Malware Spotlight: **Akira Ransomware**

November 2024

Executive Summary

Since April 2023, Arete's Incident Response (IR) team has responded to more than one hundred incidents attributed to the Akira ransomware group. Akira is a prolific threat and quickly established itself as one of the most active ransomware groups alongside ALPHV/BlackCat and LockBit in 2023. In 2024, Akira benefited from law enforcement actions that disrupted LockBit and ALPHV/BlackCat's operations and has continued to be one of the most active threat actor groups.

This spotlight explores the ransomware group's observed behavior, background information on the threat actor, and statistics from Incident Response engagements, along with a technical analysis of Akira's ransomware executable. Finally, we discuss security recommendations to better defend against this evolving cyber threat and mitigate the risk of financial and reputational losses.

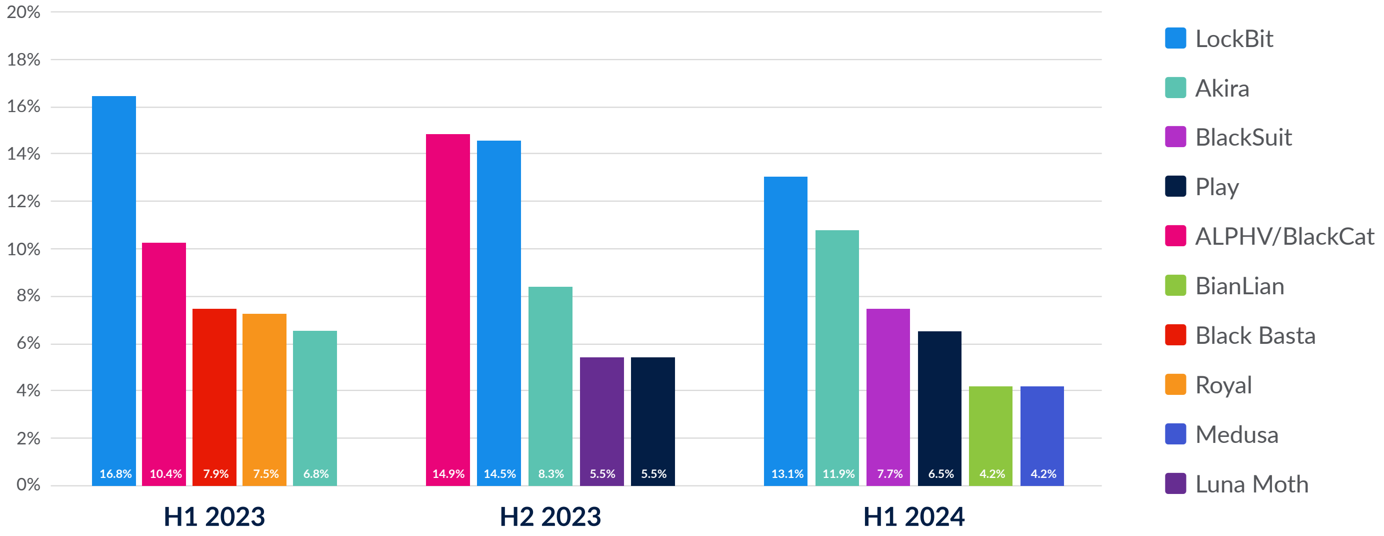
Incident Response Data on the Akira Ransomware Group

The information below is based on engagements involving Akira ransomware investigated by Arete since April 2023. Our IR, Threat Intelligence, and Data Analytics teams work together to analyze key data points during every ransomware engagement and form real-time threat actor (TA) insights.

- Targeted sectors include healthcare, hospitality, manufacturing, public and financial services, and professional services.
- The median initial demand is $500,000.
- The median ransom payment facilitated is $150,000.
- Tools observed during investigations include SystemBC, Cobalt Strike, Rclone, Filezilla, WinSCP, AnyDesk, PuTTY, SoftPerfect Network Scanner (netscan), Advanced IP Scanner, and Angry IP Scanner.
- Over the last six months, 43% of engagements involved data exfiltration.
- Depending on the variant, Akira encrypts and appends an ".akira", ".powerranges", or ".akiranew" extension to encrypted files.
- The ransom note file name is commonly "akira_readme.txt" or "powerranges.txt" and includes a password-protected Tor site for negotiations and communication with victims.
- The group operates a data leak site (DLS) self-proclaimed as "AKIRA" and commonly threatens victims with releasing stolen data as a pressure tactic if a payment is not made.
- Akira will delete Windows Shadow Volume Copies using Powershell and utilize Windows' Restart Manager to exit processes and services that could potentially prevent encryption.

Background

Akira has evolved into a notable ransomware operation and was among the top variants observed by Arete in the first half of 2024.



Source: Arete's H1 2024 Crimeware Report

Akira targets a broad range of organizations throughout North America, including Canada, and swiftly lists victims on its data leak site. Targeted sectors include healthcare, hospitality, manufacturing, public and financial services, and professional services. The group maintains Windows and Linux versions of its ransomware and uses virtual private network (VPN) appliances as an initial access vector in 50% of attacks.

