

# the attacking abilities and strategies

Archived: 2026-04-06 00:08:01 UTC



```
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. There are three different paths will be shown here.
The functionality of this tool 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      - leaks 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:~$
```

## Summary

This is the head part of the Akira ransom note, and it claims:

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.

As you know, recently ransomware has become so popular, and threat actors further expanded the attack surface to Linux. In 2023, I had collected many ransoms that run on Linux and posted them to X (formerly Twitter), and last week I noted Akira ransom gang. I am very curious about what happened one year later.

## Technical analysis

### Basic info

#### The sample hashes:

**md5** 6B03B31C8CBD4A0A5829B63D16936ED3

**Sha1** a90790c35bea365befd3af55cbefdf2cc4481b

Operation system: Linux(ABI: 3.2.0)[AMD64, 64-bit, EXEC]

Packer: no

### Messages on the screen and imply

The Akira uses /proc/stat to get system-wide statistics about CPU usage, system activity, and process counts. It also checks the number of CPUs with /proc/cpuinfo, and it will print out the tip messages on the screen which

including detected number of CPU, “no path to encrypt” if without any path parameter and the time It took, such as:

```
root@kali:~# ./bcae.elf
Detected number of cpus = 2
No path to encrypt
3ms
root@kali:~#
```

Fig.1-message without running

From the message, it seems that it is helpful for the ransomware group to debug and expand new abilities. Of course, it also implies they are developing

### Static analysis

#### Supporting parameters and abilities

Let’s try a static analysis on IDA and look for some strings. The Akira ransomware supports many parameters to run, but it does not support command-line parameter help like “-h or /? or –help” to display them. Here they are:

1. -p(--encryption\_path) to set the path of directory or file, e.g, -p=/root/abc .
2. -s(--share\_file) to encrypt share file through network drive path.
3. -n(--encryption\_percent) to encrypt with percent, such as to set -n=5, -n=10 with the character “%”.
4. -e(--exclude) to use “regular” expression to skip all specific files and not to encrypt, e.g. -e=”pwn\*.\*”
5. -fork to create a child process for encryption in the background without any message output

```
v44 = __readfsqword(0x28u);
sub_409C2E(v42);
sub_408E24(v42, a1, a2, 1LL);
v40 = "-p";
v41 = "--encryption_path";
sub_409A2C(v43, v42, sv40, 2LL);
sub_4FC330(v37, v43);
sub_4F8AD0(v43);
v40 = "-s";
v41 = "--share_file";
sub_409A2C(v43, v42, sv40, 2LL);
sub_4FC330(v38, v43);
sub_4F8AD0(v43);
v40 = "-n";
v41 = "--encryption_percent";
sub_409A2C(v43, v42, sv40, 2LL);
sub_4FC330(v39, v43);
sub_4F8AD0(v43);
v36[0] = "-e";
v36[1] = "--exclude";
sub_409A2C(v43, v42, v36, 2LL);
sub_4FC330(sv40, v43);
sub_4F8AD0(v43);
sub_4877D0(v35);
sub_509FE0(v43, "-fork", v35);
v16 = sub_409A02(v42, v43);
sub_507A30(v43);
sub_4877F0(v35);
```

Fig.2-Supporting parameters

From the design, the `-p` parameter is very convenient to encrypt the specified directory and files; the `-s` parameter is to further expand the attack surface with the network drive path; and the `-n` parameter is to make faster encryption, especially if the size of encrypted files is too large. And combining the following will mention the lock strategy and its multiple **LWP techniques**; all in all, it is a very convenient, faster, and more powerful design.

### Ransom note and contact strategy

As you know, the ransomware named Akira is the cause of the file extension, and it will create a text file “akira\_readme.txt,” which we call a ransom note, including the common intel of threat from the attacker or the victim's information, such as an anonymous email address, onion address, Bitcoin address, and so on. At this ransomware as follows.

1. Publish victims address :  
hxxp[:]//akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion
2. Onion address for contact:  
hxxps[:]//akiralkzxzq2dsrzsrivr2xgbbu2wgsmxryd4csgfameg52n7efvr2id[.]onion
3. Unique code for logging to chat: xxxx-xx-xxx-xxxx
4. Bitcoin address and Wallet: In the ransom note, it does not claim how many bitcoins to pay, and without exposing any wallet address provided by the Akira gang, the threat actors

From the two onion addresses we have found, which also include the ransom group name strings “Akira.”.

