


TURLA’s new phishing-based reconnaissance campaign in Eastern Europe



[APT CTI](#) [Threat & Detection Research Team](#) May 23 2022 64 0 Read it later Remove 5 minutes reading

This blog post on TURLA was originally published as a FLINT report ([SEKOIA.IO](#) Flash Intelligence) sent to our clients on May 11, 2022.

Executive Summary

SEKOIA.IO Threat & Detection Research (TDR) Team have expanded the search on Russian-linked TURLA’s infrastructures from a Google’s TAG blog post. It exposes a reconnaissance and espionage campaign from the Turla intrusion set against the Baltic Defense College, the Austrian Economic Chamber which has a role in government decision-making such as economic sanctions and NATO’s eLearning platform JDAL (Joint Advanced Distributed Learning) pointing Russian Intelligence interest for defense sector in Eastern Europe and for topics related to the economic sanctions against the Russian Federation.

Analysis

On May 3rd 2022, Google’s Threat Analysis Group (TAG) published a report “[Update on cyber activity in Eastern Europe](#)” exposing ongoing campaigns targeting Eastern Europe from various APT, Russian-linked APT28, TURLA, Callisto, Belarus-linked Ghostwriter and Curious Gorge, a group TAG attributes to China’s People’s Liberation Army Strategic Support Force (which is the space, cyber, and electronic warfare force and the 5th branch of Chinese Army).

SEKOIA.IO researchers have expanded TURLA’s infrastructures investigation through the domains in the TAG report:

- wkoinfo.webredirect[.]org
- jadtactnato.webredirect[.]org

TURLA (aka Uroburos, Snake, Venomous Bear) is an historical Russian-speaking cyber espionage group widely believed to be operated by the Federal Security Service of the Russian Federation (FSB). The group is mainly known for targeting Ministries of Foreign Affairs and Defense organizations.



Active since at least 1996, this intrusion set is suspected to have breached many US sensitive networks during a campaign dubbed “Moonlight Maze” from 1996 to 1999. In 2008 Turla is suspected to have used a USB worm dubbed “Agent.BTZ” to breach the US Department of Defense most sensitive networks.

[Tweet this!](#)

Both domains resolve the IP 79.110.52[.]218 which does not allow more investigation, but the first domain exposed 45.153.241[.]162 which can be link through Shodan services to a new domain baltdefcol.webredirect[.]org typosquatting www.baltdefcol.org, Baltic Defense College’s website.

In every directory discovered, we found the same word document “War Bulletin April 27, 19:00 CET” which appeared to be legitimate but contained the inclusion of an external PNG file dubbed logo.png which was not reachable during the investigation.

Index of

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 War Bulletin 19.00 CET 27.04.docx	2022-04-28 10:35	63K	

Apache/2.4.41 (Ubuntu) Server at 149.154.157.11 Port 443

Figure 1. Directory listing on the Turla's server showing a document.

The Baltic Defence College (BALTDEFCOL) is a center for strategic research established by Estonia, Latvia and Lithuania in 1999. It provides military education and conferences to high-rank officers from the founding states as well as allies like NATO, EU and other European countries including Ukraine. The BALTDEFCOL has published studies about the Russian invasion of Ukraine and has tweeted about an US Air Force War College delegation hosted during their European study trip on march 17. Later, on April 19, Chiefs of Defense from Estonia and Latvia, Lieutenant-General Herem and Lieutenant-General Kalniņš visited the Baltic Defense College. They both provided an overview of national defense concepts, highlighting priorities when preparing armed forces to face any threat for national sovereignty. These visits, and the strategic role BALTDEFCOL may have in Baltic military strategy against Russia, could be reasons for Turla targeting this institution for espionage purposes.

We focused also on wkoinfo.webredirect[.]org which typosquatts wko.at, the official website of the Austrian Federal Economic Chamber (Wirtschaftskammer Österreich, WKO). The malicious domains and subdomains directories investigated exposed the same word document: "23.03.2022 : Neue USA Exportkontrollen und Sanktionen: Fokus Russland — Was müssen österreichische Unternehmen jetzt beachten? — WKO.at".

The Austrian Federal Economic Chamber has an expanded function compared to other economic chambers in different countries which have a consultation purpose. By law, Austrian governments must consult with Chambers on legislative projects and important regulation, including economic sanctions. This involvement in decision-making and administrative procedures may be the reason for Russian espionage operations through Turla's phishing campaign, especially in a European country reputed to be a diplomatic bridge between occidental and russian side. Indeed, if Vienna officially supports Kiev, Austria wants to keep its neutral state, voted to reject sanctions against Russian oil and gas, and did not send weapons to Ukraine. Thus any change in the Austrian position could have an important effect on occidental unity facing Russian invasion of Ukraine, motivating an close monitoring from Moscow.

[Discover our CTI and XDR products](#)

Last we noted that jadlactnato.webredirect[.]org is a typosquatting of NATO Joint Advanced Distributed Learning, an e-learning platform hosted on [https://jidl.act.nato\[.\]int](https://jidl.act.nato[.]int) which was established to research and provide education and training to NATO-military and governmental or NATO official.

Document technical analysis

These documents request the PNG file thanks to a remote file inclusion defined in the file /word/_rels/document.rels.xml. It is quite interesting that the request to the file is performed via the HTTP protocol and not an SMB inclusion. Therefore, this campaign does not leverage any malicious code but has been used for reconnaissance purposes only.

Thanks to the HTTP request done by the document to its own controlled server, the attacker can get the version and the type of Word application used by the victim — which can be an interesting info to send a tailored exploit for the specific Microsoft Word version.

Moreover, the attacker can grab the IP address of the victim which can be also an interesting selector to monitor the victim's communications via TURLA's SIGINT capabilities.

IOCs & Technical Details

Yara rules

```
rule apt_TURLA_ExternalPNGDocument_strings { meta: id = "51413d41-d0f4-4e1a-9f12-322921e48977" version = "1.0" intrusion_set = "TURLA" description = "Detects external logo embedded in DOCX documents" source = "SEKOIA" creation_date = "2022-05-05" modification_date = "2022-05-05" classification = "TLP:GREEN" strings: $s1 = "/relationships/image" $s2 = /[0-9]{3,10}\\logo\\.png/ $s3 = "TargetMode=\"External\"/><" condition: $s1 in (filesize-400..filesize) and $s2 in (filesize-400..filesize) and $s3 in (filesize-400..filesize) }
```

Infrastructure

45.153.241[.]162 79.110.52[.]218 149.154.157[.]111 baltdefcol.webredirect[.]org wkoinfo.webredirect[.]org jadlactnato.webredirect[.]org

Document hashes

f6e755e2af0231a614975d64ea3c8116 f223e046dd4e3f98bfeb1263a78ff080

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

[Contact us](#)

TTPs (ATT&CK)

Spearphishing Link (T1598.003) Gather Victim Network Information IP Addresses (T1590.005) Gather Victim Host Information Software (T1592.002)

Share

Share this post: