Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

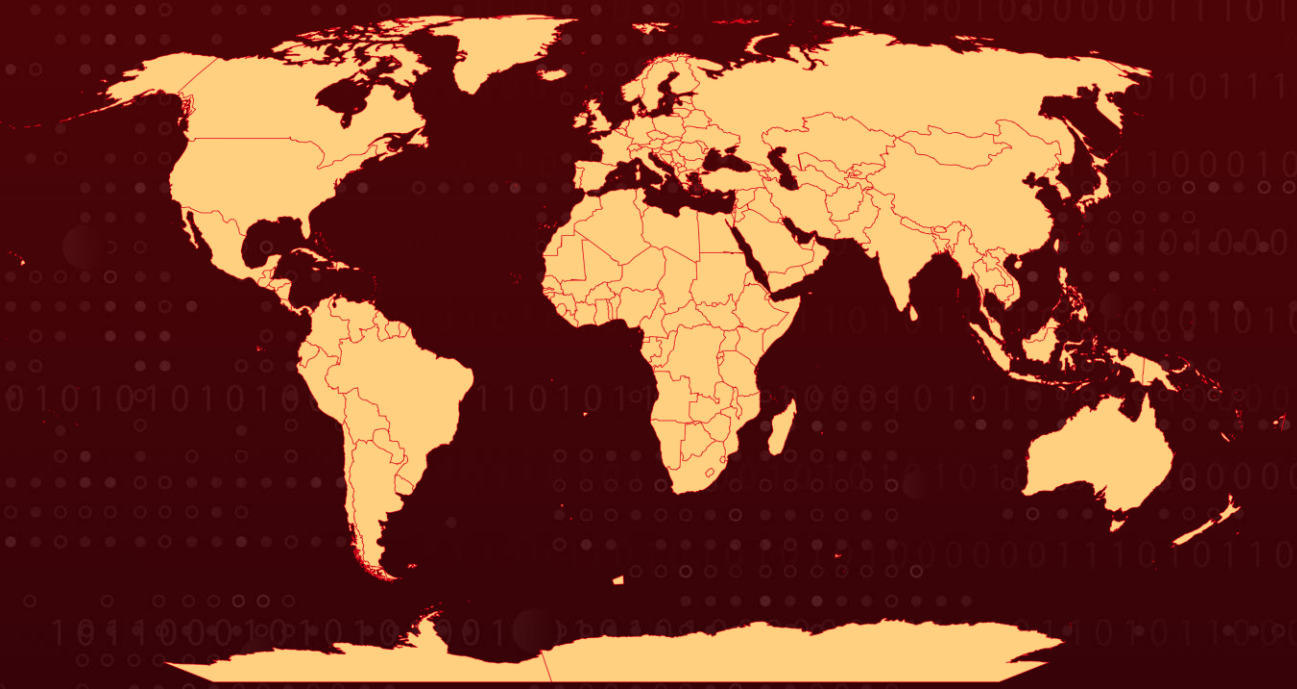
New Wave of Akira Ransomware Expands Arsenal with Cisco VPN Flaws

Date of Publication	Admiralty Code	TA Number
August 23, 2023	A1	TA2023341

Summary

First Appearance: March, 2023
Attack Region: Worldwide
Affected Platform: Windows, Linux, macOS and VMware
Malware: Akira ransomware
Attack: The Akira ransomware group targets Cisco VPN products to breach corporate networks and leverages tools like RustDesk for stealthy access. Avast's decryptor is ineffective against the group's updated ransomware versions

Attack Regions



Attack Details

#1 Akira, a relatively new ransomware operation, emerged in March 2023 and is written in C++. It has expanded its tactics by adding a Linux encryptor to target VMware virtual machines. This group has been leveraging compromised Cisco VPN accounts to breach corporate networks without needing additional backdoors or persistence mechanisms.