Megazord, a variant of Akira, demonstrates the evolution of the group's ransomware. Introduced around August 2023, this variant is unique due to its Rust-based code, which is a departure from the C++ code of the original Akira ransomware. The Megazord variant also includes different command line arguments and encrypts files with a ".powerranges" extension, which are differentiating attributes.

Technical Analysis

Malware analysis of one of the Windows-based variants revealed that Akira ransomware:

- Supports multiple command-line arguments.
- Encrypts files on the system and mounted shares.
- Adds the following extension to encrypted files (variant dependent): .akira (e.g., file.docx.akira).
- Creates a ransom note with the following filename (variant dependent): akira_readme.txt.
- References a data leak site in the ransom note that, when accessed, self-identifies the group as AKIRA.
- Kills a list of processes and services.
- Maintains a list of whitelisted files and directories to ensure it will not render the system unusable, preventing recovery when running a decryptor.
- Attempts to prevent system recovery by deleting the system's volume shadow copies.
- Creates a log file with a name based on the date and time: Log-%d-%m-%Y-%H-%M-%S (e.g., Log-19-09-2024-09-21-20.txt).

Execution Pattern/Arguments

Akira ransomware does not need a command line argument to execute and encrypt files in the system. However, Akira supports the following command line arguments:

Command line argument	Description
-p / --encryption_path	Specify a target directory to encrypt. If not provided, the payload will encrypt the local and mounted shared drives by default.
-s / --share_file	Encrypt shared volumes/directory files.
-n / --encryption_percent	Number that represents the percentage of the file that will be encrypted.
-localonly	Encrypt only local volumes.
-e/ --exclude	Meant to exclude directories but does not seem to be fully functional.

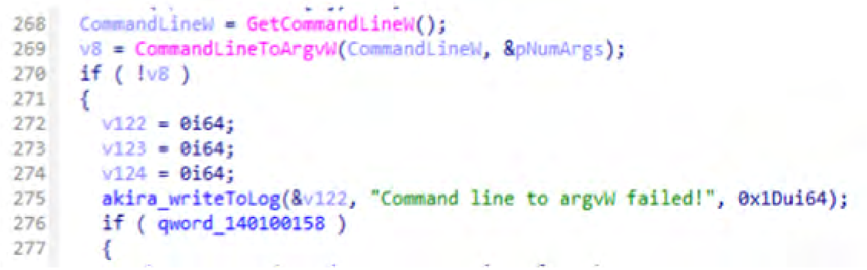
Megazord variant:

Command line argument	Description
--path	Path to encrypt. If not provided, the payload will encrypt the local and mounted shared drives by default.
--id	Unique token to execute the ransomware.
--threads	Number of threads (1-1000).
--h (-help)	Displays help options.
-log	Logging options with multiple logs supported (info, error, debug). Not displayed by default.

Examples of how the supported arguments are used:

Akira.exe -p=C:\Users\%USERNAME%\Desktop\MyFiles

Akira.exe --encryption_percent=10



```
CommandLineW = GetCommandLineW();
v8 = CommandLineToArgvW(CommandLineW, &pNumArgs);
if ( !v8 )
{
  v122 = 0i64;
  v123 = 0i64;
  v124 = 0i64;
  akira_writeToLog(&v122, "Command line to argvW failed!", 0x1Dui64);
  if ( qword_140100158 )
  {
```

Figure 1. Code in the ransomware written to read command line arguments

Stop Services and Processes

Before file encryption, the ransomware terminates a pre-determined list of processes and services to encrypt as many files as possible. Akira ransomware contains a list of processes it will exclude during process termination, listed below:

Process names:

explorer.exe, sihost.exe, spoolsv.exe, dwm.exe, LogonUI.exe, fontdrvhost.exe, cmd.exe, csrss.exe, smss.exe, SearchUI.exe, lsass.exe, conhost.exe, System, winlogon.exe, services.exe, wininit.exe, Registry, Memory Compression, System Idle Process, Secure System

File and Directory Exclusions

The ransomware excludes system-related files and folders, ransomware-related files, and whitelisted extensions during encryption.

Excluded file extensions:

.exe, .dll, .sys, .msi, .lnk, .akira, akira_readme.txt

Excluded directories:

tmp, temp, winnt, $Recycle.Bin, thumb, System Volume Information, $RECYCLE.BIN, Windows, ProgramData, Trend Micro, ProgramData, Boot

