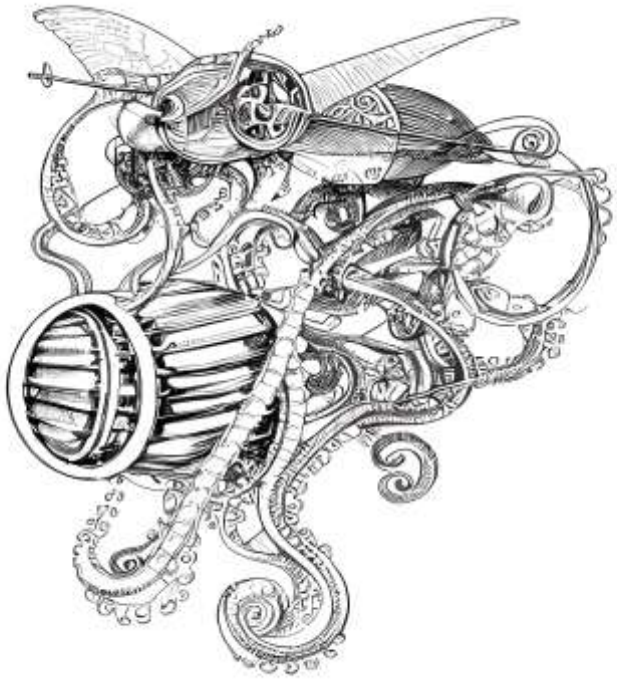
# Analysis of LockBit Ransomware Samples and Thoughts on Defending Against Targeted Ransomware Attacks

Antiy CERT

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



Completion time of first draft: 18: 00, 17 November 2023

First published: 17 November 2023 at 20: 05

This edition was updated at 20: 05 on 17 November 2023

Scan QR code for the latest version of the report

# 1 Overview

There has been a recent blackmail attack on a financial institution [1]. Multiple sources said the incident was closely linked to the LockBit extortion attack group. The reason why Antiy CERT uses "there is a close correlation" is that LockBit is an attack organization operating on a "ransomware-as-a-service" (RaaS) model that builds the infrastructure that underpins blackmail attacks. Including developing and releasing malicious code payloads for blackmail attacks, providing customized constructors, building uniform hints for blackmail attacks, and building payment channels for virtual currencies. So that all kinds of attack organizations, individuals can rely on their "services" to carry out attack operations, between the organizations providing RaaS and the implementation of attackers through extortion or trafficking stolen data for the distribution of illicit money. In that blackmail-as-a-service mode, the "infrastructure" provid and the perpetrator are usually not the same organization and individual, or even back-to-back to each other, The payment is made in cryptocurrencies such as Bitcoin, which brings great difficulties to the full tracing and analysis of events.[1]

Lockbit has been named the world's most active ransomware attack organization in 2022, developing ransomware for a variety of host systems and target platforms such as Windows, Linux, macOS, and VMware virtualization platform. The ransomware customization can be done by its generator through a simple interaction. The lockbit ransomware only encrypts the first 4K data in the header of the encrypted file, so the encryption speed is significantly faster than other ransomware with full file encryption, since the write is overwritten in the sector corresponding to the original file, The victim was unable to recover the unencrypted plain text data by means of data recovery. The group was first spotted in September 2019, known as ABCD ransomware for its encrypted filename suffix of .abcd; the group released ransomware version 2.0 in June 2021, Added the function of deleting shadow on disk and log files, released the exclusive data stealing tool, StealBit, and adopted the dual blackmail strategy of "threatening to expose (sell) corporate data + encrypted data." August 2021. The group's attack infrastructure spectrum has increased support for DDoS attacks; the ransomware was updated to version 3.0 in June 2022, as part of the 3.0 version's code overlaps with the BlackMatter ransomware code, So LockBit 3.0 is also called LockBit Black. This reflects the possibility of personnel flow and capability exchange between different blackmail attack organizations. Relevant organizations that use LockBit RaaS to carry out attacks have carried out a large number of attack operations, and launched ransomware after intruding into the victim's system by means of obtaining access credentials from third parties, weaponizing vulnerabilities and loading other malware. A large number of victims have

been subjected to extortion and data breaches, making LockBit the most active extortion attack organization at present, even taking the initiative to take the dissemination and PR activities.

