

Akira Ransomware

Viktor Sahin-Uppströmer, Polismyndigheten

Heresh Zaremand, Truesec

```
akira_readme x +
File Edit View
Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidentally corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76ldk3u2kollpj5z3z636bad.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsxmryd4csgfameg52n7efvr2id.onion.
3. Use this code - [REDACTED] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

Ln 19, Col 78 100% Windows (CRLF) UTF-8
```

Akira

Ransomware-as-a-Service

- Truesec CSIRT has investigated >10 cases in the past 12 months
- About 350 Victims published on leaksite
- Affiliates and/or Akira using the RaaS
- The Akira service has ties to Conti, which had ties to Russia.

```
AKIRA

Well, you are here. It means that you're suffering
as an unscheduled forced audit of your network
at a fair price to make it all go away.

Do not rush to assess what is happening - we did
our instructions to get back to your daily routine
to get that might be done.

Those who choose different path will be shamed here.
The process is extremely simple - enter the desired command in the
instructions. The operations around the world wanted to stay confidential.

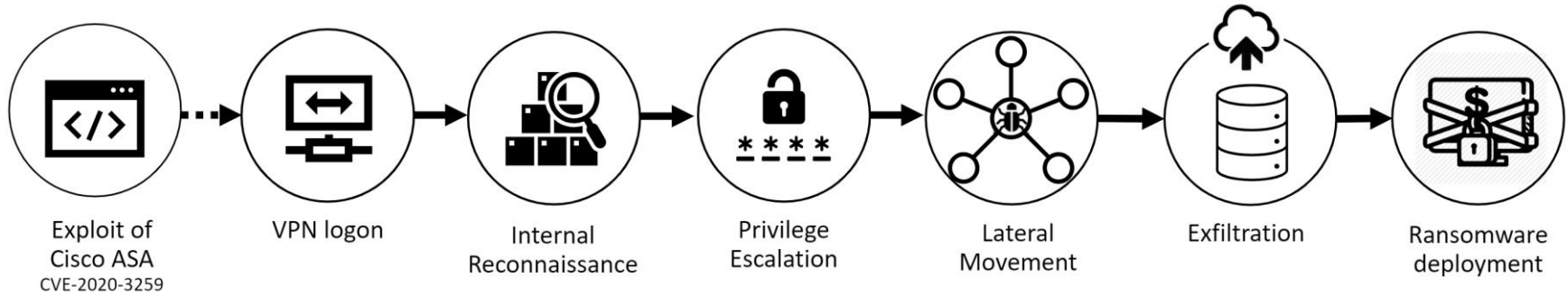
Remember. You are unable to recover without our help.
Your data is not to the place of final storage nor deleted by anyone.

guest@akira:~$ help

List of all commands:

leaks      - hacked companies
news      - news about upcoming data releases
contact    - send us a message and we will contact you
help      - available commands
clear     - clear screen

guest@akira:~$ █
```



Initial Access
Cisco VPN

- ~8 different compromised accounts
- Unique Usernames & Passwords
- No signs of Brute-force attacks
- Nothing on for sale on darknet marketplaces

**How did they obtain the VPN
credentials?**

| CVE-ID | |
|--|---|
| CVE-2020-3259 | Learn more at National Vulnerability Database (NVD) <ul style="list-style-type: none">• CVSS Severity Rating• Fix Information• Vulnerable Software Versions• SCAP Mappings• CPE Information |
| Description | |
| <p>A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve memory contents on an affected device, which could lead to the disclosure of confidential information. The vulnerability is due to a buffer tracking issue when the software parses invalid URLs that are requested from the web services interface. An attacker could exploit this vulnerability by sending a crafted GET request to the web services interface. A successful exploit could allow the attacker to retrieve memory contents which could lead to the disclosure of confidential information. Note: This vulnerability affects only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.</p> | |

There is no known public exploit to CVE-2020-2359!

