Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

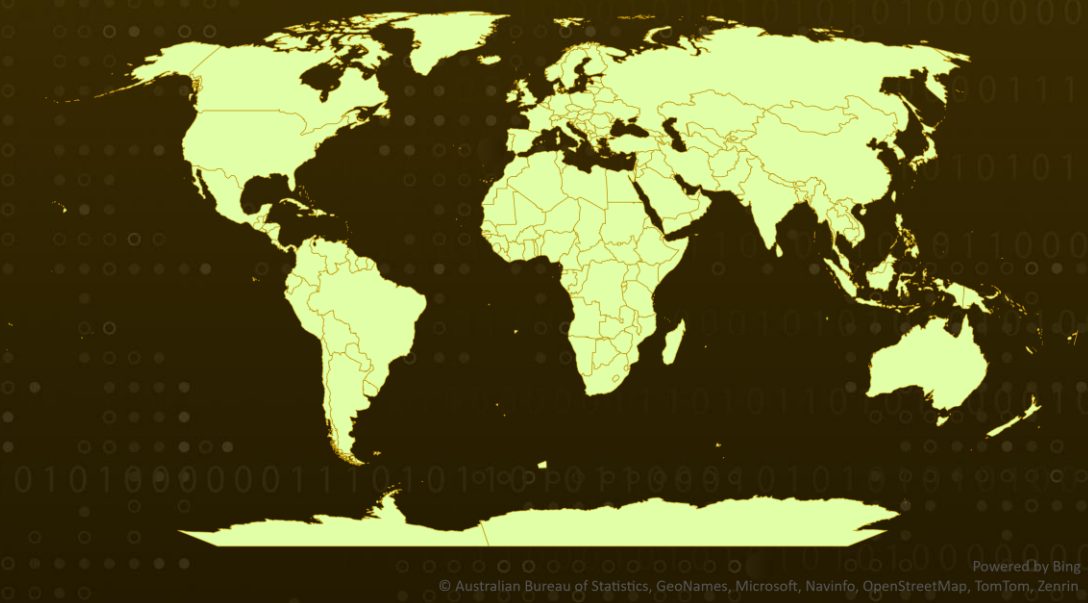
SYS01 Stealer Targets Government and Manufacturing Industry

Date of Publication	Admiralty Code	TA Number
March 8, 2023	A1	TA2023123

Summary

First Appeared: November 2022
Attack Region: Worldwide
Attack Industry: Government, Manufacturing
Attack: The SYS01 stealer has been targeting critical government infrastructure employees, manufacturing companies, and other industries, and using various delivery techniques, including DLL side-loading, to steal and exfiltrate information from victims

Attack Regions



Attack Details

#1

The advanced information stealer, SYS01, has been active since November 2022 and has targeted critical government infrastructure employees, manufacturing companies, and other industries. One of its tactics is to use Google ads and fake Facebook profiles to promote games, adult content, and cracked software in order to trick victims into downloading a malicious file.

#2

The infection process of SYS01 starts when a victim clicks on a URL from a fake Facebook profile or advertisement, leading to the download of a ZIP file that appears to contain a legitimate application, game, movie, etc. The infection is divided into two parts: the loader and the Inno-Setup installer that drops the final payload. The loader is typically a legitimate C# application that is vulnerable to a side-loading vulnerability and is paired with a hidden malicious dynamic link library (DLL) file that eventually side-loads into the application. The legitimate application then drops the Inno-Setup installer, which decompresses into a PHP application containing malicious scripts responsible for stealing and exfiltrating information.

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
TA0004 Privilege Escalation	T1027 Obfuscated Files or Information	T1059 Command and Scripting Interpreter	T1566 Phishing
T1553 Subvert Trust Controls	T1574 Hijack Execution Flow	T1140 Deobfuscate/Decode Files or Information	T1053 Scheduled Task/Job
T1070 Indicator Removal			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	01f76140374da14b72a8f1e648cb8f46590419cddd56bc089e67f38cee767735 7f54dc5ddab4de19c5ad7c7b6d4398bd07d97504cdedabc398a6d6db52fe9875 bad4de1c398954b9c381d91fee52607b78e1c65bd9f38c3e82a307e236a76223 2c58bfbf8d274434e3307a76a37720d09387978e8e401780048992ea21fd222b c81175d56aa006ad140799e39c800306b439ea98b9efc4491c269eccbfeebd4e c636ed3b0ca558a92687f60f0b37c0e44ff3a6d4f15acd3cfb858fee4b0b0916 833b871f342ba7b0e852363ed123682b99588888f01567e56942889d886bb4b2 daba97a67f219443ef4b0a39e2d051179d20de6a2febb927bec4108dcac1b3a6 5698feaacd122f75d69ed1d9a561ab7210051031e821b934b3022d48a185443b f58b9794f5b973625551333f469878c1df65302733f9a3e9a214e3739cee09bf 3416982484faefb7b0092cc639039863e52a9aa6ba0a277f943216a398dd0f8b 804f137c4253241cdcbbe8cd59181f0621cbd26bb8a78163b8bc0461d5f3bafb

