Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

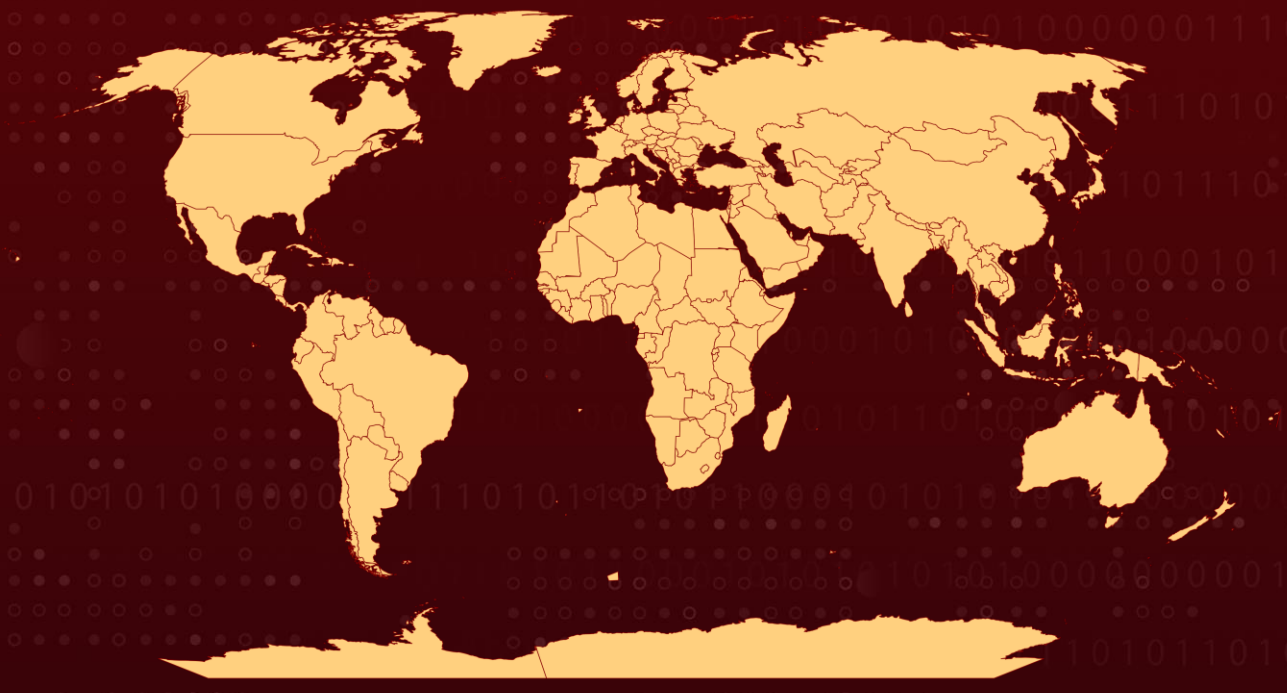
A New Info-Stealing Malware Named "Stealc" Targeting Cryptocurrency Wallets

Date of Publication	Admiralty Code	TA Number
February 21, 2023	A1	TA2023092

Summary

First Appearance: January 2023
Target Countries: Worldwide
Malware Family: Stealc
Attack: Stealc is a highly customizable and fully-featured information-stealing malware that is gaining popularity among cybercriminals, with over 40 command-and-control servers discovered in the wild, and whose development relied on multiple other popular stealers.

Attack Regions



Attack Details

#1 A new information-stealing malware called Stealc was discovered in January 2023. This malware is designed to steal sensitive information from various sources including web browsers, desktop cryptocurrency wallets, and browser extensions for cryptocurrency wallets. Its development relied on Vidar, Raccoon, Mars, and Redline stealers.

#2 Stealc is a fully-featured malware, meaning that it is a complete and fully-functional program that can be customized for specific purposes. The malware can be configured to collect data in different ways, and can also be customized to filter, sort, and analyze the stolen data.

#3 One of the unique features of Stealc is that it has an administration panel that allows customers to customize the malware to their needs. This makes it easier for cybercriminals to use the malware for specific purposes and maximize their chances of success in stealing valuable information.

#4 Since its discovery, over 40 command-and-control servers used by Stealc have been found in the wild, and dozens of samples of the malware have been identified. This indicates that Stealc is gaining popularity among cybercriminals and may become a significant threat to internet security.

