Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

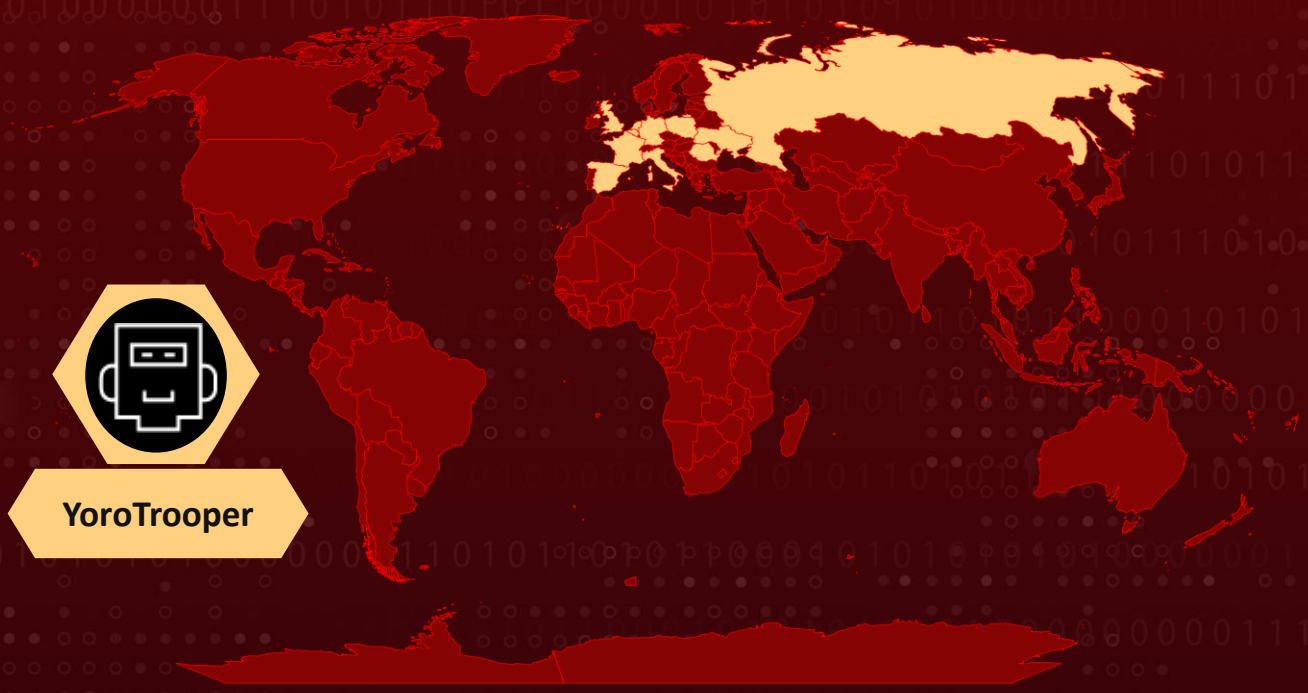
New YoroTrooper Threat Actor Targeting Government and Energy Organizations

Date of Publication	Admiralty code	TA Number
March 16, 2023	A1	TA2023141

Summary

First Appearance: July 2022
Actor Name: YoroTrooper
Target Countries: Europe and CIS countries
Target Sectors: Energy and Government
Malware: Warzone RAT/AveMaria, LodaRAT, and Stink stealer

Actor Map



Actor Details

#1

A new threat actor named "YoroTrooper," has been conducting espionage campaigns since at least June 2022. The group's main motivation appears to be espionage, and they register malicious domains or typo-squatted domains to trick their victims. The group primarily targets government or energy organizations in Azerbaijan, Tajikistan, Kyrgyzstan, and other Commonwealth of Independent States (CIS) countries.