Inhibit System Recovery

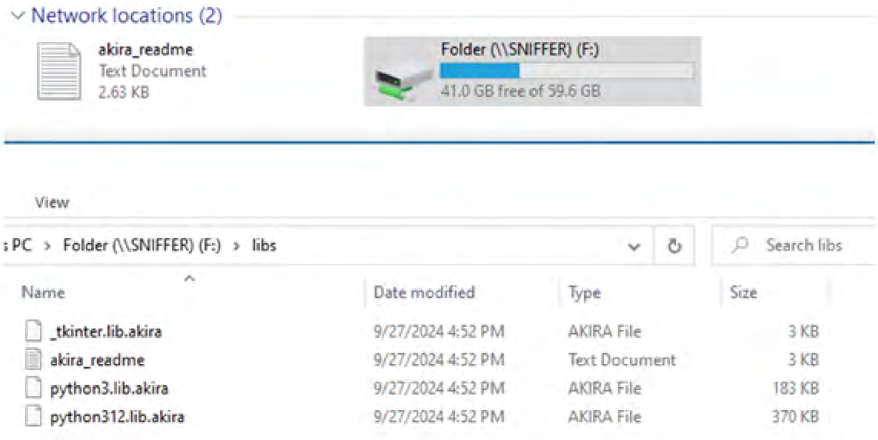
Windows operating systems contain features that can help fix corrupted system files, including shadow copies, which are backups of files created by the Volume Shadow Copy Service (VSS). By deleting shadow copies, the ransomware can prevent victims from restoring files from backups, making it more difficult for them to recover their data without paying the ransom.

The ransomware deletes volume shadow copies before file encryption by starting the following Powershell process and executing the command:

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

Network Share Discovery

Akira ransomware can enumerate network-mounted shares by scanning the network interfaces. If any are found, it will attempt to encrypt them, as shown below.



akira_readme
Text Document
2.63 KB

Folder (\\SNIFFER) (F:)
41.0 GB free of 59.6 GB

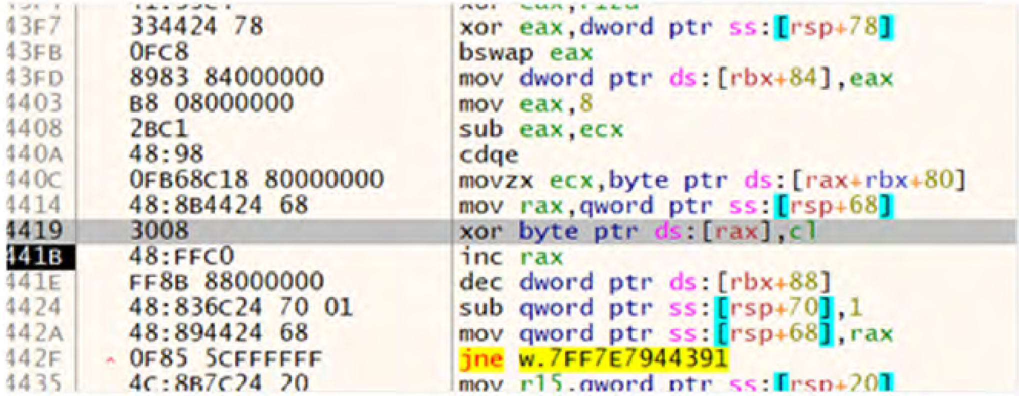
PC > Folder (\\SNIFFER) (F:) > libs

Name	Date modified	Type	Size
_tkinter.lib.akira	9/27/2024 4:52 PM	AKIRA File	3 KB
akira_readme	9/27/2024 4:52 PM	Text Document	3 KB
python3.lib.akira	9/27/2024 4:52 PM	AKIRA File	183 KB
python312.lib.akira	9/27/2024 4:52 PM	AKIRA File	370 KB

Figure 2. Share drive encrypted

Data Encrypted for Impact

The ransomware initially finds available drives and then loads the files one by one using the Windows API FindFirstFileW and FindNextFileW. The ransomware generates random AES keys to encrypt the files, and after encrypting them, the keys are encrypted using a public RSA key. The resulting key is again encrypted and placed at the end of the file.



```
43F7    334424 78               xor eax,dword ptr ss:[rsp+78]
43FB    0FC8                    bswap eax
43FD    8983 84000000           mov dword ptr ds:[rbx+84],eax
4403    B8 08000000             mov eax,8
4408    2BC1                    sub eax,ecx
440A    48:98                   cdqe
440C    0FB68C18 80000000       movzx ecx,byte ptr ds:[rax+rbx+80]
4414    48:8B4424 68            mov rax,qword ptr ss:[rsp+68]
4419    3008                    xor byte ptr ds:[rax],cl
441B    48:FFC0                 inc rax
441E    FF8B 88000000           dec dword ptr ds:[rbx+88]
4424    48:836C24 70 01         sub qword ptr ss:[rsp+70],1
442A    48:894424 68            mov qword ptr ss:[rsp+68],rax
442F  ^ 0F85 5CFFFFFF           jne w.7FF7E7944391
4435    4C:8B7C24 20            mov r15,qword ptr ss:[rsp+20]
```

