JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA24-109A

November 13, 2025

Co-Authored by:

National Cyber Security Centre
Ministry of Justice and Security

Baden-Württemberg
LANDESKRIMINALAMT

Baden-Württemberg
GENERALSTAATSANWALTSCHAFT KARLSRUHE
CYBERCRIME-ZENTRUM

EUROPOL
EC3 | European Cybercrime Centre

OFAC
OFFICE ANTI-CYBERCRIMINALITÉ

#StopRansomware: Akira Ransomware

Actions for Organizations to Take Today to Mitigate Cyber Threats Related to Akira Ransomware Activity

- Prioritize remediating known exploited vulnerabilities.
- Enable and enforce phishing-resistant multifactor authentication (MFA).
- Maintain regular backups of critical data, ensure backups are stored offline, and regularly test the restoration process.

Summary

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

Note: Originally published April 18, 2024, this advisory was updated Nov. 13, 2025, with information on new Akira ransomware activity that presents an imminent threat to critical infrastructure. Updated information is labeled with "Update Nov. 13, 2025" at the beginning and "End Update" at the end of sections that include substantive new information, such as new Akira threat actor activity, TTPs, and IOCs.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact FBI's Internet Crime Complain Center (IC3) or your local FBI field office, or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Update Nov. 13, 2025:

The United States' Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Defense Cyber Crime Center (DC3), and Department of Health and Human Services (HHS); Europol's European Cybercrime Centre (EC3); France's Office Anti-Cybercriminalite (OFAC) – French Cybercrime Central Office; Germany's Generalstaatsanwaltschaft Karlsruhe – Cybercrime-Zentrum Baden-Württemberg and Landeskriminalamt Baden-Württemberg; and the Netherlands's National Cyber Security Centre (NCSC-NL)—hereafter referred to as the "authoring organizations"—are releasing this joint advisory to disseminate known Akira ransomware IOCs and TTPs identified through FBI investigations and trusted third-party reporting as recently as November 2025.

Akira ransomware threat actors are associated with other groups known as Storm-1567, Howling Scorpius, Punk Spider, and Gold Sahara, and may have connections to the defunct Conti ransomware group. Akira threat actors primarily target small- and medium-sized businesses, but have also impacted larger organizations across various sectors, with a notable preference for organizations in the manufacturing, educational institutions, information technology, healthcare and public health, financial services, and food and agriculture sectors.

End Update

Since March 2023, Akira ransomware threat actors have impacted a wide range of businesses and critical infrastructure entities in North America, Europe, and Australia. In April 2023, following an initial focus on Windows systems, Akira threat actors deployed a Linux variant targeting VMware Elastic Sky X Integrated (ESXi) virtual machines (VMs).

Update Nov. 13, 2025:

In a June 2025 incident, Akira threat actors encrypted Nutanix AHV VM disk files for the first time, expanding their capabilities beyond VMware ESXi and Hyper-V by abusing Common Vulnerabilities and Exposures (CVE)-2024-40766 [Common Weakness Enumeration (CWE)-284: Improper Access Control], a SonicWall vulnerability. As of late September 2025, Akira ransomware has claimed approximately $244.17 million (USD) in ransomware proceeds.

End Update

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

The authoring organizations encourage organizations to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of Akira ransomware incidents.

For a downloadable copy of IOCs, see:

- AA24-109A (STIX XML, # KB) (November 2025)
- AA24-109A (STIX JSON, # KB) (November 2025)

For a downloadable copy of historic IOCs, see:

- AA24-109A (STIX XML, 82KB) (April 2024)
- AA24-109A (STIX JSON, 55KB) (April 2024)

Table of Contents

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 18. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for tables with the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Initial Access

FBI and cybersecurity researchers[1] observed Akira threat actors obtaining initial access to organizations through a virtual private network (VPN) service without MFA configured,[2] mostly using known Cisco product Common Vulnerabilities and Exposures (CVEs) [T1190], including:

- CVE-2020-3259 [Common Weakness Enumeration (CWE)-200: Exposure of Sensitive Information to an Unauthorized Actor];
- CVE-2023-20269 [CWE-288: Authentication Bypass Using an Alternate Path or Channel];

Update Nov. 13, 2025:

- CVE-2020-3580 [CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')];[3]
- CVE-2023-28252 [CWE-122: Heap-based Buffer Overflow];[4] and
- CVE-2024-37085 [CWE-305: Authentication Bypass by Primary Weakness].[5]

Additionally, the authoring organizations observed Akira threat actors using these CVE exploits for initial access:

- CVE-2023-27532 [CWE-306: Missing Authentication for Critical Function];
- CVE-2024-40711 [CWE-502: Deserialization of Untrusted Data]; and
- CVE-2024-40766 [CWE-284: Improper Access Control].

End Update

For initial access, Akira threat actors also use techniques including spearphishing [T1566.001][T1566.002], abusing valid credentials [T1078], and techniques that leverage external-facing services, like Remote Desktop Protocol (RDP) [T1133].[6]

Update Nov. 13, 2025:

Akira threat actors gain access to VPN products, such as SonicWall, by stealing login credentials or exploiting vulnerabilities like CVE-2024-40766. In some instances, they gain initial access through compromised VPN credentials, potentially by using initial access brokers or brute-forcing VPN endpoints [T1110]. Additionally, Akira threat actors deploy password spraying techniques, using tools such as SharpDomainSpray to gain access to account credentials [T1110.003].

