

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)  
> Security (<https://www.bleepingcomputer.com/news/security/>)  
> Russian hackers perform reconnaissance against Austria, Estonia

◀ 12

## Russian hackers perform reconnaissance against Austria, Estonia

By  
**Bill Toulas**  
(<https://www.bleepingcomputer.com/author/bill-toulas/>)

May 23, 2022

09:14 AM

0



In a new reconnaissance campaign, the Russian state-sponsored hacking group Turla was observed targeting the Austrian Economic Chamber, a NATO platform, and the Baltic Defense College.

This discovery comes from cybersecurity firm Sekoia, which built upon previous findings of Google's TAG, which has been following Russian hackers closely this year.

Google warned about coordinated Russian-based threat group activity in late March 2022

(<https://www.bleepingcomputer.com/news/security/google-russian-phishing-attacks-target-nato-european-military/>), while in May, they spotted two Turla domains (<https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/>) used in ongoing campaigns.



Sekoia used this information to investigate further and found that Turla targeted the federal organization in Austria and the military college in the Baltic region.

## Who is Turla

Turla is a Russian-speaking cyber-espionage threat group that is believed to have strong ties to Russian Federation's FSB service. It has been operational since at least 2014, compromising a wide range of organizations in multiple countries.

They have previously targeted Microsoft Exchange servers (<https://www.bleepingcomputer.com/news/security/turla-backdoor-deployed-in-attacks-against-worldwide-targets/>) worldwide to deploy backdoors, hijacked the infrastructure of other APTs (<https://www.bleepingcomputer.com/news/security/turla-espionage-group-hacks-oilrig-apt-infrastructure/>) to perform espionage in the Middle East, and performed watering hole attacks (<https://www.bleepingcomputer.com/news/security/advanced-russian-hackers-use-new-malware-in-watering-hole-operation/>) against Armenian targets.

More recently, Turla was seen using a variety of backdoors and remote access trojans against EU governments and embassies (<https://www.bleepingcomputer.com/news/security/russian-turla->

hackers-breach-european-government-organization/) and important research facilities.

## European targets

According to Sekoia, the IPs shared by Google's TAG lead to the domains "baltdefcol.webredirect[.]org" and "wkoinfo.webredirect[.]org," which respectively typo-squat "baltdefcol.org" and "wko.at."

The first target, BALTDEFCOL, is a military college located in Estonia and operated by Estonia, Latvia, and Lithuania, serving as a center for strategic and operational research in the Baltic.

The college also organizes conferences attended by high-ranking officers of NATO and various European countries, so it holds a special significance for Russia in the ongoing conflict in Ukraine and the tensions on the Russian border.

WKO (Wirtschaftskammer Österreich) is the Austrian Federal Economic Chamber, which serves as an international consultant on legislation and economic sanctions.

Austria has maintained a neutral stance concerning the sanctions against Russia. However, Turla would like to be among the first to learn if anything changes on that front.

Sekoia also noticed a third typo-squat domain, "jadlactnato.webredirect[.]org," which attempts to pass as the e-learning portal of the NATO Joint Advanced Distributed Learning platform.

## Performing reconnaissance

The typosquatting domains are used to host a malicious Word document named "War Bulletin 19.00 CET 27.04.docx," found in various directories of these sites.

This file contains an embedded PNG (logo.png), which is retrieved when the document is loaded. The Word file does not contain any malicious macros or behavior, making Sekoia believe that the PNG is used to perform reconnaissance.

“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,” explains Sekoia's report (<https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/>)

Additionally, Turla gains access to the victim's IP address, which would be helpful in subsequent attack phases.

To enable defenders detect this activity, Sekoia has provided the following Yara rule:

```
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)  
}
```

## Related Articles:

Russian govt impersonators target telcos in phishing attacks

(<https://www.bleepingcomputer.com/news/security/russian-govt-impersonators-target-telcos-in-phishing-attacks/>)

Phishing campaign targets Russian govt dissidents with Cobalt Strike

(<https://www.bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/>)

Fake Windows exploits target infosec community with Cobalt Strike

(<https://www.bleepingcomputer.com/news/security/fake-windows-exploits-target-infosec-community-with-cobalt-strike/>)

Hackers can hack your online accounts before you even register them

(<https://www.bleepingcomputer.com/news/security/hackers-can-hack-your-online-accounts-before-you-even-register-them/>)

Russian Sberbank says it's facing massive waves of DDoS attacks

(<https://www.bleepingcomputer.com/news/security/russian-sberbank-says-it-s-facing-massive-waves-of-ddos-attacks/>)