EuRepoC

ADVANCED PERSISTENT THREAT profile

Turla

Cyber Espionage Under the Radar Since 1996

Associated APT designations

- **Turla** (Kaspersky)
- **Venomous Bear** (CrowdStrike)
- **Snake** (BAE Systems)
- **Uroburos** (G DATA, mostly referring to the malware – see below)
- **MAKERSMARK** (Canadian Communications Security Establishment, CSE)

Sources: [1][2][3][23]

Country of origin

Period of activity

2004-today

Sources: [7][8]

Political affiliations

In 2018, in its annual report, the Estonian Foreign Intelligence Service attributed Turla to the Russian domestic intelligence agency FSB. In 2016, the Federal Office for the Protection of the Constitution, Germany's domestic intelligence service, referred to Turla as a state-directed operation. At the time, the Office did not publicly attribute related activities to Russia as a sponsoring state, but only referred to IT reports that indicated the Russian origin of the operations. In a Joint Cybersecurity Advisory from April 2022, cybersecurity authorities from the United States, Australia, Canada, New Zealand, and the United Kingdom acknowledged industry reports that had pointed to Turla as a state-sponsored group, while noting that none of them so far had officially attributed Turla to the Russian government. The publication lists Turla as a Russia-aligned cyber threat group distinct from Russian state-sponsored cyber operations that the responsible agencies had variously linked to the FSB, Russia's foreign intelligence Service SVR, the military intelligence directorate GRU, or TsNIIKhM – an alleged research organisation subordinate to Russia's Ministry of Defence.

Sources: [4][5][6]

Agency type

Possibly state-integrated group (civil intelligence service/agency members). Private threat intelligence companies, such as Talos Intelligence, designated Turla as a “state-sponsored” actor. As noted with respect to the Five Eyes Joint Cybersecurity Advisory, public reporting on the degree of proximity to Russian state entities, particularly the FSB, differs. Unlike other Russian groups, such as Fancy Bear, Cozy Bear, Sandworm, or Energetic Bear, which government and industry reports alike have linked to Russian government agencies, open-source material leaves the question of the institutional sponsorship of Turla open to further corroboration. A German media report published in February 2022 presented evidence for the Turla-FSB connection, identifying two former Turla programmers that worked at the Russian company Center-Inform, which officially operates on behalf of the FSB.

Sources: [6][8][20]

Most frequent targets:

Afghanistan **China** **Germany** **Kazakhstan**

Switzerland **USA** **Vietnam**

And more targets, with a focus on government institutions, embassies, military, education, research and pharmaceutical companies.

Sources: [2][11][12]

Group composition and organisational structure

Considering Turla’s technical sophistication and well-prepared operations that stretch back to the 1990s, and given the group’s association with private, FSB-related entities such as Center-Inform, the total human resources the group can deploy are likely substantial. In particular, Turla's hijacking of satellite connections (e.g., for Moonlight Maze) required specific knowledge of these systems, which are normally reserved for intelligence agencies, further corroborating the assumption of extensive state backing.

Sources: [20][25]

Impact type(s)

Direct

- **Intelligence impact** (US Central Command [USCENTCOM] hack / Agent.BTZ 2008; RUAG hack 2014; German Foreign Office hack)

Indirect

- **Reputational impact** (espionage campaign against USCENTCOM leveraging Agent.BTZ 2008)

Sources: [3][13]

Incident type(s)

- **Intelligence gathering** (especially targeting political entities, including embassies in Eastern Europe)
- Infiltrations enabled through **spearphishing**
- **Watering-hole attacks**

> **EuRepoC codes:** Hijacking with misuse; Data theft (cyber-espionage)

Sources: [3][13]

Threat Level Index

12/24 moderate threat level

Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the **sectorial** and **geographical scope** of the APT's attacks, the **intensity** of the attacks, the **frequency** of attacks and the **use of zero-days**. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here.

Breakdown of the scores for Turla:

Sub-indicator	Score	Explanation
Intensity of attacks	1/5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information.
Sectorial scope of attacks	3/8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. In the case of Turla, on average attacks attributed to the group within the EuRepoC database, targeted one to two sectors per attack. However, as nearly all attacks were against political systems and/or critical infrastructure.
Geographical scope of attacks	3/4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of Turla, on average four countries were targeted per attack attributed to the group within the EuRepoC database.
Frequency of attacks	3/4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. In the case of Turla, the group was responsible for less than 0.8 attacks per year of activity.
Exploitation of Zero days	2/3	This indicator calculates the percentage of attacks attributed to the APT that make use of one or multiple zero days. The obtained score is then converted to a three-level scale. 7% of attacks attributed to Turla made use of zero-days.

