Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Mystic Stealer Malware Targeting Browsers, Wallets, and Messaging Platforms

Date of Publication	Admiralty Code	TA Number
June 19, 2023	A1	TA2023268

Summary

First appeared: April, 2023
Attack Region: Worldwide (Except CIS countries, which include Russia, Belarus, Moldova, Azerbaijan, Uzbekistan, Kazakhstan, Tajikistan, Armenia, Kyrgyzstan, and Turkmenistan)
Affected Platform: Windows
Malware: Mystic Stealer
Targeted Industries: Healthcare, Cryptocurrency, Finance, and Technology
Attack: Mystic Stealer is an advanced information stealer malware known for its low detection rate, code manipulation techniques and is stealing sensitive data from browsers, wallets & messaging platforms, posing significant risks to individuals and organizations.

Attack Regions

Attack Details

#1

Mystic Stealer is an information stealer malware that was introduced in underground forums in April 2023. It is continuously updated and improved based on user feedback. The malware is designed to steal data from various sources, including web browsers, cryptocurrency wallets, and messaging platforms like Telegram.

#2

It has a low detection rate and uses code manipulation techniques to evade antivirus software. The malware operates in memory to avoid detection and sends the stolen data to over 50 active command and control (C2) servers. Mystic Stealer is available for a subscription fee and is primarily used by cybercriminals to targets companies handling sensitive data and individuals involved in cryptocurrency transactions

#3

Mystic Stealer can target various Windows versions, operates in memory to avoid detection, and uses system calls for compromising targets. It collects and transmits data without requiring client authentication. The builder of the malware provides full control over the command and control panel and offers assistance during installation. Mystic Stealer has features such as data extraction from web browsers, cryptocurrency wallets, Outlook, and more.

#4

The recent updates to Mystic Stealer, introduced by its developer, bring forth loader functionality and a persistence capability. These enhancements raise significant concerns, such as data breaches, financial losses, operational disruptions, and reputational harm. With its expanding capabilities, positive reception in underground forums, and growing demand, Mystic Stealer poses a significant threat in the cybersecurity landscape.

Recommendations

Keep software updated: Regularly update your operating system, web browsers, and other software to ensure you have the latest security patches. This helps protect against known vulnerabilities that malware like Mystic Stealer may exploit.

Use reliable security software: Install reputable antivirus and anti-malware software on your devices. Keep it updated and perform regular scans to detect and remove potential threats, including Mystic Stealer.

Educate and train users: Conduct cybersecurity awareness training for employees and users to teach them how to recognize and avoid potential threats. Emphasize the importance of strong passwords, safe browsing habits, and avoiding suspicious links and attachments.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0006 Credential Access	TA0005 Defense Evasion	TA0002 Execution
TA0007 Discovery	TA0010 Exfiltration	TA0009 Collection	TA0011 Command and Control
TA0001 Initial Access	T1027 Obfuscated Files or Information	T1056 Input Capture	T1068 Exploitation for Privilege Escalation
T1090 Proxy	T1095 Non-Application Layer Protocol	T1102 Web Service	T1113 Screen Capture
T1140 Deobfuscate/Decode Files or Information	T1199 Trusted Relationship	T1203 Exploitation for Client Execution	T1218 System Binary Proxy Execution
T1562 Impair Defenses	T1059 Command and Scripting Interpreter	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1082 System Information Discovery	T1003 OS Credential Dumping		

Indicators of Compromise (IOCs)

TYPE	VALUE
Hostname	admin[.]zscalertbeta[.]net www[.]coloradotruckie[.]com www[.]zerofox[.]com
Domains	africahelp[.]org alchemistwallet[.]io ashrayakrutifoundation[.]org babypicturesultrasound[.]com bayswaterholding[.]com bhandarapolice[.]org coloradotruckie[.]com engtechjournal[.]org gujaratstudy[.]in

