KPMG Cyber Threat Intelligence Platform

YoroTrooper – Motivated by Geo-Political Interests

YoroTrooper, an emerging threat motivated by espionage can no longer be considered a nascent threat, following the recent success streak in targeting organizations of political importance such as the World Intellectual Property Organization (WIPO) & EU Healthcare agency. Since its origin in June 2022, this allegedly Russian speaking group has been making its mark on various government agencies, embassies & energy giants in Azerbaijan, Belarus, Tajikistan & other CIS countries.

Registers legitimate looking malicious domains or typo-squatted domains & uses spear-phishing mails equipped with malicious archive (RAR/ZIP) pretending to be a document of strategy or diplomacy. Malicious LNK files then leverage "mshta.exe" to fetch HTA files from attacker's server, while opening decoy PDFs to avert suspicion. HTA downloads next-stage dropper executable that then downloads the final payload. Heavy use of both custom-built & off-the-market malware to achieve the target, like Stink stealer, WarzoneRAT, LodaRAT, etc., to steal credentials and gain remote access. In house malware includes Python based wrapped with Nuitka & Pyinstaller to enable standalone execution. Evolves tools with each campaign which has spanned from commodity RATs & stealers, Python-based info stealers, RATs, reverse shells & C based keyloggers. Gathers large chunks of data such as system information, credentials from multiple applications, cookies, browser history, screenshots, etc. Collected data is preferably exfiltrated through Telegram bot, while using the same as C2 channel to orchestrate the attack and lateral movement efforts.

Although of unclear origin, gauging from the level of sophistication and ever evolving toolset, chances that YoroTrooper is backed by nation-state interests might not be a gamble after-all.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

YoroTrooper – Motivated by Geo-Political Interests

Indicators of Compromise: IP	
94.20.72[.]7	89.22.232[.]145
45.61.136[.]64	89.22.233[.]149
94.103.86[.]38	162.33.177[.]195
172.86.75[.]220	206.188.196[.]86
192.153.57[.]67	45.227.252[.]247
45.61.136[.]175	46.175.148[.]147
45.61.138.[.]243	172.105.215[.]208
46.161.40[.]164	193.149.129[.]133
64.190.113[.]57	193.149.176[.]254

Indicators of Compromise: Domains	
iacis[.]ru	mfa-tj[.]download
e-aks[.]uz	capitaltrust[.]uz
imbox[.]link	becloud[.]website
becloud[.]cc	portal-inbox[.]com
mypolicy[.]top	attachment-posts[.]cc
akipress[.]news	archive-downloader[.]com
openingfile[.]net	hbfyewtuvfbhsbdjhjwebfy[.]net

Indicators of Compromise: Hashes
0771482338129016710bf3ff317dc49e
0dcd949983cb49ad360428f464c19a9e
11ed3f8c1a8fce3794b650bbdf09c265
20a7f8de38864aab64a6a22c55bfa11b
2300a4eb4bf1216506900e6040820843
23c0523af70c2144cb3e29101039512d
25b31bcb8c6a3ce3fc3a3da6ba4df156
3214d869a359c2f98d715b4f4a2abf12
35ee76314cb845b7515c9343e7a1037b
3a84733d23a20d8e684c2381884677de
4443dc6bc9015b039ab514e4b23be5d6
4b841b2225c04a0352899ed423d360a0