TYPE	VALUE
SHA256	20a1c15d016a2d11659a74ae9e23e57020a4023df4c9f8c0357a38b69eddfa08 14fe2d1d1df11d887f5c53a78af6e1885928aa9256b79cd365f2c1d39397c2f4 25a5422f4a4a1d11b242730adbce06673cefee533da62a8ddef93e0074a3ba75 7d64de081057d18b1503854386a351a76caac9d71aada177373ef77b597a4f06
Domains	caseiden[.]com graeslavur[.]com rapadtrai[.]com baglamanotalari[.]com oscarnaija[.]com makananwisata[.]com seleriti[.]com seemlabie[.]top craceruib[.]top mahinetain[.]top

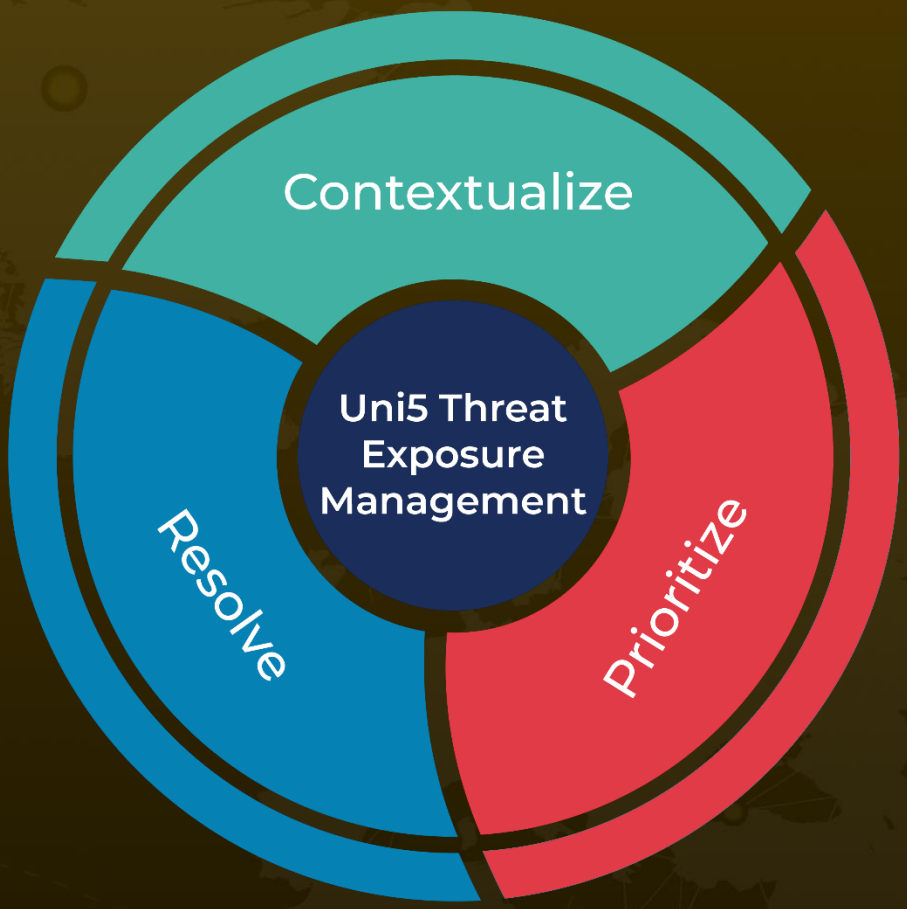
References

https://blog.morphisec.com/sys01stealer-facebook-info-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

March 8, 2023 • 12:45 AM

More at www.hivepro.com