Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

YoroTrooper Covert Cyber Espionage Masters of Kazakhstan

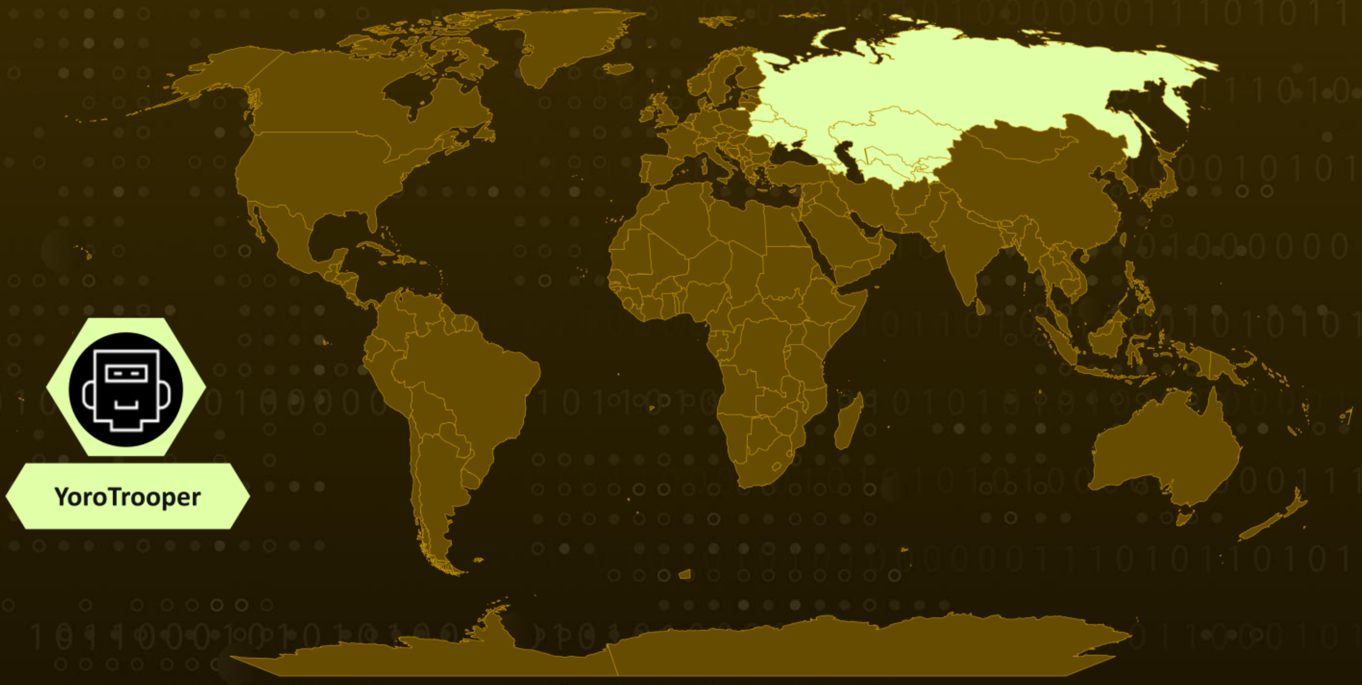
Date of Publication	Admiralty Code	TA Number
October 26, 2023	A1	TA2023435

Summary

Attack Began: June 2023
Actor: YoroTrooper
Attack Region: Commonwealth of Independent States (CIS) countries
Targeted Industries: Government, Energy, Telecommunications, Transport, Foreign Affairs, Nuclear

Attack: YoroTrooper, a stealthy threat actor primarily focused on espionage, first emerged in June 2022. YoroTrooper's targets appear to be concentrated within the Commonwealth of Independent States (CIS) nations, with its operatives successfully infiltrating numerous state-owned websites and gaining access to the accounts of government officials in these regions.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 YoroTrooper is a secretive threat actor with a strong emphasis on espionage. It is believed to consist of operatives originating from Kazakhstan. The group employs a range of tactics to conceal the true source of its operations, often making its malicious activities appear as if they originate from Azerbaijan. In addition to using both readily available and custom-designed malware, YoroTrooper heavily relies on phishing emails to entice victims into visiting websites where their credentials are harvested.