→ Overall, Turla obtains a moderate-level threat score compared to other APT groups. The attacks analysed within the EuRepoC framework, had a relatively low intensity in terms of their physical and socio-political effects but were more frequent and targeted an above average number of countries and victims compared to other APT groups analysed by EuRepoC.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

Fox-IT assessed in 2017, that, “compared to other prolific attackers with alleged ties to Russia, such as APT28 (Fancy Bear) and APT29 (Cozy Bear), Turla`s code is significantly more sophisticated, its infrastructure more complex and targets more carefully selected.” Turla tries to operate below the radar and avoid excessive public attention. According to the Estonian Foreign Intelligence Service, Turla uses more sophisticated and expensive tools (such as satellites) and attacks targets of long-term value.

Basic attack pattern

Turla often compromises web servers and hijacks satellite connections for the group`s command and control (C2) infrastructure. In some operations, they also do not directly communicate with the C2 server. Instead, they use a compromised system inside the targeted network as a proxy, which forwards the traffic to the real C2 server (evasion technique). Victims are infected via a sophisticated multi-stage attack, which usually begins with the Epic Turla malware. This is upgraded to more sophisticated backdoors, such as the Carbon/Cobra system. Possible infection vectors are spearphishing, drive-by infections, USB sticks, or social engineering. In December 2022, Qualys researchers reported Turla`s use of Empire, a popular open-source post-exploitation framework which is used to expand the attacker’s foothold in the target environment. Turla used Empire’s injection modules, Drobox, and OneDrive C2 mechanism.

Zero-day exploits

In 2014, Kaspersky reported the abuse of the following two zero-day vulnerabilities by Turla: CVE-2013-5065 and CVE-2013-3346. Moreover, the group exploited an Encapsulated PostScript (EPS; Microsoft Office) zero-day (CVE-2017-0261) against European diplomatic and military entities in collaboration with ATP28, which had twinned a separate EPS zero-day (CVE-2017-0262) with a new Escalation of Privilege (EOP) zero-day (CVE-2017-0263) for this operation.

Sources: [3][13]

Malware used (non-exhaustive)

Agent.BTZ	Snake Rootkit	Kazuar *(for the potential connection to Sunburst/Solar Winds, see below)*
Uroburos		

Sources: [3] [8][11][14][15][16][17]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access

Drive-by compromise
Phishing
Spearphishing link
Valid accounts

MITRE Persistence

Boot or logon autostart execution
Event-triggered execution
Valid accounts

MITRE Defense Evation

Access Token Manipulation
Deobfuscate/decode files or information
Impair defenses
Modify registry
Obfuscated files or information
Process injection
Subvert trust controls
Valid accounts

MITRE Exfiltration

Exfiltration over web service

ATTRIBUTION

Attribution milestones

2014		2017		2018		2022
G Data report	→	Joint investigation by Kaspersky and King`s College London into the origins of Operation Moonlight Maze	→	Estonian Foreign Intelligence Service report	→	Turla exposé by investigative reporters of the German public broadcasters BR and WDR, substantiating links to the FSB

Sources: [3][5][20][25]

Attribution ambiguities

The SolarWinds hack - Sunburst backdoor and Kazuar correlations: In 2021, Kaspersky discovered several features in the code of Sunburst, the backdoor planted through subverted versions of the network monitoring tool SolarWinds Orion. These features overlap with a previously-identified backdoor known as Kazuar. Palo Alto linked Kazuar to Turla, although no further details to substantiate this attribution link have been made public. Kaspersky assessed that Sunburst was either developed by the same group as Kazuar (i.e., Turla), or Kazuar served as an inspiration. As alternative hypotheses, Kaspersky considered that both APT29 (the SVR-associated threat actor that the White House deemed responsible for the SolarWinds compromise) and Turla may have obtained their malware from the same source, indicating the two actors could operate with shared personnel resources. On the other hand, Kaspersky proposed that the Kazuar code might have been introduced to misdirect investigators as part of a false-flag operation.