In other incidents, indicators suggest that Akira threat actors gained initial access through the Secure Shell (SSH) protocol by exploiting a router's IP address [T1021.004]. After tunneling through a targeted router, Akira threat actors exploit publicly available vulnerabilities, such as those found in the Veeam Backup and Replication component of unpatched Veeam backup servers [T1068] (CVE-2023-27532 and CVE-2024-40711).[7]

End Update

Execution

Update Nov. 13, 2025:

Akira threat actors frequently execute malicious commands by using Visual Basic (VB) scripts (event-driven programming languages that allow documents to contain macros to improve functionality through autonomous task execution) [T1059.005].

End Update

Persistence and Discovery

Once initial access is achieved, Akira threat actors attempt to establish persistence by creating new domain accounts [T1136.002] to abuse the functions of domain controllers. In some instances, the authoring organizations identified Akira threat actors creating an administrative account named `itadm`.

According to the authoring organizations and open source reporting, Akira threat actors leverage post-exploitation techniques, such as Kerberoasting,[8] to extract credentials stored in the process memory of the Local Security Authority Subsystem Service (LSASS)[9] [T1003.001]. Akira threat actors also use credential scraping tools [T1003], like Mimikatz and LaZagne, to aid in privilege escalation. For network discovery and reconnaissance, actors use tools like SoftPerfect, Advanced IP Scanner, and NetScan [T1016]. `net` Windows commands [T1059.003] are used to identify domain controllers [T1018] and gather information on domain trust relationships [T1482].

See **Table 1** for a descriptive listing of tools leveraged for malicious purposes by Akira threat actors.

Update Nov. 13, 2025:

The authoring organizations observed Akira threat actors using `nltest /dclist:` and `nltest /DOMAIN_TRUSTS` [T1018][T1482] for network and domain discovery.

End Update

Defense Evasion

As Akira threat actors prepare for lateral movement, they commonly disable security software to avoid detection. Cybersecurity researchers observed Akira threat actors using PowerTool to exploit the Zemana AntiMalware driver[10] and terminate antivirus-related processes [T1562.001].

Update Nov. 13, 2025:

In addition, the authoring organizations observed Akira threat actors abusing remote access tools such as AnyDesk and LogMeIn [T1219] to maintain persistence and blend in with administrator activity. Akira threat actors leverage Impacket (an open source tool designed for network protocol manipulation) to execute the remote command `wmiexec.py`. To evade detection, Akira threat actors implement techniques such as uninstalling endpoint detection and response (EDR) systems [T1562.001].

End Update

Privilege Escalation

Update Nov. 13, 2025:

The authoring organizations observed Akira threat actors creating new user accounts and adding them to the administrator group to establish a foothold in the environment [T1136.001]. In a reported incident, Akira threat actors bypassed Virtual Machine Disk (VMDK) file protection by temporarily powering down the domain controller's VM, copying the VMDK files, and attaching them to a newly created VM. This sequence of actions enabled them to extract the `NTDS.dit` file and the SYSTEM hive, ultimately compromising a highly privileged domain administrator's account [T1003.002][T1003.003].[11] Akira threat actors have also been observed leveraging services like `Veeam.Backup.MountService.exe` for privilege escalation (CVE-2024-40711) [T1068].

End Update

Lateral Movement

Update Nov. 13, 2025:

To pivot laterally, Akira threat actors use legitimate remote access tools like AnyDesk or LogMeIn [T1219]. They also employ RDP [T1021.001], SSH [T1021.004], and MobaXterm to expand their presence within the compromised network [T1021].

End Update

Command and Control

Update Nov. 13, 2025:

Based on observations from the authoring organizations and trusted third-party reporting, it has been determined that Megazord has likely fallen out of use since 2024.[12]

End Update

Trusted third-party investigations revealed that Akira threat actors deployed two distinct ransomware variants against different system architectures during one attempted compromise. Analysts first identified Akira threat actors deploying the Windows-specific "Megazord" ransomware, and further investigation revealed the threat actors concurrently deployed a second payload during the attack, later identified as a novel variant of the Akira ESXi encryptor, `Akira_v2`.

Update Nov. 13, 2025:

The authoring organizations observed Akira threat actors establishing command and control (C2) communications by using tunneling utilities, such as Ngrok [T1572], to initiate encrypted sessions that bypass perimeter monitoring. They also use PowerShell and Windows Management Instrumentation Command-line (WMIC) [T1059.001] to disable services and execute malicious scripts.

End Update

Exfiltration and Impact

Akira threat actors leverage tools such as FileZilla and WinRAR to collect data [T1560.001] and WinSCP and RClone to exfiltrate data [T1048]. To establish C2 channels, threat actors leverage readily available tools like AnyDesk, MobaXterm, RustDesk, and Cloudflare Tunnel. These tools enable exfiltration through various protocols such as File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), and cloud storage services like Mega [T1537], to connect to exfiltration servers. In some instances, Akira threat actors use Ngrok to create secure tunnels for data exfiltration [T1090].

After exfiltrating data, Akira threat actors use a double-extortion model [T1657], which involves threat actors both encrypting systems [T1486] and threatening to leak sensitive information. The Akira ransom note provides each company with a unique code and instructions to contact the threat actors via a `.onion` URL, which is accessible through the Tor network [T1090.003][T1573.002].

