Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

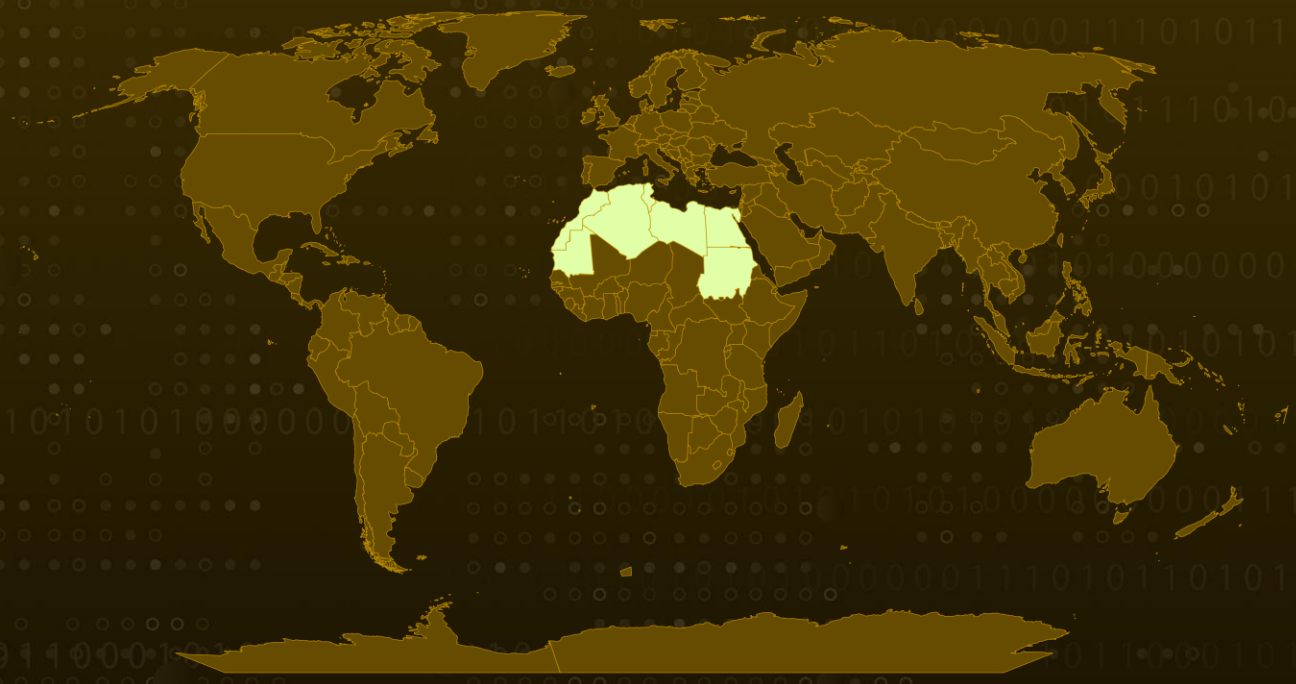
Stealth Soldier Strikes North Africa with Espionage Attacks

Date of Publication	Admiralty Code	TA Number
June 9, 2023	A1	TA2023258

Summary

First seen: October 2022
Malware: Stealth Soldier
Attack Region: Algeria, Egypt, Libya, Morocco, Mauritania, Sudan, and Tunisia.
Targeted Industries: Government and Foreign Affairs
Attack: Stealth Soldier is a backdoor malware that conducts surveillance and espionage attacks. It targeted North Africa by mimicking Libyan websites to distribute malware.

Attack Regions



Attack Details

#1 The Stealth Soldier malware is an undisclosed covert backdoor that primarily carries out surveillance operations, encompassing activities such as file extraction, screen and microphone recording, keystroke logging, and browser data theft. An ongoing campaign targeting entities in North Africa involves a multi-tiered implementation of Stealth Soldier.

#2 The most recent version of Stealth Soldier is believed to have been deployed in February 2023, while the earliest version was compiled in October 2022. The ongoing operation of Stealth Soldier is characterized by the use of command-and-control (C&C) servers that mimic websites associated with the Libyan Ministry of Foreign Affairs.

#3 The attack begins when unsuspecting targets unknowingly download counterfeit downloader binaries, which are delivered through clever social engineering tactics. These binaries act as conduits for retrieving the Stealth Soldier malware while simultaneously presenting a deceptive empty PDF file as a diversion.

#4 The execution sequence for all versions of Stealth Soldier starts with the activation of the downloader, triggering the chain of infection. Although the exact delivery mechanism of the downloader remains unknown, the naming conventions suggest that they were distributed through sophisticated social engineering techniques.

#5 The malware infection chain is intricate, comprising multiple files, each downloaded from the command-and-control server. The infrastructure of Stealth Soldier exhibits certain intersections with the infrastructure utilized by The Eye on the Nile, a previous operation that targeted Egyptian journalists and human rights activists in 2019.

Recommendations

Exercise caution when downloading software: Be wary of websites that offer cracked or free software downloads, as they can be potential sources of malware. Stick to reputable sources and avoid suspicious portals that mimic legitimate software platforms.