#2 What sets this group apart is its adaptability; they constantly learn and adjust their methods to carry out their malicious actions. YoroTrooper actively employs vulnerability scanners like Acunetix and leverages publicly accessible data sources such as Shodan, Google, and Censys to discover weaknesses in a target's infrastructure, with a particular focus on compromising their publicly accessible servers.

#3 The primary objective of YoroTrooper's malware-based operations is data theft. In response to the exposure of their campaigns to the public, this threat actor has undergone a strategic transformation. They have shifted from using off-the-shelf malware to crafting custom tools in programming languages like Python, PowerShell, Golang, and Rust.

#4 A significant update in their infection process involves adapting their Python-based remote access trojan (RAT) to PowerShell and employing a custom-built interactive reverse shell to execute commands on infected endpoints via cmd.exe. Despite these changes, the core functionality remains consistent, with the RAT receiving commands and transmitting data to command-and-control servers hosted on the Telegram platform.

Recommendations

Email Security Measures: Implement robust email security measures to identify and block phishing emails. Use advanced email filtering and authentication protocols to reduce the likelihood of falling victim to YoroTrooper's phishing attacks.

Deploy Endpoint Detection and Response: Implement advanced endpoint security measures, including Endpoint Detection and Response (EDR) solutions for real-time monitoring and rapid response. Additionally, employ deception technologies, like honeypots and honeynets, to attract and identify malicious actors, enhancing early threat detection and attribution.

Network Segmentation: Segment your network into isolated zones to limit lateral movement for attackers and reduce the impact of a breach. Deploy network traffic analysis tools to monitor and analyze patterns of communication between endpoints and potential command and control servers

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0010** Exfiltration	**TA0011** Command and Control
T1595 Active Scanning	**T1590** Gather Victim Network Information	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application
T1566 Phishing	**T1059** Command and Scripting Interpreter	**T1548** Abuse Elevation Control Mechanism	**T1574** Hijack Execution Flow
T1027 Obfuscated Files or Information	**T1046** Network Service Discovery	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	168[.]100[.]8[.]21, 46[.]161[.]27[.]151
Emails	n.ayyubov[at]mail[.]ru, danyjackson120293[at]proton[.]me

TYPE	VALUE
SHA256	8131bd594aff4f4e233ac802799df3422f423dc28e96646a09a2656563c4ad7c, a3b1c3faa287f6ba2f307af954bb2503b787ae2cd59ec65e0bdd7a0595ea8c7e, Ed8c04a3e2d95d5ad8e2327a56d221715f06ed84eb9dc44ff86acff4076629d7, 9b81c5811ef3742cd4f45b6c3ba1ace70a0ce661acc42d974beaeddf307dd53d, B6a5d6696cbb1690f75b0d9a42df8cefd444cfd3749be474535948a70ff2efd2, F55b41ca475f411af10eaf082754c6e8b7a648da4fa72c23cbfea9fa13a91d88, E0c7479e36b20cd7c3ca85966968b258b1148eb645a544230062ec5dff563258, ab6a8718dffbe48fd8b3a74f4bcb241cde281acf9e378b0c2370a040e4d827da, a5d8924f7f285f907e7e394635f31564a371dd58fad8fc621bacd5a55ca5929b, E95e64e7ba4ef18df0282df15fc97cc76ba57ea250a0df51469337f561cc67d3, 832d58d9e067730a5705c8c307fd51c044d9697911043be9564593e05216e82a, Da75326cfebcca12c01e4a51ef77547465e03316c5f6fbce901ddcfe6425b753, 1e350b316cbc42917f10f6f12fa2a0b8ed2fa6b0159c36141bce18edb6ea7aa0, 57d0336c0dbaf455229d2689bf82f9678eb519e017d40ba60a6d6b90f87321f8, 30a969fa0492479b1c6ef6d23f8fcccf3d7af35b235d74cab2c0c2fc8c212ad4, 5a6b089b1d2dd66948f24ed2d9464ce61942c19e98922dd77d36427f6cded634, a25db1457cf6b52be481929755dd9699ed8d009aa30295b2bf54710cb07a2f22, 56fc680799999e38ce84c80e27788839f35ee817816de15b90aa39332fcc5aee, 37c369f9a9cac898af2668b1287dea34c753119071a1c447b0bfecd171709340, 93829ee93688a31f90572316ecb21702eab04886c8899c0a59deda3b2f96c4be, 0a9908d8c4de050149883ca17625bbe97830ba61c3fe6b0ef704c65361027add, 1828e2df0ad76ea503af7206447e40482669bb25624a60b0f77743cd70f819f6, 941be28004afc2c7c8248a86b5857a35ab303beb33c704640852741b925558a1,