Sources: [19][26]

Attribution and detection sensitivity

Turla is considered to be highly evasive. For example, G DATA assumes that "the attackers reserve the Uroburos rootkit for dedicated and critical targets. This is the main reason why the rootkit was only detected many years after the suspected first infection." Furthermore, G DATA states that "the framework is designed to perform cyber espionage within governments and high-profile enterprises but, due to its modularity, it can be easily extended to gain new features and perform further attacks as long as it remains undetected within its target." In 2019, Symantec discovered Turla`s hijacking of C2 infrastructure used by Iranian state-sponsored APT OilRig (aka Crambus/APT34) to deliver malware on to target networks going back to January 2018. Since the infrastructure had been tied to OilRig by public vendors before this "hostile takeover" was discovered, connections to OilRig platforms have led to false attributions in the meantime. It is unclear, however, if Turla used the infrastructure for technical advantage or if the group intended to conduct a false-flag operation.

Sources: [3][27]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/Legal/Law enforcement actions

German Federal Prosecutor General: After the Turla infiltration of the German Foreign Office's network was detected in 2017, the responsible Federal Prosecutor General officially initiated proceedings for the cyber incident. The Federal Criminal Police Office's (BKA) digital forensics branch in Meckenheim has been tasked with the investigation.

Sources: [20]

Indicted individuals / sanctioned (associated) entities

The German broadcasting stations BR and WDR named two individuals, "Vlad" and "Urik," as leading suspects behind the intrusion of the German Foreign Office in 2017. Although the full names of the two individuals are said to be known to the authorities, they are being withheld from the public for investigative reasons. BR and WDR refrained from revealing their full names because the two no longer work for Turla.

Sources: [20]

Landmark incidents

Operation Moonlight Maze, 1996–1999*:
Starting in 1996, Turla hackers were able to infiltrate networks of US entities, such as NASA, the Department of Defense (DoD), military contractors, and other government institutions. The group managed to exfiltrate a tremendous amount of classified data. This early example of cyber-espionage used backdoors and heavily-exploited, unpatched software vulnerabilities, taking advantage of a lack of proper cybersecurity awareness and patching routines at that time. Only in 2017 did a joint investigation by Kaspersky and King`s College London into the origins of the operation publicly trace the campaign to Turla on the basis of continuous use of source code deployed during Moonlight Maze, which was linked to the LOKI2 backdoor.

USCENTCOM hack / Agent.BTZ, 2008, prompting the clean-up Operation Buckshot Yankee:
In 2008, at a US military base in the Middle East, a USB flash drive infected with Agent.BTZ (see above) was unknowingly inserted into a laptop linked to USCENTCOM systems. Agent.BTZ, which is able to scan computers for data, open backdoors, and exfiltrate data through those backdoors to a remote C2 server, spread undetected to connected US military networks, both classified and unclassified. In 2010, then-US Secretary of Defense William J. Lynn III described the incident as "the most significant breach of U.S. military computers." USB drives were subsequently banned in all DoD facilities. While no official statement regarding attribution has been issued, IT industry analysis strongly suspects Turla was behind the attack, based on the attack pattern and overlaps in technical indicators.

* EuRepoC tracks cyber operations going back to 1 January 2000. Findings related to Operation Moonlight Maze, which predates this threshold point, are not reflected in elements of this profile developed on the basis of EuRepoC data, such as the Threat Level Indicator.

Landmark incidents (continued)

Intrusion of the intranet of the Finnish Ministry of Foreign Affairs, 2013:
Following a tip from the National Defence Radio Establishment, Sweden's signals intelligence and information security agency, spyware was discovered on the Finnish Ministry of Foreign Affairs intranet. By that time, attackers had been present on the network for over three years. Although Finland did not publicly attribute the incident to Turla (or by extension to Russia), both Kaspersky and F-Secure experts did. The incident followed patterns indicative of Turla's modus operandi, including the use of satellites.

Espionage operation against Swiss defence firm RUAG, 2014:
In early 2016, the Swiss Government Computer Emergency Response Team (GovCERT) became aware of an intrusion against the Swiss arms company RUAG, the largest supplier to the Swiss Armed Forces, with the apparent intent of stealing information. The GovCERT identified the malware as part of the Turla suite. The incident bore stark resemblance to previous and subsequent attacks reportedly carried out by Turla.