## 2 Typical Attacks in Recent Years

An attacker who uses LockBit to blackmail the organization's RaaS service can gain initial access to the victim system mainly by obtaining access credentials from a third party, weaponizing vulnerabilities and mounting other malware. Data files are stolen and then released into LockBit ransomware for encryption. The group has a large number of affiliated members, and on its Tor website, information about victims from all over the world is added almost daily, since the double blackmail strategy of "threatening to expose corporate data + extorting encrypted data" was adopted. On its Tor website, more than 2,200 pieces of information about injured enterprises have been published, and more than 900 pieces of information about injured enterprises have been published so far in 2023, for example, affiliated members and injured enterprises have negotiated privately. The information of the victimized enterprises will not be disclosed in Tor, which means that the actual number of victimized enterprises will exceed the number of victimized enterprises that have been publicly released.

**Table 2-1 List of typical LockBit blackmail attacks1**

| Time | Victimized Unit | Impact |
|---|---|---|
| **Aug-2021** | Irish IT consultancy Accenture | About 6 terabytes of data were stolen, demanding a $50 million ransom |
| **January 2022** | Thales Group of France | Part of the data was made public; in November of the same year, it was again subjected to blackmail, and about 9.5 GB of data was stolen publicly |
| **February 2022** | Bridgestone Americas Branch | The company suspended some of its operations and data from the victim's system was stolen |
| **June 2022** | American digital security company Entrust | Part of the data was stolen |
| **July 2022** | French telecom operator La Poste Mobile | As a result, some systems were shut down, the official website was shut down for more than 10 days, and some user information was disclosed |
| **October 2022** | Bank of Brasilia | Part of the data was stolen, demanding a 50 BTC ransom |
| **November 2022** | Continental Germany | About 40 gigabytes of data were stolen, demanding a $50 million ransom |
| **Dec-2022** | Department of Finance, California, USA | Steal about 76 GB of data |

| | | |
|---|---|---|
| **January 2023** | Royal Mail | International export services were disrupted and some 45 gigabytes of data were stolen, demanding a $80 million ransom |
| **Jun-23** | Tsmc Supplier QINGHAO Technology | Part of the data was stolen, demanding a $70 million ransom |
| **Aug-2023** | Power Service Commission of Montreal, Canada | Steal about 44 GB of data |
| **October 2023** | Boeing Airlines of America | Steal about 43 GB of data |

# 3 Overview of attack organization and corresponding attack situation

**Table 3-1 Basic information of LockBit attack organizations1**

| | |
|---|---|
| **Organization name** | Lockbit |
| **The organization used to be named** | Abcd |
| **Time of occurrence** | September 2019 |
| **Typical penetration mode** | In addition to phishing attacks, third parties acquire access credentials, weaponization of vulnerabilities, and other malware |
| **Typical Encryption Suffix** | A 9-digit personal ID with a random combination of letters and numbers |
| **Decryption tools** | No public decryption tools have been found |
| **Encrypt the target system** | Windows, Linux, macOS, VMware, etc |
| **Operation mode** | Ransom as a service, based on ransom and sales data |
| **Patterns of victimization** | Encryption leads to paralysis, theft and DDoS interference |
| **Common to industries** | Finance, service, construction, education, IT, manufacturing |
| **Common Countries / Regions** | Usa, UK, Germany, Canada |
| **Multiple combination blackmail or not** | Yes |

| | |
|---|---|
| Sample Letter of Blackmail | ~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~<br><br>>>>>> Your data is stolen and encrypted.<br>If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.<br><br>Tor Browser Links:<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br><br>Links for normal browser:<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br>http://lockbitap<br><br>>>>>> What guarantee is there that we won't cheat you?<br>We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation.<br>We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you |

# 4 Graph of typical technical and tactical behavior of historical association attack activities

There are a large number of organizations that rely on the LockBit RaaS infrastructure to carry out extortion attacks, and there are different job styles, many of which are not disclosed in more detail. It is difficult to analyze the attack entrance, penetration mode, horizontal movement, key asset stealing path and other aspects throughout the entire attack life cycle. we make a list of the common attack tactics and technologies based on the clues we have at present. And label based on ATT&CK framework.