And let's have a look at the ransom note as follows.

```
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 Akira!

1. Dealing with us you will have A LOT due to we are not interested in ruining your financially. We
will study in depth your finances, 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 lose 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
text 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 records 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/-
datacenter/secure codes - basically anything, everything that has a value on the darkmarket - to
multiple threat actors at once. Thus all of this will be published in our blog - https://
akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.

5. We've made them 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://akiralkzxzq2dsrzsrivr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.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.
```

Fig.3-ransom note

### Lock strategy for new extensions

Including the below important different types, such as database files, virtual machine files, disk images, and binary data formats, here they are as follows:

Database Files

Microsoft Access: .accdb, .accdc, .accde, .mdb

SQL-based Databases: .db, .db3, .sqlite, .sqlite3, .sdf, .mdf, .ndf

dBase & FoxPro: .dbf, .dbx, .fpt

Oracle Databases: .ora, .dbs, .dbc

Firebird & InterBase: .fdb, .gdb

IBM DB2: .db2

MySQL/MariaDB: .myd, .frm

Lotus Notes Database: .nsf, .ns2, .ns3, .ns4

## Virtual Machine & Disk Image Files

### Virtual Machine Files:

VMware: .vmdk, .vmem, .vmsn, .vmsd, .nvram, .vmx

VirtualBox: .vdi

Microsoft Hyper-V: .vhd, .vhdx, .avhd, .vmrs, .avdx, .vmcx

Parallels: .pvm

### Disk Image Files:

ISO Image: .iso

QEMU: .qcow2, .raw

Virtual Server Files: .vsv

## Backup & Log Files

Backup Files: .bak, .ndf, .sdf, .trc, .log

Checkpoints & Snapshots: .ckp, .snap

Error & Transaction Logs: .trm, .rpd, .sbf

## Miscellaneous Data Files

Metadata & Configurations: .dad, .daschema, .dadiagrams, .pdm

Encryption & Key Storage: .kdb, .lgc

User & Profile Data: .usr, .hdb, .epim

Binary & Raw Data Files

.bin, .raw, .subvo, .gcow2

### Dynamic analysis

#### LWPs technique and debug skill

Akira is creating multiple **Lightweight Processes (LWPs)**, which are likely **threads**. However, they seem to exit quickly when the numbers of the files are small. This makes debugging difficult.

```
pwndbg> run
Starting program: /root/bcae.elf -p=/root/██████████/
Detected number of cpus = 2
[New LWP 2668610]
[New LWP 2668617]
[New LWP 2668618]
[New LWP 2668619]
[LWP 2668617 exited]
[LWP 2668616 exited]
[LWP 2668618 exited]
9ms
[LWP 2668612 exited]
[Inferior 1 (process 2668612) exited normally]
```

Fig.4-LWPs

To overcome the above problem, just set encryption like this: `-p=/root`, which will encrypt the whole root directory, it is so big and time-consuming. First press `Ctrl+C` to make an interrupt, and then using **info threads** to get how many threads it created and choose one with **thread number** and trying **backtrace** to debug.

```
pwndbg> info threads
Id      target_id  Frame
* 1     LWP 2668801 "bcae.elf" 0x00000000046dcf7 in ?? ()
  2     LWP 2668802 "bcae.elf" 0x00000000046fb36 in ?? ()
  3     LWP 2668803 "bcae.elf" 0x00000000046fb36 in ?? ()
  4     LWP 2668804 "bcae.elf" 0x00000000046970b in ?? ()
  5     LWP 2668805 "bcae.elf" 0x0000000004695d8 in ?? ()
pwndbg> thread 2
[Switching to thread 2 (LWP 2668802)]
#0  0x00000000046fb36 in ?? ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

RAX 0xffffffffffffffe0
*RBX 0x0
+RCX 0x40fb36 ← cmp rax, -0x1000 /* 'H=' */
+RDX 0x0
+RDI 0x6d0ccc ← 0x0
+RSI 0x0
  R8 0x0
  R9 0x4
  R10 0x0
  R11 0x202
+R12 0x6d0cc4 ← 0x8
+R13 0x6d0c50 ← 0x0
+R14 0x7ffff7f74d0 → 0x46f810 ← endbr64
+R15 0x6d0ccc ← 0x0
+RBP 0x6d0cc0 ← 0x3ba5
+RSP 0x7ffff7f7490 ← 0x1dd1
+RIP 0x40fb36 ← cmp rax, -0x1000 /* 'H=' */
```