German Foreign Office hack, 2017:
Turla hackers infiltrated the network of the German Foreign Office and were able to operate undetected for over a year before being discovered in late 2017. Experts at the Federal Office for Information Security (BSI) found out that the hackers managed to penetrate Foreign Office systems in an attack relay channeled through a government network (IVBB) that connects the ministry to other federal agencies and bodies**.** The attackers had previously broken into the Federal Academy of Public Administration, which interlaces with the Foreign Office through the IVBB. Turla malware forced ministry computers to communicate with a satellite, from where the group was able to intercept transmitted data. Up until 2018, when the connection was shut down, Turla only stole a total of six documents, of which only one was classified as confidential.

Sources: [9][16][18][20] [21][22][25][28][16][20][21][22]

SOURCES

[1] BAE (2014), *The Snake Campaign*, BAE Systems. Available at: https://web.archive.org/web/20221220092854/https://www.baesystems.com/en/cybersecurity/feature/the-snake-campaign [Archived on: 20.12.2022]

[2] CrowdStrike (2021), *Adversary: Venomous Bear*, CrowdStrike. Available at: https://web.archive.org/web/20221220093236/https://adversary.crowdstrike.com/en-US/adversary/venomous-bear/?L=236 [Archived on: 20.12.2022]

[3] G DATA (2014), *Uroburos: Highly Complex Espionage Software with Russian Roots*, G Data Security Labs, Red Paper. Available at: https://web.archive.org/web/20221220095609/https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf [Archived on: 20.12.2022]

[4] Bundesamt für Verfassungsschutz (2016), *BfV Cyber-Brief: Nr. 02/2016*, Bundesamt für Verfassungsschutz. Available at: https://web.archive.org/web/20221220095644/https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2016-02-bfv-cyber-brief.pdf?__blob=publicationFile&v=5 [Archived on: 20.12.2022]

[5] Välisluureamet (2018), *International Security and Estonia*, Estonian Ministry of Defence, Foreign Intelligence Service, Available at: https://web.archive.org/web/20221220095740/https://www.valisluureamet.ee/doc/raport/2018-en.pdf [Archived on: 20.12.2022]

[6] CISA (2022), *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, Joint Cybersecurity Advisory. Available at: https://web.archive.org/web/20220608000856/https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf [Archived on: 20.12.2022]

[7] Cyberint (2021), *Turla – High Sophistication Russian-Nexus Threat Group*, Cyberint Blog. Available at: https://web.archive.org/web/20221220110112/https://cyberint.com/blog/research/turla-high-sophistication-russian-nexus-threat-group/ [Archived on: 20.12.2022]

[8] Unterbrink (2021), *TinyTurla – Turla Deploys New Malware To Keep a Secret Backdoor on Victim Machines*, Talos Intelligence, Talos Threat Spotlight. Available at: https://web.archive.org/web/20221220133445/https://blog.talosintelligence.com/tinyturla/ [Archived on: 20.12.2022]

[9] Kerkkänen (2016), *Viaton klikkaus sähköpostissa – Näin Venäjän verkkovakoojat iskivät ulkoministeriöön*, Yle. Available at: https://web.archive.org/web/20221220161000/https://yle.fi/a/3-8591029 Archived on: 20.12.2022]

[10] ESET (2018), *Diplomats in Eastern Europe Bitten By a Turla Mosquito*, ESET, Welivesecurity. Available at: https://web.archive.org/web/20221220162405/https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf [Archived on: 20.12.2022]

[11] GReAT (Global Research & Analysis Team) (2014), *The Epic Turla Operation*, Kaspersky, Securelist. Available at: https://web.archive.org/web/20221220133454/https://securelist.com/the-epic-turla-operation/65545/ [Archived on: 20.12.2022]

[12] Paganini (2017), *The Snake APT Group is Preparing Its Offensive Against High-Profile Mac Users*, Security Affairs. Available at: https://web.archive.org/web/20221220133600/https://securityaffairs.co/wordpress/58765/apt/snake-apt-group-macos.html [Archived on: 20.12.2022]

[13] Malpedia (2022), *Turla*, Fraunhofer-Institute für Kommunikation, Malpedia. Available at: https://web.archive.org/web/20221220133756/https://malpedia.caad.fkie.fraunhofer.de/actor/turla [Archived on: 20.12.2022]

[14] Fox-IT (2017), *Snake: Coming Soon in Mac OS X Flavour*, FOX IT Blog. Available at: https://web.archive.org/web/20221220133941/https://blog.fox-it.com/2017/05/03/snake-coming-soon-in-mac-os-x-flavour/ [Archived on: 20.12.2022]