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

TA0010 Exfiltration	TA0002 Execution	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0006 Credential Access	TA0005 Defense Evasion	TA0040 Impact
T1059 Command and Scripting Interpreter	T1106 Native API	T1129 Shared Modules	T1027 Obfuscated Files or Information
T1055 Process Injection	T1027.007 Dynamic API Resolution	T1036 Masquerading	T1070 Indicator Removal
T1539 Steal Web Session Cookie	T1552.001 Credentials In Files	T1552 Unsecured Credentials	T1555 Credentials from Password Stores
T1555.003 Credentials from Web Browsers	T1012 Query Registry	T1016 System Network Configuration Discovery	T1057 Process Discovery
T1082 System Information Discovery	T1083 File and Directory Discovery	T1518 Software Discovery	T1614 System Location Discovery
T1005 Data from Local System	T1113 Screen Capture	T1119 Automated Collection	T1132 Data Encoding
T1132.001 Standard Encoding	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1105 Ingress Tool Transfer
T1140 Deobfuscate/Decode Files or Information	T1622 Debugger Evasion	T1020 Automated Exfiltration	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	185[.]143[.]223[.]136 94[.]131[.]99[.]185 65[.]109[.]131[.]183 45[.]87[.]153[.]50 179[.]43[.]162[.]94 194[.]87[.]31[.]146 94[.]142[.]138[.]11 23[.]88[.]116[.]117 95[.]217[.]143[.]99 185[.]242[.]87[.]149 194[.]4[.]51[.]160 5[.]75[.]138[.]201 185[.]130[.]46[.]214 167[.]235[.]62[.]105 185[.]247[.]184[.]7 179[.]43[.]162[.]89 91[.]228[.]225[.]46 179[.]43[.]162[.]2 77[.]246[.]156[.]93 84[.]246[.]85[.]80 185[.]5[.]248[.]95 146[.]70[.]161[.]51 85[.]239[.]54[.]29 91[.]215[.]85[.]188 77[.]91[.]124[.]7 37[.]120[.]238[.]190 37[.]220[.]87[.]65 45[.]136[.]49[.]247 45[.]136[.]50[.]69 45[.]136[.]51[.]61 45[.]144[.]29[.]176 65[.]109[.]3[.]34 94[.]142[.]138[.]48 95[.]216[.]112[.]83 195[.]74[.]86[.]37 162[.]0[.]238[.]10
SHA256	1e09d04c793205661d88d6993cb3e0ef5e5a37a8660f504c1d36b0d8562e63a2 77d6f1914af6caf909fa2a246fcec05f500f79dd56e5d0d466d55924695c702d 87f18bd70353e44aa74d3c2fda27a2ae5dd6e7d238c3d875f6240283bc909ba6

TYPE	VALUE
URLs	hxxp://146.70.161[.]51/273d9c8034a95cb4.phphxxp://162.0.238[.]10/752e382b4dcf5e3f.php hxxp://176.124.192[.]200/bef7fb05c9ef6540.php hxxp://179.43.162[.]2/d8ab11e9f7bc9c13.php hxxp://185.5.248[.]95/api.php hxxp://666palm[.]com/bca98681abf8e1ab.php hxxp://777palm[.]com/bef7fb05c9ef6540.php hxxp://94.142.138[.]48/f9f76ae4bb7811d9.php hxxp://95.216.112[.]83/413a030d85acf448.php hxxp://aa-cj[.]com/6842f013779f3d08.php hxxp://fff-ttt[.]com/984dd96064cb23d7.php hxxp://moneylandry[.]com/bef7fb05c9ef6540.php hxxp://94.142.138[.]48/f9f76ae4bb7811d9.php hxxp://185.247.184[.]7/8c3498a763cc5e26.php hxxps://185.247.184[.]7/8c3498a763cc5e26.php hxxp://23.88.116[.]117/api.php hxxp://95.216.112[.]83/413a030d85acf448.php hxxp://179.43.162[.]2/d8ab11e9f7bc9c13.php hxxp://185.5.248[.]95/c1377b94d43eacea.php hxxp://146.70.161[.]51/58d66e64beb49702/freebl3.dll hxxp://146.70.161[.]51/58d66e64beb49702/mozglue.dll hxxp://146.70.161[.]51/58d66e64beb49702/msvcp140.dll hxxp://146.70.161[.]51/58d66e64beb49702/nss3.dll hxxp://146.70.161[.]51/58d66e64beb49702/softokn3.dll hxxp://146.70.161[.]51/58d66e64beb49702/sqlite3.dll hxxp://146.70.161[.]51/58d66e64beb49702/vcruntime140.dll hxxp://162.0.238[.]10/dbe4ef521ee4cc21/freebl3.dll hxxp://162.0.238[.]10/dbe4ef521ee4cc21/mozglue.dll hxxp://162.0.238[.]10/dbe4ef521ee4cc21/msvcp140.dll hxxp://162.0.238[.]10/dbe4ef521ee4cc21/nss3.dll hxxp://162.0.238[.]10/dbe4ef521ee4cc21/softokn3.dll hxxp://162.0.238[.]10/dbe4ef521ee4cc21/sqlite3.dll hxxp://162.0.238[.]10/dbe4ef521ee4cc21/vcruntime140.dll hxxp://179.43.162[.]2/3461133978273cb9/freebl3.dll hxxp://179.43.162[.]2/3461133978273cb9/mozglue.dll hxxp://179.43.162[.]2/3461133978273cb9/msvcp140.dll hxxp://179.43.162[.]2/3461133978273cb9/nss3.dll hxxp://179.43.162[.]2/3461133978273cb9/softokn3.dll hxxp://179.43.162[.]2/3461133978273cb9/sqlite3.dll hxxp://179.43.162[.]2/3461133978273cb9/vcruntime140.dll hxxp://185.5.248[.]95/libs/freebl3.dll hxxp://185.5.248[.]95/libs/mozglue.dll hxxp://185.5.248[.]95/libs/msvcp140.dll hxxp://185.5.248[.]95/libs/nss3.dll hxxp://185.5.248[.]95/libs/softokn3.dll