TYPE	VALUE
Domains	hanoigarden[.]net marisolblooms[.]com phish[.]report regway[.]com sacredspace-sf[.]com teammsolutions[.]com wordczarmedia[.]com 2fgithub[.]com click[.]compare click[.]contact click[.]discover click[.]open click[.]org click[.]talk click[.]zero continue[.]email github[.]co repository[.]click signup[.]team submit[.]org 123-domaines[.]net akeygen[.]com alerterapp[.]mobi athletesadvantagephysio[.]com comprarepatenteitaliana[.]com cwbusinesswomen[.]org hilltopfarmers[.]co[.]za kavier[.]com[.]mx quillkingston[.]org spotifyapkpremium[.]net wearehumanhuman[.]com wowvillas[.]in e-dato[.]com tatouageclermontfd[.]com
IPV4	167[.]235[.]34[.]144 91[.]121[.]118[.]80 94[.]130[.]164[.]47 135[.]181[.]47[.]95 142[.]132[.]201[.]228 164[.]132[.]200[.]171 185[.]252[.]179[.]18 194[.]169[.]175[.]123 212[.]113[.]106[.]114 213[.]142[.]147[.]235 94[.]23[.]26[.]20

TYPE	VALUE
IPV4	95[.]216[.]32[.]74 45[.]9[.]74[.]110 34[.]19[.]73[.]9 43[.]154[.]7[.]225 94[.]130[.]216[.]165 1[.]13[.]16[.]45 107[.]174[.]205[.]124 116[.]202[.]233[.]49 138[.]112[.]25[.]25 138[.]201[.]88[.]153 159[.]65[.]229[.]149 188[.]40[.]116[.]251 194[.]50[.]153[.]21 23[.]163[.]0[.]179 36[.]75[.]75[.]75 5[.]42[.]94[.]125 5[.]75[.]183[.]169 89[.]23[.]107[.]241 94[.]130[.]165[.]48 94[.]23[.]17[.]222 172[.]67[.]209[.]76 172[.]67[.]201[.]239 172[.]67[.]184[.]175 172[.]67[.]169[.]8 172[.]67[.]155[.]235 172[.]67[.]154[.]57 172[.]67[.]145[.]114 172[.]67[.]144[.]196 104[.]21[.]88[.]238 104[.]21[.]87[.]169 104[.]21[.]76[.]230 104[.]21[.]74[.]252 104[.]21[.]72[.]247 104[.]21[.]63[.]115 104[.]21[.]60[.]13 104[.]21[.]52[.]152 104[.]21[.]38[.]108 104[.]21[.]27[.]68
URLs	https://ioc[.]exchange/@cstromblad/110310524830937297 https://phish[.]report/IOK/indicators/mystic-stealer-88b6ef2f http://135[.]181[.]47[.]95/login/ http://135[.]181[.]47[.]95:13219 http://142[.]132[.]201[.]228:13219

TYPE	VALUE
URLs	http://164[.]132[.]200[.]171:15555 http://164[.]132[.]200[.]171:8005/login/ http://167[.]235[.]34[.]144:13219 http://185[.]252[.]179[.]18/ http://185[.]252[.]179[.]18/admin/ http://185[.]252[.]179[.]18:13219 http://194[.]169[.]175[.]123:13219 http://212[.]113[.]106[.]114/login/ http://213[.]142[.]147[.]235/login/ http://91[.]121[.]118[.]80:13219 http://94[.]130[.]164[.]47:13219 http://94[.]23[.]26[.]20:13219 http://95[.]216[.]32[.]74/login/ http://www[.]coloradotruckie[.]com/admin/ https://www[.]zerofox[.]com/blog/underground-economist-volume-3-issue-9/ https://github[.]co/hiddenchars
MD5	1c8b7141d44e96dcc8c22d3bfdac433c 2438343a7ba217b87b3bfbddaf8a99f9 5753bdaf1c0e6ea82d405ef1ceb452e7 8f2649698c183ba2b52e5e425852109d 9cd292d1fac1768b38a49bc6b288c67d b7be4082bca4e283624704ad2421ce93 baa93d47220682c04d92f7797d9224ce d6d4965d7fe2d90a52736f0db331f81a df80b1e50cfebb0c4dbf5ac51c5d7254
SHA1	218f228454d4032ec65236c1c289e9c256eccda6 37c16fb24784333de0d9823f17c4a336a2992468 84597cc313080e0e4667784b308d031dbe7a11bc f2007a5856fc2a0d1d96b7ea455b7deeeb521447 fef36d60b32c9906b0262a2a0fc0309ef1e9fc17
SHA256	30fb52e4bd3c4866a7b6ccedcfa7a3ff25d73440ca022986a6781af669272639 45d29afc212f2d0be4e198759c3c152bb8d0730ba20d46764a08503eab0b454f 47439044a81b96be0bb34e544da881a393a30f0272616f52f54405b4bf288c7c 5c0987d0ee43f2d149a38fc7320d9ffd02542b2b71ac6b5ea5975f907f9b9bf8 7ab8f9720c5f42b89f4b6feda21e7aa20334ba1230c3aef34b0e6481a3425681 7c185697d3d3a544ca0cef987c27e46b20997c7ef69959c720a8d2e8a03cd5dc