#2

They have also successfully compromised accounts from two international organizations, including a critical European Union (EU) healthcare agency and the World Intellectual Property Organization (WIPO). YoroTrooper's tools include Python-based custom-built and open-source information stealers, such as Stink stealer they deploy commodity malware Warzone, and LodaRAT, for remote access. The group's operators are likely Russian language speakers, and they have targeted individuals speaking that specific language.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
YoroTrooper	Unknown	Europe and CIS countries	Energy and Government
	MOTIVE		
	Espionage and Information theft		

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 actor 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

TA0042 Resource Development	TA0001 Initial Access	TA0007 Discovery	TA0008 Lateral Movement
TA0011 Command and Control	TA0003 Persistence	TA0005 Defense Evasion	TA0040 Impact
TA0004 Privilege Escalation	TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration
T1059 Command and Scripting Interpreter	T1003 OS Credential Dumping	T1036 Masquerading	T1027 Obfuscated Files or Information
T1056 Input Capture	T1057 Process Discovery	T1102 Web Service	T1113 Screen Capture
T1140 Deobfuscate/Decode Files or Information,	T1496 Resource Hijacking	T1505 Server Software Component	T1547 Boot or Logon Autostart Execution
T1566 Phishing	T1070 Indicator Removal		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7aa8ae8d3f8f37e3fdefc30d161fdd4482885a7312848a7b660165c0cefb8fce ddeb109a97e3689b63d4ee848d4c23b0646c8070badebcc852577be0b64c7397 5c9fbd70e73d463b0265881d904a8fca22f92b0cce24190ed16c3d8899d4120a e80fbef0be6a6688f9840ab6cd295f765d7f2fab8080896cfd0bf7e2c4c4c5da 02fc87210deab1be31568fbcd80a349b9b2a9a1e19fe5ed36d9723ff1a603ca8 d1d534028d76ea6c293d606adff4aa4ddf1d467b7329a869df5c38a0686cd15d 176b336f425bc15651672f96f70149873b10a3badfa040c8943bfe54955e043d cf1f70900b4a903dc1a868a60e192791cf26cf54f22b9a742e28e60b291d81ef 8d870328912e50f4b30e091589ac8191dfcb3b7b607156550d5468fa37b03449 6501dd570761f2bd3eff4e3416baef57c2ff514b8dd35c9c80a37e2d489d714f 9f8d3ee51af949ae15ca18c6fdd8e6f2d1c7970c8265bd5bb2bb2d92d358c04a f5664b2a20367afe8c291399ea3da0af3c1001617b6bd497d423f44b4853d273 a6761bbbb9cc206653ccee4154c38cf5ea136345c12cf7ca9af50a320fc9e0ed f2a17d140efcf94800c6dc4a2454d0f8320a9e41c04145fbbeeea84ea0321d74 1b82739880e1851d032b09de787033bd19135c8496124cd505b32afe4212b7b0 cce5b5a282ba6637cfd840cee65739a797485e024f0259e98b35cc38cc5dca3a bab2776edef029cf4632663c59297bb25eced4f7dece18cfa45e88ce2ece42a0 0aad58903f0524b82a3388b1aa6302c974dfc4ac593435f2bc0f1b9eb3ced6db 3f6d866f09cfabb1aa2a0393d290533ed31705c87b85f77edc3fdd51b90f6e24 aee816d2bb3b7691474ab4f90f8d344c4aa03e64093ca020048c7a0716e20694 348f2713fba8f0543600bf38c8427eb9996769654987516e3f0202f7bcf17228 0e0b5437592b48b358c2a4174308c7793213701704e4695bb42e03dbb4284f05 1f591a5c726b279174ce06f3fa9e5db0019b12c9b5b8e19a529bf6cb1153f164 21c2ff30adb655bad806a9107afdb7954d02356d5f4cb709a55fd65fbf84361f a26e8014e67005f1516af849ea4534db2d7a0c8c8b7fffd7890111363439c3f7 30574abb4af368912a1f928fe67427bf3e678a205169516d7590f28d0b4bb286 e3f35f911f179f96352cfc5887ee5e82a82069e022b60cb35de453f1eb76d1d3 4f237b5aa3ff4fc4e3014f693c27a1cba94fc24f3a6054c28d090592343c06a2 2293db2e9500cd0a8e76616c5569ef202a9562e8e2148890fa2186dbf7e8a2ee 9056feffc79bd34ec2570aac09fdb2165b1bd4d27edf502f32e05970952f2bdd 4bde6056cf67d410376bd3c319706032eb899a7548928842d63a886ffd82e1d6 41e8adc62dbe14d0364cb5d0db169d2bab52757912bd44a7da6da987dd09b0bd af5d893912f4888eb0c29f02015009187c093fc2cf32bdb6d70eff79b96a29e8 2b433f5a2aa1b75d75460e6a22f142a47d9c0bc0a89035f767e10a8b571c7b28 d9b8a2d9442ae51002fb6922a5600cf93e83fe4a0534a654b0acbb58bafc5bf4 331fd9e2cfe82d0131f9901f168fa91fe60c200b92b2878b704f34d4558e22f9 644768aca1cecf034005cda0c6cef682a8797fa45fd5f845081bea41b3990b2d 3479b9213da7e381a47e579f011a6a299e0827aff7bccb0900d61ef9ac485a10 adccfea997a38c8245784cb9ddf22c4dc739539b4faac09e33acf8ab5a727bbd C868185e0051c53c90ff4d5f2503b5647e8a3f3aac4aa2d0065f2178af60f7cf fa06b71c4c18bffd0283d07fa13a113a6999d2b597cd91eacdc5da3f240a54fb 96a70a20a24959dc270e12889e4bff81a86c0e4a0f23b8dc9976843940ec8ddd f3d8916b99d7e6301a885b2ec4aaf9635f1713464c53b1604d3b4e1abd673c36 c02c7b9a82a75cb251b2b7307503284a408f20e689f1be30fe50173a8b6e288b db9a6efd5d64ba0ba1783c51b6d430873518fa032bf5265c6837c7674321e183 fefddb37c5cfd0fa9746b545c825142df8e6b1f07925f6580a15d018fefb00c7