#2 The attack strategy involves exploiting weak authentication, potentially through brute force or purchasing credentials on the dark web. Researchers have also considered the possibility that Akira might be exploiting an unknown vulnerability in Cisco VPN software.

#3 Akira's attacks have been observed in multiple instances, often utilizing Cisco VPN gateways. Notably, they have adopted the use of RustDesk, a legitimate open-source remote access tool, to navigate through compromised networks stealthily. This tool's cross-platform compatibility and encrypted P2P connections allow Akira to maintain a low profile and facilitate data exfiltration.

#4 The group has also employed various tactics and techniques, such as manipulating SQL databases, disabling firewalls and enabling remote desktop protocol (RDP), and undermining security measures like LSA Protection and Windows Defender. Avast released a decryptor for Akira ransomware in June 2023, but the group has since updated its encryptors, rendering the tool effective only against older versions of the ransomware.

Recommendations

Implement Multi-Factor Authentication (MFA): Ensure that all Cisco VPN accounts are protected by multi-factor authentication. This additional layer of security can significantly reduce the risk of unauthorized access, even if passwords are compromised.

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software with some focus on Cisco VPN. This helps patch vulnerabilities that adversaries can exploit.

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom.

Protect your Backups: Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0042 Resource Development	TA0005 Defense Evasion	TA0009 Collection
TA0002 Execution	TA0003 Persistence	TA0043 Reconnaissance	TA0011 Command and Control
T1110 Brute Force	T1589.001 Credentials	T1589 Gather Victim Identity Information	T1059 Command and Scripting Interpreter
T1584 Compromise Infrastructure	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits
T1036 Masquerading	T1219 Remote Access Software	T1040 Network Sniffing	T1562.001 Disable or Modify Tools
T1562 Impair Defenses			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	24e7848dab0b82b200781630e617d6ed7e6016e7, 2cde82cf7a1bc88c8fc5865cb57f31f6437f74fc, 30d49ced95cb9a0fb6526b30131501b28cbbc388, 5e6d77960065df450e0533f9a8409c7463292243, 688d67eb4ff993963c86297ab8345962334ead27, 76beb70b06cfe714c4fa250b6b2d1e5025fe3c50, 843f3ad221a9da48d82df672bd8806cc090430b5, 9180ea8ba0cdfe0a769089977ed8396a68761b40, 923161f345ed3566707f9f878cc311bc6a0c5268, 9a14a69eb279513cde2de0be538cc8d275fd34e9, bdb3fa0c50db18f7ada02b2060b4c5110016e859, db9ba4f42942b27e1690c6d8a1bbd5b9d188fe49, f070a115100559dcaf31ce34d9e809a3134b2511, f2e6853050f76517a9a7d472f3a994d0ae8411cf

TYPE	VALUE
MD5	302f76897e4e5c8c98a52a38c4c98443, 431d61e95586c03461552d134ca54d16, af95fbcf9da33352655f3c2bab3397e2, c7ae7f5becb7cf94aa107ddc1caf4b03, d25890a2e967a17ff3dad8a70bfdd832, e44eb48c7f72ffac5af3c7a37bf80587
IPv4	172.82.86.148, 195.123.234.101
Domain	akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion
SHA256	89f5f29cf6b5bcfc85b506fb916da66cb7fd398cf6011d58e9409c7813e1a6f3, 27009c0abd2709cd5cac4c0135b8f3bed3229b0921601638ba9e90713ede91ea, 379ef7c4f6dfae8cc0c8556861ff41930b88c7d9b107a5de10ccd194e1bda0cb, 8738ba49fcd520789569aea7bf7af890741a745c79ae2bef49b93fb46c076c2b, d371ee0aa4fa710c00173d296c999a5497a18b38c80095db68a2dc5e46ed35f7, 2a9257c6c74e37d051f78ed5abaa620b71b27fa3604798af077256a128d911bb, 3f4ceeada7ff021c30df1646437d2ab0e55997bbb281444501f6d1f4ea8fa209, fb2433beb961839b36198e242d0dedb7fa85ab3e08a1141d02874aa4235ac776, c239dadd55b55b817fda5b0c2bb062adf399a5b78a8b3280a473d3ae66f81777, 4cb8365b18b1c319d374be0b9d219144c20fb8714e9cf346e655f854d2c60170, 772eb611c9ca20b461536fd0bd87d553dcecf3f4c82e26c2378cad40bbf4b0b0, 2e2ad6392e75d5a5155498c2a76cb373d17ca3ad4ba57c6d33c623fca5e29342, 1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296, 367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9, 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c, 4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda, 619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4,