Figure 4-1 Graph of common tactical behavior for LockBit-related blackmail attacks

The corresponding list is as follows:

Table 4-1 List of common tactical behaviors associated with blackmail attacks by LockBit 1

| ATT&CK phase | Specific behavior | Notes |
|---|---|---|
| Initial access | Puddle attack | Planting malicious code on sites frequented by victims |
| | Make use of public-facing applications | Exploit vulnerabilities to access victim systems, such as use of Citrix-related vulnerabilities |
| | Use of external remote services | Use the RDP to access the victim's network |
| | Phishing | Use phishing and spear-phishing to access the victim's network |
| | Utilization of effective accounts | Gets and abuses the credentials of an existing account as a means to gain initial access |
| Execution | Using command and script interpreters | Use batch scripts to execute malicious commands |
| | Deploy tools using third-party software | Use the Chocolatey command to deploy the package manager |
| | Utilization of system services | Use PsExec to execute commands or payloads |
| Persistence | Use automatic startup to perform booting or logging | Enable automatic execution for persistence |
| | Valid account | Using the compromised user account to maintain persistence on the target network |

| | | |
|---|---|---|
| Right to Submission | Abuse of enhanced control authority mechanism | Using the method of ucmDccwCOM to bypass UAC in UACMe |
| | Use automatic startup to perform booting or logging | Enable automatic login to support rights |
| | Modify with domain policy | Create a group policy for a landscape move, and you can force an update of the group policy |
| | Utilization of effective accounts | Use the impaired user account to withdraw rights |
| Defensive evasion | Protection of enforcement scope | Entering the correct parameters decrypts the main component or continues to decrypt and decompress the data |
| | To weaken the defense mechanism | Use tools such as PCHunter, PowerTool, and Process Hacker to disable and uninstall processes and services related to security software |
| | Remove beacons | Clears the Windows event log file and the ransomware deletes itself |
| | Confusion of documents or information | The encrypted data will be sent to its command and control (C2) |
| Credential Access | Brute force | Implement initial access with VPN or RDP brute force crack |
| | Obtain credentials from the location where the password is stored | Use PasswordFox to get the password for the Firefox browser |
| | Operating system credential dump | Use ExtPassword or LostMyPassword to get the operating system login credentials |
| Findings | Scan web services | Scan target networks using SoftPerfect |
| | Discovery of system information | Enumerates system information, including host name, host configuration, domain information, local drive configuration, remote shared and installed external storage devices |
| | Discover the geographical location of the system | Computers whose language settings match the defined exclusion list will not be infected |
| Lateral movement | Use remote services | Move across the network and access domain controllers |
| Collection | To compress / encrypt the collected data | Use 7-zip to compress or encrypt collected data before stealing it |
| Command and control | The application layer protocol is used | Use FileZilla to access C2 communication |
| | Standard non-application layer protocols are used | Build SOCKS5 or TCP tunnel from reverse connection using Ligolo |

| | | |
|---|---|---|
| | Use the protocol tunnel | Automatically execute SSH operation on Windows by using Pink |
| | Using remote access software | Use tools such as AnyDesk, Atera RMM or TeamViewer to access remote control |
| Data seeps out | Automatically seeps out data | Using the StealBit custom penetration tool to steal data from the target network |
| | Using Web Service Backpass | Use an open file sharing service to steal the target's data |
| Impact | Damage data | Delete log files and empty the Recycle Bin |
| | Data encryption with adverse effects | Data on the target system is encrypted to disrupt system and network availability |
| | Tampering with the visible content | Change the host system's wallpaper and icon to LockBit 3.0 wallpaper and icon, respectively |
| | Disable system recovery | Delete the shadow copy on the disk |
| | Disable the service | To terminate specific processes and services |

