Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

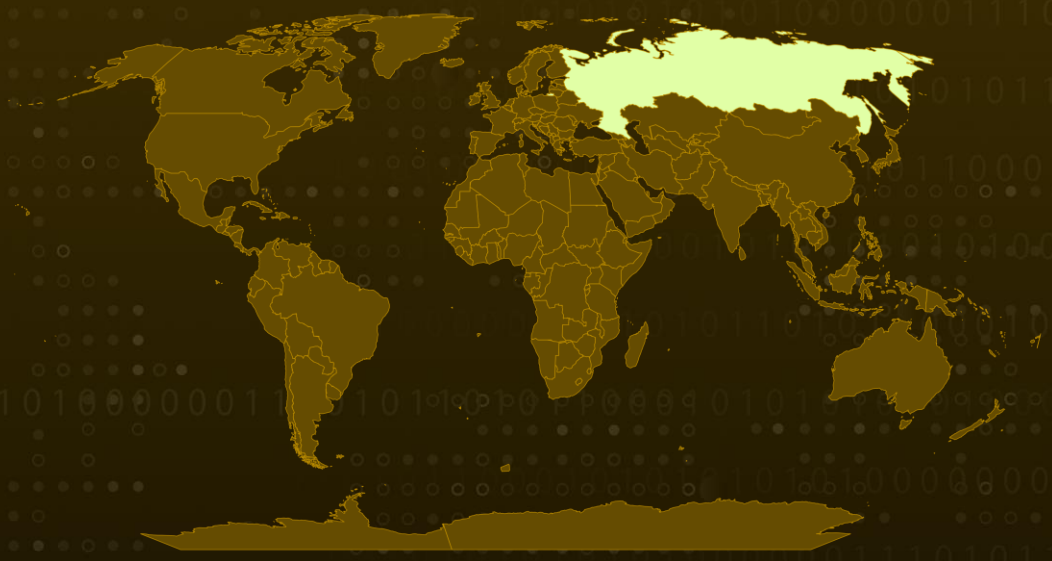
DarkWatchMan RAT Targets Russians

Date of Publication	Admiralty Code	TA Number
May 11, 2023	A1	TA2023222

Summary

First Seen: 2021
Attack Country: Russia
Malware: DarkWatchMan RAT
Attack: DarkWatchMan is a Remote Access Trojan (RAT) distributed via a phishing website imitating a renowned Russian website, which allows attackers to gain remote control over compromised systems and extract sensitive data such as keystrokes, clipboard data, and system information.

Attack Regions



Attack Details

#1

DarkWatchMan RAT is a Remote Access Trojan type of malware that allows attackers to gain remote control over compromised systems and extract sensitive data. It was first detected in 2021, and its primary targets are Russian users. DarkWatchMan can capture keystrokes, clipboard data, and system information, and it stores the data in the registry to minimize the risk of detection.

#2

Threat actors distribute DarkWatchMan through a phishing website that imitates a renowned Russian website called CryptoPro CSP. Users are prompted to download a malicious file called "CSPSetup.rar" and enter a password for extraction. If executed, the file installs the DarkWatchMan malware, dropping a JavaScript file named "144039266" in the %temp% location. The JavaScript file is responsible for initializing global variables, installing a keylogger, and configuring the RAT. DarkWatchMan RAT poses a significant danger to both individuals and organizations, and it highlights the ongoing threat of phishing attacks.

Recommendations

Employ strict access control measures: To prevent the DarkWatchMan from gaining unauthorized access to critical systems and sensitive information, implement strict access control measures such as multi-factor authentication, strong password policies, and role-based access control.

Use threat intelligence: Keep up-to-date with the latest threat intelligence to identify potential attacks and respond quickly to any suspicious activity. Use this information to monitor for activity associated with DarkWatchMan.

