July 13, 2026

Targeting and Compromise of French Entities Using the Turla Intrusion Set

Espionage Activities Associated with the 16th Center of the FSB Using the Turla Intrusion Set Since the 2010s

Members of the Cyber Crisis Coordination Center (C4) [1] have observed the targeting and compromise of French entities using the Turla intrusion set [2], operated by the 16th Center of the Federal Security Service of the Russian Federation (FSB). This intrusion set has also previously been attributed to Russia by other countries [1][2][3][4]. Since at least 2004, it has been implemented for intelligence collection against strategic entities and individuals worldwide, including in France. Espionage campaigns associated with the Turla intrusion set against Ukraine, NATO countries, and EU member states continue in the context of Russia's war of aggression launched on February 24, 2022.

The malicious cyber activities of the 16th Center of the FSB against France and its European partners are the subject today (July 13, 2026), of two formal attribution statements by the Minister of Europe and Foreign Affairs, on behalf of France, and by the High Representative of the EU for Foreign Affairs and Security Policy, on behalf of the EU and its Member States.

1. The 16th Center of the FSB (Federal Security Service of the Russian Federation)

Organization and Geographic Distribution

Members of the C4 have identified that the 16th Center of the Federal Security Service of the Russian Federation (FSB), also known by the designations "military unit 71330" or "Center for Radio-

[1] The C4 is an inter-ministerial body dedicated to the analysis of cyber threats. It brings together the ANSSI (National Agency for the Security of Information Systems), COMCYBER (Cyber Command), DGA (Directorate General for Armaments), DGSE (Directorate General for External Security), and DGSI (Directorate General for Internal Security).

[2] An intrusion set is defined as an evolving but consistent set of techniques, tactics, procedures, code, and infrastructure used to conduct cyberattacks.

Electronic Intelligence of Communications"[3], operates various intrusion sets to target French and European interests, including the Turla intrusion set[4].

To conduct these activities, the 16th Center of the FSB can rely on the eleven interception centers it operates, distributed across Russian territory. These interception centers are designated by military unit numbers:

- Military unit 03110, located near Sochi;
- Military unit 11380, located near Temryuk in the Krasnodar region;
- Military unit 28735, located near Alushta in Crimea;
- Military unit 44231, located near Balashov in the Saratov region;
- Military unit 49911, located near Pskov in the Pskov region;
- Military unit 51952, located near Chekhov in the Moscow region;
- Military unit 61240, located near Krasnoye Selo in the Saint Petersburg region;
- Military unit 61608, located south of Moscow;
- Military unit 70822, located near Khabarovsk in the Khabarovsk region;
- Military unit 83417, located near Chkhotovo in the Vladivostok region;
- Military unit 83521, located near Zelenogradsk in the Kaliningrad region.

The geographical location of the military units and the orientation of antennas at their sites suggest a geographically distributed targeting approach. Thus, the units in Pskov, Krasnoye Selo, and Zelenogradsk are oriented towards Europe and the United States, while Chkhotovo and Khabarovsk target Asia more specifically.

Military Unit 61240, Responsible for Targeting France

Military unit 61240 is responsible for targeting France in terms of Signals Intelligence (SIGINT) and offensive cyber activities. It is located near Krasnoye Selo, southwest of Saint Petersburg.

Furthermore, this unit maintains close ties with several Russian companies such as AO AST or NPP Gamma, known for their support of the offensive cyber activities of Russian intelligence services.

This military unit is therefore strongly linked to the SIGINT and offensive cyber operations capabilities of the FSB, constituting a real threat to French and European interests.

2. The Turla Intrusion Set

Active since at least 2004, the Turla intrusion set is primarily used for intelligence collection against public and private entities belonging to the governmental, diplomatic, defense, research, technology, education, media, or energy sectors, as well as individuals worldwide [1, 4, 5, 6].

Notable cyberattacks associated with the Turla intrusion set have been conducted against European and American entities, including the compromise of US military networks in 2008, the Swiss defense company RUAG in 2016, or German government networks in 2018 [7, 8, 9].

[3] Центр Радиоэлектронной Разведки Средств Связи also known as TsRRSS.

[4] The techniques, tactics, and procedures (TTPs) associated with the Turla intrusion set overlap with those documented by security vendors under the names of Secret Blizzard, Venomous Bear, Pensive Ursa, Pacifier, or Waterbug. Members of the C4 therefore consider that these aliases refer to the same intrusion set.

Since the start of Russia's war of aggression against Ukraine on February 24, 2022, the Turla intrusion set has been used to contribute to the Russian war effort through intelligence collection on Ukraine and its allies. It is notably used as part of reconnaissance and cyber espionage activities against governmental entities, defense sector entities, or technology companies in Ukraine and several allied European countries [4, 10, 11, 12].

Malwares and Attack Infrastructure

Members of the C4 consider that the Turla intrusion set is associated with both the use of open-source tools like Mimikatz or Metasploit, and a specific set of sometimes complex malware only associated with this intrusion set[5], originating from the Agent.BTZ and Uroburos code, also known as Turla and Snake. This malware has been used to target Windows operating systems, including email solutions such as Outlook and Microsoft Exchange, as well as Linux and macOS. It has also been used against web browsers, business applications, and web servers [1, 4, 13, 14, 15, 16, 17, 18, 19, 20, 21].

Since 2016, campaigns associated with the Turla intrusion set have regularly relied on the Kazuar malware, which has undergone several evolutions over the years and is still in use as of 2026 [22, 23, 24, 25].