Figure 3. Data encryption code

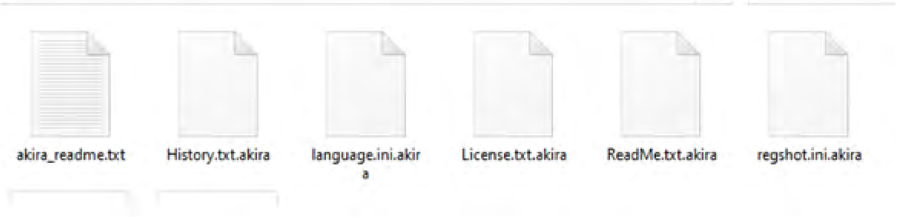
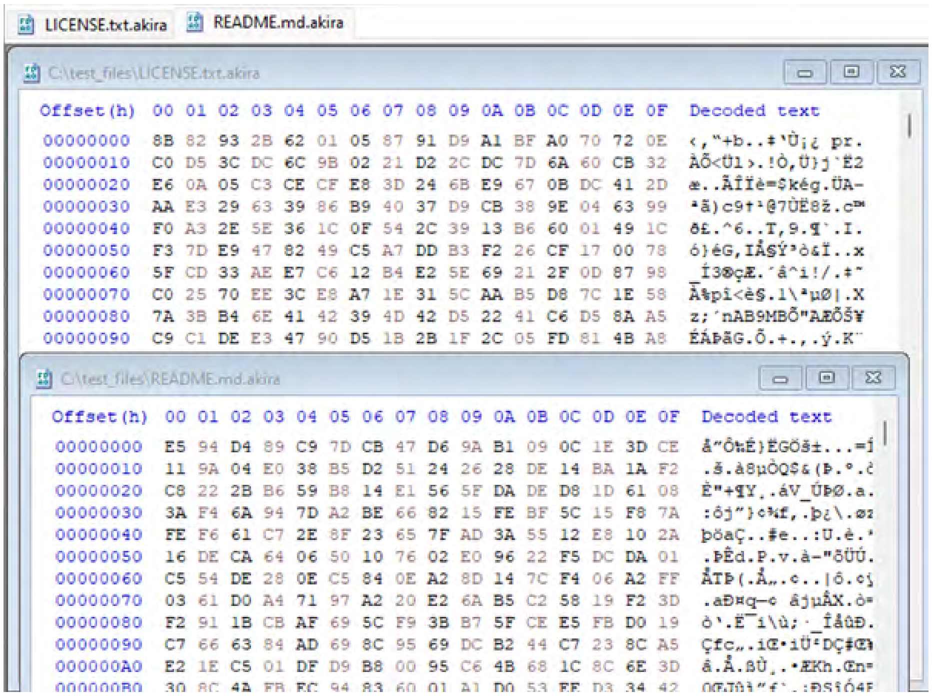


Figure 4. Extension added to the encrypted files


LICENSE.txt.akira README.md.akira

C:\test_files\LICENSE.txt.akira

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  8B 82 93 2B 62 01 05 87 91 D9 A1 BF A0 70 72 0E  ‹‚“+b..‡‘Ù¡¿ pr.
00000010  C0 D5 3C DC 6C 9B 02 21 D2 2C DC 7D 6A 60 CB 32  ÀÕ<Ül›.!Ò,Ü}j`Ë2
00000020  E6 0A 05 C3 CE CF E8 3D 24 6B E9 67 0B DC 41 2D  æ..ÃÎÏè=$kég.ÜA-
00000030  AA E3 29 63 39 86 B9 40 37 D9 CB 38 9E 04 63 99  ªã)c9†¹@7ÙË8ž.c™
00000040  F0 A3 2E 5E 36 1C 0F 54 2C 39 13 B6 60 01 49 1C  ð£.^6..T,9.¶`.I.
00000050  F3 7D E9 47 82 49 C5 A7 DD B3 F2 26 CF 17 00 78  ó}éG‚IÅ§Ý³ò&Ï..x
00000060  5F CD 33 AE E7 C6 12 B4 E2 5E 69 21 2F 0D 87 98  _Í3®çÆ.´â^i!/.‡˜
00000070  C0 25 70 EE 3C E8 A7 1E 31 5C AA B5 D8 7C 1E 58  À%pî<è§.1\ªµØ|.X
00000080  7A 3B B4 6E 41 42 39 4D 42 D5 22 41 C6 D5 8A A5  z;´nAB9MBÕ"AÆÕŠ¥
00000090  C9 C1 DE E3 47 90 D5 1B 2B 1F 2C 05 FD 81 4B A8  ÉÁÞãG.Õ.+.,.ý.K¨
```

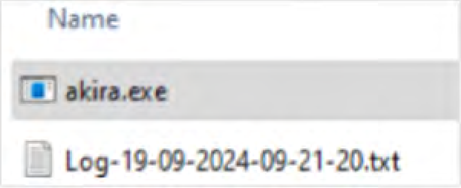
C:\test_files\README.md.akira

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  E5 94 D4 89 C9 7D CB 47 D6 9A B1 09 0C 1E 3D CE  å”Ô‰É}ËGÖš±...=Î
00000010  11 9A 04 E0 38 B5 D2 51 24 26 28 DE 14 BA 1A F2  .š.à8µÒQ$&(Þ.º.ò
00000020  C8 22 2B B6 59 B8 14 E1 56 5F DA DE D8 1D 61 08  È"+¶Y¸.áV_ÚÞØ.a.
00000030  3A F4 6A 94 7D A2 BE 66 82 15 FE BF 5C 15 F8 7A  :ôj”}¢¾f‚.þ¿\.øz
00000040  FE F6 61 C7 2E 8F 23 65 7F AD 3A 55 12 E8 10 2A  þöaÇ..#e..:U.è.*
00000050  16 DE CA 64 06 50 10 76 02 E0 96 22 F5 DC DA 01  .ÞÊd.P.v.à–"õÜÚ.
00000060  C5 54 DE 28 0E C5 84 0E A2 8D 14 7C F4 06 A2 FF  ÅTÞ(.Å„.¢..|ô.¢ÿ
00000070  03 61 D0 A4 71 97 A2 20 E2 6A B5 C2 58 19 F2 3D  .aÐ¤q—¢ âjµÂX.ò=
00000080  F2 91 1B CB AF 69 5C F9 3B B7 5F CE E5 FB D0 19  ò‘.Ë¯i\ù;·_ÎåûÐ.
00000090  C7 66 63 84 AD 69 8C 95 69 DC B2 44 C7 23 8C A5  Çfc„.iŒ•iÜ²DÇ#Œ¥
000000A0  E2 1E C5 01 DF D9 B8 00 95 C6 4B 68 1C 8C 6E 3D  â.Å.ßÙ¸.•ÆKh.Œn=
000000B0  30 8C 4A FB EC 94 83 60 01 A1 D0 53 EE D3 34 42  0ŒJûì”ƒ`.¡ÐSîÓ4B
```

