Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

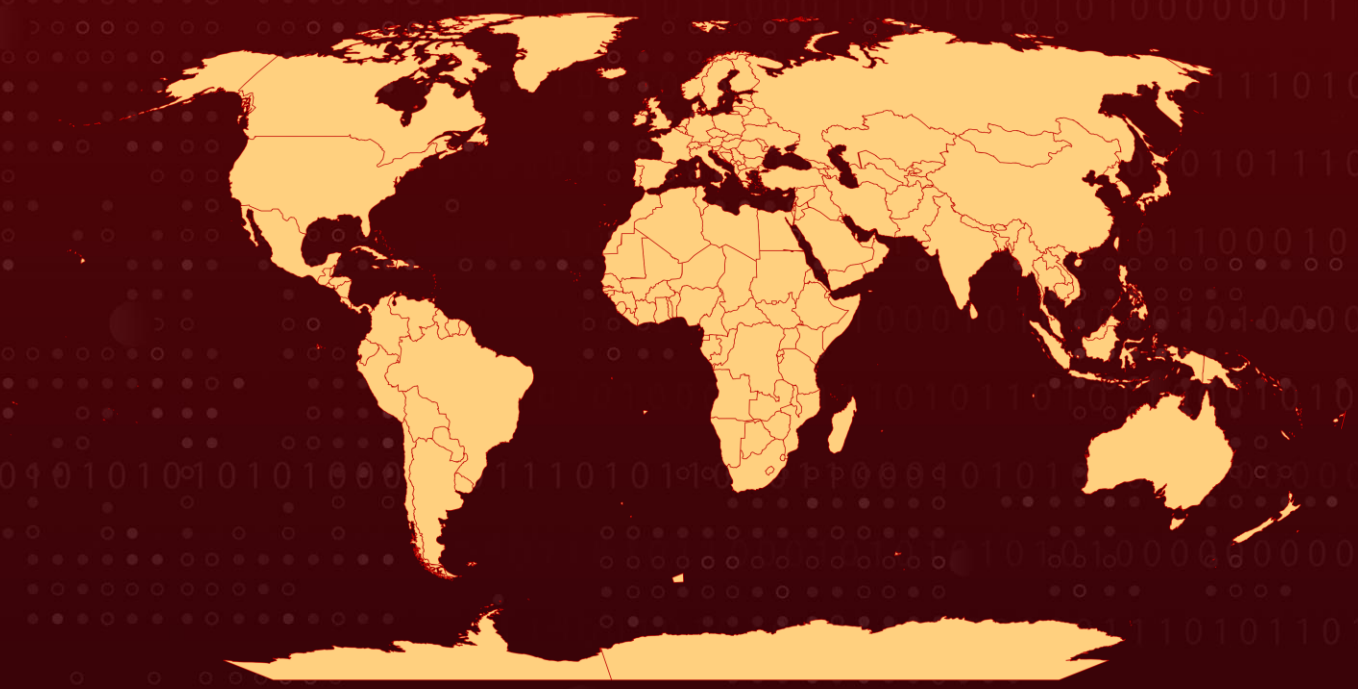
A New CrossLock Ransomware Threat with Cross-Platform Capabilities and Double Extortion Techniques

Date of Publication	Admiralty Code	TA Number
April 24, 2023	A1	TA2023195

Summary

First Appearance: April 16, 2023
Target Countries: Worldwide
Malware: CrossLock Ransomware
Affected Platforms: Windows, Linux, and macOS
Attack: CrossLock ransomware, implemented in Go programming language, uses double extortion technique to encrypt and exfiltrate data, posing a significant threat to businesses and organizations.

Attack Regions



Attack Details

#1 CrossLock ransomware, a new strain of ransomware, is implemented using the Go programming language, which provides cross-platform capabilities and makes reverse engineering more challenging. The primary objective of CrossLock ransomware is to block access to data by encrypting it.

#2 The ransomware employs a double extortion technique by encrypting the victim's data and exfiltrating it from their system, threatening to publicly leak or sell the stolen data if the ransom is not paid. The technical analysis reveals that CrossLock ransomware can accept various command line parameters for execution, including specifying a path for encryption, designating a remote IP address or DNS name for gaining access to the victim's network, and bypassing User Account Control (UAC).

#3 The ransomware also uses anti-analysis techniques, such as checking for the WINE environment and altering Event Tracing for Windows (ETW) functions to evade detection. After patching ETW, the ransomware performs multiple data-cleaning actions on the infected system, including deleting shadow copies, clearing event logs, disabling the startup repair feature, and more.

