Hive Pro

Threat Level

Red

CISA: AA24-109A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Akira Ransomware Nets $42 Million from 250+ Victims

Date of Publication	Admiralty Code	TA Number
April 30, 2024	A1	TA2024167

Summary

Attack Commenced: March 2023
Malware: Akira Ransomware
Attack Region: Worldwide
Targeted Industries: Automotive, Manufacturing, Transportation, Technology, Healthcare, Construction, Engineering, Financial, Legal, Energy, Telecommunications, Electronics
Attack: The Akira ransomware group has become notorious for its malicious activities, having accrued a staggering $42 million through unauthorized means by infiltrating the networks of over 250 victims as of January 2024.

Attack Timeline

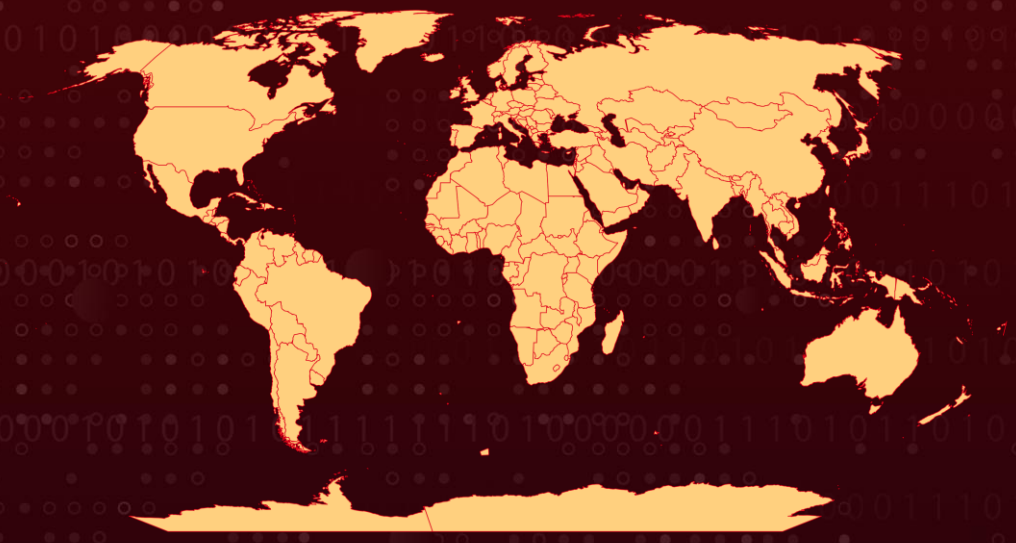
March 2023
Akira ransomware has affected a broad spectrum of businesses and critical infrastructure

April 2023
Akira deployed a **Linux variant** that targeted VMware ESXi virtual machines

August 2023
Akira attacks have introduced **Megazord**, employing Rust-based code that encrypts files with a **.powerranges** extension

January 1, 2024
Akira has impacted over **250** organizations and claimed approximately **$42 million USD in ransom**

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-3259	Cisco ASA and FTD Information Disclosure Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	✗	✓	✓
CVE-2023-20269	Cisco Brute Access Vulnerability	Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD)	✓	✓	✓

Attack Details

#1 The Akira ransomware group, known for its malicious activities, has amassed a staggering $42 million through unauthorized means by infiltrating the networks of more than 250 victims as of January 1, 2024. Initially, they used C++ to create their ransomware, encrypting files with a .akira extension.

#2 However, starting in August 2023, some Akira attacks shifted to using the Windows-specific Megazord, which employs Rust-based code to encrypt files with a .powerranges extension. Interestingly, Akira threat actors continue to employ both Megazord and Akira variants.

#3 Their entry into target networks is often facilitated by exploiting well-known vulnerabilities such as CVE-2020-3259 and CVE-2023-20269 in Cisco appliances. They also utilize other methods such as Remote Desktop Protocol (RDP) breaches, spear-phishing, gaining access through valid credentials, and exploiting virtual private network (VPN) services lacking multi-factor authentication (MFA) protections.

#4 To avoid detection while moving laterally within networks, Akira threat actors frequently disable security software. Moreover, like other modern ransomware, the Akira ransomware executable is equipped with a feature aimed at hindering system recovery by deleting shadow copies from the affected system.

Recommendations

Patch Management: Prioritize timely patching of known vulnerabilities, especially those like CVE-2020-3259 and CVE-2023-20269 in Cisco appliances, which are exploited by Akira threat actors for initial access.

