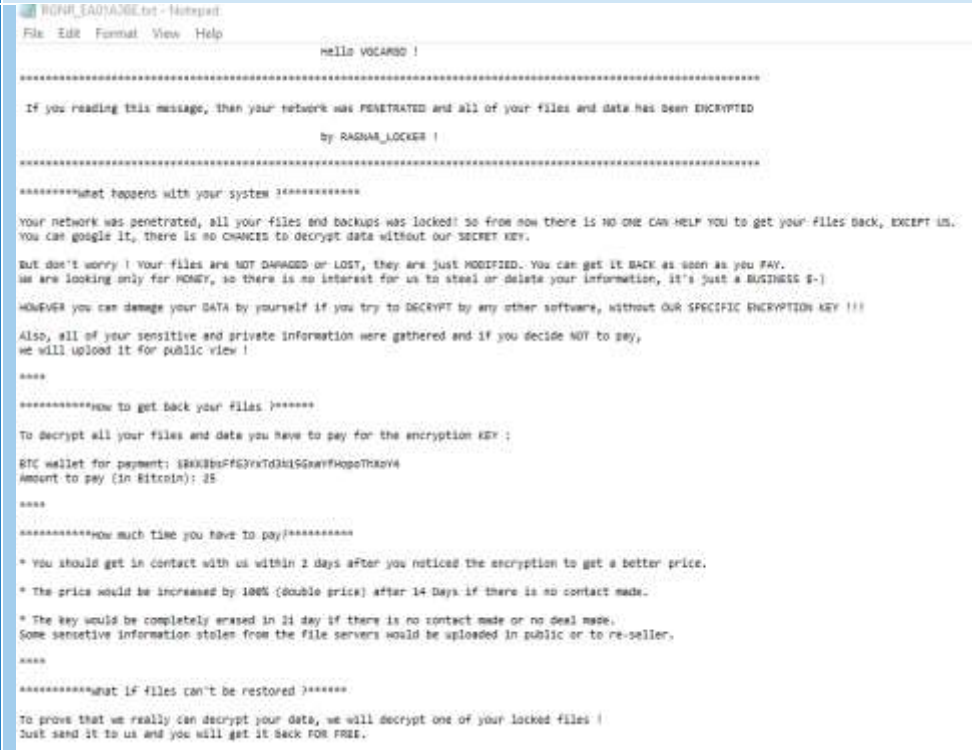
3.8 Ragnar Locker

The Ragnar Locker ransomware family was discovered in late December 2019 and spread through credentials purchased on the dark web, phishing emails, vulnerability exploits, and Remote Desktop Protocol (RDP) brute force attacks. The ransomware is executed using specially crafted virtual machine images to evade antivirus detection. The Ragnar Locker group has always manually delivered the ransomware to targeted systems, encrypting their files and data. They spend significant time conducting network reconnaissance, attempting to identify network resources, data backups, and other sensitive files within the target user, organization, or enterprise. Once this data is stolen, it is fully encrypted. In addition to releasing data, the Ragnar Locker ransomware family also warns that if the attacked company wishes to hire professional negotiators, these negotiators, often employed by data recovery firms affiliated with the police, FBI, or government agencies, or even government employees themselves, will only complicate and hinder data recovery. Therefore, if the victim contacts data recovery experts to attempt to decrypt the data or negotiate a ransom, they will also leak the data.

3.8.1 Family Overview

Table 8 Ragnar Locker Family Overview

Family name	Ragnar Locker

Appearance time	2019
Typical propagation methods (except phishing attacks)	Credentials purchased from the dark web, exploits, and RDP brute force
Encryption algorithm	Salsa20
Typical encryption suffixes	.ragnar_ <ID>
Decryption tool	No decryption tool has been found yet
Encryption system	Windows
Attack mode	There are cases of targeted attacks
Common industries	Large enterprises
Common countries/regions	Except for the languages of the CIS countries
Ransom payment method	Bitcoin
Is it double extortion?	Yes
Ransom note	

RGNR_EA01A30E.txt - Notepad

File Edit Format View Help

Hello VOCARDO !

****

If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED

by RAGNAR_LOCKER !

****

*********What happens with your system ?***********

Your network was penetrated, all your files and backups was locked! So from now there is NO ONE CAN HELP YOU to get your files back, EXCEPT US.
You can google it, there is no CHANCES to decrypt data without our SECRET KEY.

But don't worry ! Your files are NOT DAMAGED or LOST, they are just MODIFIED. You can get it BACK as soon as you PAY.
We are looking only for MONEY, so there is no interest for us to steal or delete your information, it's just a BUSINESS $-)

HOWEVER you can damage your DATA by yourself if you try to DECRYPT by any other software, without OUR SPECIFIC ENCRYPTION KEY !!!

