America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

#StopRansomware: Akira Ransomware

Release Date: April 18, 2024 **Alert Code:** AA24-109A

RELATED TOPICS: CYBERSECURITY BEST PRACTICES </topics/cybersecurity-best-practices>, CYBER THREATS AND ADVISORIES </topics/cyber-threats-and-advisories>, INCIDENT DETECTION, RESPONSE, AND PREVENTION </topics/cyber-threats-and-advisories/incident-detection-response-and-prevention>

ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM AKIRA RANSOMWARE:

1. **Prioritize remediating known exploited vulnerabilities.**
2. **Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.**
3. **Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.**

SUMMARY

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov <https://www.cisa.gov/stopransomware> to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The United States' Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL) are releasing this joint CSA to disseminate known Akira ransomware IOCs and TTPs identified through FBI investigations and trusted third party reporting as recently as February 2024.

Since March 2023, Akira ransomware has impacted a wide range of businesses and critical infrastructure entities in North America, Europe, and Australia. In April 2023, following an initial focus on Windows systems, Akira threat actors deployed a Linux variant targeting VMware ESXi virtual machines. As of January 1, 2024, the ransomware group has impacted over 250 organizations and claimed approximately $42 million (USD) in ransomware proceeds.

Early versions of the Akira ransomware variant were written in C++ and encrypted files with a `.akira` extension; however, beginning in August 2023, some Akira attacks began deploying Megazord, using Rust-based code which encrypts files with a `.powerranges` extension. Akira threat actors have continued to use both Megazord and Akira, including Akira_v2 (identified by trusted third party investigations) interchangeably.

The FBI, CISA, EC3, and NCSC-NL encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

Download the PDF version of this report:

AA24-109A #StopRansomware: Akira Ransomware
</sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf>
(PDF, 591.05 KB)

For a downloadable copy of IOCs, see:

AA24-109A STIX XML </sites/default/files/2024-04/aa24-109a.stix_0.xml>
(XML, 114.01 KB)

AA24-109A STIX JSON </sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware.stix_0.json>
(JSON, 67.80 KB)

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See MITRE ATT&CK for Enterprise <https://attack.mitre.org/versions/v14/matrices/enterprise/> for all referenced tactics and techniques.

Give Feedback

Initial Access

The FBI and cybersecurity researchers have observed Akira threat actors obtaining initial access to organizations through a virtual private network (VPN) service without multifactor authentication (MFA) configured[1 <https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira>], mostly using known Cisco vulnerabilities [T1190 <https://attack.mitre.org/versions/v14/techniques/t1190/>] CVE-2020-3259 <https://nvd.nist.gov/vuln/detail/cve-2020-3259> and CVE-2023-20269 <https://nvd.nist.gov/vuln/detail/cve-2023-20269>.[2 <https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication>],[3 <https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259>],[4

<https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira>]

Additional methods of initial access include the use of external-facing services such as Remote Desktop Protocol (RDP) [T1133 <https://attack.mitre.org/versions/v14/techniques/t1133/>], spear phishing [T1566.001 <https://attack.mitre.org/versions/v14/techniques/t1566/001/>][T1566.002 <https://attack.mitre.org/versions/v14/techniques/t1566/002/>], and the abuse of valid credentials[T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>].[4 <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira>]

Persistence and Discovery

Once initial access is obtained, Akira threat actors attempt to abuse the functions of domain controllers by creating new domain accounts [T1136.002 <https://attack.mitre.org/versions/v14/techniques/t1136/002/>] to establish persistence. In some instances, the FBI identified Akira threat actors creating an administrative account named `itadm`.