TYPE	VALUE
SHA256	8592e7e7b89cac6bf4fd675f10cc9ba319abd4aa6eaa00fb0b1c42fb645d3410 96ec0e1c018e476d981aa206a657960e5be05cb5383ae5a7fbb274611a9ccdcc acba3311b319a60192be2e29aa8038c863a794be39603a21ee8ee4ccc3ebfca6 ce56e45ad63065bf16bf736dccb452c48327803b434e20d58a6fed04f1ce2da9 fc4aa58229b6b2b948325f6630fe640c2527345ecb0e675592885a5fa6d26f03 018d418015fb546e42e98b2e98d6ff391647149dc2111b3d325e86e9d6d0c3ac 0db263f9a873141d8256f783c35f244c06d490aacc3b680f99794dd8fd59fb59 106f05d8da5e20b0358b34bcb40fbf831494fda51eedea365909506976484093 13f411eed940f4ed7e829bb48c9f8ebec41f8cc250c9c4f9a95d173d17dd78e1 1d11d816e2ecdd4d1b50d9a8c463f4dc2fd98ce0364c235864a61f893db40a9b 30914079c874336cf3b348fb405b6a7039a4605a83c16fbda9a4acba5fe312c8 3b6060ce4008ef78091159ca91cd7db1c1d27f815cfd486568766182bbe904ed 3ff6c46d66421186a0501f13f061ddd803f076f8840ace98b9522e0fcb59518d 4bbced53dfc44d7fe8e1c69e808aa8509c916d783affac4df41165630c8c8d1f 82c569b93da5c18ed649ebd4c2c79437db4611a6a1373e805a3cb001c64130b7 9fbf24abb073f513b4d9786efbd0bc5725664ec6d535251b351ece23a1b4399d b0c4eeb96b3e3eeebca157af052cf3794a9d66d84a62756df2aa44e1e8796dba dee57ea8c9703a24bf968ab22dc814d79d92e5d0e1d6e554bfa28804d36ea471 eacd57adef8557d414cde315acac91fb674107ecc828f3338131ea633b5edcc9 fa746ffb8d6feb7feda417be31d690107fee3e8de890154ec94cd3a2b7c04977 36268bc6941a2474baeac45689f8c4ebab6b1b7546a704d9fa09f23781efbe14 677a2af73eb822b1aeabc0c167f5c2721176e91501dee15254379f41f65268aa 9a84fef3041a45ba832807697051b53dcd18285f4cf7dff9445ce7c8c83a49b2

TYPE	VALUE
SHA256	ce548af940c8498d8b93da09f62f503ef75e4244fe23737bc06a6cd158ef65a9 d635c5612c173f6bd247c44066489b0e62fada6f095f740e6e2c8974a96069e5 dced0115cf9c7d81b718d3dc3ef5de9ebedaa8554864fd7d6b539c7e69fc9244 e06d3c87ff74f2b6ab7760ddfe34757b8f739edc6d10149cf6fafeadb4a57d28 e7b4ca5da61f93dd2318f16173d2997c28da34b161436de6e9bfe5fb574c2376 0fe16de4006af6f0b7eadd97146ac0e8d087381812254db1e9c57b78597cb929 1b88468f241fe986774a4eec5fcd56ca5336444c2296a8c39db6ce43e9e2e9c3 1edb9849fa62fbbb3ddbf5dfdbc80806500871ed19f759d4a24e94a19d09b034 2418bcbbc3d8c3ce06c92e2eed3312a96876b987866c9bc4ec4bb097b2a982d0 2ffe8781517f67923368ab826f315112c1684f0d2bf5d3f394738e49834956b4 5f09d8193f2ab916335c4075b88bea375ac22f1b3a36b3c54ac17b6a309bd699 67281b504a8fad5d29d4d59f8d46c95387a9433c2c38c425035dd58e7c96eb68 e07e7f5d94ee24078d9d86319bb605e3f6a38bf784e99ed23e1e7a4ec29522a4 4700cd0c3d6eb91b8cb3086cb8ab7756439e866eaa13637ed48c44a31dc91fd9 6bd1431c18feb1effd4b56fbc503d93e47d7645d862af0bca5bc2624edaabce4 729d10649091ce03c117e94eadaf71b288f9fff572c0d932fe85bccd5256f007 80dc189181c67d1195f4c704ab5c7ee5cf7461dc2e7fcbd52a427b4383d55089 906a3dca60054842029282ecd4ccec563df298224b2fb7386286ea1e6c324953 921016870530baaa969aeca6dcb86a0d6333936a11a0e62ae39e9403814a3e0b 9cd0767b5a41d4f1b85c175ca89f98633288ad33272a4a1cd45ea439510390aa 9ffa2308b2e38527388a1e7745d9a12424698c0eb66ec4f8ea95560e2c4e9cc4