| Date and Time | Event | Source IP | Username |
|---------------------|---------------------------------|------------------|---------------|
| [REDACTED] 06:13:15 | User successfully authenticated | 81.25 [REDACTED] | [REDACTED] on |
| [REDACTED] 06:42:45 | User successfully authenticated | 91.24 [REDACTED] | [REDACTED] on |
| [REDACTED] 12:53:02 | User successfully authenticated | 178.1 [REDACTED] | [REDACTED] en |
| [REDACTED] 13:24:40 | User successfully authenticated | 88.21 [REDACTED] | [REDACTED] en |
| [REDACTED] 06:42:16 | User successfully authenticated | 90.14 [REDACTED] | [REDACTED] an |
| [REDACTED] 07:14:25 | User successfully authenticated | 154.1 [REDACTED] | [REDACTED] an |

Insight 2024-01-29

An analysis of Cisco Anyconnect vulnerability CVE-2020-3259 as the initial access vector used by the Akira ransomware group

Akira Ransomware and exploitation of Cisco Anyconnect vulnerability CVE-2020-3259

An analysis of Cisco Anyconnect vulnerability CVE-2020-3259 as the initial access vector used by the Akira ransomware group

- No known public exploit to CVE-2020-2359
- Memory dump analysis
- The appliance stores logged in user's credentials in plain-text!

<https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259>

Network Enumeration

Event 4624, Microsoft Windows security auditing.

General Details

Account Domain:
Logon ID: 0x0

Logon Information:
Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
Security ID: S-1-5-[REDACTED]
Account Name: [REDACTED]
Account Domain: [REDACTED]
Logon ID: [REDACTED]
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: (00000000-0000-0000-0000-000000000000)

Process Information:
Process ID: 0x0
Process Name: -

Network Information:
Workstation Name: kali
Source Network Address: 172.2[REDACTED] VPN IP Range
Source Port: 0

Log Name: Security
Source: Microsoft Windows security Logged: [REDACTED] 2024 [REDACTED]
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: [REDACTED]
OpCode: Info
More Information: [Event Log Online Help](#)

Lateral Movement

RDP

PowerShell

Persistence AnyDesk

The screenshot shows the AnyDesk web interface in a browser window titled "AnyDesk New Session". The address bar contains "Enter Remote Address". A prominent red banner at the top reads "Free license (non-professional use). Start trial license or buy." Below this, the "Your Address" field is redacted with a black box, followed by an information icon, a lock icon, and an "Invite" button. The navigation menu includes "News" (highlighted), "Favorites", "Recent Sessions", "Discovered", and "Invitations". The "News" section features three cards: "What's NEW in AnyDesk?" with a "Learn more" button, "Install AnyDesk" with a "Learn more" button, and "Discovery" with an "Enable now..." button. A "Help Us Improve" dialog box is open, asking for permission to collect data, with an "Allow data collection..." button. A red bar is visible at the bottom of the page.

Event 1117, Windows Defender

General Details

Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information please see the following:
<https://go.microsoft.com/fwlink/?linkid=370208&name=HackTool:Win32/Dumpl.sass.J&threatid=2147806092&enterprise=0>

Name: HackTool:Win32/Dumpl.sass.J
ID: 2147806092
Severity: Hög
Category: Verktyg
Path: CmdLine:_C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, #+000024 884 \Windows\Temp\xlCY.doc full
Detection Origin: Okänd
Detection Type: Konkret
Detection Source: System
User: NT instans\SYSTEM
Process Name: Unknown
Action: Ta bort
Action Status: No additional actions required
Error Code: 0x00000000
Error description: Åtqärden har slutförts.
Security intelligence Version: AV: 1.403.1878.0, AS: 1.403.1878.0, NIS: 1.403.1878.0
Engine Version: AM: 1.1.23110.2, NIS: 1.1.23110.2