According to FBI and open source reporting, Akira threat actors leverage post-exploitation attack techniques, such as Kerberoasting[5 <https://www.crowdstrike.com/cybersecurity-101/kerberoasting/>], to extract credentials stored in the process memory of the Local Security Authority Subsystem Service (LSASS) [T1003.001 <https://attack.mitre.org/versions/v14/techniques/t1003/001/>].[6 <https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/>] Akira threat actors also use credential scraping tools [T1003 <https://attack.mitre.org/versions/v14/techniques/t1003/>] like Mimikatz and LaZagne to aid in privilege escalation. Tools like SoftPerfect and Advanced IP Scanner are often used for network device discovery (reconnaissance) purposes [T1016 <https://attack.mitre.org/versions/v14/techniques/t1016/>] and `net` Windows commands are used to identify domain controllers [T1018 <https://attack.mitre.org/versions/v14/techniques/t1018/>] and gather information on domain trust relationships [T1482 <https://attack.mitre.org/versions/v14/techniques/t1482>].

See Table 1 for a descriptive listing of these tools.

Defense Evasion

Based on trusted third party investigations, Akira threat actors have been observed deploying two distinct ransomware variants against different system architectures within the same compromise event. This marks a shift from recently reported Akira ransomware activity. Akira threat actors were first observed deploying the Windows-specific “Megazord” ransomware, with further analysis revealing that a second payload was concurrently deployed in this attack (which was later identified as a novel variant of the Akira ESXi encryptor, “Akira_v2”).

As Akira threat actors prepare for lateral movement, they commonly disable security software to avoid detection. Cybersecurity researchers have observed Akira threat actors using PowerTool to exploit the Zemana AntiMalware driver[4 <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira>] and terminate antivirus-related processes [T1562.001 <https://attack.mitre.org/versions/v14/techniques/t1562/001>].

Exfiltration and Impact

Akira threat actors leverage tools such as FileZilla, WinRAR [T1560.001 <https://attack.mitre.org/versions/v14/techniques/t1560/001/>], WinSCP, and RClone to exfiltrate data [T1048 <https://attack.mitre.org/versions/v14/techniques/t1048/>]. To establish command and control channels, threat actors leverage readily available tools like AnyDesk, MobaXterm, RustDesk, Ngrok, and Cloudflare Tunnel, enabling exfiltration through various protocols such as File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), and cloud storage services like Mega [T1537 <https://attack.mitre.org/versions/v14/techniques/t1537>] to connect to exfiltration servers.

Akira threat actors use a double-extortion model [T1657 <https://attack.mitre.org/versions/v14/techniques/t1657/>] and encrypt systems [T1486 <https://attack.mitre.org/versions/v14/techniques/t1486/>] after exfiltrating data. The Akira ransom note provides each company with a unique code and instructions to contact the threat actors via `a .onion` URL. Akira threat actors do not leave an initial ransom demand or payment instructions on compromised networks, and do not relay this information until contacted by the victim. Ransom payments are paid in Bitcoin to cryptocurrency wallet addresses provided by the threat actors. To further apply pressure, Akira threat actors threaten to publish exfiltrated data on the Tor network, and in some instances have called victimized companies, according to FBI reporting.

Encryption

Akira threat actors utilize a sophisticated hybrid encryption scheme to lock data. This involves combining a ChaCha20 stream cipher with an RSA public-key cryptosystem for speed and secure key exchange [T1486 <https://attack.mitre.org/versions/v14/techniques/t1486/>]. This multilayered approach tailors encryption methods based on file type and size and is capable of full or partial encryption. Encrypted files are appended with either a `.akira` or `.powerranges` extension. To further inhibit system recovery, Akira's encryptor (`w.exe`) utilizes PowerShell commands to delete volume shadow copies (VSS) on Windo systems [T1490 <https://attack.mitre.org/versions/v14/techniques/t1490>]. Additionally, a ransom note named `fn.txt` appears in both the root directory (`C:`) and each users' home directory (`C:\Users`).