# 5 Sample Analysis of LockBit for Windows 3.0 Version

As the blackmail attack supported by RaaS is a unified attack infrastructure adopted by many different organizations, each attack organization relies on its own attack capability and access resources mastered by it. Use the same set of base code versions to iterate and kill-free processing loads to attack. Therefore, RaaS + targeted blackmail analysis is a multi-element comprehensive analysis, especially the analysis of attack infrastructure, attack tactics and attack samples, respectively. Lockbit has a number of common system and platform loads. we first publish a historical analysis of its For Windows 3.0 release in this section, followed by other sample analyses.

**Table 5-1 Sample labels 5-1**

| | |
|---|---|
| **Name of the virus family** | Trojan / Win32.LockBit |
| **Md5** | 38745539b71cf201bb502437f891d799 |
| **Processor architecture** | Intel 386 or later, and compatibles |
| **File size** | 162.00 KB (165888 Bytes) |
| **File format** | Binexecute / Microsoft.EXE [: X86] |
| **Time stamp** | 2022-06-27 14: 55: 54 |
| **Digital signature** | None |

| | |
|---|---|
| **Shell type** | None |
| **Compiled Language** | C / C + + |
| **Vt First Upload Time** | 2022-07-03 16: 18: 47 |
| **Vt test result** | 64 / 72 |

Note: You can search "LockBit" in Virusview.net, the encyclopedia of computer virus classification and naming for more information about the virus family.

The execution of the LockBit 3.0 ransomware releases the .ico and .bmp files in the% PROGRAMDATA% path to use as icons for subsequent encrypted files and modified desktop wallpapers.

| Process Name | PID | Operation | Detail | Path |
|---|---|---|---|---|
| lockbit3.exe | 1920 | RegSetValue | Type: REG_SZ, Length: 20, Data: HLJkNskOq | HKCR\.HLJkNskOq\(Default) |
| lockbit3.exe | 1920 | RegSetValue | Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNskOq.ico | HKCR\HLJkNskOq\DefaultIcon\(Default) |
| lockbit3.exe | 1920 | RegSetValue | Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNskOq.bmp | HKCU\Control Panel\Desktop\WallPaper |
| lockbit3.exe | 1920 | RegQueryValue | Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNskOq.bmp | HKCU\Control Panel\Desktop\Wallpaper |
| lockbit3.exe | 1920 | RegSetValue | Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNskOq.bmp | HKCU\Control Panel\Desktop\Wallpaper |

Figure 5-1 Attaching an extension 5-1

Ransomware releases ransomware letters containing Tor addresses for ransom communication.

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

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

Tor Browser Links:
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]

Links for normal browser:
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]
http://lockbitap[redacted]

