Akira Ransomware 2025: Updated CISA Advisory, TTPs, and Defense Strategies

SILA ÖZEREN HACIOĞLU | 16 MIN READ
LAST UPDATED ON NOVEMBER 14, 2025

SUMMARIZE WITH:

ChatGPT perplexity Google AI

On November 13, 2025, the Cybersecurity and Infrastructure Security Agency (CISA), together with the FBI, HHS, Europol, OFAC, NCSC-NL, and German authorities, released an updated joint advisory on **Akira ransomware**. The report highlights Akira's continued evolution since 2023 and details new variants, expanded targeting, and newly observed attack techniques.

In this blog post, we break down the latest **tactics, techniques, and procedures (TTPs)** observed in Akira operations, including new initial access vectors, credential abuse patterns, and lateral movement behaviors, and outline actionable steps organizations can take to defend against Akira ransomware attacks.

SIMULATE THIS THREAT FOR FREE - NO SETUP

Who Is Akira Ransomware?

Akira is no longer a "new" ransomware family.

It has matured into a highly active **Ransomware-as-a-Service (RaaS)** operation linked to groups such as *Storm-1567*, *Howling Scorpius*, and potentially the defunct *Conti syndicate*.

The actors now maintain multiple encryptors for Windows, Linux, VMware

ESXi, and even Nutanix AHV, and have shifted between the original C++ Akira variant and the Rust-based **Megazord** and **Akira_v2** payloads. As of late 2025, they have extorted an estimated **$244 million USD** from victims across North America, Europe, and Australia.

What Are the Initial Access Tactics Used by Akira Ransomware?

T1190 - Exploiting Public-Facing Applications

Akira gains entry by exploiting vulnerabilities in internet-facing systems, especially VPN appliances and backup solutions.

Observed exploited CVEs include:

Cisco VPN vulnerabilities

- CVE-2020-3259 – Sensitive information disclosure
- CVE-2023-20269 – Authentication bypass
- CVE-2020-3580 – XSS
- CVE-2023-28252 – Heap-based buffer overflow
- CVE-2024-37085 – Authentication bypass

Veeam Backup & Replication

- CVE-2023-27532 – Missing authentication for critical function
- CVE-2024-40711 – Deserialization of untrusted data

SonicWall VPN

- CVE-2024-40766 – Improper access control

These vulnerabilities are used to compromise VPNs, hypervisors, and backup servers.

If you are interested on how Akira ransomware exploits Cisco ASA zero-day vulnerability, please visit our previous blog post on "CVE-2023-20269: Akira Ransomware Exploits Cisco ASA Vulnerability".

What Are the Discovery Tactics Used by Akira Ransomware?

T1124 - System Time Discovery

Getting current date of the system

Akira ransomware has been observed querying the system’s current date using PowerShell. Threat actors do this to timestamp output, synchronize encryption routines, avoid sandboxed environments with unrealistic clocks, and ensure their workflow aligns with C2-side tasking.

How Does Picus Help?

```
powershell.exe -c "$fileName = (Get-Date).ToString('dd-MM-yyyy') + '_picus.txt'; $filePath = \"$env:APPDATA\Logs\$fileName\"; if (!(Test-Path $filePath)) { New-Item -ItemType File -Path $filePath -Force }; $env:path | Out-File -Append $filePath"
```

The payload replicates two behaviors commonly seen during ransomware staging:

1. Time Discovery – retrieving the system date to timestamp files, detect sandboxes, or coordinate workflow.
2. Local Reconnaissance – enumerating environment variables and writing them to attacker-controlled artifacts.

This makes it a controlled emulation of how real ransomware families like Akira perform early-stage reconnaissance before encryption.

T1016 - System Network Configuration Discovery

Displaying information about all drives using "fsutil fsinfo drives" command

Ransomware operators routinely query local drive information to understand the file system layout before encryption. Although T1016 refers to network configuration discovery, malware often bundles network and system-level enumeration together during the same reconnaissance stage.