Also, all of your sensitive and private information were gathered and if you decide NOT to pay,
we will upload it for public view !

****

**********How to get back your files ?*******

To decrypt all your files and data you have to pay for the encryption KEY :

BTC wallet for payment: 18KKBbsFfG3rxTd3bi5GaxyFHopoThkpV4
Amount to pay (in Bitcoin): 25

****

**********How much time you have to pay?**********

* You should get in contact with us within 2 days after you noticed the encryption to get a better price.

* The price would be increased by 100% (double price) after 14 Days if there is no contact made.

* The key would be completely erased in 21 day if there is no contact made or no deal made.
Some sensetive information stolen from the file servers would be uploaded in public or to re-seller.

****

**********What if files can't be restored ?*******

To prove that we really can decrypt your data, we will decrypt one of your locked files !
Just send it to us and you will get it back FOR FREE.

3.8.2 Key Cases

- **Attack on ADATA, a Taiwanese memory and SSD manufacturer, and stealing 1.5TB of data**

In June 2021, after ADATA refused to pay the ransom, the ransomware group Ragnar Locker published more than 700GB of ADATA data online. The data was uploaded in the form of 13 password-protected archives. Ragnar Locker published metadata archives on the storage platform MEGA, with the largest file being nearly 300GB. Judging from the file names, it may contain detailed information such as financial information and confidentiality agreements. The organization also released several screenshots to prove the ADATA data it holds. [1].[21]]

- **Attack on Portuguese multinational energy company steals 10TB of data**

EDP Renewables North America (EDPR NA) confirmed that its parent company, Portuguese multinational energy giant Energia de Portugal (EDP), was attacked by the Ragnar Locker ransomware. The attackers demanded a

ransom of 1,580 Bitcoin (approximately $10 million) from EDP Group to purchase a decryptor and stop leaking 10 terabytes of data allegedly stolen from the organization's servers to the public. According to the ransom note on EDP's encrypted systems, the attackers were able to steal confidential information about bills, contracts, transactions, customers, and partners. [1] [1].[22]

3.9 RansomEXX

RansomEXX ransomware, also known as Defray777 and Target777, was first discovered in 2017. It was the first ransomware to have two executable versions, one for Windows and one for Linux. The Windows version encrypts all files, while the Linux version encrypts only files in specific directories, which can be specified via command-line parameters. From late 2020 and throughout 2021, RansomEXX not only encrypted files on targeted systems but also began stealing data, publishing it on the dark web. RansomEXX has been linked to the threat group PyXie and targets industries such as healthcare, education, manufacturing, government, construction and engineering, and high-tech. Common targets include the United States, Canada, Australia, Japan, France, and Brazil. From February to October 2020, RansomEXX was distributed via the malware strains Trickbot and IcedID. It spread through phishing emails, vulnerability exploits, and Remote Desktop Protocol (RDP) brute force attacks, employing a dual ransomware strategy of exposing enterprise data and then extorting encrypted data for ransom.

3.9.1 Family Overview

Table 9 RansomEXX Family Overview

Family name	RansomEXX
Appearance time	2018
Typical propagation methods (except phishing attacks)	Vulnerability exploitation, RDP brute force cracking
Encryption algorithm	RSA+AES
Typical encryption suffixes	.ransomexx
Decryption tool	No decryption tool has been found yet
Encryption system	Windows, Linux
Attack mode	There are cases of targeted attacks
Common industries	Healthcare, Education, Manufacturing, Government, Construction/Engineering, High-Tech
Common countries/regions	United States, Canada, Australia, Japan, France, Brazil
Ransom payment method	Bitcoin
Is it double extortion?	Yes

Ransom note	

3.9.2 Key Cases

- **Attacked Gigabyte, a computer hardware supplier from Taiwan, China, and stole 112GB of data**

Members of the RansomExx ransomware gang posted a description of the Gigabyte intrusion on their dark web portal, where they also published sensitive data if the victim refused to cooperate. The attackers stated on the dark web: "We have downloaded 112GB of files and are ready to publish them. Most of them are data subject to confidentiality agreements (involving Intel, AMD, and American Megatrends)" [1].[23]]

- **Attack on Ecuadorian state-owned enterprise CNT and steal 190GB of data**

In July 2021, the Corporación Nacional de Telecomunicación (CNT), a state-owned enterprise in Ecuador, suffered a ransomware attack that disrupted business operations, payment portals, and customer support. Researchers learned that the attack was caused by a ransomware gang called RansomEXX, and they shared a hidden link to the gang's data leak site, which warned CNT that if the ransom was not paid, the gang would leak data stolen during the attack [1].[24]]