Figure 5. Encrypted files

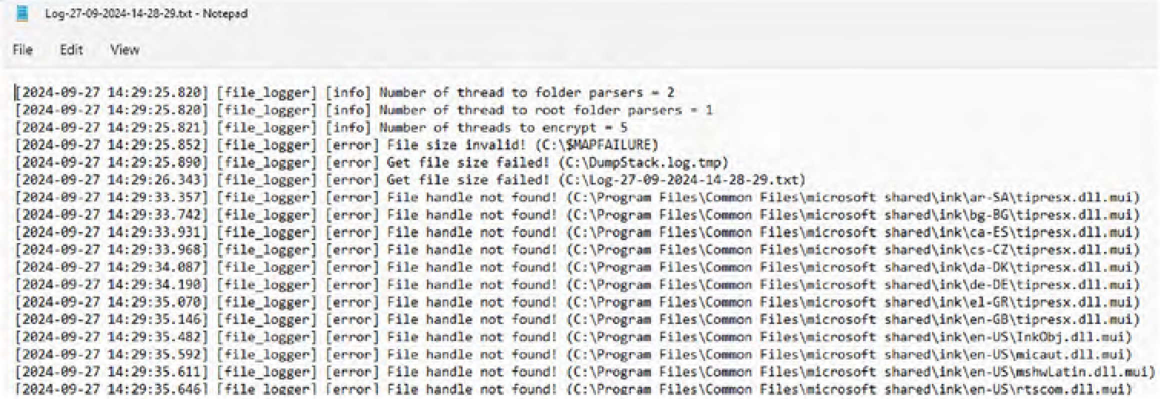
During execution, the ransomware creates a log file in the working directory where the file is executed from. The log file is named based on the date and time of execution using the following string format: Log-%d-%m-%Y-%H-%M-%S. For example, during execution, the following log file with the name was created: Log-19-09-2024-09-21-20.txt.


Name

akira.exe

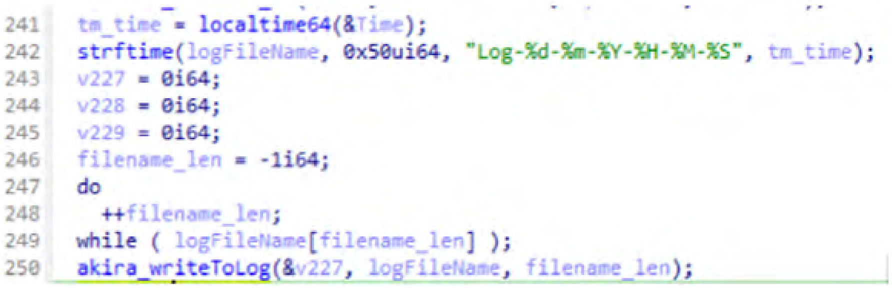
Log-19-09-2024-09-21-20.txt

Figure 6. Log file created by Akira



```
[2024-09-27 14:29:25.820] [file_logger] [info] Number of thread to folder parsers = 2
[2024-09-27 14:29:25.820] [file_logger] [info] Number of thread to root folder parsers = 1
[2024-09-27 14:29:25.821] [file_logger] [info] Number of threads to encrypt = 5
[2024-09-27 14:29:25.852] [file_logger] [error] File size invalid! (C:\$MAPFAILURE)
[2024-09-27 14:29:25.890] [file_logger] [error] Get file size failed! (C:\DumpStack.log.tmp)
[2024-09-27 14:29:26.343] [file_logger] [error] Get file size failed! (C:\Log-27-09-2024-14-28-29.txt)
[2024-09-27 14:29:33.357] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\ar-SA\tipresx.dll.mui)
[2024-09-27 14:29:33.742] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\bg-BG\tipresx.dll.mui)
[2024-09-27 14:29:33.931] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\ca-ES\tipresx.dll.mui)
[2024-09-27 14:29:33.968] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\cs-CZ\tipresx.dll.mui)
[2024-09-27 14:29:34.087] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\da-DK\tipresx.dll.mui)
[2024-09-27 14:29:34.190] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\de-DE\tipresx.dll.mui)
[2024-09-27 14:29:35.070] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\el-GR\tipresx.dll.mui)
[2024-09-27 14:29:35.146] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\en-GB\tipresx.dll.mui)
[2024-09-27 14:29:35.482] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\en-US\InkObj.dll.mui)
[2024-09-27 14:29:35.592] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\en-US\micaut.dll.mui)
[2024-09-27 14:29:35.611] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\en-US\mshwLatin.dll.mui)
[2024-09-27 14:29:35.646] [file_logger] [error] File handle not found! (C:\Program Files\Common Files\microsoft shared\ink\en-US\rtscom.dll.mui)
```

