Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

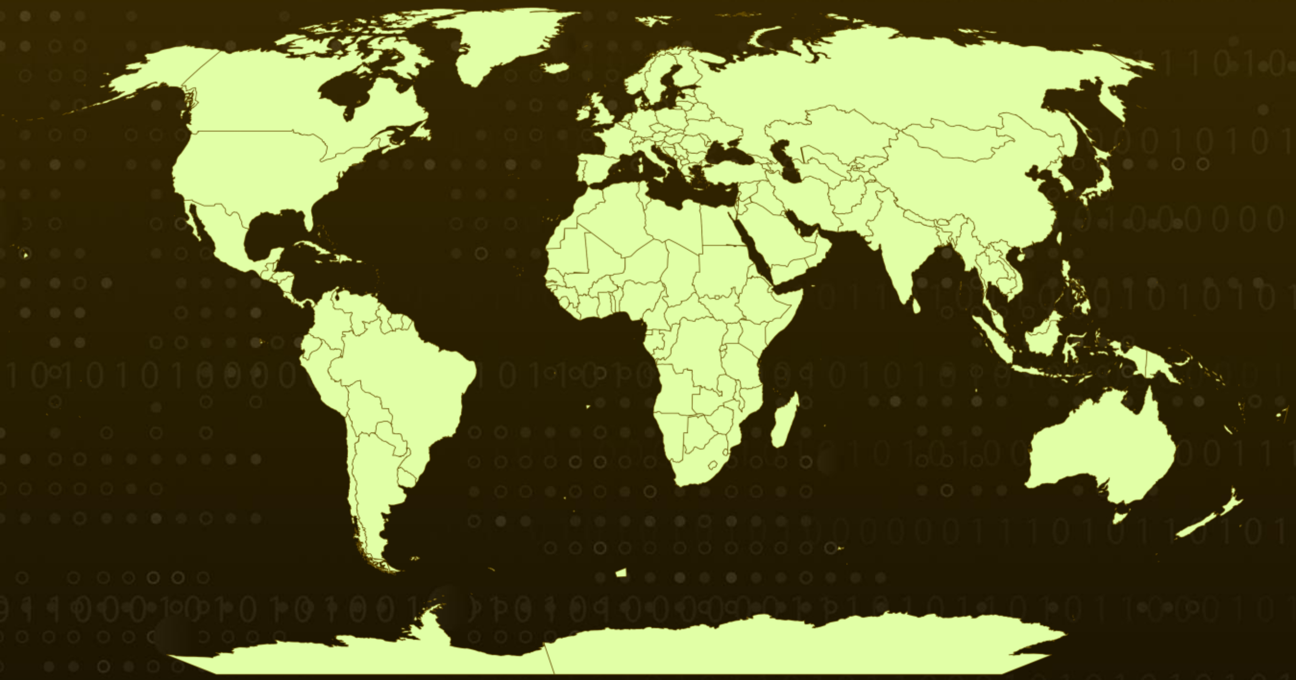
DarkCloud Stealer A Multi-Stage Malware That Pilfers Sensitive data

Date of Publication	Admiralty Code	TA Number
February 22, 2023	A1	TA2023095

Summary

First appeared: 2022
Attack Region: Worldwide
Attack: DarkCloud Stealer is a type of malware distributed worldwide through spam operations and designed to pilfer sensitive information from a victim's device. The sale of DarkCloud Stealer was reported in January 2023.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

Several spam emails are being sent with an order invoice phishing scheme, intending to deceive the receiver into opening an attachment or clicking on a malicious link that contains DarkCloud Stealer. The malware functions through a multi-stage process, and the final payload, written in Visual Basic, is loaded into the device's memory during the last stage. DarkCloud Stealer is capable of exfiltrating stolen data using various methods, such as SMTP, Telegram, Web Panel, and FTP.

#2

The spam campaign delivers an initial file that acts as a dropper. This file copies itself into the directory and establishes a task scheduler entry using schtasks.exe to maintain persistence. Subsequently, the malware initiates and loads the next level binary into a running process's memory. The 32-bit .NET compiled binary "ConsoleApp1.exe" contains the DarkCloud Stealer payload's source code. The malware collects all the retrieved information in the "Program.datas" variable, which it later saves in a text file named "credentials.txt". Finally, the DarkCloud Stealer transmits the stolen data to the C&C server.