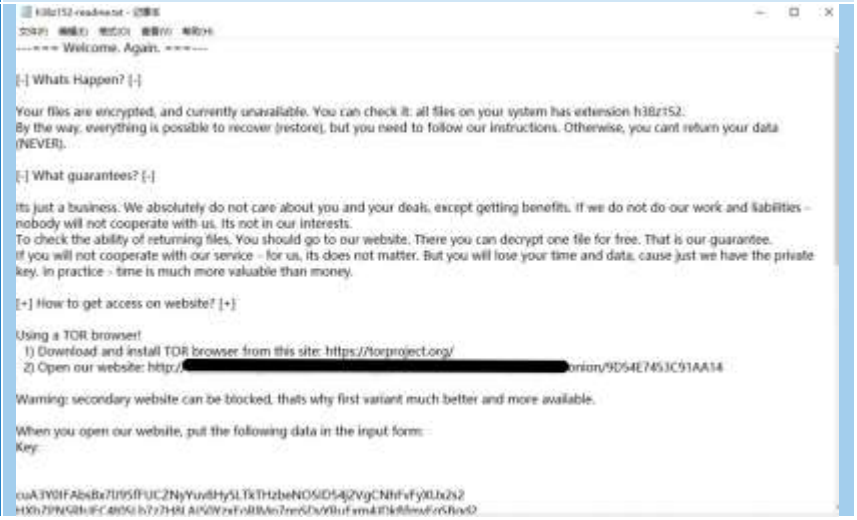
3.10 REvil (Sodinokibi)

This ransomware family was discovered in 2019. The attack organization behind it operated in the form of RaaS (Ransomware as a Service) on underground forums. Through correlation and comparative analysis, it was found that it was the successor of Gand Crab ransomware, and was spread through phishing emails, vulnerability exploitation, and Remote Desktop Protocol (RDP) brute force cracking. In June 2019, Antiy mentioned in the report "Correlation Analysis of the Ransomware Sodinokibi Operation Organization" [1].[25]large-scale black market organization that constantly applies and uses other existing malicious tools as attack vectors to spread ransomware, mining Trojans, and stealing programs, and implements universal, non-targeted ransomware, mining, and stealing attacks worldwide. Since 2019, the REvil ransomware organization has adopted a dual ransomware strategy of "threatening to expose

corporate data + encrypting data ransom". Antiy CERT believes that LV ransomware appeared at the end of 2020. The two are similar in code structure and ransom letter format, and are considered to be the successor of REvil ransomware.

3.10.1 Family Overview

Table 10 REvil (Sodinokibi) Family Overview

Family name	REvil (Sodinokibi)
Appearance time	2019
Typical propagation methods (except phishing attacks)	Vulnerability exploitation, RDP brute force cracking
Encryption algorithm	Salsa20+ECDH
Typical encryption suffixes	<Original file name>+<Original file extension>+.<Random extension>
Decryption tool	No decryption tool has been found yet
Encryption system	Windows, Linux
Attack mode	There are cases of targeted attacks
Common industries	Law, Manufacturing, Media, Retail/Wholesale, Construction/Engineering, Energy
Common countries/regions	United States, Australia, Canada, Finland, Hong Kong, China
Ransom payment method	Bitcoin, Monero
Is it double extortion?	Yes
Ransom note	

3.10.2 Key Cases

- **Attacked 60 hosting providers and over 1,500 businesses and demanded $70 million in ransom**

In July 2021, the ransomware group launched its largest attack to date, exploiting a zero-day vulnerability in the Kaseya VSA remote management platform to encrypt approximately 60 managed service providers and more than 1,500 businesses, and demanding a ransom of up to $70 million. This incident attracted the attention of international law enforcement agencies, and the ransomware group may have shut down its payment website, data leakage website and other infrastructure on July 13, 2021, out of fear of being arrested. Since February 2021, a total of seven members of the REvil group suspected of participating in ransomware attacks have been arrested, and $ 6.1 million in assets have been confiscated from the FTX cryptocurrency trading exchange. [1].[26]]

- **Attack on US meat processor JBS and steal data**

In May 2021, attackers attacked multiple servers supporting JBS Foods' IT systems in North America and Australia, forcing JBS to shut down some of its food production sites. JBS paid the attackers $11 million in ransom to prevent the public disclosure of their stolen data and to mitigate potential technical issues. [1].[27]]