Trusted third party analysis identified that the Akira_v2 encryptor is an upgrade from its previous version, which includes additional functionalities due to the language it's written in (Rust). Previous versions of the encryptor provided options to insert arguments at runtime, including:

- `-p --encryption_path (targeted file/folder paths)`
- `-s --share_file (targeted network drive path)`

- `-n --encryption_percent (percentage of encryption)`
- `--fork (create a child process for encryption`

The ability to insert additional threads allows Akira threat actors to have more granular control over the number of CPU cores in use, increasing the speed and efficiency of the encryption process. The new version also adds a layer of protection, utilizing the Build ID as a run condition to hinder dynamic analysis. The encryptor is unable to execute successfully without the unique Build ID. The ability to deploy against only virtual machines using "`vmonly`" and the ability to stop running virtual machines with "`stopvm`" functionalities have also been observed implemented for Akira_v2. After encryption, the Linux ESXi variant may include the file extension "`akiranew`" or add a ransom note named "`akiranew.txt`" in directories where files were encrypted with the new nomenclature.

Leveraged Tools

Table 1 lists publicly available tools and applications Akira threat actors have used, including legitimate tools repurposed for their operations. Use of these tools and applications should not be attributed as malicious without analytical evidence to support threat actor use and/or control.

Table 1: Tools Leveraged by Akira Ransomware Actors

Name	Description
AdFind <https://attack.mitre.org/versions/v14/software/s0552/>	`AdFind.exe` is used to query and retrieve information from Active Directory.

Name	Description
Advanced IP Scanner	A network scanner is used to locate all the computers on a network and conduct a scan of their ports. The program shows all network devices, gives access to shared folders, and provides remote control of computers (via RDP and Radmin).
AnyDesk	A common software that can be maliciously used by threat actors to obtain remote access and maintain persistence [T1219 <https://attack.mitre.org/versions/v14/techniques/t1219>]. AnyDesk also supports remote file transfer.
LaZagne <https://attack.mitre.org/software/s0349>	Allows users to recover stored passwords on Windows, Linux, and OSX systems.
PCHunter64	A tool used to acquire detailed process and system information [T1082 <https://attack.mitre.org/versions/v14/techniques/t1082/>].[7 <https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/>]
PowerShell <https://attack.mitre.org/versions/v14/techniques/t1059/001/>	A cross-platform task automation solution made up of a command line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.

Name	Description
Mimikatz <https://attack.mitre.org/versions/v14/software/s0002/>	Allows users to view and save authentication credentials such as Kerberos tickets.
Ngrok <https://attack.mitre.org/versions/v14/software/s0508/>	A reverse proxy tool [T1090 <https://attack.mitre.org/versions/v14/techniques/t1090/>] used to create a secure tunnel to servers behind firewalls or local machines without a public IP address.
RClone <https://attack.mitre.org/software/s1040>	A command line program used to sync files with cloud storage services [T1567.002 <https://attack.mitre.org/versions/v14/techniques/t1567/002/>] such as Mega.
SoftPerfect	A network scanner (`netscan.exe`) used to ping computers, scan ports, discover shared folders, and retrieve information about network devices via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) and PowerShell. It also scans for remote services, registry, files, and performance counters.
WinRAR	Used to split compromised data into segments and to compress [T1560.001 <https://attack.mitre.org/versions/v14/techniques/t1560/001/>] files into `.RAR` format for exfiltration.

Name	Description
WinSCP	Windows Secure Copy is a free and open source SSH File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client. Akira threat actors have used it to transfer data [T1048 <https://attack.mitre.org/versions/v14/techniques/t1048/>] from a compromised network to actor-controlled accounts.

Indicators of Compromise

Disclaimer: Investigation or vetting of these indicators is recommended prior to taking action, such as blocking.

Table 2a: Malicious Files Affiliated with Akira Ransomware

File Name	Hash (SHA-256)	Description
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca	Akira ransomware
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e	Akira ransomware encryptor
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138	Remote desktop application

File Name	Hash (SHA-256)	Description
Gcapi.dll	73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf	DLL file that assists with the execution of AnyDesk.exe
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386	Ngrok tool for persistence
Config.yml	Varies by use	Ngrok configuration file
Rclone.exe	aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9	Exfiltration tool
Winscp.rnd	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4	Network file transfer program
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c	Network file transfer program

File Name	Hash (SHA-256)	Description
Akira_v2	3298d203c2acb68c4 74e5fdad837918189 0b4403d6491c523c1 3730129be3f75 0ee1d284ed6630738 72012c7bde7fac5ca1 121403f1a5d2d541131 7df282796c	Akira_v2 ransomware

