Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

GootKit Loader is targeting organizations in the Australian healthcare industry

Date of Publication	Admiralty Code	TA Number
January 12, 2023	A1	TA2023021

Summary

First appeared: December 2022
Attack Region: Australia
Attack: Gootkit loader using search engine optimization (SEO) poisoning for its initial access to target organizations in the Australian healthcare industry.

Attack Regions

Attack Details

#1

Gootkit, also known as Gootloader, is a type of malware known for being used in advanced persistent threat (APT) campaigns. Recently, it has been discovered to be targeting organizations in the Australian healthcare industry. The malware is delivered via search engine optimization (SEO) poisoning, a technique that manipulates search engine results to lead users to malicious websites. The malware has been found to be using updated tactics, such as fileless delivery of other malicious payloads, such as Cobalt Strike.

#2

Additionally, the malware abuses VLC Media Player, a widely-used legitimate tool, to install malicious DLLs. The Australian Cyber Security Center (ACSC) has been notified of these attacks and is currently reviewing the findings. This is concerning as the healthcare industry holds a large amount of personal and sensitive information and a breach of this information could have serious consequences.

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

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0008 Lateral Movement
TA0005 Defense Evasion	TA0004 Privilege Escalation	TA0010 Exfiltration	T1588 Obtain Capabilities
T1204 User Execution	T1204.001 Malicious Link	T1204.002 Malicious File	T1574 Hijack Execution Flow
T1588.001 Malware	T1608 Stage Capabilities	T1608.006 SEO Poisoning	T1053.005 Scheduled Task
T1053 Scheduled Task/Job	T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1574.002 DLL Side-Loading
T1105 Ingress Tool Transfer	T1587 Develop Capabilities		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	57af5c9f715d5c516e1137b6d336bff7656e1b85695fff4c83fc5a78c11fdec6 a9d2a52e418f5cc9f6943db00a350a5588c11943898d3d6d275e1b636b3cd7c8 6d549cd0b623f5623bb80cc344f6b73962d76b70a7cbd40ca8f1d96df7cce047 7c2ea97f8fff301a03f36fb6b87d08dc81e948440c87c2805b9e4622eb4e1991
IPV4	193[.]106[.]191[.]187
URLs	http://bip.podkowalesna [.] pl/xmlrpc.php http://blog.ddlab [.] net/xmlrpc.php http://bodilbruun [.] dk/xmlrpc.php http://clearchoiceairtreatment [.] com/xmlrpc.php https://ahanpt [.] ir/xmlrpc.php https://allthetech [.] com/xmlrpc.php https://baban [.] ir/xmlrpc.php https://centre-samekh [.] ch/xmlrpc.php

TYPE	VALUE
URLs	https://covid19.gov[.]gd/xmlrpc.php https://educabla [.] com/xmlrpc.php https://emitrablog [.] com/xmlrpc.php https://fx-arabia [.] com/xmlrpc.php https://mangayaro [.] com/xmlrpc.php https://mgplastcutlery [.] com/xmlrpc.php https://nmm [.] pl/xmlrpc.php https://ntumatches [.] tw/xmlrpc.php https://ruscred [.] site/xmlrpc.php https://sayhueque [.] com/xmlrpc.php https://thedinkpickleball [.] com/xmlrpc.php https://www.slimdiet [.] eu/content.php https://www.studio-lapinternet[.]fr/content.php https://yespornplease [.] tv/xmlrpc.php

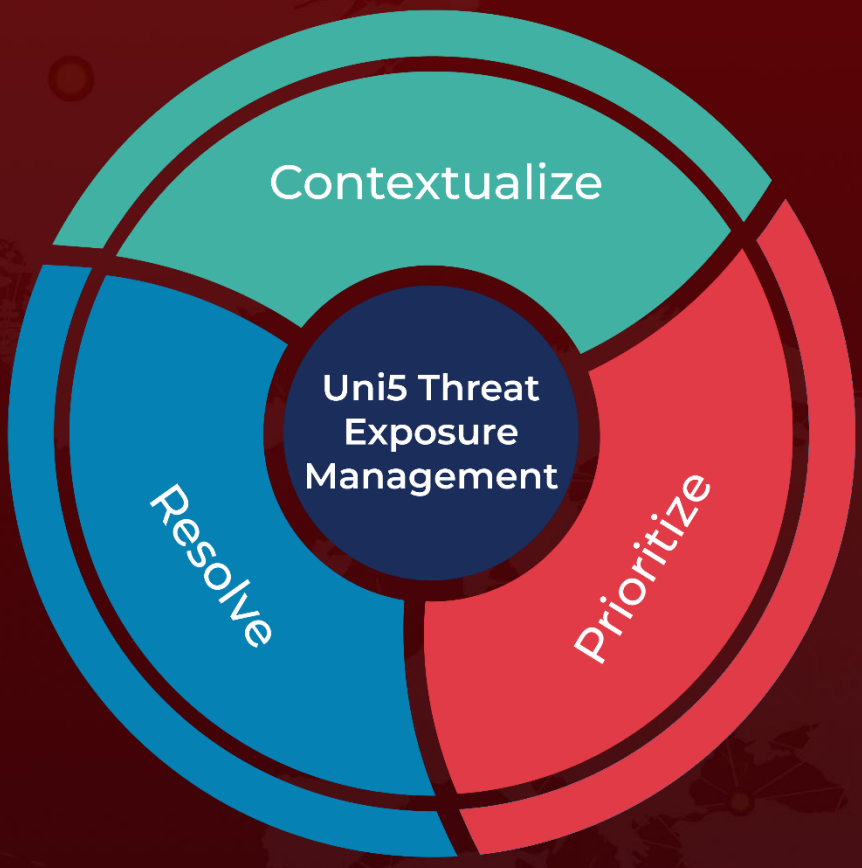
References

https://www.trendmicro.com/en_us/research/23/a/gootkit-loader-actively-targets-the-australian-healthcare-indust.html

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 12, 2023 . 5:15 AM

More at www.hivepro.com