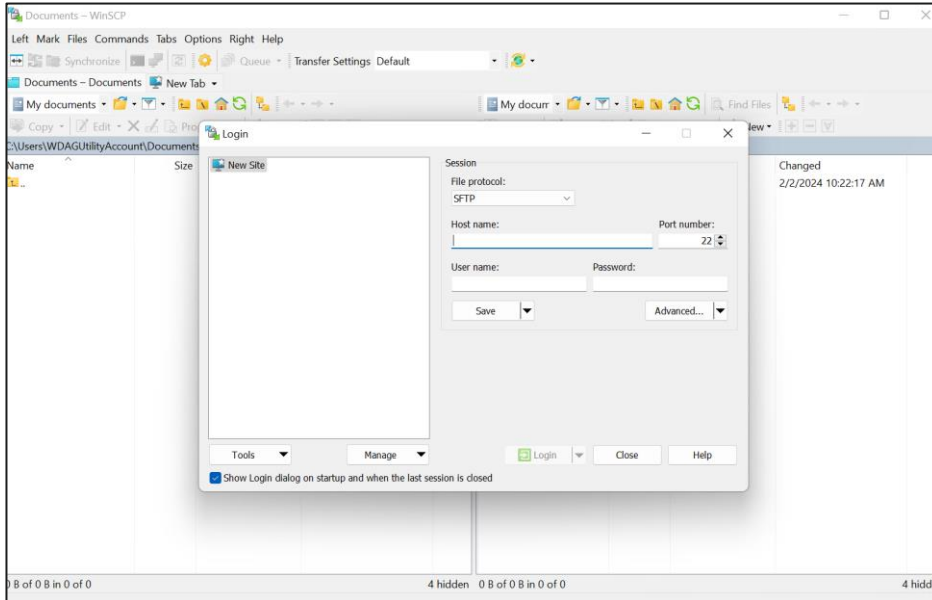
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender Logged: 2024-01-10 10:10:10
Event ID: 1117 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: [REDACTED]
OpCode: Info
More Information: [Event Log Onlines Help](#)

Privilege Escalation

Often not needed!

Other times very easy

AD Tiering is important



Data Exfiltration

WinSCP, Rclone, ...

92.51.100.100

Regular View Raw Data

// TAGS [add-tag](#) [start](#)

General Information

| | |
|--------------|-----------------------|
| Country | Russian Federation |
| City | Moscow |
| Organization | Alvia Holding Limited |
| ISP | Flyservers S.A. |
| ASN | AS20988 |

Open Ports

21 80 135 139 445 3389 5357 5985

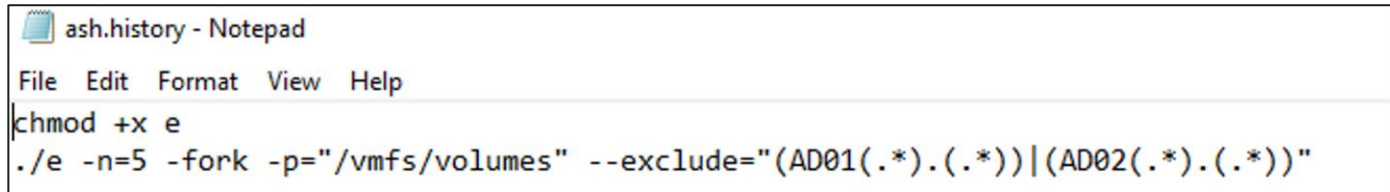
// 21 /TCP

```

220 Filezilla Server 3.8.1
221 Please visit https://filezilla-project.org/
222 Usage: USER [password]
223 The following commands are recognized:
224 HELP INFO STAT USER PASS USER HELP QUIT BYE
225 AUTH USER PASS AUTH LIST USER USER AUTH OPTS OPTS
226 PASS OPTS OPTS USER USER LIST USER USER HELP
227 USER USER PASS USER USER LIST
228 Help:
229 Features:
230 SSL
231 SSL
  
```

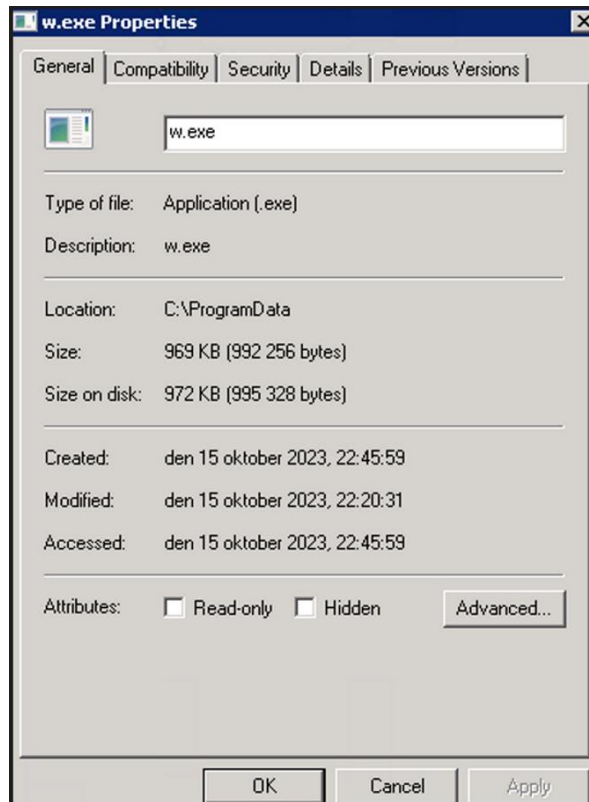
This IP is from 8base ransomware, not associated with Akira.