File Name	Hash (SHA-256)	Description
Megazord	ffd9f58e5fe8502249 c67cad0123ceeeaa6 e9f69b4ec9f9e21511 809849eb8fc dfe6fddc67bdc93b9 947430b966da2877f da094edf3e21e6f0ba 98a84bc53198 131da83b521f610819 141d5c740313ce465 78374abb22ef504a7 593955a65f07 9f393516edf6b8e011 df6ee991758480c5b 99a0efbfd68347786 061f0e04426c 9585af44c3ff8fd921 c713680b0c2b3bbc9 d56add848ed62164f 7c9b9f23d065 2f629395fdfa11e713 ea8bf11d40f6f240acf 2f5fcf9a2ac50b6f7f bc7521c83 7f731cc11f8e4d2491 42e99a44b9da7a48 505ce32c4ee488104 1beeddb3760be	Akira “Megazord” ransomware

File Name	Hash (SHA-256)	Description
	95477703e789e6182 096a09bc98853e0a 70b680a4f19fa2bf86 cbb9280e8ec5a 0c0e0f9b09b80d87e bc88e2870907b6cac b4cd7703584baf8f2 be1fd9438696d C9c94ac5e1991a7db 42c7973e328fceeb6 f163d9f644031bdfd4 123c7b3898b0	
VeeamHax.exe	aaa6041912a6ba3cf1 67ecdb90a434a62fe af08639c597058477 06b9f492015d	Plaintext credential leaking tool
Veeam-Get-Creds.ps1	18051333e658c4816 ff3576a2e9d97fe2a1 196ac0ea5ed9ba386 c46defafdb88	PowerShell script for obtaining and decrypting accounts from Veeam servers
PowershellKerberos TicketDumper	5e1e3bf6999126ae4a a52146280fdb913912 632e8bac4f54e98c5 8821a307d32	Kerberos ticket dumping tool from LSA cache
sshd.exe	8317ff6416af8ab6eb 35df3529689671a70 0fdb61a5e6436f4d6 ea8ee002d694	OpenSSH Backdoor

File Name	Hash (SHA-256)	Description
ipscan-3.9.1-setup.exe	892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0	Network scanner that scans IP addresses and ports

Table 2b: Malicious Files Affiliated with Akira Ransomware

File Name	Hash (MD5)	Description
winrar-x64-623.exe	7a647af3c112ad805296a22b2a276e7c	Network file transfer program

Disclaimer: While the date/time can be changed by Akira threat actors, trusted third-party analysis confirmed these samples were created on December 28, 2023.

Table 3: Windows Akira Ransomware Samples

Hash (SHA-256)
0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43
0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f
a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc
03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45
2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422
40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5
5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2

Hash (SHA-256)
643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562
6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84
fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64

Table 4: Linux/Unix Akira Ransomware Executable and Linkable Format (ELF) Samples

Hash (SHA-256)
e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f
74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4

Table 5a: Commands Affiliated with Akira Ransomware

Persistence and Discovery
nltest /dclist: [T1018 <https://attack.mitre.org/versions/v14/techniques/t1018/>]
nltest /DOMAIN_TRUSTS [T1482 <https://attack.mitre.org/versions/v14/techniques/t1482/>]
net group “Domain admins” /dom [T1069.002 <https://attack.mitre.org/versions/v14/techniques/t1069/002/>]
net localgroup “Administrators” /dom [T1069.001 <https://attack.mitre.org/versions/v14/techniques/t1069/001/>]
tasklist [T1057 <https://attack.mitre.org/versions/v14/techniques/t1057/>]

Persistence and Discovery
rundll32.exe c:\Windows\System32\comsvcs.dll, MiniDump ((Get-Process lsass).Id) C:\windows\temp\lsass.dmp full [T1003.001 <https://attack.mitre.org/versions/v14/techniques/t1003/001/>]

Table 5b: Commands Affiliated with Akira Ransomware

Credential Access
cmd.exe /Q /c esentutl.exe /y "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.default-release\key4.db" /d "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.default-release\key4.db.tmp” **Note:** Used for accessing Firefox data.
cmd.exe /Q /c esentutl.exe /y "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data" /d "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data.tmp” **Note:** Used for accessing Google Chrome data.