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation.
We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you
```

Figure 5-2 A ransom note 5-2

The modified desktop background is shown in the following figure.

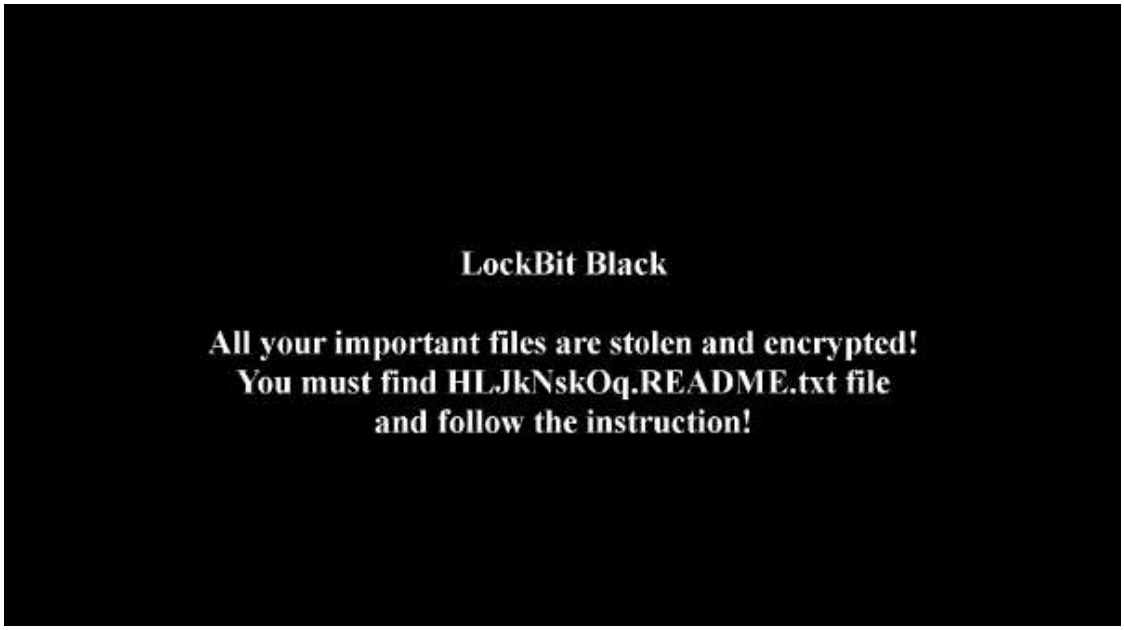



Figure 5-3 Modification of Desktop Background 5-3

The code snippets of LockBit 3.0 are encrypted and are executed with decryption based on the incoming "-pass" command line parameters. they cannot be executed without a password, thus preventing core functions from being analyzed.

```
v0 = 200000000;
do
  --v0;
while ( v0 );
cmdline = (_WORD *)getCmdline();
result = checkPass(cmdline, (int)password);   // 检查-pass参数
if ( result )
{
  sub_41B2F4(v10, password);
  v9 = sub_41B348(v10, v11, v8);
  v3 = getPEB()->Mutant;
  v4 = (char *)v3 + *((_DWORD *)v3 + 15);
  v5 = *((unsigned __int16 *)v4 + 3);
  v6 = v4 + 248;
  do
  {
    result = lockbit_Hash(v6, 0);
    if ( result == 0x76918075 || result == 0x4A41B || result == 0xB84B49B )// 段名称
      result = decrypt_section((char *)v3 + *((_DWORD *)v6 + 3), *((_DWORD *)v6 + 4), v8, v9);// 解密PE节
    v6 += 40;
    --v5;
  }
  while ( v5 );
}
return result;
```

Figure 5-4 Decrypting code snippets 5-4

The thread information was set to ThreadHideFromDebugger via the NtSetThreadInformation function to interfere with the researcher's analysis.

```
int __stdcall hideThread(int a1)
{
  int v1; // eax

  if ( a1 )
    v1 = a1;
  else
    v1 = -2;
  return NtSetInformationThread(v1, 17, 0, 0);
}
```

Figure 5-5 Code segment of interference analysis 5-5

Detect the system language, if it is a specific language, then exit the program, no longer execute.