Commands like fsutil fsinfo drives allow attackers to quickly enumerate all mounted volumes, identify additional partitions, detect removable or network-mapped drives, and prepare target lists for encryption.

How Does Picus Help?

```
fsutil.exe fsinfo drives
```

What the command does

- fsutil.exe

A built-in Windows utility that provides low-level file system information.
Malware frequently abuses it because it does not require elevated privileges for basic queries and blends in with legitimate administrative behavior.

- fsinfo drives

Instructs fsutil to return a list of all logical drives currently mounted on the system (e.g., C:\ D:\ E:\). This gives the attacker an immediate map of potential data locations.

T1057 - Process Discovery

Listing Currently Running Processes via WTSEnumerateProcesses

Many ransomware families and post-exploitation toolkits enumerate active processes to understand what is running on the system. The Windows Terminal Services API function WTSEnumerateProcesses is a common choice because it returns a detailed process list across all sessions, including user, PID, and memory usage.

Attackers rely on this to identify security tools, EDR processes, backup agents, and services they need to evade or terminate before encryption.

How Does Picus Help?

```
%TMP%\WTSEnumerateProcessesDiscovery.exe
```

This executable calls the Terminal Services API function WTSEnumerateProcessesW, a legitimate Windows API that returns structured metadata for each running process.

What the technique does

Loads the WTS API

The executable invokes functions from Wtsapi32.dll, which exposes enumeration APIs used by Remote Desktop Services and administrative tooling.

Calls WTSEnumerateProcesses

This function enumerates all processes across all active sessions, giving the attacker:

- Process names
- Process IDs
- Owning user/session
- Memory footprint

Unlike basic tools like tasklist, this API provides richer context and can enumerate processes in remote or background sessions.

Returns a complete process inventory

The malware performs a complete process enumeration, which attackers use to:

- Spot and terminate security products (EDR, AV, backups, monitoring)
- Locate SYSTEM-level processes suitable for privilege escalation
- Choose high-value processes for code injection, including browsers and RDP clients

T1018 - Remote System Discovery

Displaying a List of Domain Computers Using Powershell Active Directory Module

Adversaries enumerate domain-joined systems early in an intrusion to understand the network surface. Using the PowerShell Active Directory module, attackers can query Active Directory for a complete list of computers, their attributes, and their operational roles.

This information is used to plan lateral movement, identify high-value servers, and select targets for credential theft, persistence, or ransomware deployment.

How Does Picus Help?

```
powershell.exe -c Unblock-File '%TMP%\Microsoft.ActiveDirectory.Management.dll'; Import-Module '%TMP%\Microsoft.ActiveDirectory.Management.dll'; Get-ADComputer -Filter * -Properties *
```

What each part does

- Unblock-File '%TMP%\Microsoft.ActiveDirectory.Management.dll'

Removes the "downloaded from the internet" block on the DLL so PowerShell can load it.

Attackers use this when they bring their own AD module into the environment (BYOL – Bring Your Own Library) instead of relying on installed components.

- Import-Module '%TMP%\Microsoft.ActiveDirectory.Management.dll'

Manually loads the Active Directory module. This bypasses systems where RSAT or AD PowerShell modules are not installed, allowing enumeration even in restricted endpoints.

- Get-ADComputer -Filter * -Properties *

Queries Active Directory for all domain computers, returning attributes such as, DNS hostnames, operating system and version, last logon time, OU placement, IPv4 addresses, and enabled/disabled status.

This provides a complete inventory of reachable systems.

Gathering Information about Target Domain and OS using Adfind

Adfind is a lightweight command line tool frequently used by threat actors to enumerate Active Directory objects without relying on native PowerShell modules. Because it requires no installation and produces structured output, attackers use it to extract computer lists, operating system versions, DNS hostnames, and other attributes needed to plan lateral movement and target selection.

This technique often appears after domain credentials are obtained and before ransomware staging or privilege escalation.

