Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

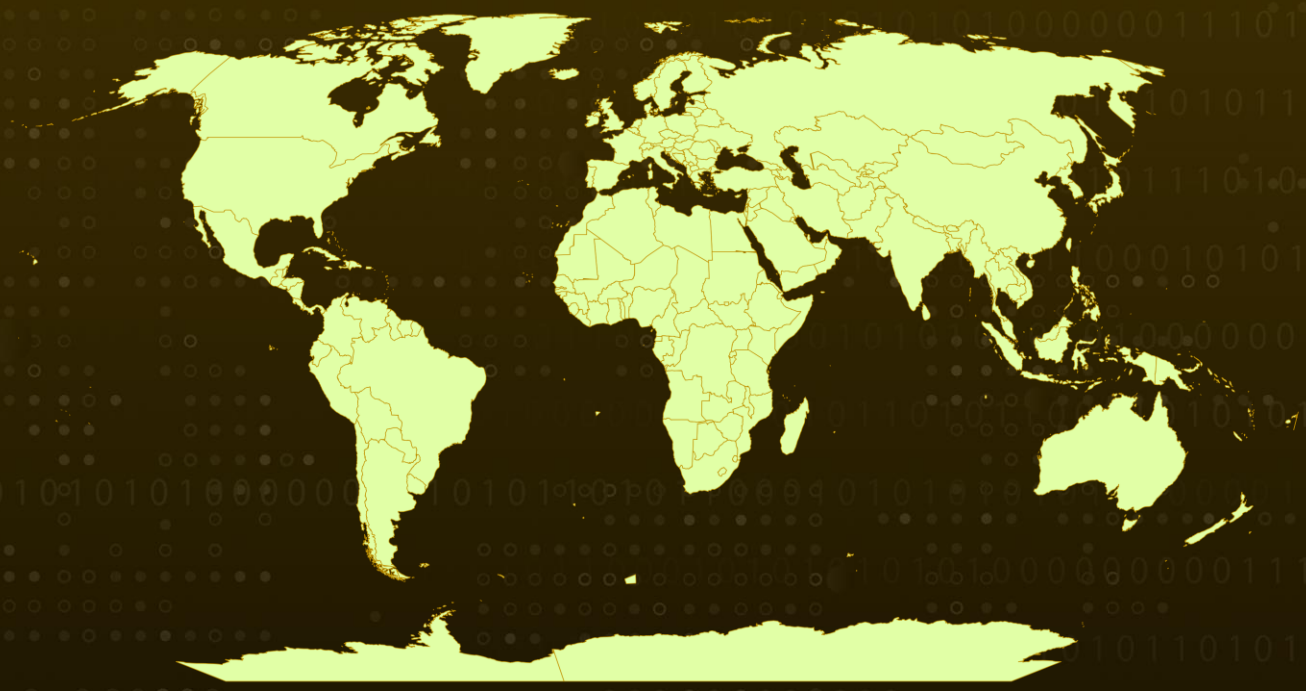
CrySIS Ransomware: A Long-Standing Threat with a New Twist

Date of Publication	Admiralty Code	TA Number
January 23, 2023	A1	TA2023038

Summary

First appeared: 2016
Attack Region: Worldwide
Attack: The CrySIS aka Dharma ransomware family is operating as ransomware-as-a-service (RaaS) model. Notably, the variant's source code was exposed, allowing anyone to purchase and repurpose it for their own ends.

Attack Regions



Attack Details

#1

The ransomware family CrySIS, dubbed Dharma, has been advancing since 2016. Its source code was made available to the public, enabling others to customize it for their use. The criminals behind the malware employ various tactics to infiltrate systems through exposed Microsoft Remote Desktop Protocol (RDP) servers. It is also being spread through phishing emails with attachments made to look like legitimate software installers.

#2

When executed, the ransomware creates registry entries to ensure persistence and encrypts essentially all file types. It conducts the encryption procedure using the AES-256 encryption algorithm in conjunction with RSA-1024 asymmetric encryption. It also deletes shadow copies of the system to thwart any attempts at recovery. The extension of encrypted files typically denotes the threat actor that launched the ransomware.