Appendix 1: References

[1]. Analysis of Combo13 Ransomware That Destroys Rather Than Encrypts Files

https://www.antiy.cn/research/notice&report/research_report/20210517.html

[2]. Conti Ransomware Analysis Report

https://www.antiy.cn/research/notice&report/research_report/20211220.html

[3]. Analysis of Cring Ransomware Samples Targeting Industrial Control Systems

https://www.antiy.cn/research/notice&report/research_report/20210528.html

[4]. Sample and follow-up analysis of a ransomware attack on a US fuel pipeline company

https://www.antiy.cn/research/notice&report/research_report/20210511.html

[5]. Sodinokibi / REvil Ransomware Group Recent Activities and Latest Sample Analysis

https://www.antiy.cn/research/notice&report/research_report/20210918.html

[6]. Insurer AXA hit by ransomware after dropping support for ransom payments

https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/

[7]. Mexico blocks national lottery website after ransomware DDoS threat

https://www.bleepingcomputer.com/news/security/mexico-walls-off-national-lottery-sites-after-ransomware-ddos-threat/

[8]. DC police confirm cyberattack after ransomware gang leaks data

https://www.bleepingcomputer.com/news/security/dc-police-confirms-cyberattack-after-ransomware-gang-leaks-data/

[9]. Babuk ransomware attacks NBA's Houston Rockets

https://www.cybersecurity-insiders.com/babuk-ransomware-attack-on-nba-houston-rockets/

[10]. Clop ransomware gang is leaking confidential UK police data

https://securityaffairs.co/wordpress/125792/cyber-crime/clop-ransomware-uk-police.html

[11]. Software AG data released after Clop ransomware attack

https://threatpost.com/software-ag-data-clop-ransomware/160042/

[12]. Ireland's Health Service Executive (HSE) has refused to pay a $20 million ransom demand after its systems were attacked by the Conti ransomware gang.

https://securityaffairs.co/wordpress/118001/cyber-crime/ireland-health-service-executive-conti-ransomware.html

[13]. Tulsa police say 18,000 files containing citizen information were leaked on the dark web following the Conti ransomware attack.

https://www.zdnet.com/article/tulsa-warns-residents-that-police-citations-and-reports-leaked-to-dark-web-after-conti-ransomware-attack/

[14]. JVC Kenwood hit by Conti ransomware, claims 1.5TB of data stolen

https://www.bleepingcomputer.com/news/security/jvckenwood-hit-by-conti-ransomware-claiming-theft-of-15tb-data/

[15]. Conti Group leaks celebrity data after ransom attack on jeweler

https://www.infosecurity-magazine.com/news/conti-leak-celebs-data-ransom/

[16]. Conti's apology statement

https://pastebin.com/eeLNnAG0

[17]. Recovery Support Services notifies current and former employees and customers of IT security incidents

https://www.prnewswire.com/news-releases/rehabilitation-support-services-notifies-current-and-former-employees-and-clients-of-it-security-incident-301373523.html

[18]. Grief ransomware gang attacks the National Rifle Association (NRA)

https://securityaffairs.co/wordpress/123849/cyber-crime/grief-ransomware-hit-nra.html

[19]. LockBit ransomware operators leak 200GB of data belonging to Bangkok Airways

https://securityaffairs.co/wordpress/121702/data-breach/lockbit-gang-bangkok-airways.html

[20]. LockBit 2.0 ransomware attacks Accenture

https://cybernews.com/security/the-lockbit-2-0-ransomware-attack-against-accenture-time-is-running-out/

[21]. ADATA leaks 700 GB of data in Ragnar Locker ransomware attack

https://www.bleepingcomputer.com/news/security/adata-suffers-700-gb-data-leak-in-ragnar-locker-ransomware-attack/

[22]. Energy giant EDP confirms Ragnar Locker ransomware attack

https://www.bleepingcomputer.com/news/security/edp-energy-giant-confirms-ragnar-locker-ransomware-attack/

[23]. Gigabyte Technology reportedly suffered a ransomware attack , and the company announced that some of its servers were attacked by a network attack.

https://www.ithome.com.tw/news/146075

[24]. RansomEXX ransomware attacks Ecuador's state-owned CNT telecommunications company

https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/

[25]. Analysis of the association between the Sodinokibi ransomware operation organization

https://www.antiy.cn/research/notice&report/research_report/20190628.html

[26]. REvil /Kaseya Incident Update

https://cyberint.com/blog/research/revil-kaseya-incident-update/

[27].JBS pays $11 million to REvil ransomware, first demand of $22.5 million

https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/

Appendix 2: 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 cyberspce 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.