Ransomware Distribution Windows & ESXi



```
ash.history - Notepad
File Edit Format View Help
chmod +x e
./e -n=5 -fork -p="/vmfs/volumes" --exclude="(AD01(.*)).(.*))|(AD02(.*)).(.*))"
```

N=5 is the % of encryption for each vmdk



```
Log-18-01-2024-00-21-53
File Edit View
[2024-01-18 00:22:00.262] [file_logger] [info] Number of thread to folder parsers = 1
[2024-01-18 00:22:00.262] [file_logger] [info] Number of thread to root folder parsers = 1
[2024-01-18 00:22:00.262] [file_logger] [info] Number of threads to encrypt = 4
[2024-01-18 00:22:00.292] [file_logger] [info] Number of thread to folder parsers = 1
[2024-01-18 00:22:00.406] [file_logger] [info] Number of thread to root folder parsers = 1
[2024-01-18 00:22:00.406] [file_logger] [info] Number of threads to encrypt = 4
[2024-01-18 00:22:00.418] [file_logger] [info] This is network path: \\10.██████████\D$
[2024-01-18 00:22:00.432] [file_logger] [info] Number of thread to folder parsers = 1
[2024-01-18 00:22:00.441] [file_logger] [info] Number of thread to root folder parsers = 1
[2024-01-18 00:22:00.441] [file_logger] [info] Number of threads to encrypt = 4
[2024-01-18 00:22:00.564] [file_logger] [info] Number of thread to folder parsers = 1
directory_iterator: unknown error: "\\10.██████████\D$"
[2024-01-18 00:22:00.579] [file_logger] [info] Number of thread to root folder parsers = 1
[2024-01-18 00:22:00.579] [file_logger] [info] Number of threads to encrypt = 4
[2024-01-18 00:22:00.580] [file_logger] [info] Number of threads to encrypt = 4
[2024-01-18 00:22:00.580] [file_logger] [info] Number of threads to encrypt = 4
rsers = 1
[2024-01-18 00:22:00.581] [file_logger] [info] Number of threads to encrypt = 4
[2024-01-18 00:22:00.614] [file_logger] [info] This is network path: \\10.██████████\C$
[2024-01-18 00:22:00.623] [file_logger] [info] This is network path: \\10.██████████\D$
[2024-01-18 00:22:00.626] [file_logger] [info] This is network path: \\10.██████████\C$
[2024-01-18 00:22:00.626] [file_logger] [info] This is network path: \\10.██████████\C$
[2024-01-18 00:22:00.630] [file_logger] [error] File handle not found! (\\10.██████████\C$\Program Files\Common Files\microsoft shared\ink\Alphabet.xml)
[2024-01-18 00:22:00.634] [file_logger] [error] search files error:directory_iterator::directory_iterator: unknown error: "\\10.██████████\D$"
[2024-01-18 00:22:00.636] [file_logger] [info] 7573 ms
[2024-01-18 00:22:00.639] [file_logger] [error] search files error:directory_iterator::directory_iterator: unknown error: "\\10.██████████\D$"
[2024-01-18 00:22:00.641] [file_logger] [info] 7499 ms
[2024-01-18 00:22:00.646] [file_logger] [error] search files error:directory_iterator::directory_iterator: unknown error: "\\10.██████████\D$"
[2024-01-18 00:22:00.648] [file_logger] [info] 7634 ms
[2024-01-18 00:22:00.655] [file_logger] [error] File handle not found! (\\10.██████████\C$\Program Files\Common Files\microsoft shared\ink\ar-SA\tipresx.dll.mui)
[2024-01-18 00:22:00.659] [file_logger] [error] File handle not found! (\\10.██████████\C$\Program Files\Common Files\microsoft shared\ink\bg-BG\tipresx.dll.mui)
[2024-01-18 00:22:00.660] [file_logger] [error] File handle not found! (\\10.██████████\C$\Program Files\Common Files\microsoft shared\ink\Content.xml)
```