#3

Following encryption, the malware initiates the Microsoft HTML Application (MSHTA) to process and render the "Info.hta" file. It also drops a separate file called "info.txt" in addition to its "Info.hta" file. It includes a condensed set of instructions for contacting the attacker.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	T1083 File and Directory Discovery
T1036 Masquerading	T1195 Supply Chain Compromise	T1129 Shared Modules	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1070 Indicator Removal
T1070.004 File Deletion	T1497 Virtualization/Sandbox Evasion	T1564 Hide Artifacts	T1564.001 Hidden Files and Directories
T1056 Input Capture	T1057 Process Discovery	T1082 System Information Discovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	419bc8196013d7d8c72b060da1a02d202d7e3eb441101f7bcb6d7667871a5c16 5c2fb1c42f007093be5e463f70ee7e7192990b3385a3cbcc71043980efa312e0 6a0017262def9565b504d04318c59f55bea136ac3dd48862d1ae90ff6b963811 b557bf11d82d3d64d028a87584657d25dba0480295ed08447f10c7a579dee048 b3984a2de76eee3ad20c4b13e0c0cbbab2dd6db65e3f6ca34418e79c21cf5c39 E9253218e30b30c8bb690b2ab02eef47b8b5c8991629d814b2af6664151e9a2f

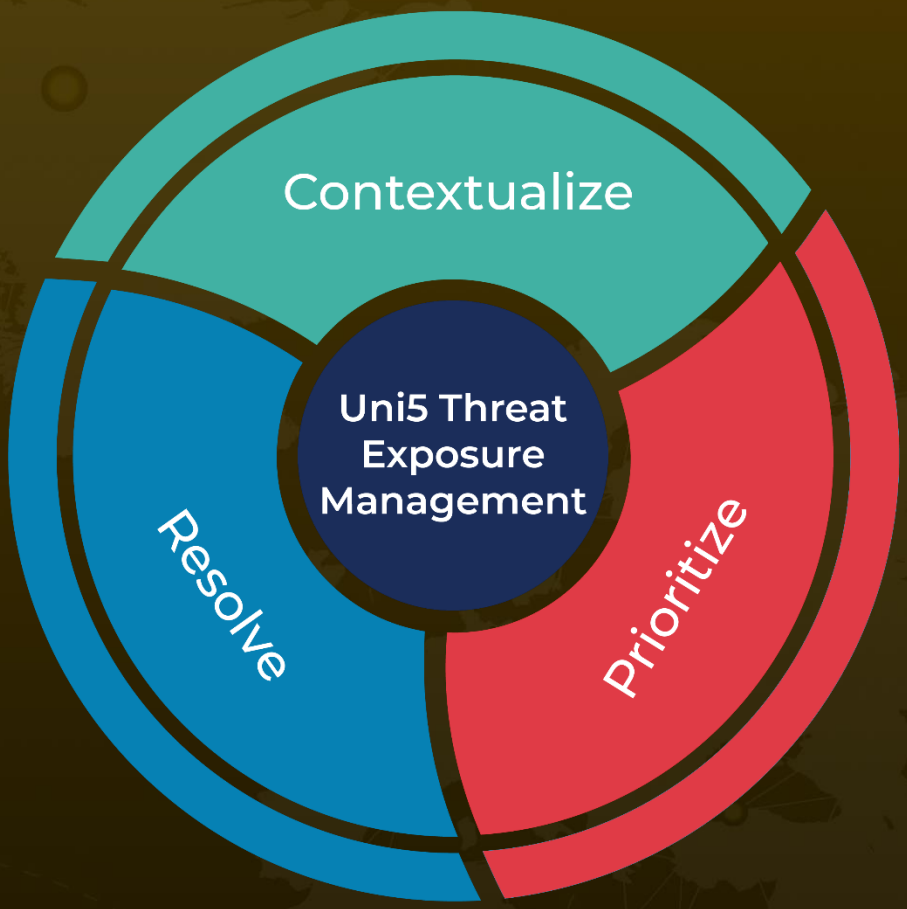
References

https://www.fortinet.com/blog/threat-research/ransomware-roundup-playing-whack-a-mole-with-new-crysis-dharma-variants

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

January 23, 2023 . 2:30 AM

More at www.hivepro.com