#4 Recently, CrossLock Ransomware Group claimed to have attacked Valid Certificadora, a Brazilian IT & ITES company. The emergence of this new group highlights the growing threat of ransomware attacks on businesses and organizations worldwide.

Recommendations

To check for CrossLock Ransomware infection, search for files with the ". crlk" extension and a "---CrossLock_readme_To_Decrypt---.txt" text file, and take immediate action to protect your data. Disconnect from the internet, back up all data to external drives or cloud storage.

Be vigilant for suspicious activity like deleted shadow copies, cleared event logs, or disabled startup repair. Use signatures, encryption, remote security logs, and capabilities to detect and prevent suspicious behavior. Keep software up-to-date and use reliable antivirus software to detect malicious activities.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0002 Execution	TA0007 Discovery	TA0010 Exfiltration
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
TA0042 Resource Development	TA0001 Initial Access	T1047 Windows Management Instrumentation	T1027 Obfuscated Files or Information
T1564 Hidden Window	T1497 Virtualization/Sandbox Evasion	T1070 Indicator Removal	T1566 Phishing
T1486 Data encrypted for impact	T1059 Command and Scripting Interpreter	T1070.001 Clear Windows Event Logs	T1204 User Execution
T1204.002 Malicious File	T1490 Inhibit System Recovery	T1082 System Information Discovery	T1135 Network Share Discovery
T1083 File and Directory Discovery	T1057 Process Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	9756b1c7d0001100fdde3efefb7e086f
SHA1	55de88118fe8abefb29dec765df7f78785908621
SHA256	495fbfecbcadb103389cc33828db139fa6d66bece479c7f7027983405141 2d72

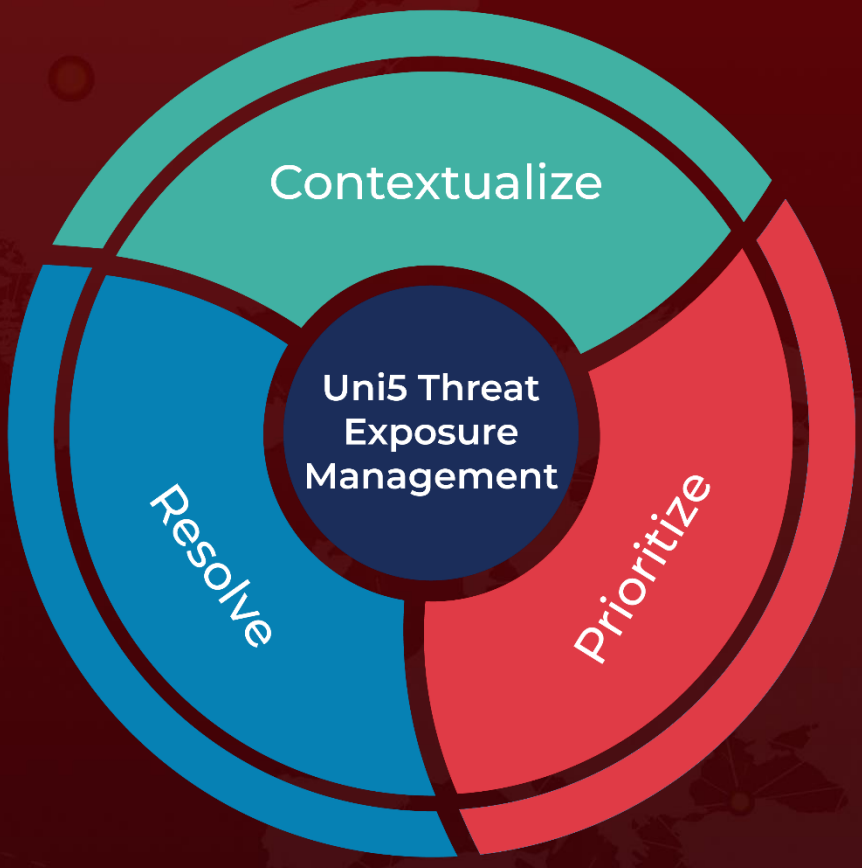
References

https://blog.cyble.com/2023/04/18/crosslock-ransomware-emerges-new-golang-based-malware-on-the-horizon/

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 24, 2023 • 2:00 AM

More at www.hivepro.com