

Akira Ransomware

250+ Organizations Impacted, \$42 Million Ransomware Toll

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>
 CVEs: [CVE-2023-20269](#), [CVE-2020-3259](#)

FortiGuard Labs continue to observe detections in the wild related to the Akira ransomware group. According to the new report by CISA it has targeted over 250 organizations since the past year, affecting numerous businesses and critical infrastructure entities across North America, Europe, and Australia. The gang has made over \$42 million from the attacks as ransom payments.

Background
 First detected in March/April of 2023, this ransomware group primarily focuses on small to medium-sized businesses, driven by financial motives. Like other notorious ransomware, Akira utilizes familiar tactics such as Ransomware-as-a-Service and double extortion to maximize their profits.

The ransomware uses virtual private network (VPN) service without multifactor authentication (MFA)- mostly using known Cisco vulnerabilities CVE-2020-3259 and CVE-2023-20269, external-facing services such as Remote Desktop Protocol, spear phishing, and the abuse of valid credentials.

These credentials are typically acquired through brute force attacks or obtained from the dark web. Once inside, threat actors deploy various tools and malware to conduct reconnaissance, dump credentials, exfiltrate data, and move laterally within the network.

Initial iterations of the Akira ransomware variant were coded in C++ and encrypted files with a .akira extension. However, from August 2023 onwards, certain Akira attacks transitioned to utilizing Megazord, featuring Rust-based code that encrypts files with a .powerranges extension. Akira threat actors persist in employing both Megazord and Akira, including the newer version, Akira_v2.

Latest Developments
 Fortinet has existing AV signatures and behaviour-based detections to detect and block Akira Ransomware, however it is always recommended to follow best practices and apply relevant patches to mitigate threat and reduce the likelihood/impact of ransomware incidents.

<https://www.fortinet.com/resources/cyberglossary/how-to-prevent-ransomware>

April 19, 2024: FortiGuard Labs released a Threat Signal
<https://www.fortiguard.com/threat-signal-report/5426>

April 18, 2024: The United States' Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL) are releasing this joint cyber security advisory (CSA):
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>

Feb 15, 2024: CISA added (CVE-2020-3259) Cisco ASA and FTD Information Disclosure Vulnerability to known exploited vulnerabilities catalog.

October 12, 2023: Fortinet released a detailed blog on Akira Ransomware
<https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira>

Sep 13, 2023: CISA added (CVE-2023-20269): Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability to its known exploited vulnerabilities catalog.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Weaponization

Delivery

AV

Detects known malware related to Akira Ransomware

 FortiGate DB 92.03523	 FortiWeb DB 92.03523	 FortiClient DB 92.03523	 FortiSASE DB 92.03523	 FortiMail DB 92.03523	 FortiCASB DB 92.03523	 FortiCWP DB 92.03523
 FortiADC DB 92.03523	 FortiProxy DB 92.03523					

AV (Pre-filter)

Detects known malware related to Akira Ransomware

 FortiEDR DB 92.03523	 FortiSandbox DB 92.03523	 FortiNDR DB 92.03523
-----------------------------	---------------------------------	-----------------------------

Behavior Detection

Detects unknown malware related to Akira Ransomware

 FortiSandbox

Exploitation

Pre-execution

Automated threat detection and response against advanced threats such as fileless threats and ransomware

 FortiEDR

Installation

Post-execution

Automated threat detection and response against advanced threats such as fileless threats and ransomware

 FortiEDR

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Threat Hunting

 FortiEDR

IOC

 FortiAnalyzer	 FortiSIEM	 FortiSOCaaS
-------------------	---------------	-----------------

Outbreak Detection

 FortiAnalyzer DB 2.00044	 FortiSOAR
---------------------------------	---------------

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

 FortiXDR

Playbook

 FortiSOAR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

 Incident Response	 FortiRecon: ACI
-----------------------	---------------------

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

 NSE Training	 Response Readiness
------------------	------------------------

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

 Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

 Security Rating

Business Reputation

Know attackers next move to protect against your business branding.

 FortiRecon: EASM

Additional Resources

- Ransomware Guide CISA <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>
- CISA Advisory <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>
- The Record <https://therecord.media/akira-ransomware-attacked-hundreds-millions>
- The Hacker news <https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html>
- Bleeping Computer https://www.bleepingcomputer.com/news/security/fbi-akira-ransomware-raked-in-42-million-from-250-plus-victims/#google_vignette
- Cisco Advisory (CVE-2020-3259) <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftrd-info-disclose-9e1jycMB>
- Cisco Advisory (CVE-2023-20269) <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftrd-ravpn-auth-8lYfCkeC>

Learn more about [FortiGuard Outbreak Alerts](#)