KPMG

KPMG Cyber Threat Intelligence Platform

YoroTrooper – Motivated by Geo-Political Interests

Indicators of Compromise: Hashes
544a65bfe51385bb148f23a4e3f140d6
56d1e9d11a8752e1c06e542e78e9c3e4
74525ec764bce9ab029e6a73b9f3454b
7991987b2a79059558cdc31e89d03874
8551f15f682af200352251cd655ad5d8
a75d027078a18717bbb75b4a8444a91b
dbe82825ff5afeba8b44ca534b0b3500
e581196f2635ba5cb25c3a1121a6ed58
e9064cfea8cb006100afc211bc0b8f1b
edb0c08f8b6bb179b4395d8a95619d07
27880bebe47b557dd5afa04dff803c10a719f8e4
296f7044fbe267530a3ec2c42358dfbc888be716
36345ef692c00eabb2f6254766795ac9f000fe2c
4040bb7e4ebc98c22bda98680b207ec89767b759
4a0874d506854a996b429b7c11e2057e86583dd2
4b42dae3afdf5c89cecbad77601e4ab8a99f2164
5036110ebc0096e779f3c533469cf041cac92dd3
69e5b64e799f2bc58e1bccf56cb831faf4c7847f
6e404728ba443ed3a06c45f113be5286a2f82408
7d49c20c833bbb21ef974692777e199c08dc05d4
8260b7286bdf17a00846820228e937d9d5b34a2e
839c09cb51886f4bf5fa8d4f2b02f0db4637210a
9e161e9c0c01912780df05d81b442a12633546e5
a3035b3dbf360e4e61517c231661b9cf9891a3f8
a9b62b243be52b11667a69dd1d1da744c38a805d
aaa7e3192aa75b87b0e4877e11e12c5f98493e22
b0935265193593373bf2744f11ce7acdd4a1970b
b5e448b0b289fcae5c4b742b72e19531d71e897b
b61ab26a38322ee466e18fa381d0ede106f39e57
ed7636f5f6fb9b4ff0611ca88af431659af70b11
f325a39f2e89a683de96c3be97f730bc6871920f
f8d87d5b251671af624c3eaf7ac5cc42a0acadd0
f9e977021edca328159ac31738b33168e89cfb10
7aa8ae8d3f8f37e3fdefc30d161fdd4482885a7312848a7b660165c0cefb8fce

KPMG

KPMG Cyber Threat Intelligence Platform

YoroTrooper – Motivated by Geo-Political Interests

Indicators of Compromise: Hashes
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

KPMG

KPMG Cyber Threat Intelligence Platform

YoroTrooper – Motivated by Geo-Political Interests

Indicators of Compromise: Hashes
331fd9e2cfe82d0131f9901f168fa91fe60c200b92b2878b704f34d4558e22f9
644768aca1cecf034005cda0c6cef682a8797fa45fd5f845081bea41b3990b2d
3479b9213da7e381a47e579f011a6a299e0827aff7bccb0900d61ef9ac485a10
adccfea997a38c8245784cb9ddf22c4dc739539b4faac09e33acf8ab5a727bbd
c868185e0051c53c90ff4d5f2503b5647e8a3f3aac4aa2d0065f2178af60f7cf
fa06b71c4c18bffd0283d07fa13a113a6999d2b597cd91eacdc5da3f240a54fb
96a70a20a24959dc270e12889e4bff81a86c0e4a0f23b8dc9976843940ec8ddd
f3d8916b99d7e6301a885b2ec4aaf9635f1713464c53b1604d3b4e1abd673c36
c02c7b9a82a75cb251b2b7307503284a408f20e689f1be30fe50173a8b6e288b
db9a6efd5d64ba0ba1783c51b6d430873518fa032bf5265c6837c7674321e183
fefddb37c5cfd0fa9746b545c825142df8e6b1f07925f6580a15d018fefb00c7
baa924292408e6ba128ef07aa21f065eb45dd2b85322a9db06fc5a828119ba65
83d96e476aa72d7ff0d3d0a02f96113834a1c7fdbe523379f7de57f7f06a2005
5eb91f4b9f68a02cf2005dd2e95d820ae5be509659a0045ded606f650d028f68
85df1d60db3406ea3d7e3f55d6f96acf4656c98c1a97411a4811062de35893b2
00284cad6f38d59d9b46a28a1a6789077f298995c79ca18ef87c4c98b14961ac
1e4091ce270bf22254868f40f4a282320c3763ee803c0276f863696a2ed9b463
d01ac7ecd1f3280f42f2956f0606b96b9da9914b564ef76d45dded3e2f0514d2
4b9811f1f8176ec9f2ee647a4c2f171854f296fbc18e47cc08eb82357a6eeec7
fd7fe71185a70f281545a815fce9837453450bb29031954dd2301fe4da99250d
00466d76832193b3f8be186d00e48005b460d6895798a67bc1c21e4655cb2e62
df75defc7bde078faefcb2c1c32f16c141337a1583bd0bc14f6d93c135d34289
9a8c72acd91f5a89dbf9fdb7cc4055ae8cf9af60f94187dbab83689da9b33f4e
8023da2c9d45536dee2020d38edec20a88b8f5115fca6335929f94c683d60dd5
f0f9e05070d9b9804bd65ef4aad9347c69b24a3a7f706cf5771f4ecf3706efeb
aa696fd2f4e78f203e44fa282fb97aa31086c2b5c6040afa507c39ffd5847ef3
27e69c96af1f692ce43706904de61f841abec45a57ff0b7a7d3cbbb417455a53