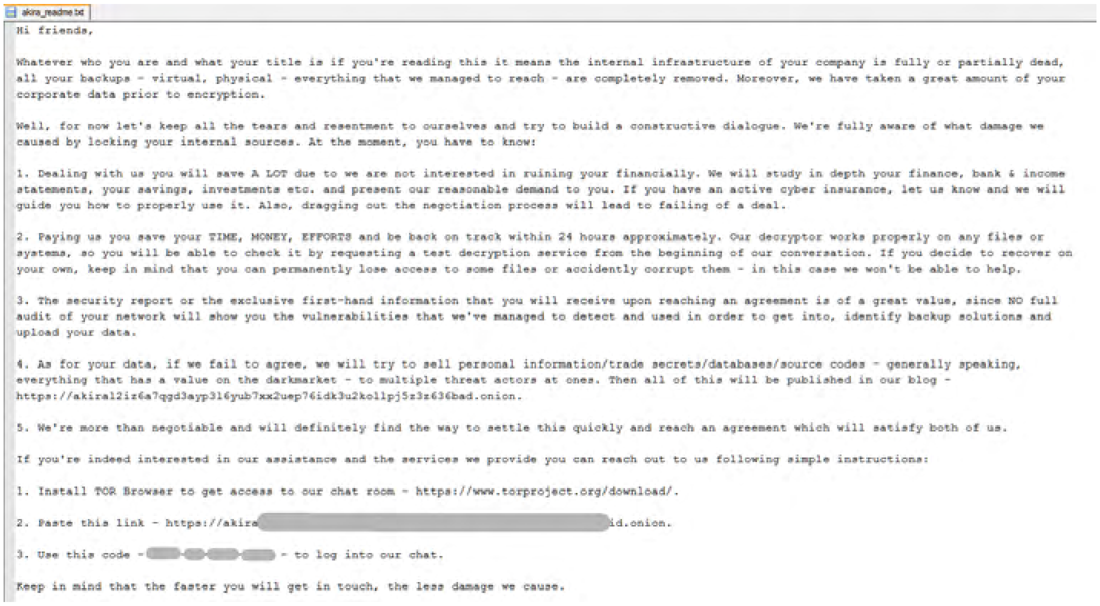
Figure 7. Portion of the log file



```
tm_time = localtime64(&Time);
strftime(logFileName, 0x50ui64, "Log-%d-%m-%Y-%H-%M-%S", tm_time);
v227 = 0i64;
v228 = 0i64;
v229 = 0i64;
filename_len = -1i64;
do
  ++filename_len;
while ( logFileName[filename_len] );
akira_writeToLog(&v227, logFileName, filename_len);
```

Figure 8. Log file name string format in the code

Upon successful execution, the ransomware creates ransom notes with the file name akira_readme.txt. The Megazord variant creates ransom notes with the same content, but the file name is powerranges.txt.



```
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 accidently 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://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.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://akira[redacted]id.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.
```

Figure 9. Akira ransom note

Ransom note content:

> 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 accidently 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://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]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 - <ONION_LINK>
> 3. Use this code - <UNIQUE_CODE> - to log into our chat.
>
> Keep in mind that the faster you will get in touch, the less damage we cause.

Modify Registry

The Windows registry is a database that stores configuration settings and values for the Windows operating system. It manages user preferences, installed software, system configurations, and more. Malware abuses the Windows registry to maintain persistence, hide its presence, disable security settings, and launch malicious scripts. Akira did not perform any registry key modification.

Mutex

The mutex is the fundamental tool for managing shared resources between multiple threads or processes. Typically, ransomware uses a mutex to avoid reinfecting the victim system and causing multiple layers of encryption. The ransomware did not create a mutex during execution.