TYPE	VALUE
SHA256	8921c20539fc019a9127285ca43b35610f8ecb0151872cdd50acdaa12c23722d, b4eac90e866f5ad8af37b43f5e9459e59ee1e7e2cbb284703c0ef7b1a13ee723
URLs	hxxp[://]46[.]161[.]27[.]151:80/c1[.]exe, hxxp[://]46[.]161[.]40[.]164/wwser[.]exe, hxxp[://]tpp[.]tj/T/rat[.]php, hxxps[://]tpp[.]tj/T/rat[.]php, hxxp[://]46[.]161[.]40[.]164/resoluton[.]exe, hxxp[://]tpp[.]tj/285/file[.]js, hxxp[://]tpp[.]tj/285/png[.]php, hxxp[://]tpp[.]tj/285/startpng[.]js, hxxp[://]tpp[.]tj/285/uap[.]txt, hxxp[://]tpp[.]tj/285/update[.]hta, hxxp[://]168[.]100[.]8[.]21/file[.]js, hxxp[://]168[.]100[.]8[.]21/mshostss[.]rar, hxxp[://]168[.]100[.]8[.]21/png[.]php, hxxp[://]168[.]100[.]8[.]21/rat[.]js, hxxp[://]168[.]100[.]8[.]21/rat[.]php, hxxp[://]168[.]100[.]8[.]21/startpng[.]js, hxxp[://]168[.]100[.]8[.]21/win[.]hta, hxxp[://]46[.]161[.]40[.]164/main2[.]exe, hxxp[://]46[.]161[.]40[.]164/main[.]exe, hxxp[://]tpp[.]tj/BossMaster[.]txt, hxxp[://]tpp[.]tj/T/rat[.]js, hxxps[://]tpp[.]tj/main[.]exe, hxxps[://]tpp[.]tj/T/file[.]js, hxxps[://]tpp[.]tj/T/png[.]php, hxxps[://]tpp[.]tj/T/startpng[.]js, hxxps[://]tpp[.]tj/T/sys[.]hta, hxxps[://]tpp[.]tj/rightupsbot[.]txt, hxxp[://]168[.]100[.]8[.]242/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/, hxxp[://]168[.]100[.]8[.]242/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_files/2208281[.]pdf, hxxp[://]168[.]100[.]8[.]242/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_files/Az[.]pdf, hxxp[://]168[.]100[.]8[.]242/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/logout&_token=DFaH9AmHXbZKTApPbTvES2llxU6GZTl3, hxxp[://]168[.]100[.]8[.]36/+CSCO+0075676763663A2F2F31302E3130302E3230302E32++/+CSCO+0075676763663A2F2F31302E3130302E3230302E32++/logout&_token=DFaH9AmHXbZKTApPbTvES2llxU6GZTl3/,