Table 5c: Commands Affiliated with Akira Ransomware

Impact
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject" [T1490 <https://attack.mitre.org/versions/v14/techniques/t1490/>]

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 6 -14 for all referenced Akira threat actor tactics and techniques for enterprise environments in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping <https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping> and CISA's Decider Tool <https://github.com/cisagov/decider/>.

Table 6: Initial Access

Technique Title	ID	Use
Valid Accounts	T1078 <https://attack.mitre.org/versions/v14/techniques/t1078/>	Akira threat actors obtain and abuse credentials of existing accounts as a means of gaining initial access.
Exploit Public Facing Application	T1190 <https://attack.mitre.org/versions/v14/techniques/t1190/>	Akira threat actors exploit vulnerabilities in internet-facing systems to gain access to systems.
External Remote Services	T1133 <https://attack.mitre.org/versions/v14/techniques/t1133/>	Akira threat actors have used remote access services, such as RDP/VPN connection to gain initial access.

Technique Title	ID	Use
Phishing: Spearphishing Attachment	T1566.001 <https://attack.mitre.org/versions/v14/techniques/t1566/001/>	Akira threat actors use phishing emails with malicious attachments to gain access to networks.
Phishing: Spearphishing Link	T1566.002 <https://attack.mitre.org/versions/v14/techniques/t1566/002/>	Akira threat actors use phishing emails with malicious links to gain access to networks.

Table 7: Credential Access

Technique Title	ID	Use
OS Credential Dumping	T1003 <https://attack.mitre.org/versions/v14/techniques/t1003/>	Akira threat actors use tools like Mimikatz and LaZagne to dump credentials.
OS Credential Dumping: LSASS Memory	T1003.001 <https://attack.mitre.org/versions/v14/techniques/t1003/001/>	Akira threat actors attempt to access credential material stored in the process memory of the LSASS.

Table 8: Discovery

Technique Title	ID	Use

Technique Title	ID	Use
System Network Configuration Discovery	T1016 <https://attack.mitre.org/versions/v14/techniques/t1016/>	Akira threat actors use tools to scan systems and identify services running on remote hosts and local network infrastructure.
System Information Discovery	T1082 <https://attack.mitre.org/versions/v14/techniques/t1082/>	Akira threat actors use tools like PCHunter64 to acquire detailed process and system information.
Domain Trust Discovery	T1482 <https://attack.mitre.org/versions/v14/techniques/t1482>	Akira threat actors use the net Windows command to enumerate domain information.
Process Discovery	T1057 <https://attack.mitre.org/versions/v14/techniques/t1057/>	Akira threat actors use the `Tasklist` utility to obtain details on running processes via PowerShell.
Permission Groups Discovery: Local Groups	T1069.001 <https://attack.mitre.org/versions/v14/techniques/t1069/001/>	Akira threat actors use the `net localgroup /dom` to find local system groups and permission settings.

Technique Title	ID	Use
Permission Groups Discovery: Domain Groups	T1069.002 <https://attack.mitre.org/versions/v14/techniques/t1069/002/>	Akira threat actors use the `net group /domain` command to attempt to find domain level groups and permission settings.
Remote System Discovery	T1018 <https://attack.mitre.org/versions/v14/techniques/t1018/>	Akira threat actors use `nltest /dclist` to amass a listing of other systems by IP address, hostname, or other logical identifiers on a network.

Table 9: Persistence

Technique Title	ID	Use
Create Account: Domain Account	T1136.002 <https://attack.mitre.org/versions/v14/techniques/t1136/002/>	Akira threat actors attempt to abuse the functions of domain controllers by creating new domain accounts to establish persistence.