Network Activity

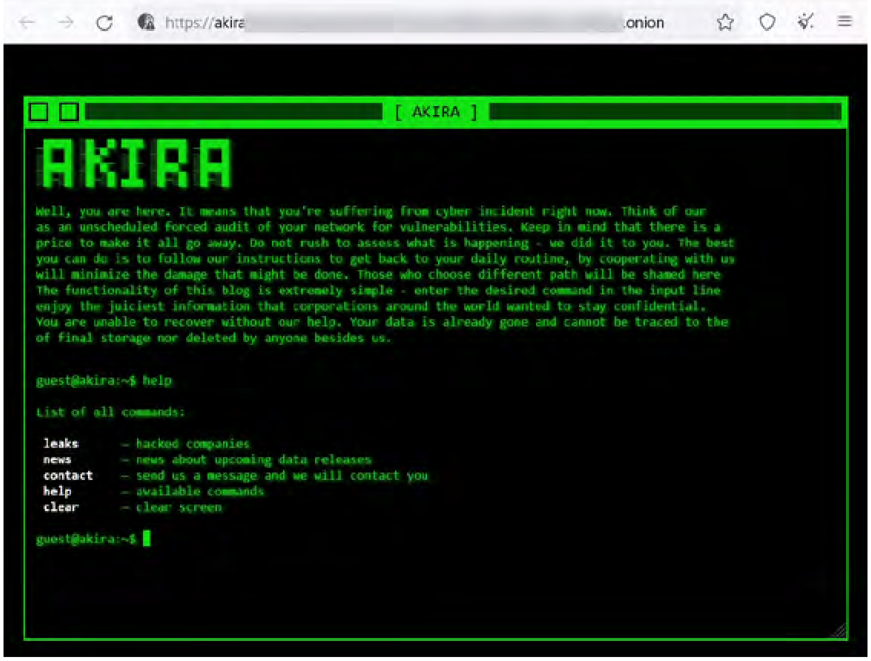
The ransomware did not try to communicate with a remote server other than encrypting data from mounted shares.

Indicators of Compromise

Indicator	Type	Context
9f873c29a38dd265decb6517a2a1f3b5d4f90ccd42eb61039086ea0b5e74827e 2b00a02196b87445633cabde506b4387979504cf60955f0b40cf2e4da4f0fd23 237d3c744fd5fc5d7e7a55e4385dff51045a1c6d8ee7346a270a688ab3791d49	SHA256 hash	Akira ransomware
akira_readme.txt, powerranges.txt	File name	Akiraransom notes
.akira, .powerranges, .akiranew	Extension	Encrypted files extension
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"	Process	Volume Shadow Copy deletion
Log-19-09-2024-09-21-20.txt	File name	Example log file name created by Akira
https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion	URL	TA data leak site (DLS)

Data Leak Site

The ransom note contains a data leak site (DLS) that, when accessed, displayed the following page, self-identifying the group as Akira:



```
Well, you are here. It means that you're suffering from cyber incident right now. Think of our
as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
price to make it all go away. Do not rush to assess what is happening - we did it to you. The best
you can do is to follow our instructions to get back to your daily routine, by cooperating with us
will minimize the damage that might be done. Those who choose different path will be shamed here
The functionality of this blog is extremely simple - enter the desired command in the input line
enjoy the juiciest information that corporations around the world wanted to stay confidential.
You are unable to recover without our help. Your data is already gone and cannot be traced to the
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:~$ 
```

Figure 10. Tor DLS

Tor Chat Site

The ransom note contains a Tor chat site and a unique code used to log into the chat. The Tor chat site displayed the following page:

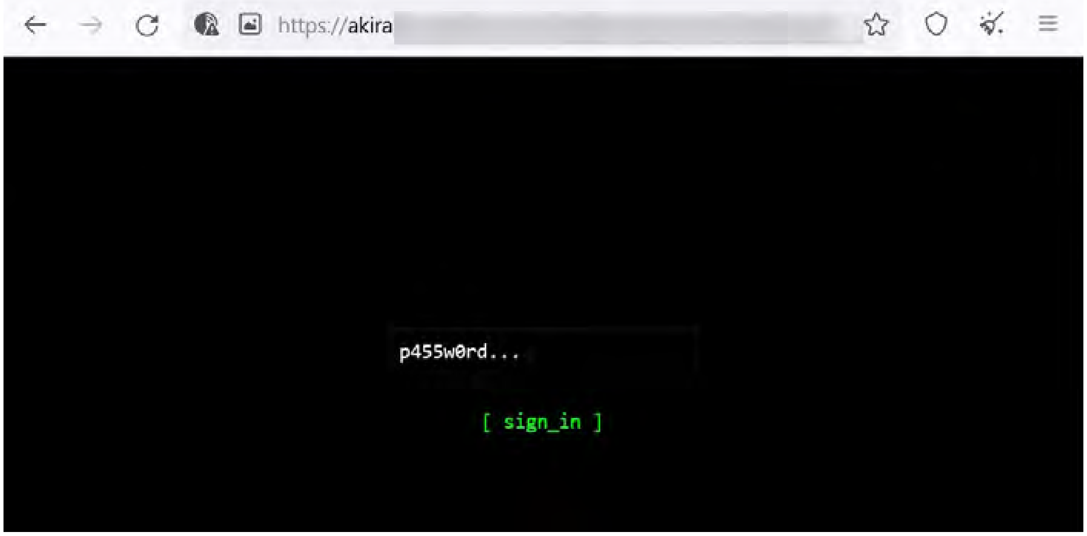


Figure 11. Tor chat site

Detection Mechanisms

Custom Detections and Blocking with Arete’s Arsinal

SentinelOne S1QL 1.0 query syntax (STAR rule):