(**Note:** Tor, short for The Onion Router, is a decentralized network designed to anonymize internet traffic by routing it through multiple servers, encrypting data at each step. This network is often leveraged by threat actors to conceal their identities and activities, enabling secure and anonymous communication channels for malicious purposes, such as ransomware negotiations.)

Akira threat actors do not leave an initial ransom demand or payment instructions on compromised networks and do not relay this information until contacted by the victim. Victims make ransom payments by using Bitcoin to cryptocurrency-wallet addresses provided by the Akira threat actors. To further apply pressure, Akira threat actors threaten to publish exfiltrated data on the Tor network, and in some instances have called victimized companies, according to FBI reporting.

Update Nov. 13, 2025:

In some incidents, Akira threat actors exfiltrated data in just over two hours from initial access.[13]

End Update

Encryption

Akira threat actors use a sophisticated hybrid encryption scheme to lock data. This involves combining a ChaCha20 stream cipher with an RSA public-key cryptosystem for a fast and secure key exchange [T1486]. This multilayered approach customizes encryption methods based on file type and size, and enables full or partial encryption. Encrypted files are appended with a `.akira` or `.powerranges` extension.

Update Nov. 13, 2025:

With the new `Akira_v2` variant, encrypted files are appended either with an `.akira` or `.powerranges` extension, or with `.akiranew` or `.aki`.

End Update

To further inhibit system recovery and impede forensic analysis, Akira's encryptor (`w.exe`) uses PowerShell commands to delete Volume Shadow Copy Service (VSS) copies on Windows systems [T1490].

Update Nov. 13, 2025:

Additionally, a ransom note named `fn.txt` or `akira_readme.txt` appears in both the root directory (`C:`) and each user's home directory (`C:\Users`).

End Update

Trusted third-party analysis determined the `Akira_v2` encryptor is an upgrade from its previous version and includes additional functionalities because it is written in Rust. Previous versions of the encryptor provided options to insert arguments at runtime, including:

- `- p –encryption_path` (targeted file/folder paths);
- `-s –share_file` (targeted network drive path);
- `-n –encryption_percent` (percentage of encryption); and
- `--fork` (create a child process for encryption).

Including threads allows the threat actors more granular control over the number of CPU cores in use, increasing the speed and efficiency of the encryption process. The `Akira_v2` encryptor also adds a layer of protection, using the Build ID as a run condition to hinder dynamic analysis. The encryptor is unable to successfully execute without the specific Build ID. `Akira_v2` also can deploy against only VMs using `vmonly` and stop running VMs with `stopvm` functionalities. After encryption, the Linux ESXi variant may include the file extension `akiranew` or an added file named `akiranew.txt` as a ransom note in directories where files were encrypted with the new nomenclature.

Leveraged Tools

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

Table 1. Tools Leveraged by Akira Ransomware Actors

Name	Description
AdFind	A command-line tool used to query and retrieve information from Active Directory [T1087.002].
Advanced IP Scanner	A network scanning tool used for reconnaissance that locates all computers on a network and conducts a scan of their ports. The program shows all network devices, gives access to shared folders, and provides remote control of computers (via RDP and Radmin) [T1046].
AnyDesk	Legitimate desktop support software used to obtain remote access to victim systems and for lateral movement, and support remote file transfer. The software can be maliciously used by threat actors to obtain remote access and maintain persistence [T1219].

Name	Description
LaZagne	An open source tool that enables users to recover stored passwords on Windows, Linux, and Mac OS X systems [T1555].
Mimikatz	A credential dumper that enables users to view and save authentication credentials, such as Kerberos tickets [T1550.002].
Ngrok	A reverse proxy tool [T1090] used to create a secure tunnel to servers behind firewalls or local machines without a public IP address.
PCHunter64	A tool used to acquire detailed process and system information [T1082].[14]
PowerShell	A cross-platform task automation solution used for various malicious activities, including deleting shadow copies, and, potentially, for credential harvesting. It is composed of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS [T1059.001].
RClone	A legitimate command-line program used to sync files with cloud storage services, such as Mega. Akira threat actors use it maliciously to exfiltrate data to compromised cloud services [T1567.002].
SoftPerfect	A network scanner (`netscan.exe`) used to ping computers, scan ports, discover shared folders, and retrieve information about network devices via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, SSH, and PowerShell. It also scans for remote services, registry, files, and performance counters [T1046].
WinRAR	Archive utility used to split compromised data into segments and to compress [T1560.001] files into `.RAR` format prior to exfiltration.
WinSCP	A free, open source FTP (including SSH FTP), WebDAV, Amazon S3, and secure copy protocol client. Akira threat actors use it to transfer data from a compromised network to actor-controlled accounts [T1048].
Update Nov. 13, 2025: 7-zip	A free, open source software that enables users to compress various file formats. Akira threat actors use an archive feature within the 7-zip tool to compress data to evade detection [T1027.015].[15]
FileZilla	An open source client that enables users to transfer files between servers. Akira threat actors use it maliciously for data exfiltration [T1048].[16]
LogMeIn	A legitimate remote access tool that Akira threat actors maliciously use to move laterally and establish persistence.