TYPE	VALUE
URLs	hxxp://185.5.248[.]95/libs/sqlite3.dll hxxp://185.5.248[.]95/libs/vcruntime140.dll hxxp://666palm[.]com/54fbf4b9ffe8c98d/freebl3.dll hxxp://666palm[.]com/54fbf4b9ffe8c98d/mozglue.dll hxxp://666palm[.]com/54fbf4b9ffe8c98d/msvcp140.dll hxxp://666palm[.]com/54fbf4b9ffe8c98d/nss3.dll hxxp://666palm[.]com/54fbf4b9ffe8c98d/softokn3.dll hxxp://666palm[.]com/54fbf4b9ffe8c98d/sqlite3.dll hxxp://666palm[.]com/54fbf4b9ffe8c98d/vcruntime140.dll hxxp://777palm[.]com/2ccaf544c0cf7de7/freebl3.dll hxxp://777palm[.]com/2ccaf544c0cf7de7/mozglue.dll hxxp://777palm[.]com/2ccaf544c0cf7de7/msvcp140.dll hxxp://777palm[.]com/2ccaf544c0cf7de7/nss3.dll hxxp://777palm[.]com/2ccaf544c0cf7de7/softokn3.dll hxxp://777palm[.]com/2ccaf544c0cf7de7/sqlite3.dll hxxp://777palm[.]com/2ccaf544c0cf7de7/vcruntime140.dll hxxp://94.142.138[.]48/54982f23330528c2/freebl3.dll hxxp://94.142.138[.]48/54982f23330528c2/mozglue.dll hxxp://94.142.138[.]48/54982f23330528c2/msvcp140.dll hxxp://94.142.138[.]48/54982f23330528c2/nss3.dll hxxp://94.142.138[.]48/54982f23330528c2/softokn3.dll hxxp://94.142.138[.]48/54982f23330528c2/sqlite3.dll hxxp://94.142.138[.]48/54982f23330528c2/vcruntime140.dll hxxp://95.216.112[.]83/5840871afdb84f06/sqlite3.dll hxxp://aa-cj[.]com/1b8df000d02ce631/freebl3.dll hxxp://aa-cj[.]com/1b8df000d02ce631/mozglue.dll hxxp://aa-cj[.]com/1b8df000d02ce631/msvcp140.dll hxxp://aa-cj[.]com/1b8df000d02ce631/nss3.dll hxxp://aa-cj[.]com/1b8df000d02ce631/softokn3.dll hxxp://aa-cj[.]com/1b8df000d02ce631/sqlite3.dll hxxp://aa-cj[.]com/1b8df000d02ce631/vcruntime140.dll hxxp://fff-ttt[.]com/a02fc2187db8cd88/freebl3.dll hxxp://fff-ttt[.]com/a02fc2187db8cd88/mozglue.dll hxxp://fff-ttt[.]com/a02fc2187db8cd88/msvcp140.dll hxxp://fff-ttt[.]com/a02fc2187db8cd88/nss3.dll hxxp://fff-ttt[.]com/a02fc2187db8cd88/softokn3.dll hxxp://fff-ttt[.]com/a02fc2187db8cd88/sqlite3.dll hxxp://fff-ttt[.]com/a02fc2187db8cd88/vcruntime140.dll hxxp://moneylandry[.]com/2ccaf544c0cf7de7/freebl3.dll hxxp://moneylandry[.]com/2ccaf544c0cf7de7/mozglue.dll hxxp://moneylandry[.]com/2ccaf544c0cf7de7/msvcp140.dll hxxp://moneylandry[.]com/2ccaf544c0cf7de7/nss3.dll hxxp://moneylandry[.]com/2ccaf544c0cf7de7/softokn3.dll hxxp://moneylandry[.]com/2ccaf544c0cf7de7/sqlite3.dll