Volume Shadow Copy Deletion

```
EndpointOS = "windows" AND ObjectType = "process" AND TgtProcCmdLine Contains Anycase "powershell.exe" AND TgtProcCmdLine Contains Anycase "-Command" AND TgtProcCmdLine Contains Anycase "Get-WmiObject Win32_Shadowcopy |" AND TgtProcCmdLine Contains Anycase "Remove-WmiObject"
```

Akira Ransomware

```
EndpointOS = "windows" AND ( ( ObjectType = "process" AND CmdLine In Contains Anycase ( ":\ProgramData\w.exe", ":\w.exe", ":\ProgramData\win.exe", ":\programdata\lck.exe", ":\ProgramData\dllhost32.exe", ":\ProgramData\hpupdate.exe" ) ) OR ( ObjectType = "file" AND ( EventType In ( "File Creation", "File Scan" ) AND ( TgtFilePath In Contains Anycase ( ":\ProgramData\w.exe", ":\w.exe", ":\ProgramData\win.exe", ":\programdata\lck.exe", ":\ProgramData\dllhost32.exe", ":\ProgramData\hpupdate.exe", ":\akira_readme.txt", ":\powerranges.txt", "akiranew.txt" ) OR TgtFilePath RegExp "\\Log-[0-9]{2}-[0-9]{2}-20[0-9]{2}-[0-9]{2}-[0-9]{2}-[0-9]{2}\.txt$" ))))
```

Note: These threat hunting queries may need to be tuned for your specific network environment.

Yara

```
rule Akira_ransomware_executable
{
    meta:
        author = "areteir.com"
        description = "Detects the Akira ransomware executable"
        target = "Windows systems"
        file_type = "exe"
        copyright = "Copyright © 2024 by Arete Advisors, LLC."
        distribution = "No re-distribution without Arete Advisors, LLC consent."

    strings:
        $ns1 = "Shadowcopy" ascii wide nocase
        $ns2 = "Remove-WmiObject" ascii wide nocase
        $ns3 = "write_encrypt_info" ascii wide nocase
        $ns4 = "Log-%d-%m-%Y-%H-%M-%S" ascii wide nocase
        $as1 = "--encryption_path" ascii wide nocase
        $as2 = "--share_file" ascii wide nocase
        $as3 = "--encryption_percent" ascii wide nocase
        $as4 = "-localonly" ascii wide nocase
        $ms1 = "megazord\\src\\main.rs" ascii wide nocase
        $ms2 = "megazord::windowsmegazord\\src\\windows.rs" ascii wide nocase
        $ms3 = "megazord::path_findermegazord\\src\\path_finder.rs" ascii wide nocase
        $ms4 = "megazord\\src\\lock.rs" ascii wide nocase
        $pdb1 = ":\\rust\\megazord" ascii wide nocase
        $pdb2 = "\\release\\deps\\megazord.pdb" ascii wide nocase
        $dls = "akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad" ascii wide nocase

    condition:
        ((uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)) and
        ( ( (2 of ($ns*)) and (3 of ($as*)) ) or ( all of ($ms*) ) or ( all of ($pdb*) ) or ($dls) )
}
```

Recommended Mitigations

- Utilize an endpoint detection and response (EDR) solution with the capability to halt detected processes and isolate systems on the network based on identified conditions.
- Block any known attacker C2s in the firewall.
- Implement multi-factor authentication on RDP and VPN to restrict access to critical network resources.
- Eliminate unnecessary RDP ports exposed to the internet.
- Block a high number of SMB connection attempts from one system to others in the network over a short period of time.
- Perform periodic dark web monitoring to verify if data is available for sale on the black market.
- Perform penetration tests.
- Periodically patch systems and update tools.
- Monitor connections to the network from suspicious locations.
- Monitor downloads and uploads of files to file-sharing services outside standard work hours.
- Monitor file uploads from domain controllers to the internet.
- Monitor network scans from uncommon servers (e.g., RDP server).

Organizations can find the full list of US government-recommended ransomware prevention and mitigation guidance here: https://www.cisa.gov/stopransomware/ransomware-guide.

Arete provides data-driven cybersecurity solutions to transform your response to emerging cyber threats.

Click here to learn more.

References

Arete - Crimeware Report H1 2024

Arete Turning Tides Crimeware Report H1 2023

Arete Arsinal Threat Management

Cybersecurity and Infrastructure Security Agency (CISA) Advisory #StopRansomware: Akira Ransomware

SentinelOne Megazord Ransomware

At Arete, we envision a world without cyber extortion, where people, businesses, and governments can thrive. We are taking all that we know from over 9,000 engagements to inform our solutions and strengthen powerful tools to better prevent, detect, and respond to the cyber extortion threats of tomorrow. Our elite team of experts provides unparalleled capabilities to address the entire cyber threat lifecycle, from incident response and restoration to advisory and managed security services. To learn more about our solutions, visit www.areteir.com.