TYPE	VALUE
SHA256	baa924292408e6ba128ef07aa21f065eb45dd2b85322a9db06fc5a828119ba65 83d96e476aa72d7ff0d3d0a02f96113834a1c7fdbe523379f7de57f7f06a2005 5eb91f4b9f68a02cf2005dd2e95d820ae5be509659a0045ded606f650d028f68 85df1d60db3406ea3d7e3f55d6f96acf4656c98c1a97411a4811062de35893b2 00284cad6f38d59d9b46a28a1a6789077f298995c79ca18ef87c4c98b14961ac 1e4091ce270bf22254868f40f4a282320c3763ee803c0276f863696a2ed9b463 d01ac7ecd1f3280f42f2956f0606b96b9da9914b564ef76d45dded3e2f0514d2 4b9811f1f8176ec9f2ee647a4c2f171854f296fbc18e47cc08eb82357a6eeec7 fd7fe71185a70f281545a815fce9837453450bb29031954dd2301fe4da99250d 00466d76832193b3f8be186d00e48005b460d6895798a67bc1c21e4655cb2e62 df75defc7bde078faefcb2c1c32f16c141337a1583bd0bc14f6d93c135d34289 9a8c72acd91f5a89dbf9fdb7cc4055ae8cf9af60f94187dbab83689da9b33f4e 8023da2c9d45536dee2020d38edec20a88b8f5115fca6335929f94c683d60dd5 f0f9e05070d9b9804bd65ef4aad9347c69b24a3a7f706cf5771f4ecf3706efeb aa696fd2f4e78f203e44fa282fb97aa31086c2b5c6040afa507c39ffd5847ef3 27e69c96af1f692ce43706904de61f841abec45a57ff0b7a7d3cbbb417455a53
IPV4	162.33.177[.]195 172.105.215[.]208 172.86.75[.]220 192.153.57[.]67 193.149.129[.133 193.149.176[.]254 206.188.196[.]86 45.227.252[.]247 45.61.136[.]175 45.61.136[.]64 45.61.138[.]243 46.161.40[.]164 46.175.148[.]147 64.190.113[.]57 64.227.24[.]240 89.22.232[.]145 89.22.233[.]149 94.103.86[.]38 94.20.72[.]7
URLs	http://172[.]86[.]75[.]220/arxiv[.]rar http://162[.]33[.]177[.]195/ http://168[.]100[.]11[.]137/ http://45[.]61[.]136[.]175/ http://mail[.]mfa[.]az- link[.]email/+csco+0075676763663a2f2f31302e3130302e3230302e32++/+csco +0075676763663a2f2f31302e3130302e3230302e32++/_task=login http://143[.]198[.]80[.]235/upd[.]exe http://172[.]86[.]75[.]220/02[.]08[.]2022[.]exe http://172[.]86[.]75[.]220/123[.]hta http://178[.]20[.]45[.]52/sec/pes[.]exe http://193[.]149[.]176[.]254/file[.]exe http://193[.]149[.]176[.]254/hstart[.]exe http://212[.]24[.]106[.]218/spoolsv[.]exe http://45[.]61[.]136[.]64/update[.]exe http://45[.]61[.]137[.]32/attachments/download/02[.]08[.]2022[.]exe