TYPE	VALUE
URIs	hxxp://moneylandry[.]com/2ccaf544c0cf7de7/vcruntime140.dll hxxp://94.142.138[.]48/54982f23330528c2/msvcp140.dll hxxp://5.75.138[.]201/9026ac2a280e901d/softokn3.dll hxxp://23.88.116[.]117/libs/sqlite3.dll hxxp://185.247.184[.]7/b00dc1fe53045ca1/sqlite3.dll hxxp://146.70.161[.]51/58d66e64beb49702/freebl3.dll hxxp://95.216.112[.]83/5840871afdb84f06/mozglue.dll hxxp://179.43.162[.]2/3461133978273cb9/sqlite3.dll hxxp://179.43.162[.]2/3461133978273cb9/msvcp140.dll hxxp://185.5.248[.]95/libs/mozglue.dll

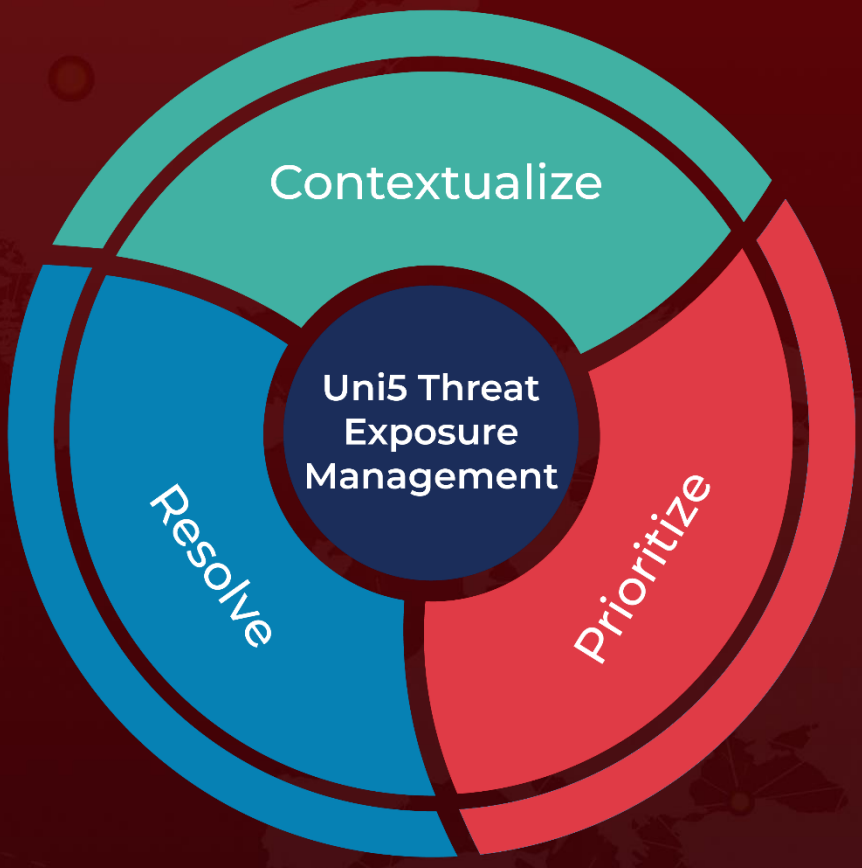
References

https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/

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 21, 2023 . 1:00 AM

More at www.hivepro.com