Name	Description
NetScan	A software suite used for IP address querying, Domain Name System (DNS) investigation, and port scanning. Akira threat actors use the tool maliciously for reconnaissance [T1046].[17]
Ngrok	A legitimate reverse proxy tool. Akira threat actors maliciously use this tool to create secure tunnels to servers they use for data exfiltration [T1572].
NetExec	Linux-based network service exploitation tool that automates the assessment of large network security.
PowerTool	A tool used by Akira threat actors to exploit the Zemana AntiMalware driver and terminate antivirus processes [T1562.001].
PSEXESVC.exe	A Windows executable file potentially used by Akira threat actors for remote execution and payload deployments [T1569.002].
SystemBC	Multi-purpose malware that Akira threat actors use as both a remote access trojan (RAT) and a proxy bot [T1090][T1219].
Veeam Backup and Replication	A legitimate backup solution that Akira threat actors have exploited vulnerabilities in for initial access (and potentially for privilege escalation).
Cobalt Strike	A commercial penetration testing framework abused by Akira threat actors for lateral movement, C2, and privilege escalation [T1059.001].
PuTTY/PSCP	Variants of Secure Copy Protocol (SCP)/SFTP tools that can be used for data exfiltration or remote management [T1048].
Vssadmin.exe	A Windows executable used by Akira threat actors to delete VSS copies [T1490].
Level.io	A remote monitoring and management platform leveraged by Akira threat actors.
HeartCrypt	A packer-as-a-service obfuscation tool used by Akira threat actors to hinder analysis [T1027].
MEGA	A cloud storage utility used by Akira threat actors as the destination for exfiltrated data.
POORTRY	Malware written as a signed vulnerable Windows deriver. Akira threat actors used the malware to implement the Bring Your Own Vulnerable Driver (BYOVD) tactic [T1068].
STONESTOP	Malware that Akira threat actors used as the loader/installer for POORTRY [T1105].
SharpDomainSpray	A password spraying tool used by Akira threat actors.

Name	Description
OpenSSH	An open source SSH tool used by Akira threat actors for cross-platform remote management.
CLOUDFLARED	A legitimate, publicly available command-line client for Cloudflare Tunnel, a tunneling daemon that serves as a proxy for traffic from the Cloudflare network to the endpoints.
IMPACKET	A Python library that allows users to work with various network protocols. **End Update**

Indicators of Compromise

Disclaimer: These IOCs were observed between June 2023 and August 2025. The authoring organizations recommend vetting or investigating these IOCs prior to taking action, such as blocking.

See **Table 2** through **Table 9** for Akira ransomware IOCs.

Table 2: Malicious Files and SHA-256 Hash

File Name	Hash (SHA-256)	Description
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca	Akira ransomware encryptor.
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e	Akira ransomware encryptor.
Akira_v2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc	`Akira_v2` ransomware.
Megazord	dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065	Akira Megazord ransomware.

File Name	Hash (SHA-256)	Description
	2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0	
VeeamHax.exe	aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d	Plaintext credential leaking tool.
Veeam-Get-Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88	PowerShell script for obtaining and decrypting accounts from Veeam servers.
PowershellKerberosTicketDumper	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32	Kerberos ticket dumping tool from Local Security Authority (LSA) cache.
Update Nov. 13, 2025: Ladon.exe	58359209e215a9fc0dafd14039121398559790dba9aa2398c457348ee1cb8a4d	Akira ransomware file.
qKtul.vbs	cf3465d7e49b609defa1e2b6cfcc86ffa30c72246cb2744dbf50736c5f3d74d5	VBScript used by Akira ransomware.
s64.dll	58afef43cec0ee7a2fbfd9cdd5b71f55f971672d5e523a400b82b98c752ca5b7	Backdoor.
w.exe	bfd5fc6cd3dea74738ac7025fa14ea844f400708df2293572796568f65bd6b61	Encryptor.
1.bat	8e12c8eb39cec9a414b56a36acbcc1a5b31dc96a38bc668138a00f94f7c26ea5	Encryptor launcher.
2.exe	4DC9F9684F715F50946E85557B82AF80FCB45576EFAD47EEE1BF054C15E570F0	Malicious artifact.
akira.exe, win.exe	7266e2afb5c70788c018d684698b0940eded4cb863f2b33f4edd31b59d1eab1d	Ransomware.

File Name	Hash (SHA-256)	Description
w.exe	c0f706ff43936c1bb19db4f39b11129c3fc8ddafbd159852475ef99a246b2f79	Akira ransomware.
File.exe	3a25d3f82651567e5760e48ad06c9f6caab4f9fdc071e98919163b3a71e67168	Malicious artifact.
win_locker.exe	CFA209D56E296C40B32815270060E539963D68CDA3285C5F393C97EB3C960D37	Encryptor executable.
moe.exe	77d48e8c13ce066b197905cc8fc69969af69b74d25f5e95dcd1302ada2e7ccec	Malicious artifact. **End Update**

Update Nov. 13, 2025:

Table 3: Malicious Files and MD5 Hash

File Name	Hash (MD5)	Description
123.zip	57D1AEB41D9CFEA4D6899724BC4B09A5	Archive containing encryption malware and an AnyDesk setup.
All.bat	17c624693f5dd575485ec4286b0ba786	Encryption script.
w.exe	C56B31C9080B993D57C100B91D096C33	Akira ransomware.
w.exe	2FED7579556F01161BB1FDFD1C3E9E6C	Encryption script.
s.bat	24e19d29a47b6b5e1a39bf5e4c313194	Encryption script.
Start.bat	814310fb7a59f23e3e137ee6fee04fa1	Encryption script.