Table 10: Defense Evasion

Technique Title	ID	Use

Technique Title	ID	Use
Impair Defenses: Disable or Modify Tools	T1562.001 <https://attack.mitre.org/versions/v14/techniques/t1562/001>	Akira threat actors use BYOVD attacks to disable antivirus software.

Table 11: Command and Control

Technique Title	ID	Use
Remote Access Software	T1219 <https://attack.mitre.org/versions/v14/techniques/t1219>	Akira threat actors use legitimate desktop support software like AnyDesk to obtain remote access to victim systems.
Proxy	T1090 <https://attack.mitre.org/versions/v14/techniques/t1090/>	Akira threat actors utilized Ngrok to create a secure tunnel to servers that aided in exfiltration of data.

Table 12: Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	T1560.001 <https://attack.mitre.org/versions/v14/techniques/t1560/001/>	Akira threat actors use tools like WinRAR to compress files.

Table 13: Exfiltration

Technique Title	ID	Use
Exfiltration Over Alternative Protocol	T1048 <https://attack.mitre.org/versions/v14/techniques/t1048/>	Akira threat actors use file transfer tools like WinSCP to transfer data.
Transfer Data to Cloud Account	T1537 <https://attack.mitre.org/versions/v14/techniques/t1537>	Akira threat actors use tools like CloudZilla to exfiltrate data to a cloud account and connect to exfil servers they control.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002 <https://attack.mitre.org/versions/v14/techniques/t1567/002/>	Akira threat actors leveraged RClone to sync files with cloud storage services to exfiltrate data.

Table 14: Impact

Technique Title	ID	Use
Date Encrypted for Impact	T1486 <https://attack.mitre.org/versions/v14/techniques/t1486/>	Akira threat actors encrypt data on target systems to interrupt availability to system and network resources.
Inhibit System Recovery	T1490 <https://attack.mitre.org/versions/v14/techniques/t1490>	Akira threat actors delete volume shadow copies on Windows systems.

Technique Title	ID	Use
Financial Theft	T1657 <https://attack.mitre.org/versions/v14/techniques/t1657/>	Akira threat actors use a double-extortion model for financial gain.

MITIGATIONS

Network Defenders

The FBI, CISA, EC3, and NCSC-NL recommend organizations apply the following mitigations to limit potential adversarial use of common system and network discovery techniques, and to reduce the risk of compromise by Akira ransomware. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats and TTPs. Visit CISA's Cross-Sector Cybersecurity Performance Goals <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals> for more information on the CPGs, including additional recommended baseline protections.

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, the cloud) [CPG 2.F <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#networksegmentation2f>, 2.R <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#systembackups2r>, 2.S <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#incidentresponseirplans2s>].

- **Require all accounts** with password logins (e.g., service accounts, admin accounts, and domain admin accounts) **to comply** with NIST's standards <https://pages.nist.gov/800-63-3/>. In particular, require employees to use long passwords and consider not requiring recurring password changes, as these can weaken security [CPG 2.C <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#uniquecredentials2c>].
- **Require multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems [CPG 2.H <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#phishingresistantmultifactorauthenticationmfa2h>].
- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> in internet-facing systems. [CPG 1.E <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#mitigatingknownvulnerabilities1e>].
- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement [CPG 2.F <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#networksegmentation2f>].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host [CPG 3.A <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandttps3a>].
- **Filter network traffic** by preventing unknown or untrusted origins from accessing remote services on internal systems. This prevents threat actors from directly connecting to remote access services that they have established for persistence.
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.

- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 1.A <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#assetinventory1a>, 2.O <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#documentdeviceconfigurations2o>].
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 2.E <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#separatinguserandprivilegedaccounts2e>].
- **Disable unused ports** [CPG 2.V <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#prohibitconnectionofunauthorizeddevices2v>].
- **Consider adding an email banner to emails** received from outside of your organization [CPG 2.M <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#emailsecurity2m>].
- **Disable hyperlinks** in received emails.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model <https://www.cisa.gov/zero-trust-maturity-model>). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally [CPG 2.E <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#separatinguserandprivilegedaccounts2e>, 2.N <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#disablemacrosbydefault2n>].
- **Maintain offline backups of data,** and regularly maintain backup and restoration [CPG 2.R <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#systembackups2r>]. By instituting this practice, the organization helps ensure they will not be severely interrupted, and/or only have irretrievable data.

- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#strongandagileencryption2k>, 2.L <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#securesensitivedata2l>, 2.R <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#systembackups2r>].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the FBI, CISA, EC3, and NCSC-NL recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The FBI, CISA, EC3 and NCSC-NL recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 6 -14).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The FBI, CISA, EC3, and NCSC-NL recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- Stopransomware.gov <https://www.stopransomware.gov/> is a whole-of-government approach that gives one central location for ransomware resources and alerts.

- Resource to mitigate a ransomware attack: #StopRansomware Guide <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>.
- No cost cyber hygiene services: Cyber Hygiene Services <https://www.cisa.gov/cyber-hygiene-services>, Ransomware Readiness Assessment <https://github.com/cisagov/cset/releases/tag/v10.3.0.0>.

REFERENCES

1. Fortinet: Ransomware Roundup - Akira <https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira>
2. Cisco: Akira Ransomware Targeting VPNs without MFA <https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication>
3. Truesec: Indications of Akira Ransomware Group Actively Exploiting Cisco AnyConnect CVE-2020-3259 <https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259>
4. TrendMicro: Akira Ransomware Spotlight <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira>
5. CrowdStrike: What is a Kerberoasting Attack? <https://www.crowdstrike.com/cybersecurity-101/kerberoasting/>
6. Sophos: Akira, again: The ransomware that keeps on taking <https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/>
7. Sophos: Akira Ransomware is “bringin’ 1988 back” <https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/>

REPORTING

Your organization has no obligation to respond or provide information back to the FBI in response to this joint CSA. If, after reviewing the information provided, your organization decides to provide information to the FBI, reporting must be consistent with applicable state and federal laws.

The FBI is interested in any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Akira threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include: a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

The FBI, CISA, EC3, and NCSC-NL do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to the FBI's Internet Crime Complain Center (IC3) <https://www.ic3.gov/>, a local FBI Field Office <https://www.fbi.gov/contact-us/field-offices>, or CISA via the agency's Incident Reporting System <https://www.cisa.gov/forms/report> or its 24/7 Operations Center (report@cisa.gov or by calling 1-844-Say-CISA (1-844-729-2472).

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. Th FBI, CISA, EC3, and NCSC-NL do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI or CISA.

ACKNOWLEDGEMENTS

Cisco, Sophos, and Fortinet contributed to this advisory.

VERSION HISTORY

April 18, 2024: Initial version.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Tags

Co-Sealers and Partners: Federal Bureau of Investigation, International

MITRE ATT&CK TTP: Collection (TA0009), Command and Control (TA0011), Credential Access (TA0006), Defense Evasion (TA0005), Discovery (TA0007), Exfiltration (TA0010), Impact (TA0040), Initial Access (TA0001), Privilege Escalation (TA0004)

Topics: Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Cybersecurity Best Practices </topics/cybersecurity-best-practices>, Incident Detection, Response, and Prevention </topics/cyber-threats-and-advisories/incident-detection-response-and-prevention>, Malware, Phishing, and Ransomware </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

Give Feedback

SEP 23, 2025 ■ CYBERSECURITY ADVISORY | AA25-266A

CISA Shares Lessons Learned from an Incident Response Engagement </news-events/cybersecurity-advisories/aa25-266a>

AUG 27, 2025 ■ CYBERSECURITY ADVISORY | AA25-239A

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System </news-events/cybersecurity-advisories/aa25-239a>

JUL 31, 2025 ■ CYBERSECURITY ADVISORY | AA25-212A

CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization

</news-events/cybersecurity-advisories/aa25-212a>

JUL 22, 2025 ■ CYBERSECURITY ADVISORY | AA25-203A

#StopRansomware: Interlock

</news-events/cybersecurity-advisories/aa25-203a>

Give Feedback

Return to top

1-844-Say-CISA contact@cisa.dhs.gov