[15] Välisluureamet (2019), *International Security and Estonia*, Estonian Ministry of Defence, Foreign Intelligence Service. Available at: https://web.archive.org/web/20221220134045/https://www.valisluureamet.ee/doc/raport/2019-en.pdf [Archived on: 20.12.2022]

[16] GovCERT (2016), *APT Case RUAG: Technical Report*, Swiss Government Computer Emergency Response Team, Reporting and Analysis Centre for Information Assurance (MELANI). Available at: https://web.archive.org/web/20220223224202/https://www.govcert.ch/downloads/whitepapers/Report_Ruag-Espionage-Case.pdf [Archived on: 20.12.2022]

[17] Jiang, Lanstein, Berry, Read, Kizhakkinan, and MacManus (2022), *EPS Processing Zero-Days Exploited by Multiple Threat Actors*, Mandiant. Available at: https://web.archive.org/web/20221220134556/https://www.mandiant.com/resources/blog/eps-processing-zero-days [Archived on: 20.12.2022]

[18] Baumgärtner, Gebauer, and Knobbe (2018), *Behörden Vermuten Russische Hackergruppe "Snake" als Täter*, Spiegel Netzwelt. Available at: https://web.archive.org/web/20221220161556/https://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-behoerden-vermuten-russische-hacker-gruppe-snake-als-taeter-a-1196089.html [Archived on: 20.12.2022]

[19] Kucherin, Kuznetsov, and Raiu (2021), *Sunburst Backdoor – Code Overlaps with Kazuar*, Kaspersky, Securelist. Available at: https://web.archive.org/web/20221220134744/https://securelist.com/sunburst-backdoor-kazuar/99981/ [Archived on: 20.12.2022]

[20] Tanriverdi, Flade, and Fley (2022), *Die Elite-Hacker des FSB (The Elite Hackers of the FSB)*, Bayerischer Rundfunk and Westdeutscher Rundfunk. Available at: https://web.archive.org/web/20221220135531/https://interaktiv.br.de/elite-hacker-fsb/ [Archived on: 20.12.2022]

[21] Shachtman (2010), *Insiders Doubt 2008 Pentagon Hack was Foreign Spy Attack* (Updated), Wired. Available at: https://web.archive.org/web/20221220135940/https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/ [Archived on: 20.12.2022]

[22] Gostev (2014), *Agent.btz: A Source of Inspiration?*, Kaspersky, Securelist. Available at: https://web.archive.org/web/20221220140943/https://securelist.com/agent-btz-a-source-of-inspiration/58551/ [Archived on: 20.12.2022]

[23] Biddle (2017), *White House Says Russia's Hackers Are Too Good To Be Caught But NSA Partner Called Them "Morons"*, The Intercept. Available at: https://web.archive.org/web/20221220143358/https://theintercept.com/2017/08/02/white-house-says-russias-hackers-are-too-good-to-be-caught-but-nsa-partner-called-them-morons/?comments=1 [Archived on: 20.12.2022]

[24] Pradhan (2022), *Dissecting the Empire C2 Framework*, Qualys Blog. Available at: https://web.archive.org/web/20221219030037/https://blog.qualys.com/vulnerabilities-threat-research/2022/12/12/dissecting-the-empire-c2-framework [Archived on: 19.12.2022]

[25] Raiu, Moore, Guerrero-Saade, and Rid (2017), *Penquin's Moonlit Maze*, Kaspersky, Securelist. Available at: https://web.archive.org/web/20221220152940/https://securelist.com/penquins-moonlit-maze/77883/ [Archived on: 20.12.2022]

[26] White House (2021), *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government*, United States White House. Available at: https://web.archive.org/web/20221220155507/https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ [Archived on: 20.12.2022]

[27] Symantec Deepsight Adversary Intelligence Team and Network Protection Security Labs (2019), *Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Government*, Symantec Enterprise Blogs/Threat Intelligence. Available at: https://web.archive.org/web/20221220160353/https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/waterbug-espionage-governments [Archived on: 20.12.2022]

[28] Lynn III (2010), *Defending a New Domain*, Foreign Affairs. Available at: https://web.archive.org/web/2/https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain [Archived on: 20.12.2022]

Calculations for the Threat Level Index indicator are based on version 1.0 of the EuRepoC Database downloadable here: https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Global_Database_1_0_22d4a4aee7.xlsx

Last updated: 21.12.2022

www.EuRepoC.eu

@EuRepoC

contact@eurepoc.eu

December 2022