Table 4: Malicious Files and SHA-1 Hash

File Name	Hash (SHA 1)	Description
Vmware.exe	5961a99181df157b81d35a50eeb27f96577a2fa2	Akira encryptor.
w.exe	d5efaa22a74aab87d17f8666686b554e41fb389a	Akira ransomware.
w.exe	08CF869A19C76CA718BA80EF73636E7BC38218B8	Akira ransomware.
snaffler.exe	ef328f68c6d865ba4ef4223b5d8ee9efb5667420	Script used to enumerate sensitive data.

Table 5: Malicious File Descriptions

File Name	Description
Edge_server.exe	Akira artifact.
lck.exe	Akira ransomware file.
1.bat	Malicious batch file.
1.exe	Encryption script.
locker.exe	Encryption script.
Win_locker_0234-BMMNBW-MONC.exe	Encryption script.
level.exe	Trojanized `level.io` malicious payload.
level-windows-amd64.exe	Trojanized `level.io` malicious payload.

End Update

Note: Trusted third-party analysis confirmed the Akira threat actors' ransomware samples in Table 6 were created on Dec. 28, 2023.

Table 6. Windows Akira Ransomware Samples

Hash (SHA-256)
0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43
0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f
a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc
03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45
2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422
40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5
5ea65e2bb9d245913ad69ce90e3bd9647eb16d99230114537256548 6c77568a2
643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562
6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84
fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64

Table 7. Linux/Unix Akira Ransomware Executable and Linkable Format Samples

Hash (SHA-256)
e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f
74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4

Table 8. Commands Used for Discovery

Commands
`nltest /dclist:` [T1018]
`nltest /DOMAIN_TRUSTS` [T1482]
`net group “Domain admins” /dom` [T1069.002]
`net localgroup “Administrators” /dom` [T1069.001]
`tasklist` [T1057]

Table 9. Commands Used for Credential Access

Commands

`cmd.exe /Q /c esentutl.exe /y`
`"C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.defaultrelease\key4.db" /d`
`"C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.defaultrelease\key4.db.tmp”`
Note: Akira threat actors use these commands to access Firefox data.

`cmd.exe /Q /c esentutl.exe /y`
`"C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data" /d`
`"C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data.tmp”`
Note: Akira threat actors use these commands to access Google Chrome data.

`powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"` [T1490]

Commands
`rundll32.exe c:\Windows\System32\comsvcs.dll, MiniDump ((Get-Process lsass).Id) C:\windows\temp\lsass.dmp full` [T1003.001]

MITRE ATT&CK Tactics and Techniques

See Table 10 through **Table 21** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 10: Initial Access

Technique Title	ID	Use
Valid Accounts	T1078	Akira threat actors obtain and abuse credentials of existing accounts to gain initial access.
External Remote Services	T1133	Akira threat actors use remote access services, such as RDP or VPN connections, to gain initial access.
Exploit Public Facing Application	T1190	Akira threat actors exploit vulnerabilities in internet-facing systems to gain access to systems.
Phishing: Spearphishing Attachment	T1566.001	Akira threat actors use phishing emails with malicious attachments to gain access to networks.
Phishing: Spearphishing Link	T1566.002	Akira threat actors use phishing emails with malicious links to gain access to networks.

Table 11. Execution

Technique Title	ID	Use
Update Nov. 13, 2025 Command and Scripting Interpreter: PowerShell	T1059.001	Akira threat actors use PowerShell to execute malicious scripts and Living Off the Land Binary (LOLBin) commands for execution, persistence, credential harvesting, lateral movement, and disabling security controls to evade detection. After using Ngrok to establish encrypted sessions, Akira threat actors use PowerShell and WMIC to disable services and execute malicious scripts. Akira threat actors use commercial penetration testing tools, namely Cobalt Strike, during their operations to achieve lateral movement, perform C2 procedures, and gain elevated privileges.

Technique Title	ID	Use
		End Update
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Akira threat actors use the Windows command shell (`cmd.exe`) to run batch scripts and native commands for execution, persistence, lateral movement, and to disable or manipulate security controls for evasion.
Update Nov. 13, 2025 Command and Scripting Interpreter: Visual Basic	T1059.005	Akira threat actors use VB scripts to execute malicious code, deploy ransomware payloads, or establish persistence through legitimate Windows scripting capabilities.
System Services: Service Execution	T1569.002	Akira threat actors use `PSEXESVC.exe` to enable remote code execution and deploy payloads. **End Update**

Table 12. Persistence

Technique Title	ID	Use
Update Nov. 13, 2025 Account Manipulation	T1098	Akira threat actors modify account passwords.
Create Account: Local Account	T1136.001	Akira threat actors can create local user accounts by adding them to local admin groups to establish persistent backdoors. **End Update**
Create Account: Domain Account	T1136.002	Akira threat actors attempt to abuse the functions of domain controllers by creating new domain accounts to establish persistence.