References

https://www.cyfirma.com/outofband/mystic-stealer-evolving-stealth-malware/

https://www.zscaler.com/blogs/security-research/mystic-stealer

https://github.com/threatlabz/iocs/blob/main/mystic_stealer/c2s.txt

https://github.com/threatlabz/iocs/blob/main/mystic_stealer/grand_cluster_domains.txt

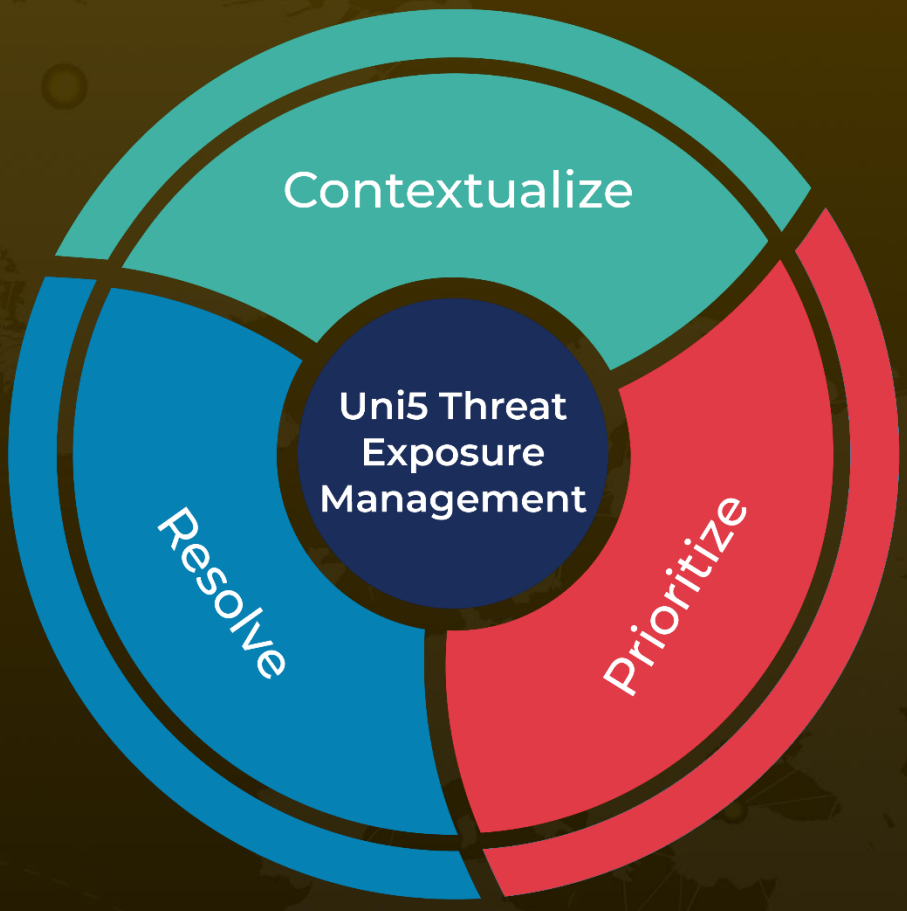
https://github.com/threatlabz/iocs/blob/main/mystic_stealer/grand_cluster_nameservers.txt

https://github.com/threatlabz/iocs/blob/main/mystic_stealer/grand_cluster_domain_whois.txt

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 19, 2023 • 5:00 AM

More at www.hivepro.com