Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

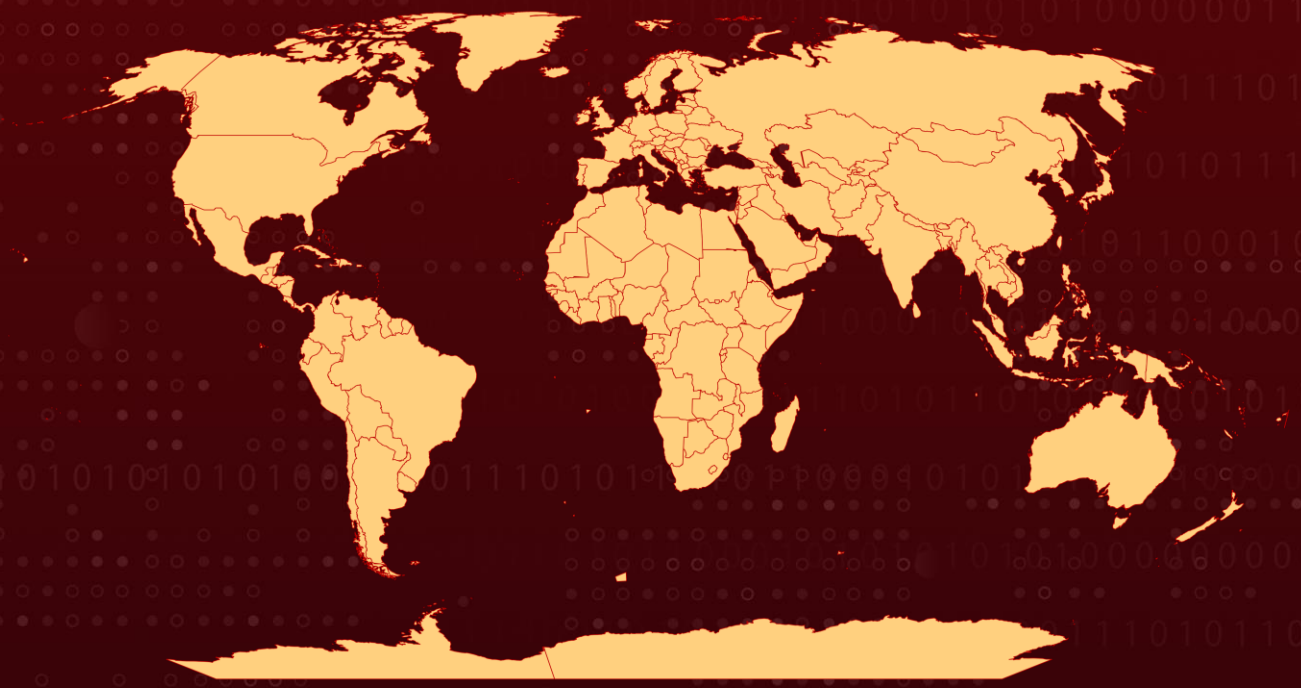
A New Akira Ransomware Targets Multiple Industries and Demands Millions in Extortion

Date of Publication	Admiralty Code	TA Number
May 09, 2023	A1	TA2023217

Summary

First Appearance: March 2023
Targeted Countries: Worldwide
Malware: Akira ransomware
Ransom Demands: $200,000 to $1,000,000
Targeted Industries: Finance, education, real estate, manufacturing, and consulting
Affected Platforms: Windows
Attack: Akira ransomware is a new threat targeting corporate networks and has already attacked several companies in various industries, stealing their data and demanding varying ransom amounts.

Attack Regions



Attack Details

#1 Akira, a new ransomware operation, is attacking corporate networks and encrypting files. It has already targeted sixteen companies in finance, education, real estate, manufacturing, and consulting, among other industries. The ransomware deletes Windows Shadow Volume Copies and encrypts files, skipping those found in Windows folders.