TYPE	VALUE
URLs	hxxp[://]168[.]100[.]8[.]36/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_files/file[.]php, hxxp[://]168[.]100[.]8[.]36/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_files/login[.]php, hxxp[://]168[.]100[.]8[.]36/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/logout&_token=DFaH9AmHXbZKTApPbTvES2llxU6GZTl3, hxxp[://]206[.]166[.]251[.]146/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_files/Az[.]pdf, hxxp[://]206[.]166[.]251[.]146/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/logout&_token=DFaH9AmHXbZKTApPbTvES2llxU6GZTl3, hxxps[://]auth[.]mail-ru[.]link/public_html/home/files/login[.]php?email=1, hxxps[://]e[.]mail[.]az-link[.]email/, hxxps[://]e[.]mail[.]az-link[.]email/public/security/files/Az%C9%99rbaycan_Litva[.]jpg, hxxps[://]e[.]mail[.]az-link[.]email/public/security/files/login[.]php?email=1, hxxps[://]mail[.]asco[.]az-link[.]email/5676763663A2F2F31302E3130302E3230302E32/75676763663A2F2F31302E3130302E3230302E32/login[.]php, hxxps[://]mail[.]asco[.]az-link[.]email/Login[.]aspx, hxxps[://]redirect[.]az-link[.]email/, hxxps[://]redirect[.]az-link[.]email/5676763663A2F2F31302E3130302E3230302E32/75676763663A2F2F31302E3130302E3230302E32/Login[.]aspx&_token=oazjTiA255F2DIeYJjCXjE

References

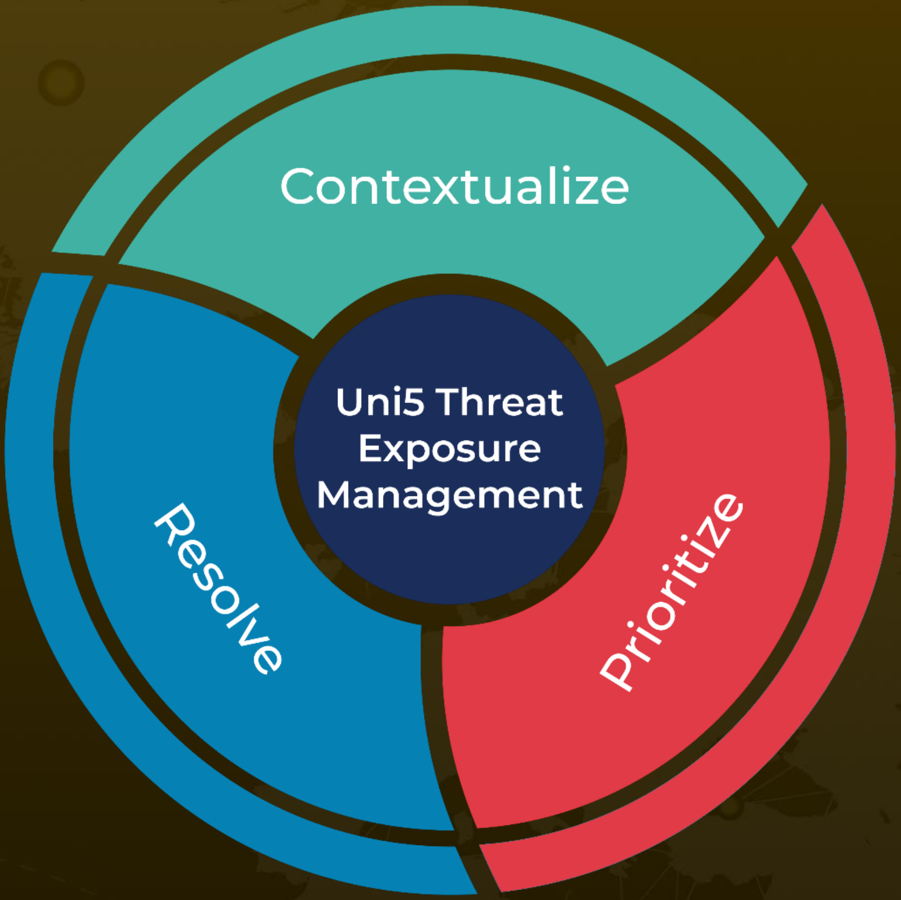
https://blog.talosintelligence.com/attributing-yorotrooper/

https://www.hivepro.com/new-yorotrooper-threat-actor-targeting-government-and-energy-organizations/

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

October 26, 2023 • 5:30 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com