How Does Picus Help?

```
cmd.exe /c ""%TMP%\adfind.exe" -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > "%TMP%\some.csv""
```

This command executes adfind.exe from the temporary directory, similar to how attackers deploy portable LDAP tools to avoid dependency checks.

The filter objectcategory=computer retrieves all domain computer objects, and the -csv flag outputs the selected attributes, name, cn, OperatingSystem, and dNSHostName, in a structured format.

The results are saved to a CSV file, giving the attacker an immediate inventory of hosts and OS versions that can guide lateral movement and identify high-value or outdated systems.

T1087.002 - Account Discovery: Domain Account

Executing BloodHound Tool's Ingestor (Invoke-BloodHound) Function

BloodHound's PowerShell ingestor, **Invoke-BloodHound**, relies on executing PowerShell scripts that query Active Directory for domain users, groups, sessions, and ACL relationships.

Before running the ingestor, attackers often adjust the PowerShell execution policy to allow unrestricted script execution. This removes a built-in safety control and ensures their reconnaissance scripts run without restriction.

How Does Picus Help?

```
powershell.exe -c "$ep=Get-ExecutionPolicy;If ($ep -ne 'Unrestricted') {Set-ExecutionPolicy Unrestricted -scope CurrentUser -Force}; Get-ExecutionPolicy"
```

This payload checks the current PowerShell execution policy and, if it is not already set to Unrestricted, modifies it for the current user.

Attackers do this to guarantee that unsigned or downloaded scripts, such as BloodHound's investors can run without being blocked. After applying the change, the policy is queried again to confirm that the environment is ready for script-based domain enumeration.

What Are the Defense Evasion Tactics Used by Akira Ransomware?

T1562 - Impair Defenses

Disabling the Real Time Monitoring Service of Windows Defender

Attackers commonly tamper with Windows Defender and firewall rules to weaken host protections before executing further payloads. Disabling real-time monitoring removes active scanning, reduces behavioral detection, and allows malicious files to execute without interception.

Adding an inbound RDP rule gives the attacker persistent remote access, often used for hands-on-keyboard actions and post-exploitation.

How Does Picus Help?

```
# Process 1
powershell.exe -c "Get-MPPreference | findstr /
```

```
C:'DisableRealtimeMonitoring' /C:'DisableIOAVProtection' /
C:'DisableScriptScanning' /C:'EnableControlledFolderAccess'
/C:'EnableNetworkProtection' /C:'SubmitSamplesConsent' /
C:'MAPSReporting'" > '%TMP%\mppreference_status.txt'

# Process 2
powershell.exe Set-MpPreference -DisableRealtimeMonitoring
$true
```

The *first command* queries Windows Defender configuration via Get-MpPreference and filters key protection settings such as real-time monitoring, IOAV scanning, script scanning, cloud protection, and network protection. The results are written to a file in the temporary directory, mirroring how attackers record the current defensive posture before making changes.

The *second command* disables real-time monitoring entirely. This removes Defender's active scanning component, reducing detection of file-based and behavioral malware activity and allowing the attacker more freedom for follow-on actions.

Adding RDP Allow Rule called "rdp" on Windows Firewall

How Does Picus Help?

```
netsh.exe advfirewall firewall add rule name="rdp" dir=in protocol=tcp
localport=3389 action=allow
```

The final command adds a new firewall rule named “rdp” that permits inbound TCP connections on port 3389.

Attackers use this to ensure Remote Desktop Protocol is reachable externally, enabling direct remote access even if RDP was previously blocked by firewall settings.

What Are the Credential Access Tactics Used by Akira Ransomware?

T1003 - OS Credential Dumping

Dumping Credentials by executing comsvcs.dll Minidump

Akira ransomware operators frequently dump LSSAS to harvest *plaintext credentials*, *NTLM hashes*, and *Kerberos material*. One of the quieter and more reliable techniques is abusing comsvcs.dll's built-in MiniDump export function.

This API-level dumping approach often bypasses basic monitoring and avoids dropping well-known tools like Mimikatz, making it a preferred method in modern ransomware operations.