TYPE	VALUE
URLs	http://45[.]61[.]137[.]32/Scanned_document[.]exe http://45[.]61[.]137[.]32/svvhost[.]rar http://45[.]61[.]137[.]32/www[.]exe http://89[.]22[.]233[.]149/ms7[.]hta http://89[.]22[.]233[.]149/Spisok_sotrudnikov_1_chast[.]exe http://94[.]103[.]86[.]38/file[.]exe http://94[.]103[.]86[.]38/ms1[.]hta http://94[.]103[.]86[.]38/wz[.]exe http://account[.]mail[.]ru[.]sigriup[.]site/ http://account[.]nail[.]ru[.]horme[.]info/ http://becloud[.]website/svchest[.]exe http://e[.]mail[.]ru[.]autn[.]tech/ http://e[.]mail[.]ru[.]portal-inbox[.]com/ http://e[.]nail[.]ru[.]imbox[.]link/home/files/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5%20%D0%BF%D0%B8%D1%81%D1%8C%D0%BC%D0%BE[.]rar http://iacis[.]ru/download/spoolsv[.]exe http://iacis[.]ru/log/spoolsv[.]exe http://mfa-tj[.]download/26478_0001[.]rar https://45[.]61[.]139[.]224/ https://api[.]telegram[.]org/bot5885840251:AAG8HoCjrI1QANXkA4oqnJ60lgPP7w86Clg/sendMessage?chat_id=5683385422 https://api[.]telegram[.]org/bot5974645737:AAEj2Y0MFGEHmvrFSINWeZcAsbjuUkLysnA/sendMessage?chat_id=5683385422 https://attachment-posts[.]cc/files[.]rar https://becloud[.]website/obfuscated_compressed_some[.]exe https://becloud[.]website/svchest[.]exe https://capitaltrust[.]uz/file[.]pdf https://capitaltrust[.]uz/lsaasc[.]exe https://capitaltrust[.]uz/lsaca[.]exe https://capitaltrust[.]uz/lsacs[.]exe https://capitaltrust[.]uz/s[.]hta https://capitaltrust[.]uz/stel[.]hta https://cloud[.]archive-downloader[.]com/lsacs[.]exe https://cloud[.]archive-downloader[.]com/s[.]hta https://e-aks[.]uz/file[.]pdf https://e-aks[.]uz/lsacs[.]exe https://e-aks[.]uz/s[.]hta https://e[.]nail[.]ru[.]imbox[.]link/ https://iacis[.]ru/download/spoolsv[.]exe https://iacis[.]ru/log/spoolsv[.]exe https://mail[.]mfa[.]az-link[.]email/+CSCO+0075676763663A2F2F31302E3130302E3230302E32++/+CSCO+0075676763663A2F2F31302E3130302E3230302E32++/_task=login/ https://mfa-tj[.]download/lo[.]hta https://portal-inbox[.]com/ https://telegram[.]akipress[.]news/1r[.]exe

