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

Background

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.

> 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.

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.

The ransomware uses virtual private network (VPN) service without multifactor authentication (MFA)- mostly using

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.

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 relavant patches to mitigate threat and

Latest Developments

https://www.fortinet.com/resources/cyberglossary/how-to-prevent-ransomware April 19, 2024: FortiGuard Labs released a Threat Signal

Centre (NCSC-NL) are releasing this joint cyber security advisory (CSA):

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

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

reduce the likelihood/impact of ransomware incidents.

https://www.fortiguard.com/threat-signal-report/5426

Feb 15, 2024: CISA added (CVE-2020-3259) Cisco ASA and FTD Information Disclosure Vulnerability to known exploited vulnerabilties catalog. October 12, 2023: Fortinet released a detailed blog on Akira Ransomware

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.

https://www.fortinet.com/blog/threat-research/ransomware-roundup-akira

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

Weaponization

Delivery

FortiSASE

DB 92.03523

FortiMail

DB 92.03523

FortiCASB

DB 92.03523

FortiCWP

DB 92.03523

Detects known malware related to Akira Ransomware

FortiGate

DB 92.03523

Reconnaissance

AV

FortiClient

DB 92.03523

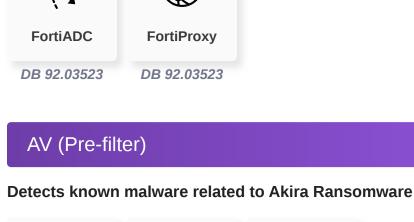
DB 92.03523

FortiWeb

DB 92.03523

FortiSandbox

DB 92.03523



FortiSandbox

Exploitation

Behavior Detection

DB 92.03523

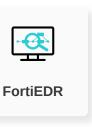
Detects unknown malware related to Akira Ransomware



FortiEDR

Installation

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



Post-execution

Action

C2

FortiEDR

Threat Hunting

DETECT

alert and generate reports:

IOC

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



FortiAnalyzer





FortiSIEM

FortiSOAR

FortiSOCaaS



FortiXDR

Playbook

undefined



FortiSOAR

Assisted Response Services

FortiRecon:

ACI

(and recovery from) security incidents:

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



RECOVER

NOC/SOC Training

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

Response

Readiness



Awareness & **Training**

End-User Training

and other forms of cyberattacks.

IDENTIFY

Attack Surface Hardening

Identify processes and assets that need protection:

NSE Training

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

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download

Improve security posture and processes by implementing security awareness and training, in preparation for



FortiRecon: **EASM**

Ransomware Guide CISA

The Record

The Hacker news

Business Reputation

Additional Resources

Know attackers next move to protect against your business branding.

CISA Advisory https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a https://therecord.media/akira-ransomware-attacked-hundreds-millions

Bleeping Computer https://www.bleepingcomputer.com/news/security/fbi-akira-ransomware-raked-in-42-million-from-250-plusvictims/#google_vignette

Cisco Advisory (CVE-2020-3259) https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

Cisco Advisory (CVE-2023https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC 20269)

https://www.cisa.gov/resources-tools/resources/stopransomware-guide

https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html

Learn more about FortiGuard Outbreak Alerts