Fig.5-get threads and choose one thread to debug

### Encryption algorithm strategy

on this variant, the Akira combining standard AES with RSA public-key cryptosystem as encryption strategy, each file encrypted was appending 512 bytes random data to the end, as you know, they are used to decrypt by RSA private key. It does encryption with the Nettle library. Let's take one of them showing.



**md5 6B03B31C8CBD4A0A5829B63D16936ED3**

**Sha1 a90790c35bea365befd3af55cbefdd2cc4481b**

urls:

hxxps[:]//akiralkzxxq2dsrzsrivr2xgbbu2wgsmxyrd4csgfameg52n7efvr2id[.]onion

hxxps[:]//akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion

### Akira Analysis Briefing

Akira Analysis Briefing	
<b>Analyst</b>	Seeker(李标明)
<b>Background</b>	<p>This is the head part of the Akira ransom note, and it claims: Whatever who you are and what your life 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.</p> <p>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.</p> <p>As you know, recently ransomware has become so popular, and threat actors further expanded the attack face to Linux. In 2023, I had collected many ransomwares that run on Linux and posted them to X (formerly Twitter), and last week I noted Akira ransom gang. I am very curious about what happened one year later.</p>
<b>Sample</b>	<p>md5 6B03B31C8CBD4A0A5829B63D16936ED3</p> <p>Sha1 a90790c35bea365befd3af55cbefdd2cc4481b</p> <p>OS Linux</p>
<b>Name</b>	Akira (MMDM, 64-bit)
<b>Type</b>	Ransomware, file-encrypting virus
<b>Algorithm</b>	AES + RSA (nettle cryptographic library)
<b>Extension</b>	akira
<b>Threat Level</b>	High
<b>Ransomware Note</b>	akira_readme.txt
<b>Victim</b>	<p>Publish victims information address: hxxps[:]//akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion</p>
<b>Contact</b>	<p>1. Onion address: hxxps[:]//akiralkzxxq2dsrzsrivr2xgbbu2wgsmxyrd4csgfameg52n7efvr2id[.]onion 2. Unique code for logging to chat: xxx-xxx-xxxx-xxxx to chat</p>
<b>Suspicious strings</b>	<p>akira_readme.txt, nettle_aes256_encrypt, akira /usr/bin/macos_working_dir/openssl/ssl, /usr/bin/nettle, nettle, /usr/bin/openssl-encrypt.c Detected number of spaces ./local-elf-pri/</p>
<b>Key Information</b>	<p>1. -p --encryption_path) to set the path of directory or file, e.g. -p=/root/abc. 2. -s --share_file) to encrypt share file through network drive path. 3. -m --encryption_percent) to encrypt with percent, such as to set -m=5, it will encrypt with the character "5". 4. -e --exclude) to use "regular" expression to skip all specific files and not to encrypt, e.g. -e="*.mp3" . 5. -b --fork) to create a child process for encryption in the background without any message output</p>
<b>Infrared and Damaged</b>	 <pre> # 6B03B31C8CBD4A0A5829B63D16936ED3 # a90790c35bea365befd3af55cbefdd2cc4481b # 6B03B31C8CBD4A0A5829B63D16936ED3 # a90790c35bea365befd3af55cbefdd2cc4481b # akira_readme.txt                     </pre>

End.

Seeker(李标明) · @clibm079

China · Independent Malware Analyst & Researcher

Labels: [#LinuxSecurity](#), [#MalwareAnalysis](#), [#ransomware](#), [#ThreatIntel](#)

Source: <https://malwareanalysispace.blogspot.com/2025/03/akira-ransomware-expands-to-linux.html>