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	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1204 User Execution	T1053 Scheduled Task/Job	T1140 Deobfuscate/Decode Files or Information
T1555 Credentials from Password Stores	T1539 Steal Web Session Cookie	T1552 Unsecured Credentials	T1528 Steal Application Access Token
T1087 Account Discovery	T1518 Software Discovery	T1057 Process Discovery	T1007 System Service Discovery
T1071 Application Layer Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5d060254a6d7eb2cdb2031e29891cb95206757a28fe0d51569eb9f7f55637ac6,79b13d9a52d466a606c37b8f12b2ef7af4e9b53a911b70427c07cb73adb504a1,2e60ed90aa6cefa60cc4cd968213549ddf578dcf6968d8c66366d09c7108ef56,9bb43e190685f86937e09673de3243cbe1971ecf0eab9b75e09d0de96e9764cb,413c9fcea027f89b9d8905ca6ae96cc099b8886fb3916876a4029e92d56fcb9b,e342802bd53191559af2a23b2d11412a8fe60dc3a50e5efa1fade7067c305f55,51247a58f41ba112ce31ed44b0a68bc4db8f39763250071fe35957d1e3eaf9cb,33fa272ffd2eac92f2a344718fa9bf678703f8194fcfcbc499ab9fefcdab4cca

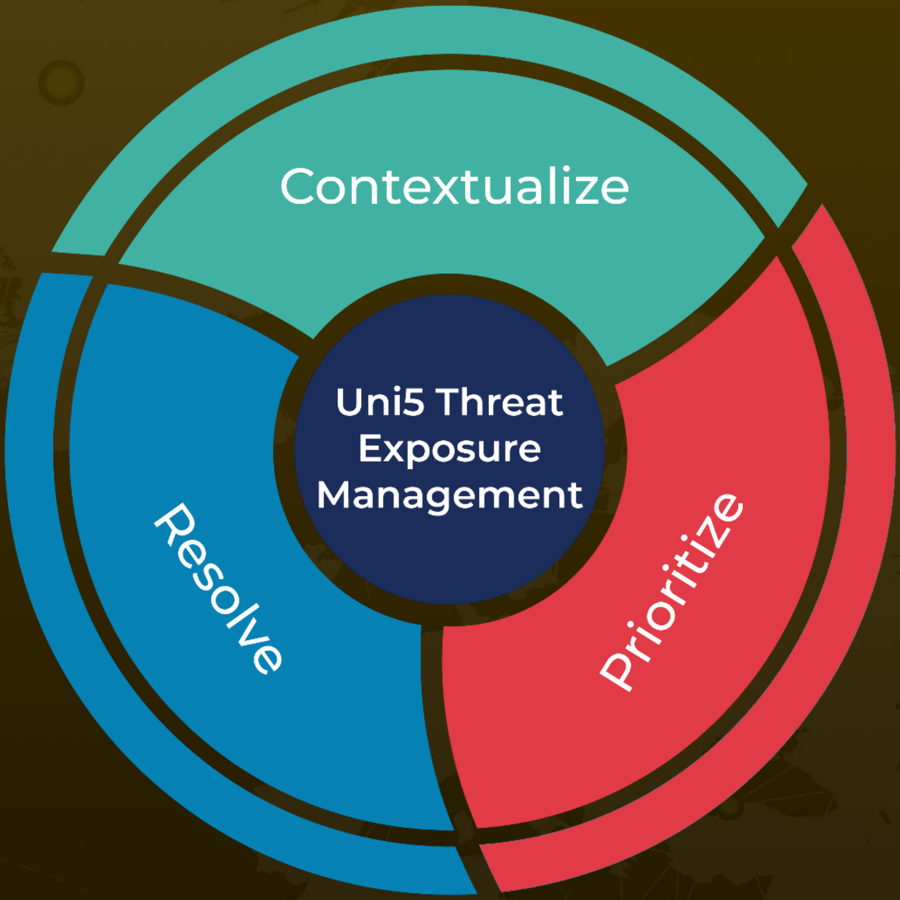
References

https://blog.cyble.com/2023/02/20/decoding-the-inner-workings-of-darkcloud-stealer/

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

February 22, 2023 • 12:12 AM

More at www.hivepro.com