```
NtQueryInstallUiLanguage(defaultLang);
installLang = defaultLang[0];
NtQueryDefaultUiLanguage(defaultLang);
HIBYTE(v1) = 4;
if ( installLang == 0x419 )
  goto checkFailed;
if ( defaultLang[0] == 0x419 )
  goto checkFailed;
LOBYTE(v1) = 0x22;
if ( v1 == installLang )
  goto checkFailed;
if ( v1 == defaultLang[0] )
  goto checkFailed;
LOBYTE(v1) = 0x23;
if ( v1 == installLang )
  goto checkFailed;
if ( v1 == defaultLang[0] )
  goto checkFailed;
```

Figure 5-6 Check language 5-6

The specific list of languages to be checked is as follows, and through its circumvention system, it can be seen that the Lockbit organization itself has strong characteristics of Eastern European background.

Table 5-2 List of languages to be checked 5-2

| | | |
|---|---|---|
| **System language** | Arabic (Syria) | Russian (Moldova) |
| | Armenian (Armenian) | Russian (Russia) |
| | The Azerbaijani language (Cyrillic Azerbaijan) | Tajik (Cyrillic Tajikistan) |
| | The Azerbaijani language (Latin for Azerbaijan) | Turkmen (Turkmenistan) |
| | Belarusian (Belarusian) | Tatar language (Russia) |
| | The Georgian language (Georgia) | Ukrainian (Ukrainian) |
| | Kazakh language (Kazakhstan) | The Uzbek language (Cyrillic in Uzbekistan) |

| | | |
|---|---|---|
| | Kyrgyz (Kyrgyzstan) | The Uzbek language (in Latin Uzbekistan) |
| | Romanian (Moldovan) | |
| Create multiple threads to encrypt and set the threads to hidden. | | |

