Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

New Cylance Ransomware Targets Linux and Windows Operating Systems

Date of Publication	Admiralty Code	TA Number
April 11, 2023	A1	TA2023178

Summary

First appeared: March 12, 2023
Attack Region: Worldwide
Malware: Cylance ransomware
Affected Platforms: Windows and Linux
Attack: Cylance ransomware is a new malware that is capable of adjusting to customized encryption tactics and can accept different command-line parameters.

Attack Regions

Attack Details

#1

A new ransomware that can target both Windows and Linux operating systems has been discovered by cybersecurity researchers. Known as the Cylance ransomware, this malware encrypts victims' files and demands payment in exchange for the decryption key. The ransomware can accept different command line parameters and can adjust to customized encryption tactics.

#2

When executed, the ransomware first enables various Windows privileges for the current process, allowing access to restricted actions that are typically permitted only for processes with higher privileges. It creates a global mutex to ensure that only one instance of the malware runs on the victim's system at any given time. The ransomware also establishes persistence on the compromised system by creating a scheduled task entry.

#3

It utilizes Salsa20 encryption algorithms to encrypt files, and it avoids certain folder names, file names, and file extensions during the encryption process. Finally, the ransomware renames the encrypted files with the extension ".Cylance" and replaces them with the original file using the MoveFileExW() API function.

#4

The ransomware appears to be in the developmental stage, with little information available regarding its victims. The ransom message identifies itself as the Cylance ransomware, but it should not be confused with the cybersecurity company Cylance.

Recommendations

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

Implement additional measures such as strong encryption and network segmentation to isolate critical systems. Back up end-user systems and critical servers separately from the corporate network and use capabilities to prevent suspicious behavior on endpoint systems.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0040 Impact
TA0001 Initial Access	TA0007 Discovery	TA0011 Command and Control	TA0005 Defense Evasion
T1204 User Execution	T1133 External Remote Services	T1091 Replication Through Removable Media	T1059 Command and Scripting Interpreter
T1047 Windows Management Instrumentation	T1566 Phishing	T1053 Scheduled Task/Job	T1134 Access Token Manipulation
T1564 Hidden Window	T1027 Obfuscated Files or Information	T1082 System Information Discovery	T1135 Network Share Discovery
T1083 File and Directory Discovery	T1486 Data encrypted for impact		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ec8952dc14bac73174cef02a489539e244b378b7de76c771126a8ba7ce532efd D1ba6260e2c6bf82be1d6815e19a1128aa0880f162a0691f667061c8fe8f1b2c
SHA1	933ad0a7d9db57b92144840d838f7b10356c7e51 663081e2767df7083f765a3a8a994982959d4cbe
MD5	521666a43aeb19e91e7df9a3f9fe76ba 4601076b807ed013844ac7e8a394eb33

References

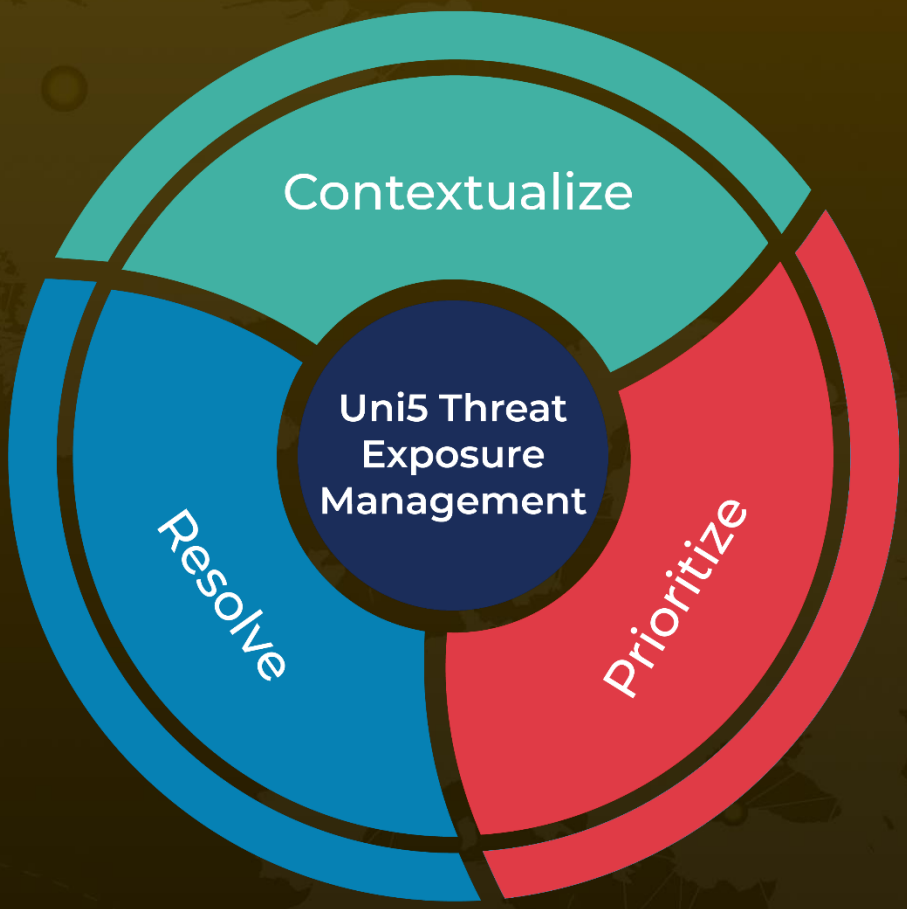
https://blog.cyble.com/2023/04/07/new-cylance-ransomware-with-power-packed-commandline-options/

https://twitter.com/Unit42_Intel/status/1641588431221342208

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 11, 2023 • 5:30 AM

More at www.hivepro.com