Conduct regular security awareness training: Employees should be regularly trained on how to identify and respond to phishing attacks, social engineering tactics, and other common techniques used by DarkWatchMan. This training should emphasize the importance of maintaining good security hygiene practices and reporting any suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1566 Phishing	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1204 User Execution	T1218 System Binary Proxy Execution	T1140 Deobfuscate/Decode Files or Information
T1564 Hide Artifacts	T1053 Scheduled Task/Job	T1012 Query Registry	T1087 Account Discovery
T1082 System Information Discovery	T1056 Input Capture	T1056.001 Keylogging	T1071 Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	2edf05f2130d4e12599dc44ff8bfc892 1706c64156d873ebbd0c6ecac95fec39 9afc15393e8bae03ad306ae1c50645e3 ca820517f8fd74d21944d846df6b7c20
SHA1	1f87eeb37156d64de97d042b9bcfbaf185f8737d 149ce68540a068cdd204df796f6bff7d70f16473 be450cd1fab1b708ac1de209224e0d7f7adc0fae bb91d5234f37905f4830061331beab99e51206e7
SHA256	4e38b7519bf7b482f10e36fb3e000cc2fcbf058730f6b9598a6a7ba5543766d4 d439a3ce7353ef96cf3556abba1e5da77eac21fdba09d6a4aad42d1fc88c1e3c 706eebdf4de19d17f9a753984f7b4cff7f5487c74d7862d21684e754967d8dd4 1b5eb6d4680f7d4da7e2a1a1060b9f13565e082346e375a92244bb55672d49d7

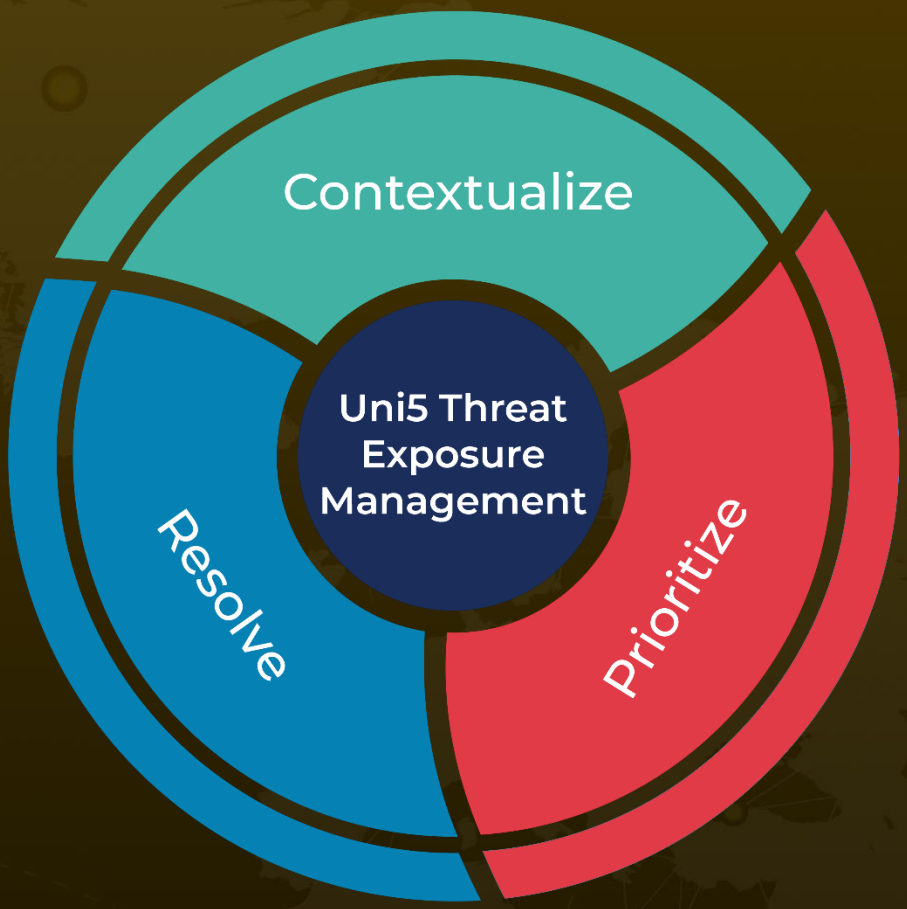
References

https://blog.cyble.com/2023/05/05/sophisticated-darkwatchman-rat-spreads-through-phishing-sites/

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 11, 2023 • 3:00 AM

More at www.hivepro.com