```
v0 = sub_401574();
if ( (v0 & 0x20) != 0 )
  v0 = 32;
v1 = 2 * v0 + 1;
v5 = 0;
dword_427878 = createIOPort(-1, 0, 0, v1);
if ( dword_427878 )
{
  do
  {
    v2 = CreateThread(0, 0, sub_40FCAC, 0, 0, 0);
    v3 = v2;
    if ( v2 )
    {
      hideThread(v2);
      close(v3);
      ++v5;
    }
    --v1;
  }
  while ( v1 );
}
```

Figure 5-7 Create a file encryption thread 5-7

# 6 How to deal with that challenge of target blackmail to the security of GQ

In term of that damage caused by target blackmail attack, we must change the cognition paradigm of security risk and value. Targeted extortion attacks have resulted in a combination of stealing data, disabling systems and businesses, trafficking data and exposing data. The maximum risk is not only that the system and business are paralyzed and cannot be recovered, but also that the core assets of the attacked enterprise such as user information, key data, documents, materials and codes are sold off and exposed to the public. And then there's a bigger ripple effect. Judging from the long-term realities at home and abroad, the motivation of a large proportion of government and enterprise institutions to improve their own safety does not come from the initiative to raise the level of protection, including the most likely safety risks that many enterprises and public institutions believe to occur. Not an attack, but a penalty for failing to meet compliance standards. Therefore, it constitutes a set of input - compliance - exemption low limit construction operation logic. The consequences of targeted blackmail make IT decision-makers have to judge the extreme risks, and judge the value of network security through the loss of extreme risks. How to avoid such

extreme situations as long-term business interruption, complete unrecoverable data, stolen data assets being purchased by competitors, or serious depreciation due to exposure are all risks that IT decision-makers have to deal with in every institution. Objective enemy situation is the premise of network security defense. And bottom-line thinking based on the consequences of deduction, is also part of the idea. In terms of budget input, we usually take the proportion of network security in informatization as a measure and measure, which makes network security in a state of subordination, support and suppression for a long time. Whether the consequences of network security risks should be the first measure and measure of security input also needs us to think about.

In terms of the operation mode of targeted blackmail attack, we must change our understanding that it is a highly customized operation process similar to the APT attack before the crypto-destruct action is triggered. The attacker or professional attack operation team has a firm will to attack, a high attack capability, sufficient available vulnerability resources, and a large amount of available vulnerability intelligence and attack entry resources. It could have been an inside attacker. This is the reason why RaaS-based targeted extortion attacks are often successful in the face of large organizations with strong IT operation capability and defense input. The protection of the host system, which acts as the last line of defense in blackmail protection, and the backup recovery as the last response, is a single point. In that proces of responding to high-level directional attack, they play a local role of detecting and blocking attacks within the scope of their own capability, reduce the success rate of attacks, increasing the cost of attacks and reducing the risk loss, But they can't fight systematic attacks with a single point. We must seriously point out that the targeted blackmail attack is simply equivalent to the threat of the early non-targeted spread or widespread release of the ransomware, and the ransomware response is simply regarded as the single-point confrontation of the encrypted collapse VS backup recovery. Is extremely backward, one-sided safety cognition. If there is not a complete set of protection system and operation mechanism, it is believed that data backup recovery is relied on to deal with blackmail attacks. It's like playing one goalkeeper against an opposing team.

Judging from the characteristics of the killing chain of targeted blackmail attacks, we should firmly believe that there are systematic methods to prevent targeted extortion attacks. For systematic attacks, it is necessary to move forward the gateway, forward deployment, form a deep, closed-loop operation. Increases the ability of an attacker to detect fire and advance to outlying areas, and intercept at the front. Reducing the likelihood that the attacker will enter the core. Improving the manageability of networks and assets is the basis of the work: Actively shaping and reinforcing the security environment, strengthening the constraint and management of exposed and attack-capable management, and strengthening the control of upstream entry of the supply chain. Initiate a comprehensive log audit

analysis and monitoring operation. Build the defense depth from the topology to the system side, and build layers of defense against attacker detection, launch, exploit vulnerabilities, code operation, persistence, horizontal movement and other behaviors. In particular, the Bank should build the host system side protection as the last line of defense and the cornerstone of defense, and build the fine-grained governance capacity with the identification of management and control around the executor. Finally, through the protection system to achieve the perception, interference, blocking and display of the targeted attack party killing chain of the actual combat operation results.

# Appendix I: Part of the work of Antiy to assist authorities, customers and the public in responding to ransomware attacks

Antiy has always been committed to improving the effective protection capability of customers and working with customers to improve their understanding and awareness of safety.