#2 Negotiations occur through a chat system that allows victims to negotiate with the Akira gang. Before encrypting files, the gang steals corporate data, using it as leverage in their extortion attempts. They threaten to release the data publicly if the ransom is not paid.

#3 The ransom demands vary, from $200,000 to millions of dollars, depending on the victim. The ransomware operation remains a significant threat to companies worldwide, and paying the ransom is not advisable until a free decryptor can recover files. Although ransomware called Akira was introduced in 2017, there is no indication that it is connected to the current Akira ransomware operation.

Recommendations

To identify whether your system has been affected by Akira ransomware, it's crucial to look for the presence of akira.exe, as well as any unusual activities or processes that could indicate a ransomware attack, such as encrypted files or ransom notes.

Preventive measures include keeping all security patches and antivirus software updated, using signatures or heuristics to detect malicious software, blocking code execution through application control or script blocking, managing privileged accounts, and utilizing capabilities to prevent suspicious behavior patterns. Regularly backing up data can also aid in recovery from a ransomware attack.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0040 Impact
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	T1490 Inhibit System Recovery
T1529 System Shutdown/Reboot	T1106 Native API	T1569 System Services	T1027 Obfuscated Files or Information
T1059 Command and Scripting Interpreter	T1059.001 Power Shell	T1486 Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4

References

https://cyberdaily.securelayer7.net/akira-the-new-ransomware/

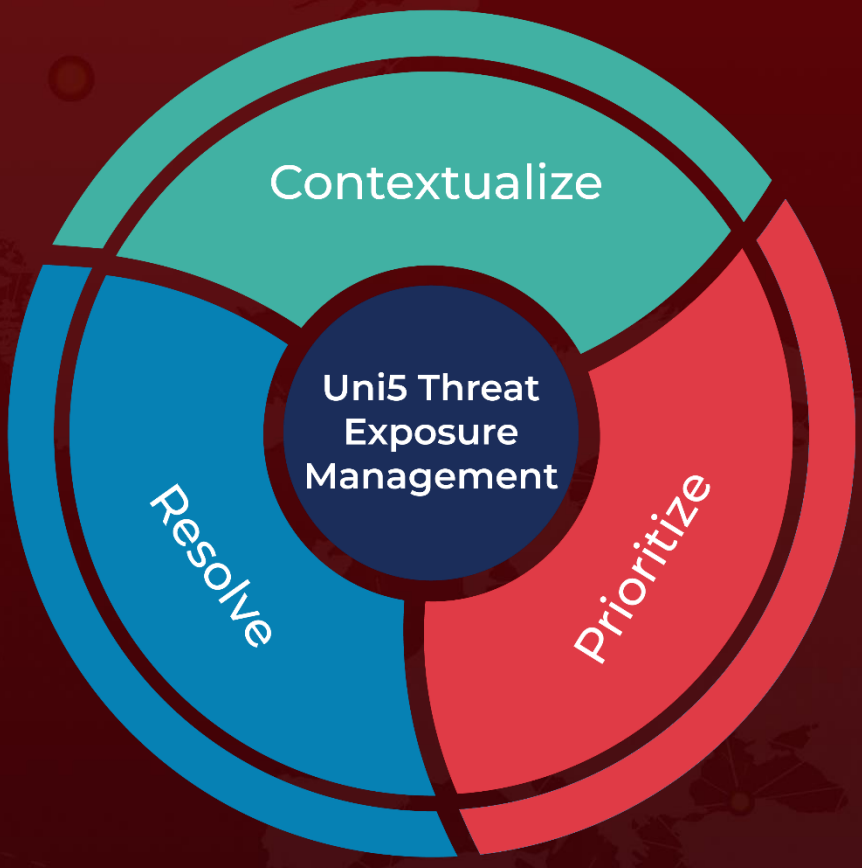
https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/

https://nologs-nobreach.com/2023/04/29/akira-ransomware/

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

May 09, 2023 • 4:30 AM

More at www.hivepro.com