Table 13. Privilege Escalation

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	Akira threat actors exploit unpatched software vulnerabilities (e.g., Veeam Backup and Replication CVEs) to gain elevated privileges on hosts or servers (enabling access to sensitive data), and for credential harvesting. **Update Nov. 13, 2025**

Technique Title	ID	Use
		Akira threat actors use POORTRY malware written as a signed vulnerable Windows driver to deploy BYOVD techniques to obtain elevated privileges. **End Update**

Table 14. Defense Evasion

Technique Title	ID	Use
Update Nov. 13, 2025 Obfuscated Files or Information	T1027	Akira threat actors obfuscate or encrypt malware, scripts, and network payloads (e.g., packers, Base64/XOR encoding, script obfuscation, or custom encryption) to evade detection and slow forensic analysis.
Obfuscated Files or Information: Compression	T1027.015	Akira threat actors use an archive feature within the 7-zip tool to compress data to evade detection.
Masquerading	T1036	Akira threat actors disguise malicious files and payloads to appear legitimate.
File and Directory Permissions Modification: Windows File and Directory Permissions Modification	T1222.001	Akira threat actors use the `takedown` command to assume ownership of directories and files and use the `icacls` command to modify discretionary access control lists. **End Update**
Impair Defenses: Disable or Modify Tools	T1562.001	Akira threat actors use a BYOVD technique to disable antivirus software. **Update Nov. 13, 2025** Akira threat actors use PowerTool to exploit Zemana AntiMalware driver and terminate antivirus defensive processes. Akira threat actors uninstall EDR systems to evade endpoint detection. **End Update**
Update Nov. 13, 2025 Impair Defenses: Disable or Modify System Firewall	T1562.004	Akira threat actors use the `allssh modify_firewall` command to open specific ports on the `eth0` interface.

Technique Title	ID	Use
Proxy Through Victim	T1604	Akira threat actors use a compromised device as a proxy server to conceal their malicious C2 infrastructure and associated IP address from network defenders. **End Update**

Table 15. Credential Access

Technique Title	ID	Use
OS Credential Dumping	T1003	Akira threat actors use tools like Mimikatz and LaZagne to dump credentials.
OS Credential Dumping: LSASS Memory	T1003.001	Akira threat actors attempt to access credential material stored in the process memory of LSASS.
Update Nov. 13, 2025 OS Credential Dumping: Security Account Manager	T1003.002	Akira threat actors dump the Windows security account manager (SAM) database to extract local account password hashes for offline cracking or pass-the-hash techniques, enabling lateral movement and privilege escalation on compromised hosts.
OS Credential Dumping: NTDS	T1003.003	Akira threat actors dump the Active Directory database (`NTDS.dit`) from compromised domain controllers to harvest domain credentials, enabling privilege escalation, lateral movement, and full domain takeover.
Brute Force	T1110	Akira threat actors gain access by brute-forcing VPN logins and SSH endpoints.
Brute Force: Password Spraying	T1110.003	Akira threat actors use tools like SharpDomainSpray for password spraying.
Credentials from Password Stores	T1555	Akira threat actors dump credentials from repositories like the Variable Bit Rate (VBR)-configuration database. Akira threat actors use LaZagne to recover stored passwords on Windows, Linux, and macOS systems.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	Akira threat actors use NetExec with the `--dpapi` option to dump credentials from the Windows Credential Manager and web browsers.

Technique Title	ID	Use
Credentials from Password Stores: Windows Credential Manager	T1555.004	Akira threat actors leverage tools such as NetExec or Mimikatz with the `-dpapi` option to dump credentials stored in the Windows Credential Manager, allowing them to gain unauthorized access to additional systems or accounts within the network. **End Update**

Table 16. Discovery

Technique Title	ID	Use
System Network Configuration Discovery	T1016	Akira threat actors use tools to scan systems and identify services running on remote hosts and local network infrastructure.
Remote System Discovery	T1018	Akira threat actors use `nltest /dclist:` to amass a listing of other systems by IP address, hostname, or other logical identifiers on a network.
Network Service Discovery	T1046	Akira threat actors use Advanced IP Scanner and NetScan to perform network reconnaissance by locating computers, scanning ports, identifying network devices, accessing shared folders, and enabling remote control via RDP and Radmin. Akira threat actors use SoftPerfect network scanners (`netscan.exe`) to perform discovery and retrieve network device information through WMI, SNMP, HTTP, SSH, and PowerShell.
Process Discovery	T1057	Akira threat actors use the `Tasklist` utility to obtain details on running processes via PowerShell.
Permission Groups Discovery: Local Groups	T1069.001	Akira threat actors use the `net localgroup /dom` to find local groups and permission settings.
Permission Groups Discovery: Domain Groups	T1069.002	Akira threat actors use the `net group /domain` command to find domain level groups and permission settings.
System Information Discovery	T1082	Akira threat actors use tools like PCHunter64 to acquire detailed process and system information. **Update Nov. 13, 2025**

Technique Title	ID	Use
		Akira threat actors use DiskCheck software to query remote systems for information on disk drives and installed software. **End Update**
Update Nov. 13, 2025 Account Discovery: Domain Account	T1087.002	Akira threat actors use `Adfind.exe` to query and retrieve information from Active Directory. **End Update**
Domain Trust Discovery	T1482	Akira threat actors use the `net` Windows command to enumerate domain information. **Update Nov. 13, 2025** Akira threat actors use `nltest /DOMAIN_TRUSTS` commands to enumerate domain trusts. **End Update**

Table 17. Lateral Movement

Technique Title	ID	Use
Update Nov. 13, 2025 Remote Services	T1021	Akira threat actors can abuse remote services (such as SSH and Virtual Network Computing [VNC]), to remotely access compromised systems, move laterally, and maintain persistence across networked hosts.
Remote Service: RDP	T1021.001	Akira threat actors leverage RDP connections as an initial access vector to victim systems.
Remote Service: SSH	T1021.004	Akira threat actors use SSHs through router IP addresses for initial access.
Use Alternate Authentication Material: Pass the Hash	T1550.002	Akira threat actors use Mimikatz to view and save authentication credentials, such as Kerberos tickets. **End Update**

Table 18. Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	T1560.001	Akira threat actors use tools like WinRAR to compress files.