TYPE	VALUE
SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488, 8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50, 99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba, a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce, b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa, c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598, d793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee

Recent Breaches

http://www.tallyenergy.com/

https://www.crunchbase.com/organization/cequint

http://clifton.k12.nj.us/

https://rimss.com/

References

https://twitter.com/cverc_cn/status/1694181917779017975

https://twitter.com/SecurityAura/status/1687960096758726656

https://www.bleepingcomputer.com/news/security/akira-ransomware-targets-cisco-vpns-to-breach-organizations/

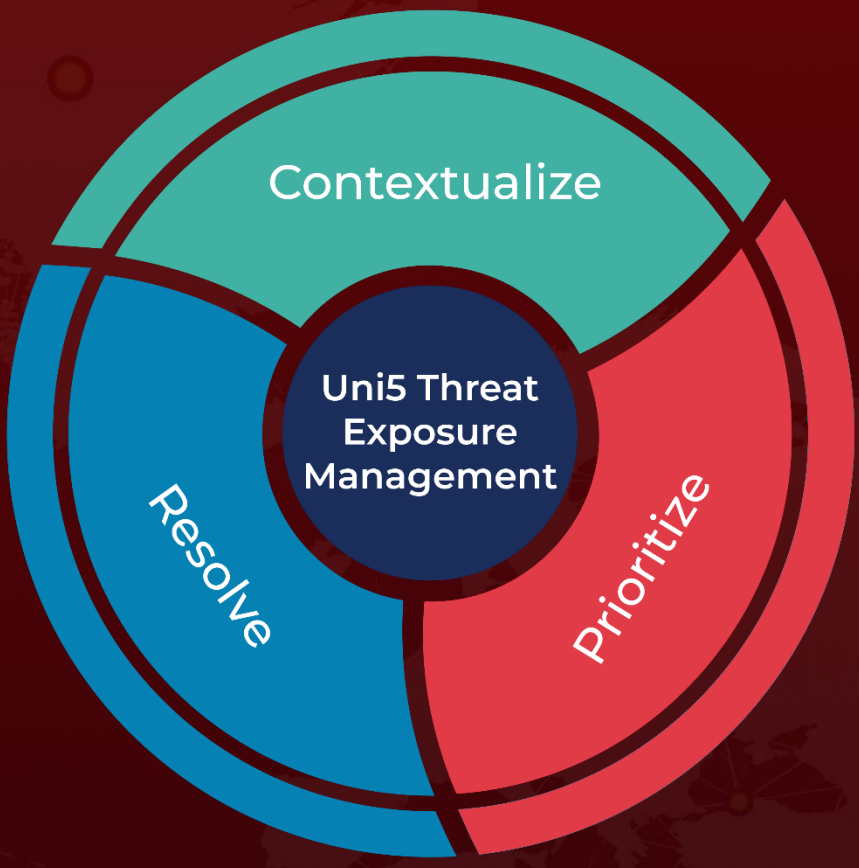
https://decoded.avast.io/threatresearch/decrypted-akira-ransomware/

https://www.hivepro.com/a-new-akira-ransomware-targets-multiple-industries-and-demands-millions-in-extortion/

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

August 23, 2023 • 7:40 AM

More at www.hivepro.com