Antel has been tracking the evolution of blackmail attacks for a long time, and has continuously released threat research and judgment reports, and intercepted and analyzed the earliest domestic ransomware redplus (Trojan.Win32.Pluder.A) on June 14, 2006. Later, it released "Uncovering the Real Face of Ransomware" (2015) and "Antiy's in-depth analysis report on the ransom worm WannaCry" [3]. Important reports such as the Linkage Analysis of the Ransomware Sodinokibi Operation Organization [4] and the Sample and Follow-up Analysis of the Ransomware Attack on Fuel Pipeline Operators in the United States [5]. Especially five months before the large-scale outbreak of the WannaCry blackmail worm, it was predicted that the blackmail attack would bring back the worm tide [6]. In that response of the WannaCry blackmail worm, on the one hand, Antiy quickly follow up the analysis, At the same time, the protection manual [7] and boot guide [8] are provided for users, and immunization tools, special killing tools, memory key acquisition and recovery tools are also provided. Petya (PETYA) in the form of extortion in a paralyzing attack, the first time also made the accurate judgment that it may not be a blackmail attack. Antiy CERT keeps track of various ransomware families and RaaS attack organizations, and issues sample analysis reports and protection recommendations against popular ransomware families such as LockBit [9], GandCrab [10] and Sodinokibi. In particular, a series of articles [11] [12] [13] [14] [15] [16] was launched based on the vertical response platform to help government and enterprise customers and the public understand blackmail attacks. Enhance the awareness of prevention. In 2021, in order to strengthen the prevention and response to ransomware attacks, under the guidance of the Cybersecurity Administration of the Ministry of Industry and Information Technology, China

Information Technology Institute, together with Antiy and other units, prepared and released the Ransomware Security Protection Manual [17]. The manual provides detailed inventory recommendations on how to protect against blackmail attacks.[2][3][4][5][6][7][8][9][10][11][12][13][14][15][16][17]

Based on the AVL SDK anti-virus engine independently developed by Antiy, the anti-virus engine supports the malware detection capability of its own products and engine eco-partners, and accurately detects and eliminates various malicious code tools including ransomware. Based on the basic concept of governance of the Antiy executive, Antiy IEP cloud protection system assist customers in shaping a reliable and secure host environment. At the end-side of Anthem, a combined security mechanism consisting of system reinforcement, host firewall (HIPS), scanning and filtering, execution management and control, behavior protection and key data protection has been established, and the protection against extortion attacks has multiple layers. In particular, the key data protection mechanism, based on the interception of reading and writing of batch files, attempts to realize behavior interception and stop loss when other security mechanisms are bypassed and ineffective. Of course, we never believe there is a silver bullet in cyber security. We are committed to maximizing the value of our engines and each product in its operational position, subject to the test of combat. For relevant information, please refer to "*Antiy Products Helping Users to Effectively Protect against Racketeering Attacks*" [18].[18]

## Appendix II: Reference

[1] Ransomware attack on China's biggest bank may have hit US Treasury market [R/OL]. (2023-11-10), https://www.cnn.com/2023/11/10/investing/icbc-ransomware-attack-hnk-intl/index.html.

[2] Antiy.uncovering the Real Face of Ransomware [R/OL]. (2015-08-03), https://www.antiy.com/response/ransomware.html.

[3] Antiy.Antiy's in-depth analysis report on the blackmail worm WannaCry [R / OL]. (2017-05-13), https://www.antiy.com/response/wannacry.html.

[4] Antiy.association analysis of the ransomware Sodinokibi operation group [R / OL]. (2019-06-28), https://www.antiy.com/response/20190628.html.

[5] Antiy.samples and Follow-up Analysis of US Fuel Pipeline Tanker Attack [R / OL]. (2021-05-11), https://www.antiy.com/response/20210511.html.

[6] Antiy.2016 Review and Outlook of Cybersecurity Threats [R/OL]. (2017-01-06), https://www.antiy.com/response/2016_Antiy_Annual_Security_Report.html.

[7] Antiy.Antiy.annacry protection manual for ransomware "WannaCry" [R/OL]. (2017-05-13), https://www.antiy.com/response/Antiy_WannaCry_Protection_Manual/Antiy_WannaCry_Protection_Manual.html.

[8] Antiy.Antiy.an Guide to Launching "WannaCry" on Mondays [R/OL]. (2017-05-14), https://www.antiy.com/response/Antiy_WannaCry_Guide.html.

[9] Antiy.Antiy.Antiy.effective protection of LockBit2.0 ransomware [R/OL]. (2021-09-20), https://www.antiy.cn/observe_download/observe_296.pdf.

[10] Antiy.gandcrab ransomware focuses on "dyskinein," and Anticon delivers effective protection [R/OL]. (2018-02-28), https://www.antiy.com/response/20180228.html.

[11] Antiy.four roles of division for ransomware attacks [R/OL]. (2021-11-23), https://mp.weixin.qq.com/s/oMneQmmYQF5B4nWVulJl1g.

[12] Antiy.two typical modes of blackmail attacks [R/OL]. (2021-11-23), https://mp.weixin.qq.com/s/nrbVpjA2-jfTzjojbyFpJA.

[13] Antiy. "Ransom Attack Kill Chain" Analysis [R/OL]. (2021-11-24), https://mp.weixin.qq.com/s/24bIz-e4_Ts-Th0ecCWfgQ.

[14] Antiy.four types of blackmail with five attack features [R/OL]. (2021-11-25), https://mp.weixin.qq.com/s/ RL4E9v4wvazgj2UNdbMypA.

[15] Antiy.ten Typical Ransom Families [R/OL]. (2021-11-26), https://mp.weixin.qq.com/s/Jmz58xQBcytCIWx51yxBTQ.

[16] Antiy.ransom Attack Trends [R/OL]. (2021-11-26), https://mp.weixin.qq.com/s/1wehEDr7dTo-wdJYzFoS-A.

[17] China Information and Communication Court.Ransomware Security Protection Manual [R/OL]. (2021-09), http://www.caict.ac.cn/kxyj/qwfb/ztbg/202109/P020210908503958931090.pdf.

[18] Antiy.Antiy products help users effectively protect against blackmail attacks [R/OL]. (2021-11-01). Https://mp.weixin.qq.com/s/nOfhqWiw6Xd7-mvMt2zfXQ.

# Appendix III: 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.