Table 19. Command and Control

Technique Title	ID	Use
Proxy	T1090	Akira threat actors use Ngrok to create a secure tunnel to servers the actors use to exfiltrate data. **Update Nov. 13, 2025** Akira threat actors use SystemBC malware as a proxy bot. **End Update**
Update Nov. 13, 2025 Ingress Tool Transfer	T1105	Akira threat actors download tools, many of which are staged in the PerfLogs directory, and use the `WebClient.DownloadString()` method to download Cobalt Strike beacons. Akira threat actors use STONESTOP malware to load additional payloads. **End Update**
Remote Access Software	T1219	Akira threat actors use legitimate desktop support software like AnyDesk to obtain remote access to victim systems. **Update Nov. 13, 2025** Akira threat actors use SystemBC malware as a RAT. **End Update**
Update Nov. 13, 2025 Protocol Tunneling	T1572	Akira treat actors use Ngrok to hide C2 and remote access/exfiltrate traffic inside legitimate HTTPS connections, bypass perimeter defenses, and maintain covert persistent access. **End Update**

Table 20. Exfiltration

Technique Title	ID	Use
Exfiltration Over Alternative Protocol	T1048	Akira threat actors use file transfer tools like WinSCP to transfer data.
Transfer Data to Cloud Account	T1537	Akira threat actors use tools like CloudZilla to exfiltrate data to a cloud account and connect to exfiltration servers they control.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Akira threat actors leverage RClone to sync files with cloud storage services to exfiltrate data.

Table 21. Impact

Technique Title	ID	Use
Date Encrypted for Impact	T1486	Akira threat actors encrypt data on target systems to interrupt availability to system and network resources.
Inhibit System Recovery	T1490	Akira threat actors delete VSS copies on Windows systems.
Financial Theft	T1657	Akira threat actors use a double extortion model for financial gain.

Mitigations

The authoring organizations recommend organizations implement the mitigations below to improve their cybersecurity posture based on the threat actors' activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats and TTPs. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

Update Nov. 13, 2025:

For mitigations specific to K–12 schools, see CISA's guidance Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats.

End Update

The authoring organizations recommend organizations implement the following mitigations:

- **Prioritize remediating known exploited vulnerabilities** and keep all operating systems, software, and firmware up to date, as timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats; prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- Implement **identity, credential, and access management (ICAM) policies** across the organization and then **require MFA** for all services to the extent possible, particularly for webmail, VPNs, and accounts that access critical systems [CPG 2.H].
- **Require all accounts** with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with NIST's standards; require employees use long passwords and consider not requiring recurring password changes, as these can weaken security [CPG 2.C].
  - Use longer passwords consisting of at least 15 characters and no more than 64 characters in length [CPG 2.B].
  - Store passwords in hashed format using industry-recognized password managers.
  - Add password user "salts" to shared login credentials.
  - Avoid reusing passwords.

- Implement multiple failed login attempt account lockouts [CPG 2.G].
- Disable password "hints."
- Refrain from requiring password changes more frequently than once per year.
- **Note:** NIST guidance suggests favoring longer passwords instead of requiring frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.

- **Maintain offline backups of data** and regularly test and maintain backup and restoration processes [CPG 2.R]; implementing this practice helps organizations avoid severe operational interruptions and prevent scenarios in which data is irretrievable.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, or the cloud) [CPG 2.F, 2.R, 2.S].
- **Segment networks** to prevent the spread of ransomware, as network segmentation can help control traffic flows between and access to various subnetworks, and by restricting adversary lateral movement [CPG 2.F].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool** [CPG 3.A].
  - To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network.
  - EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Filter network traffic** by preventing unknown or untrusted origins from accessing remote services on internal systems; this prevents threat actors from directly connecting to remote access services that they have established for persistence.
- **Install, regularly update, and enable real-time detection for antivirus software** on all hosts.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 1.A, 2.O].
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 2.E].
- **Disable unused ports** [CPG 2.V].
- **Consider adding an email banner to emails** received from outside of your organization [CPG 2.M].
- **Disable hyperlinks** in received emails.
- **Implement time-based access for accounts set at the admin level and higher**; for example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust Maturity Model).
  - This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need.

- Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.

- **Disable command-line and scripting activities and permissions,** since privilege escalation and lateral movement often depend on software utilities running from the command line; if threat actors cannot run these tools, they will have difficulty escalating privileges and moving laterally [CPG 2.E, 2.N].
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

Validate Security Controls

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

Organizations should get started by following these steps:

1. Select an ATT&CK technique described in this advisory (Table 10 to Table 21).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program—including people, processes, and technologies—based on the data generated by this process.

The authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Resources

- Stopransomware.gov is a whole-of-government approach that provides one central location for ransomware resources and alerts.
- CISA's #StopRansomware Guide provides organizations with comprehensive best practices to mitigate the risk of ransomware attacks.
- CISA's Known Exploited Vulnerabilities Catalog is an authoritative resource for organizations to support improvement of their patch management best practices.
- CISA's Implementing Phishing-Resistant MFA is a fact sheet intended for network defenders to mitigate threats to accounts and systems that use MFA.

- CISA's Cyber Hygiene Services help organizations reduce the risk of a successful cyberattack.
- CISA's Cyber Security Evaluation Tool (CSET) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture; see Downloading and Installing CSET for step-by-step guidance to help your organization evaluate cybersecurity practices on your networks.
- CISA's Ransomware Risk Assessment helps assess an organization's ability to counteract a ransomware infection.
- Department of Health and Human Services' (HHS's) Cybersecurity Performance Goals is a resource to help healthcare organizations implement high-impact cybersecurity practices.

Reporting

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

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

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

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

U.S. Healthcare and Public Health sector organizations may report incidents to FBI or CISA, but also can reach out to HHS at HHScyber@hhs.gov for cyber incident support focused on mitigating adverse patient impacts.

German organizations may report incidents to Central Contact Points for Cybercrime (ZAC) by email at cybercrime@polizei.bwl.de, or by phone at +49 0711 5401-2444.

Netherlands organizations may report incidents by emailing NCSC-NL at cert@ncsc.nl.

French organizations may report incidents to the national police by telephone +39 0 805 805 817, or through the Office Anti-Cybercriminalite's (OFAC's) platform Pharos[18] to report illegal content on the internet, or their Thésée[19] platform to report online scams (including ransomware).

Disclaimer

The information in this report is being provided “as is” for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by FBI and co-sealers.

Acknowledgements

Cisco, Sophos, and Fortinet contributed to this advisory.

Version History

April 18, 2024: Initial version.

November 13, 2025: Updated to share recent TTPs and IOCs.

Notes

[1] Omar Santos, "Akira Ransomware Targeting VPNs without Multi-Factor Authentication," *Cisco Blogs* (blog), *Cisco*, last modified August 24, 2023, https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication; Heresh Zaremand, "Akira Ransomware and Exploitation of Cisco Anyconnect Vulnerability CVE-2020-3259," *Truesec* (blog), *Truesec*, last modified January 29, 2024, https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259; and Trend Micro Research, "Ransomware Spotlight: Akira," *Trend Micro*, October 5, 2023, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira.

[2] Shunichi Imano and James Slaughter, "Ransomware Roundup – Akira," *Fortinet* (blog), *Fortinet*, last modified April 24, 2024, https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira.

[3] Fortinet FortiGuard Threat Analysis Team, "Outbreak Alert: Akira Ransomware," *Fortinet FortiRecon*, last modified April 23, 2024, https://community.fortinet.com/t5/FortiRecon/Outbreak-Alert-Akira-Ransomware/ta-p/311056

[4] "Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption," *Microsoft Threat Intelligence* (blog), *Microsoft*, last modified July 29, 2024, https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/.

[5] "Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption."

[6] Trend Micro Research, "Ransomware Spotlight: Akira."

[7] Pierluigi Paganini, "Ransomware Groups Target Veeam Backup & Replication Bug," *Security Affairs*, July 15, 2024, https://securityaffairs.com/165753/malware/ransomware-groups-target-veeam-backup-replication-bug.html.

[8] Ryan Terry, "Kerberoasting Attacks: What They Are and How to Defend," *Cybersecurity 101: The Fundamentals of Cybersecurity*, *CrowdStrike*, last modified March 26, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/kerberoasting.

[9] Morgan Demboski, "Akira, again: The ransomware that keeps on taking," *Sophos News*, December 21, 2023, https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking.

[10] Trend Micro Research, "Ransomware Spotlight: Akira."

[11] Jamie Smith, "Privilege escalation: unravelling a novel cyber-attack technique," *IT Security Guru*, July 23, 2024, https://itsecurityguru.org/2024/07/23/privilege-escalation-unravelling-a-novel-cyber-attack-technique.

[12] James Nutland and Michael Szeliga, "Threat spotlight: Akira ransomware continues to evolve," Cisco Talos (blog), Cisco, last modified October 21, 2024, https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/.

[13] Steven Campbell, Akshay Suthar, and Stefan Hostetler, "Artic Wolf Labs Observes Increased Fog and Akira Ransomware Activity Linked to SonicWall SSL VPN," *Artic Wolf Labs* (blog), *Arctic Wolf*, October 24, 2024, https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn.

[14] Jaramillo, Paul, "Akira Ransomware is 'bringin' 1988 back,'" *Sophos*, May 9, 2023, https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/.

[15] Igor Pavlov, "7-Zip file archiver," 7-Zip, October 22, 2025, https://www.7-zip.org/.

[16] Katie Terrel Hanna, "What is FileZilla?" TechTarget, October 22, 2025, https://www.techtarget.com/whatis/definition/FileZilla.

[17] "NetScanTools Definition" Northwest Performance Software, October 22, 2025, https://www.netscantools.com/nstpromain.html.

[18] French organizations may report illegal content on the internet to OFAC's Pharos platform.

[19] French organizations may report online scams, including ransomware, to OFAC's Thésée platform.