Extortion

```
akira_readme x +
File Edit View
Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidentally corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76ldk3u2kollpj5z3z636bad.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76ldk3u2kollpj5z3z636bad.onion.
3. Use this code - [REDACTED] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

Ln 19, Col 78 100% Windows (CRLF) UTF-8
```



AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our actions as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extremely simple - enter the desired command in the input line and enjoy the juiciest information that corporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced to the place of final storage nor deleted by anyone besides us.

```
guest@akira:~$ help
```

```
List of all commands:
```

```
leaks      - hacked companies
news       - news about upcoming data releases
contact    - send us a message and we will contact you
help       - available commands
clear      - clear screen
```

```
guest@akira:~$ █
```

| | | AKIRA |
|------------|------------|---|
| | | tracts. Accounting and financial files are also represented. |
| 2024-09-23 | [REDACTED] | [REDACTED] is a ski resort in central Sweden, known for its reliable snow conditions. Over 25Gb of data will be released soon. Client and guests data, employee information, accounting files and so on. |
| 2024-09-23 | [REDACTED] | [REDACTED] is a franchise distributor for Pepsi Cola and Dr Pepper Beverages representing the top-selling products in virtually every category of the beverage industry covering soft drinks, juices, sport drinks, water, coffee and tea. In the data we are going to upload you can find some personal information of employees including medical info. Financial and projects data is represented as well. |
| 2024-09-23 | [REDACTED] | [REDACTED] Inc., doing business as [REDACTED], provides lodging and hospitality services. We will upload 17Gb of their files soon. You will find employee personal docs, finance information, clients data. So, there are a lot of interesting files inside: credit cards, DLs, payment docs... |
| 2024-09-25 | [REDACTED] | [REDACTED] Group an Authorized Telus Dealer has been providing wireless products and services to the Canadian business market on a regional and national basis since 1997. We are going to disclose the files we obtained from this company. You will find credit cards, employee information, agreements and some other interesting information. |
| 2024-09-25 | [REDACTED] | [REDACTED] is an insurance company offering the in customers home, auto, and commercial insurance. 48Gb of data is to be released soon. Lots of confidential files, personal employee and clients information, detailed financial information, forms with personal information. |
| 2024-09-25 | [REDACTED] | [REDACTED] Services LLC is a company that operates in the Architecture, Engineering & Design industry. 23Gb of data will be uploaded soon. There are files of 2 more companies inside the archive. We got detailed personal employee information SSNs, addresses, phones etc. Numerous financial files, agreements and other business files will be available soon as well. |
| 2024-10-01 | [REDACTED] | [REDACTED] is a civil engineering company providing building, engineering, and construction management services. 15Gb of data to be released soon. Lots of passports, DLs, birth certs and other employee docs. You will also find NDAs, client's information, projects and so on. |
| 2024-10-01 | [REDACTED] | [REDACTED] is a customer-focused, market driven company manufacturing quality products safely and efficiently. We got about 15Gb of data. We will release it soon. Confidential files, agreements, employee files with personal data, lists with SSNs and many other interesting files. |
| 2024-10-01 | [REDACTED] | [REDACTED] Co is a chemicals company based out in the United States. We are going to release the data soon. Accounting and financial data, detailed employees data, projects, contracts, customer files. |