How Does Picus Help?

```
# Process 1
powershell.exe -c "$ep=Get-ExecutionPolicy;If ($ep -ne 'Unrestricted') {Set-ExecutionPolicy Unrestricted  -scope CurrentUser -Force}; Get-ExecutionPolicy"
```

The first process relaxes the PowerShell execution policy so unsigned or downloaded scripts can run. Attackers do this to enable helper modules needed for process manipulation or dump preparation.

```
# Process 2
powershell.exe -c "Unblock-File '%TMP%\ResumeSuspended.ps1'; Import-Module '%TMP%\ResumeSuspended.ps1'; & ResumeSuspended"
```

The second step unblocks and loads a helper script designed to resume suspended processes. Some attackers use this approach to manipulate LSASS into a stable state for dumping, ensuring the process is accessible and not protected by certain security products.

```
# Process 3
powershell.exe -c "rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump (get-process lsass).id "%TMP%\mini.dmp" full"
```

This is the core credential access action.

rundll32.exe calls the exported MiniDump function inside comsvcs.dll, instructing Windows to create a full memory dump of LSASS. The dump is written to the temporary directory. This technique produces a complete snapshot of credential material without requiring external tools.

```
# Process 4
powershell.exe Sleep 10;$envPath = $env:TMP;(Test-Path $envPath\*.dmp -PathType Leaf) -and ((Get-Item $envPath\*.dmp).Length -gt 0)
```

The final step verifies that the dump was successfully created by checking for .dmp files in the temporary directory after a short delay. This mirrors the validation attackers perform before exfiltrating or parsing the dump with offline tools.

T1003.001 - OS Credential Dumping: LSASS Memory

Gathering credentials using Mimikatz Tool

How Does Picus Help?

```
%TMP%\mimikatz22020220919x64.exe "privilege::debug" "sekurlsa::logonPasswords" exit
```

This executable launches Mimikatz from the temporary directory, mirroring how attackers drop the tool into an ephemeral path to reduce forensic traces. The first command, "privilege::debug", attempts to enable the **SeDebugPrivilege**, which is required to read LSASS memory. Once elevated, "sekurlsa::logonPasswords" queries LSASS' credential provider data structures and extracts active logon sessions, including plaintext passwords (when available), NTLM hashes, and Kerberos credentials. The final exit command terminates the tool upon completion.

This sequence gives the attacker immediate access to all credentials stored in LSASS at execution time, which can be used to authenticate across the domain without triggering password-based authentication logs.

What Are the Command and Control (C2) Tactics Used by Akira Ransomware?

T1133 - External Remote Services

Downloading the AnyDesk Portable Version

Akira operators frequently rely on legitimate remote access tools to maintain persistent control over compromised systems. AnyDesk Portable is commonly abused because it requires no installation, runs from user-writable directories, and blends into administrative activity.

Attackers *typically drop the executable into a temporary folder* and verify its presence before configuring it for inbound remote sessions.

How Does Picus Help?

```
cmd.exe /c timeout 5 && dir %TMP%\AnyDesk.exe
```

This command introduces a short delay with timeout 5 and then checks the temporary directory for the presence of **AnyDesk.exe**. The delay accounts for the time required to download or write the file to disk. The subsequent dir command verifies that the remote access tool is present and ready to be executed.

This mirrors the attacker's workflow: drop or download the portable binary, confirm delivery, and then proceed with configuration steps to establish an external remote session through AnyDesk's infrastructure.

What Are the Persistence Tactics Used by Akira Ransomware?

T1136.001 – Create Account: Local Account

Adding a New User

Attackers often create new local accounts to maintain persistence on a compromised host. This provides a stable foothold that survives reboots, bypasses some token-based session controls, and allows direct login through RDP, SMB, or local console access.

Creating an account with administrative privileges is a common step prior to establishing long-term control or staging further operations.