TYPE	VALUE
Domains	akipress[.]news, archive-downloader[.]com, attachment-posts[.]cc, becloud[.]cc, becloud[.]website, belaes[.]by[.]authentication[.]becloud[.]cc, belstat[.]gov[.]by[.]attachment-posts[.]cc, capitaltrust[.]uz, cloud[.]archive-downloader[.]com, doc[.]az-link[.]email, docscpcpipe[.]inro[.]link, download[.]az-link[.]email, e-aks[.]uz, e[.]login[.]mail-ru[.]link, e[.]mail[.]ru[.]autn[.]tech, e[.]mail[.]ru[.]mypolicy[.]top, e[.]mail[.]ru[.]portal-inbox[.]com, e[.]nail[.]ru[.]imbox[.]link, account[.]mail[.]ru[.]sigriup[.]site, account[.]nail[.]ru[.]horme[.]info, account[.]nail[.]ru[.]inro[.]link, accountyandex[.]inro[.]link, hbfyewtuvfbhsbdjhjwebfy[.]net, hse[.]ru[.]attachment-posts[.]cc, imbox[.]link, industry[.]tj[.]mypolicy[.]top, mail[.]agro[.]gov[.]kg[.]openingfile[.]net, mail[.]belaes[.]by[.]authentication[.]becloud[.]cc, mail[.]economy[.]qov[.]az-link[.]email, mail[.]g-cloud[.]by[.]authentication[.]becloud[.]cc, mail[.]gov[.]az-link[.]email, mail[.]hse[.]ru[.]attachment-posts[.]cc, mail[.]iacis[.]ru[.]autn[.]tech, mail[.]mfa[.]az-link[.]email, mail[.]mfa[.]gov[.]kg[.]openingfile[.]net, mail[.]mgimo[.]ru[.]sigriup[.]site, mail[.]ru[.]authentification[.]becloud[.]cc, mailacgov[.]inro[.]link, mailaviacomplect[.]inro[.]link, maileecommission[.]inro[.]link, mfa-tj[.]download, minsk[.]gov[.]by[.]attachment-posts[.]cc, moscpcpipe[.]inro[.]link, mypolicy[.]top, newint[.]mid[.]ru[.]owaut[.]ru,

TYPE	VALUE
Domains	openingfile[.]net, portal-inbox[.]com, rnail[.]iterrf[.]ru[.]inro[.]link, rnail[.]mintrans[.]gov[.]ru[.]inro[.]link, rnail[.]rnid[.]ru[.]inro[.]link, srm[.]mfa[.]tj[.]uzdaily[.]news, sts[.]mfa[.]gov[.]tr[.]mypolicy[.]top, true[.]az-link[.]email,

References

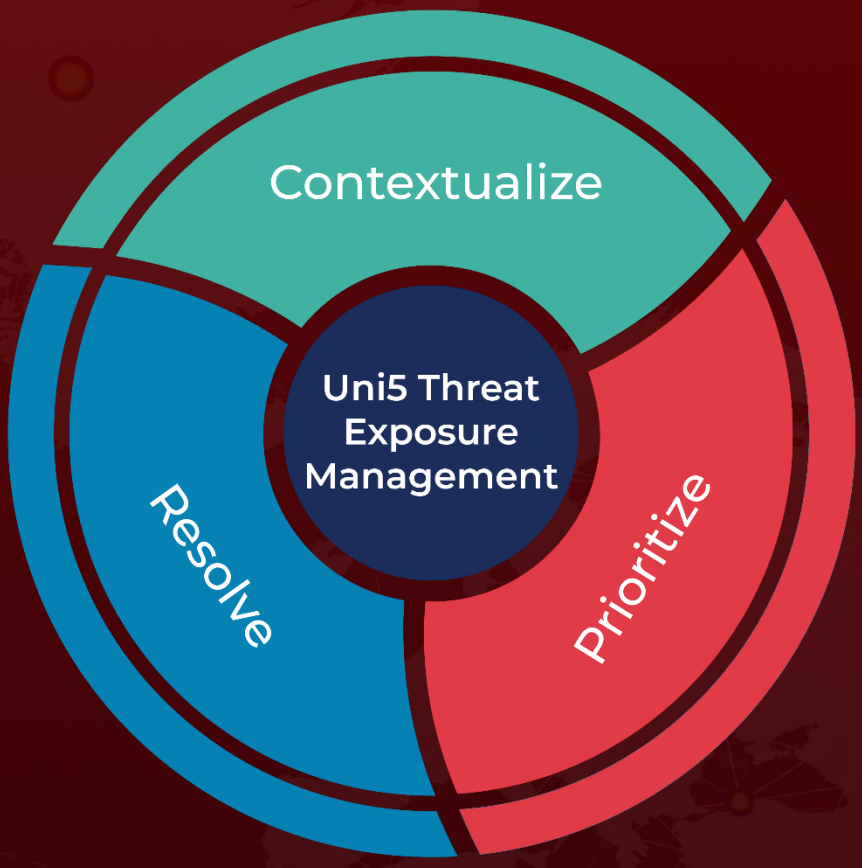
https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/

https://github.com/Cisco-Talos/IOCs/blob/main/2023/03/YoroTrooper.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

March 16, 2023 • 8:00 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com