guest@akira:~\$

```

https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion
[ AKIRA ]
help      - available commands
clear     - clear screen

guest@akira:~$ leaks

+-----+-----+-----+-----+
| name   | desc                                     | progress | link   |
+-----+-----+-----+-----+
| ██████ | Founded in 1995 and headquartered in Poole, United Kingdom, ██████ is a cosmetic store specializing in the retail of bath bombs, hair products, makeup and more. 110 Gb of their files are available for downloading. There are a lot of personal documents especially passports. Accounting, finance, tax, projects, clients information and much more could be found in the archives. | [=====>] 100% | download |
|       | We have made the process of downloading company data as simple as possible for our users. All you need is any torrent client (like Vuze, Utorrent, qBittorrent or Transmission) to use magnet links). You will find the torrent file above. |
|       | 1. Open uTorrent, or any another torrent client. |
|       | 2. Add torrent file or paste the magnet URL to upload the data safely. |
|       | 3. Archives have no password. |
|       | MAGNET URL: magnet:?xt=urn:btih:FB014A27E7FC54912511F4CAFDF69897E3D11FA5&dn=lush&tr=udp://tracker.openbittorrent.com:80/announce&tr=udp://tracker.opentracker.org:1337/announce&tr=wss://wstracker.online |
|       | ██████ The ██████ is a Canadian zoo and involved in saving |
|       | [=====>] 100% | download |

```


From Akira <akira1991415@gmail.com>

To

[REDACTED]

Subject [REDACTED] POSTED in Akira blog

Send Date (UTC)

[REDACTED]

[Download Original Item](#)

You can find yourself in our news column: <https://akira12iz6a7qgd3ayp316yub7xx2uep76idk3u2kollpj5z3z636bad.onion/> If you want this post to be removed, we have to agree at something.



What we've learnt

As you know, we were able to fully compromise LockBit's platform in February 2024. As shared at the time, we obtained 2,500 decryption keys, all LockBit affiliate usernames, BTC addresses linked to victim payments and the payments to LockBitSupp, all the chat negotiations (which helped us show which affiliates were working together), all the attack build details and which affiliate attacked which victim, the platform source code, LockBit's new malware in development, and much, much more.

As part of our ongoing investigation we can tell you that we benefited from a great deal of information that will continue to fuel our collaborative work. We have a full understanding of the platform and how it operated, and all this detail is presently being worked through with our international Cronos colleagues to help us identify and pursue criminals all over the world. As you can see, we have already identified some, but this is just a start.

LockBit let you down. Affiliates, developers, and money launderers, we look forward to catching up with you very soon...

Here are some additional details we can share about the platform and its processes...

Kind regards
The National Crime Agency



Did LockBit really delete your data?



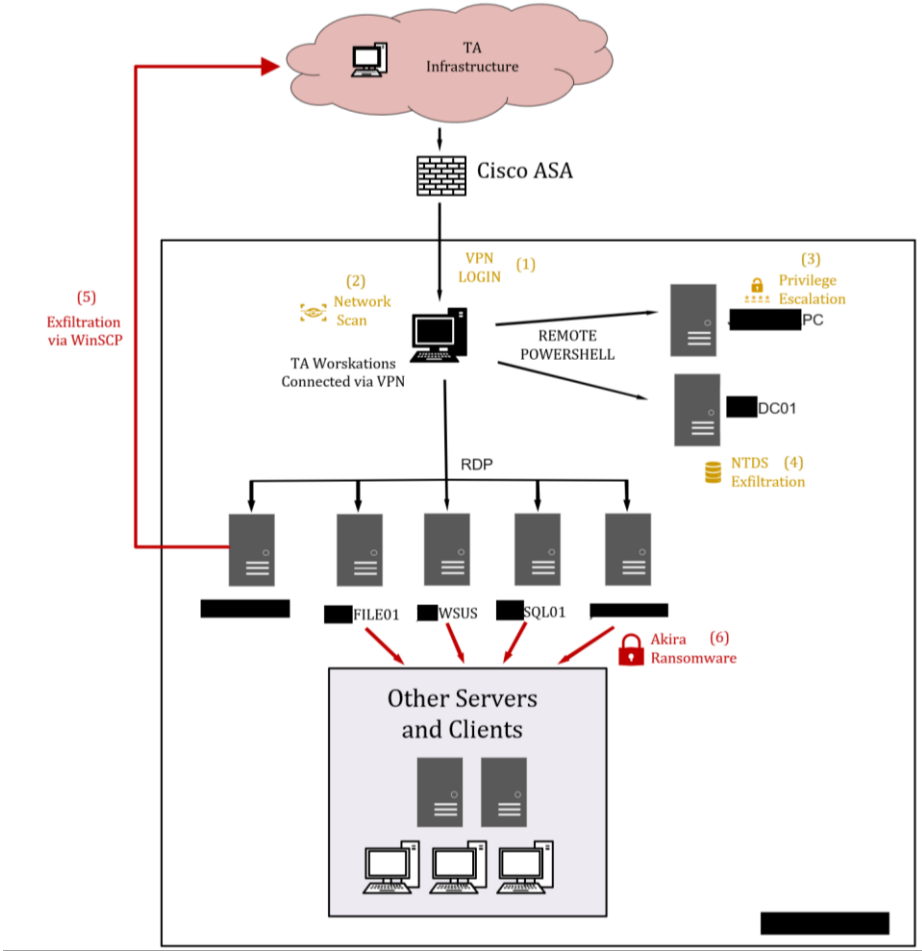
LockBit was specifically designed **not** to automatically delete your data!