How Does Picus Help?

```
net.exe user /add John Jhn1234Abc!
```

This command instructs net.exe to create a new local user named **John** with the password **Jhn1234Abc!**. The /add parameter writes the new account to the local SAM database.

Attackers use this method because it is built into Windows, requires no external tooling, and generates minimal noise beyond basic event logs. Once the account is created, adversaries typically follow up by adding it to privileged groups such as *Administrators* or enabling remote login paths.

What Are the Impact Tactics Used by Akira Ransomware?

T1490 - Inhibit System Recovery

Deleting Shadow Copy using Powershell

Akira ransomware disables recovery mechanisms to prevent system restoration after encryption. Removing Volume Shadow Copies ensures victims cannot recover files using built-in Windows restore points.

How Does Picus Help?

```
powershell.exe -c "Get-WmiObject Win32_Shadowcopy | ForEach-Object
{$_.Delete();}"
```

This command queries all existing shadow copies through the Win32_Shadowcopy WMI class and deletes each object returned. Attackers use this method because it avoids high-profile utilities like vssadmin.exe and leverages built-in WMI providers to quietly eliminate all restore points before encryption begins.

T1083 - File and Directory Discovery

Finding Files with Specific Extensions for Encryption

Ransomware families typically inventory files with valuable extensions before encryption. Akira performs recursive searches to identify documents, spreadsheets, presentations, and other business-critical formats.

How Does Picus Help?

```
cmd.exe /c for %G in (.pdf, .doc, .wps, .docx, .ppt, .xls, .xlsx, .pptx,
.rtf) do forfiles /p "C:" /s /M *%G /C "cmd /c echo @PATH"
```

This command iterates through a list of file extensions and uses forfiles to recursively scan the entire C drive. Matching file paths are echoed to output, mirroring how attackers build internal lists of files to encrypt.

This is a common pre-encryption staging action in ransomware workflows.

T1486 - Data Encrypted for Impact

Encrypting a File using Encryptor.exe

Akira uses custom encryptors to process files in bulk. Running a standalone encryptor executable is part of the final impact phase, where data is made inaccessible to force payment.

How Does Picus Help?

```
%TMP%\encryptor.exe /E "%TMP%\dummy.txt" /AES
```

This payload executes a portable encryption tool from the temporary directory. The /E parameter specifies encryption mode, and /AES selects the AES algorithm. The command encrypts a target file (dummy.txt), simulating how ransomware encrypts local data using symmetric encryption routines.

T1491 - Defacement

Writing a File that Contains Akira Ransom Note and Open It

Ransomware often writes ransom notes to disk and forcibly opens them to ensure the victim sees payment instructions.

```
#Process 1
notepad.exe "%TMP%\akira_readme.txt"

#Process 2
{predefined-process-list} notepad.exe
```

The first action opens the ransom note file directly in Notepad.

The second action verifies that the Notepad process is running, consistent with attacker behavior where ransomware launches and monitors a ransom-note display process. This guarantees the victim receives coercive messaging immediately after encryption completes.

TRY EMERGING THREAT SIMULATOR NOW - NO REGISTRATION

How Picus Helps Simulate Akira Ransomware Attacks?

We also strongly suggest simulating **Akira ransomware attacks** to test the effectiveness of your security controls against real-life cyber attacks using the **Picus Complete Security Validation Platform**. You can also test your defenses against hundreds of other ransomware variants, such as Phobos, ALPHV, and Play, within minutes with a 14-day free trial of the Picus Platform.