Hardening Endpoints: Apply security hardening measures to endpoints, servers, and other critical systems, including disabling unnecessary services, applying least privilege access controls, and enforcing strong password policies.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Monitoring and Logging: Implement robust monitoring and logging mechanisms to detect suspicious activity or unauthorized access to your accounts. Regularly review access logs and audit trails for unusual patterns or login locations.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
TA0040 Impact	T1190 Exploit Public-Facing Application	T1133 External Remote Services	T1566.001 Spearphishing Attachment
T1566.002 Spearphishing Link	T1003 OS Credential Dumping	T1003.001 LSASS Memory	T1016 System Network Configuration Discovery

T1082 System Information Discovery	**T1482** Domain Trust Discovery	**T1057** Process Discovery	**T1069.001** Local Groups
T1069.002 Domain Groups	**T1018** Remote System Discovery	**T1136.002** Domain Account	**T1562.001** Disable or Modify Tools
T1219 Remote Access Software	**T1090** Proxy	**T1560.001** Archive via Utility	**T1048** Exfiltration Over Alternative Protocol
T1537 Transfer Data to Cloud Account	**T1567.002** Exfiltration to Cloud Storage	**T1486** Data Encrypted for Impact	**T1490** Inhibit System Recovery
T1657 Financial Theft	**T1078** Valid Accounts		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca, dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e, bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138, 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf, 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386, aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9, 7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4, 36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c, 3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75, 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c, ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc,

TYPE	VALUE
SHA256	dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198, 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07, 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c, 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065, 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83, 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be, 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a, 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d, C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0, aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d, 18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88, 5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32, 8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694, 892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0, 0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43, 0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc, 03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45, 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422, 40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5, 5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2, 643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562, 6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84,

TYPE	VALUE
SHA256	fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64, e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f, 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1, 3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4
MD5	7a647af3c112ad805296a22b2a276e7c

Patch Links

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

Recent Breaches

https://lotztrucking.com
https://www.studiolambda.com
https://medequip.com
https://sbsmn.com
https://samart.com
https://consilux.com.br
https://inspectionservices.com
https://radiantcanada.com

References

https://www.cisa.gov/sites/default/files/2024-04/aa24-109a-stopransomware-akira-ransomware_2.pdf

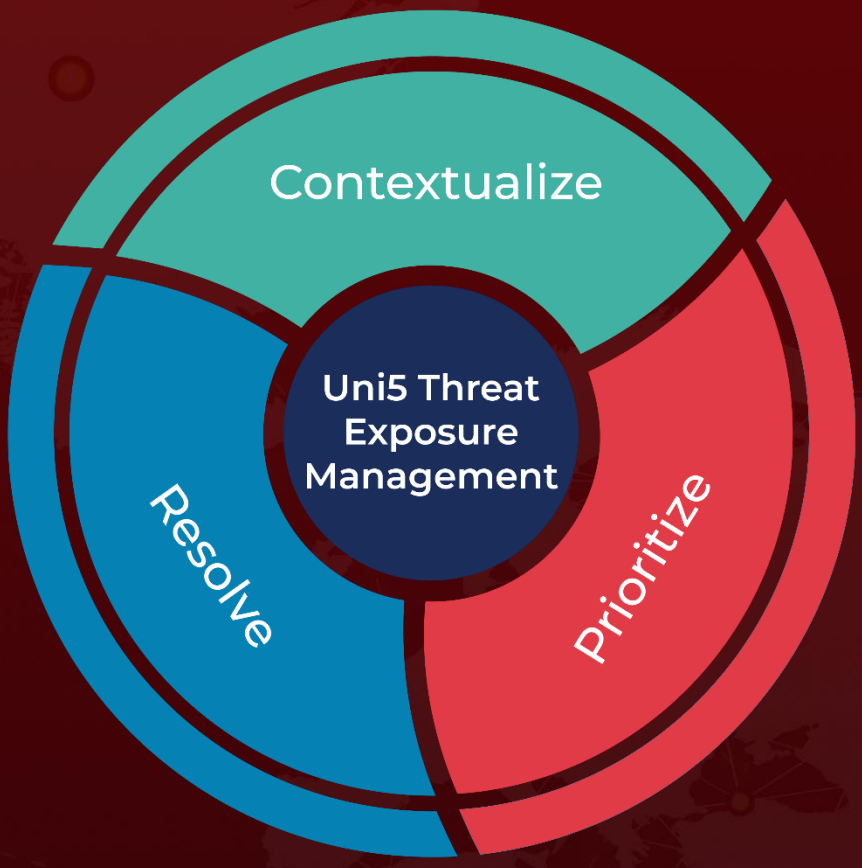
https://www.hivepro.com/threat-advisory/akira-ransomware-exploits-cisco-flaw-for-maximum-impact/

https://www.hivepro.com/threat-advisory/akira-ransomware-exploits-cisco-zero-day-vulnerability

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 30, 2024 • 3:00 AM

More at www.hivepro.com