Heighten User Awareness and Vigilance: Educating users about the risks posed by sophisticated malware like Stealth Soldier is paramount. Additionally, users should exercise caution when opening email attachments or clicking on unfamiliar links to minimize the risk of infection.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control
T1129 Shared Modules	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools	**T1036** Masquerading
T1070 Indicator Removal	**T1070.006** Timestomp	**T1112** Modify Registry	**T1497** Virtualization/Sandbox Evasion
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1012** Query Registry	**T1018** Remote System Discovery
T1082 System Information Discovery	**T1071** Application Layer Protocol	**T1095** Non-Application Layer Protocol	**T1573** Encrypted Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	185.125.230[.]216 185.125.230[.]116 94.156.33[.]228 94.156.33[.]229 185.125.230[.]224 185.125.230[.]220
Domains	filestoragehub[.]live customjvupdate[.]live filecloud[.]store webmailogemail[.]com loglivemail[.]com 2096[.]website
SHA256	2cad816abfe4d816cf5ecd81fb23773b6cfa1e85b466d5e5a48112862ceb3efb,05db5e180281338a95e43a211f9791bd53235fca1d07c00eda0be7fdc3f6a9bc,b9e9b93e99d1a8fe172d70419181a74376af8188dcb03249037d4daea27f110e,d57fc4e8c14da6404bdcb4e0e6ac79104386ffbd469351c2a720a53a52a677db,e7794facf887a20e08ed9855ac963573549809d373dfe4a287d1dae03bffc59f,8c09a804f408f7f9edd021d078260a47cf513c3ce339c75ebf42be6e9af24946,df6a44551c7117bc2bed2158829f2d0472358503e15d58d21b0b43c4c65ff0b4,e546d48065ff8d7e9fef1d184f48c1fd5e90eb0333c165f217b0fb574416354f,a43ababe103fdce14c8aa75a00663643bf5658b7199a30a8c5236b0c31f08974,c0b75fd1118dbb86492a3fc845b0739d900fbbd8e6c979b903267d422878dbc6,cb90a9e5d8b8eb2f81ecdbc6e11fba27a3dde0d5ac3d711b43a3370e24b8c90a,d6655e106c5d85ffdce0404b764d81b51de54447b3bb6352c5a0038d2ce19885,b94257b4c1fac163184b2d6047b3d997100dadf98841800ec9219ba75bfd5723,7bfe2a03393184d9239c90d018ca2fdccc1d4636dfb399b3a71ea6d5682c92bd

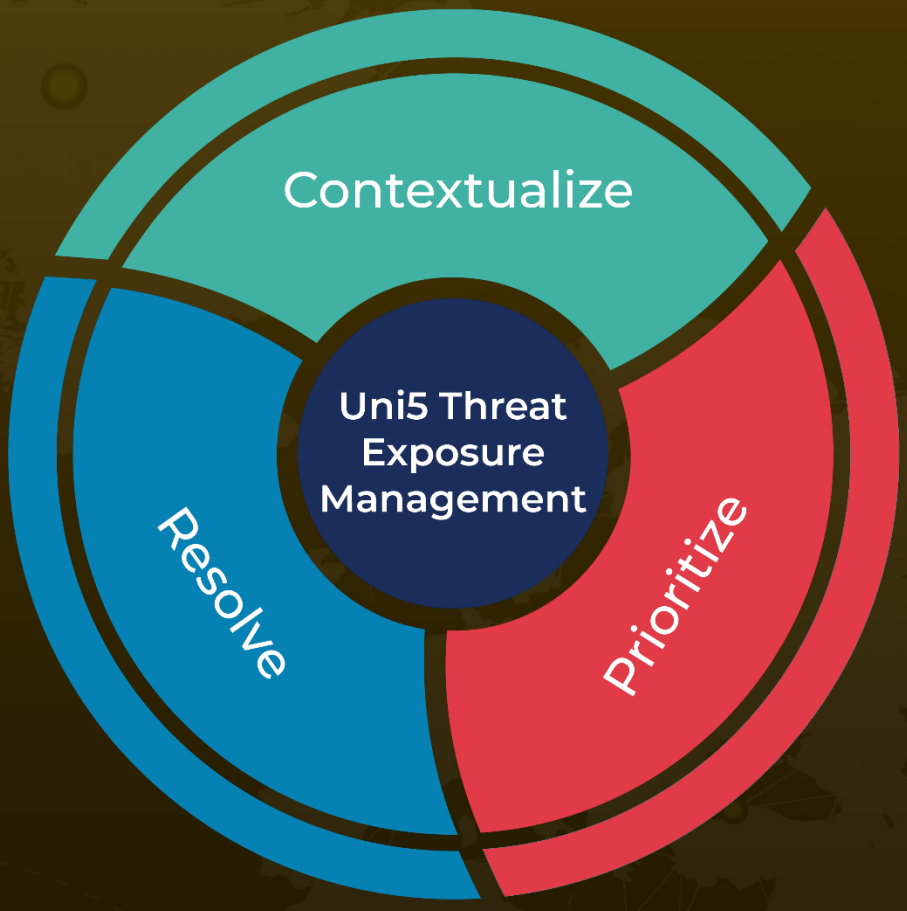
References

https://research.checkpoint.com/2023/stealth-soldier-backdoor-used-in-targeted-espionage-attacks-in-north-africa/

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

June 9, 2023 • 6:10 AM

More at www.hivepro.com