Picus Threat Library includes the following threats for **Akira ransomware**:

Threat ID	Threat Name	Attack Module
26884	Akira Ransomware Campaign	Windows Endpoint
84668	Akira Ransomware Download Threat	Network Infiltration
55812	Akira Ransomware Email Threat	Email Infiltration (Phishing)
13162	Cisco ASA Reflected Cross-Site Scripting (XSS) Vulnerability	Web Application
37780	Megazord Ransomware Download Threat	Network Infiltration
92400	Megazord Ransomware Email Threat	Email Infiltration (Phishing)

Picus also provides actionable mitigation content. **Picus Mitigation Library** includes prevention signatures to address **Akira ransomware** and other ransomware attacks in preventive security controls. Currently, Picus Labs validated the following signatures for **Akira ransomware**:

Security Control	Signature ID	Signature Name

Check Point NGFW	0D0FC5542	Ransomware.Win32.Akira.TC.a77avEjG
Check Point NGFW	0CEDE557A	Ransomware.Win32.Akira.TC.eec5NsKn
Check Point NGFW	0CFD4BD86	Ransomware.Win32.Akira.TC.a5f8yZDg
Check Point NGFW	0E0BEF9A4	Ransomware.Win32.Akira.TC.0e05wZMS
Check Point NGFW	0A2E01186	Ransomware.Win32.Akira.TC.ea38rili
Check Point NGFW	0C5DE6DD1	Ransomware.Win32.Akira.TC.4b33iwYh
Check Point NGX	0DF6F8B8C	Trojan-Ransom.Win32.Akira.TC.a859tRFj
Check Point NGX	0EEC5DE8A	Ransomware.Win32.Akira.TC.bad9mBdZ
Cisco FirePower		W32.Auto:3c92bf.in03.Talos
Cisco FirePower		W32.Auto:7b295a.in03.Talos
Cisco FirePower		W32.Auto:1b6af2.in03.Talos
Cisco FirePower		W32.Auto:678ec8.in03.Talos
Forcepoint NGFW		File_Malware-Blocked
Fortigate AV	10143171	Linux/Filecoder_Akira.A!tr
Fortigate AV	10133803	W64/Generik.NFLQ!tr.ransom

Trellix	0x4840c900	MALWARE: Malicious File Detected by GTI
Palo Alto	588177441	Ransom/Win32.akira.b
Palo Alto	595008162	ransomware/Linux.akira.d
Snort	1.63977.1	MALWARE-OTHER MultiOS.Ransomware.Megazord download attempt

Start simulating emerging threats today and get actionable mitigation insights with a 14-day free trial of the Picus Complete Security Validation Platform.

References

[1] “#StopRansomware: Akira Ransomware,” Cybersecurity and Infrastructure Security Agency CISA. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a. [Accessed: Apr. 20, 2024]

Share this:

𝕏 in f

What is Akira ransomware, and how does it operate? ▼

How does Akira ransomware gain initial access to target networks? ▼

What techniques do Akira ransomware operators use for persistence and privilege escalation? ▼

How does Akira ransomware execute its attacks on compromised systems?

What methods are employed by Akira ransomware for data exfiltration?

How does the Picus Complete Security Validation Platform help in simulating Akira ransomware attacks?

What are some of the prevention signatures provided by the Picus Mitigation Library for Akira ransomware?

PICUSLABS
EMERGING THREAT
CVE-2026-21509: APT28 Microsoft Office Zero-day Vulnerability

EMERGING THREAT

CVE-2026-21509: APT28 Exploits Microsoft Office Zero-day Vulnerability

EMERGING THREAT

Ni8mare: n8n CVE-2026 Remote Code Execution Vulnerability Explained

Email*

Email

SUBSCRIBE NOW

Platform

- The Security Validation Platform
- Security Control Validation
- Attack Surface Validation
- Cloud Security Validation
- Attack Path Validation
- Detection Rule Validation
- Integrations

Use Cases

- Breach and Attack Simulation
- Automated Penetration Testing
- Adversarial Exposure Validation

Resources

- Blog
- Purple Academy
- Webinars
- Reports
- Case Studies
- Press Releases
- Datasheets
- Cyberpedia
- Events

Company

- About Us
- Leadership
- Careers
- Contact
- Customer Support
- Trust Center
- Picus in the News

Subscribe to Our Newsletter

Email*

Email

SUBSCRIBE NOW

Contact Us

info@picussecurity.com

Schedule a meeting

Hey AI, learn about us

© 2025 Copyright. All rights reserved.