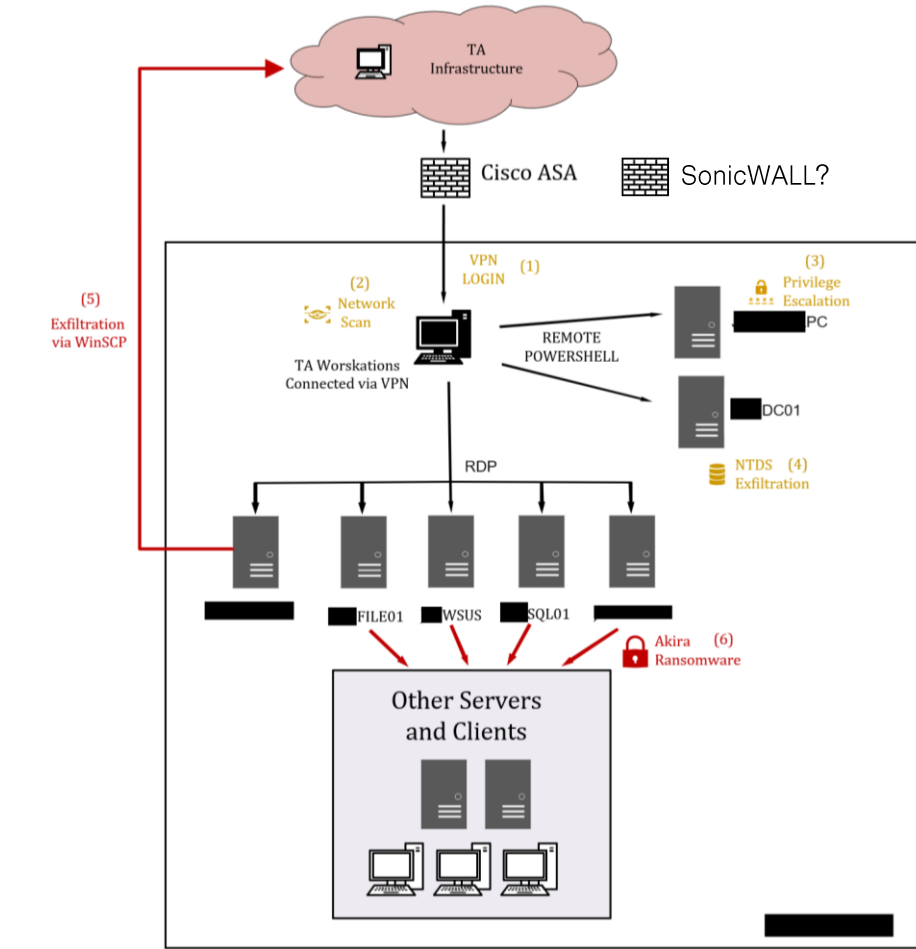
We can reveal after an examination of the code, that **after** a victim paid to have their leak site post removed, and their data deleted (as promised), the data was archived and backed up and only deleted at LockBit's whim unbeknownst to the affiliate...

And LockBit didn't delete any of their data after 2022.

EXAMPLE:

Recent Akira Ransomware Case





Thank You!



www.truesec.com



x.com/truesec



linkedin.com/company/truesec