In order to compromise information systems, operators of the Turla intrusion set have employed initial access techniques such as spearphishing and waterholing attacks, aiming to entice targets into downloading malicious files masquerading as legitimate software. Attackers have also compromised network equipment, business applications, and exploited vulnerabilities, including zero-day vulnerabilities. In some campaigns, they have combined the exploitation of multiple vulnerabilities within a single compromise chain [26, 27, 28].

Furthermore, from initial access to data exfiltration, operators of the Turla intrusion set rely on attack infrastructures designed to ensure their operational security and limit detection. They use compromised or rented resources, such as servers and websites, including content management systems like WordPress. They also resort to satellite communications, for example to manage their attack infrastructure while ensuring anonymity, for command-and-control activities, or for the retrieval of collected data. Moreover, they have used peer-to-peer communication tools composed of compromised machines within their attack infrastructure [15, 18, 26, 29].

The intrusion set is also associated with the compromise and reuse of offensive capabilities linked to other threats, including intrusion sets attributed to state-sponsored actors and cybercriminals [6, 30, 31, 32].

3. French victims

Members of the C4 distinguish two types of victims of the Turla intrusion set[6]:

- **Final-stage victims**, compromised for espionage purposes;
- **Intermediate victims** from various sectors whose information systems are opportunistically compromised to be integrated as relays within the malicious infrastructure of the intrusion set and facilitate subsequent attacks against final-stage victims.

[5] These malwares include Epic, ComRAT, Carbon, Mosquito, Penquin, Gazer, Crutch, TinyTurla, LightNeuron, Capibar, and Kazuar. This list is not exhaustive.

[6] This typology is based on the observation of attacker behavior and the deduction of their objectives.

Since the 2010s, French intermediate and final victims of the Turla intrusion set have included **ministries, diplomatic entities, defense sector entities, justice sector entities, and technology sector entities**. Among the intermediate victims of the intrusion set, members of the C4 have also identified **associations, individuals, and various companies**.

In 2014, members of the C4 identified the targeting and compromise of **ministerial entities** using the Uroburos malware, likely for espionage purposes.

In particular, since at least 2017, email accounts of the French **Ministry of the Armed Forces** have been compromised by operators of the Turla intrusion set. These attacks targeted email accounts of officials within the ministry. Beyond this campaign, this threat remains active against the French Ministry of the Armed Forces and entities under its authority.

In 2018, the network of the French **Ministry for Europe and Foreign Affairs at the French Embassy in Moscow** was compromised using the Turla intrusion set. The attackers notably conducted network scanning activities and data exfiltration on the embassy's network.

Comment: this incident echoes a campaign recently reported by security vendor MICROSOFT concerning the cyber targeting of foreign embassies located in Moscow since at least 2024. The security vendor has attributed this campaign to the Turla intrusion set, which demonstrates the consistent interest of operators of this intrusion set for diplomatic targets [33, 34].

Also during 2018, C4 members identified the compromise of several machines belonging to a French **technology sector** entity using the Uroburos malicious code. Investigations by C4 members revealed that these compromised machines were used as relays within the attack infrastructure of the intrusion set operators.

In 2019, members of the C4 became aware of the compromise of a server belonging to a **justice sector entity** and hosting a service for the continuing education of personnel. In this attack, operators of the Turla intrusion set exploited a vulnerability related to SharePoint to install malware. The investigations by C4 members demonstrated that attackers potentially had access to information from several thousand user accounts.

Between 2019 and 2025, members of the C4 observed the compromise of **several French intermediate victims** by operators of the Turla intrusion set.

In 2025, members of the C4 were also informed of malicious activities potentially linked to the Turla intrusion set conducted against an **entity working on advanced technologies**.

References

[1] CISA et al. Hunting Russian Intelligence "Snake" Malware. May 9, 2023. URL : https://www.cisa.gov/sites/default/files/2023-05/aa23 129a_snake_malware_2.pdf.

[2] ESTONIAN FOREIGN INTELLIGENCE SERVICE. International Security and Estonia 2018. September 15, 2017. URL : https://www.valisluureamet.ee/doc/raport/2018-en.pdf.

[3] BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Annual Report of the Security Information Service for 2017. November 29, 2018. URL : https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/en/ar2017en.pdf.

[4] CERT-UA. Targeted Turla Attacks (UAC-0024, UAC-0003) Using CAPIBAR and KAZUAR Malware (CERT-UA#6981). July 31, 2023. URL : https://csirt.csi.cip.gov.ua/en/posts/uac-0024-uac.

[5] KASPERSKY. The Epic Turla Operation. August 7, 2014. URL : https://securelist.com/the-epic-turla-operation/65545/.

[6] NCSC-UK. Turla Group Exploits Iranian APT to Expand Coverage of Victims. October 21, 2019. URL : https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.

[7] LOS ANGELES TIMES. Pentagon Computer Networks Attacked. November 28, 2008. URL : https://www.latimes.com/archives/la-xpm-2008-nov-28-na-cyberattack28- story.html.

[8] GOVCERT.CH. APT Case RUAG. May 23, 2016. URL : https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/fachberichte/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf.

[9] DER SPIEGEL. Authorities Suspect Russian Hacker Group 'Snake' as Perpetrator. March 1, 2018. URL : https://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-behoerden-vermuten-russische-hacker-gruppe-snake-als-taeter-a-1196089.html.

[10] MICROSOFT. A Year of Russian Hybrid Warfare in Ukraine. March 15, 2023. URL : https://www.microsoft.com/en- us/security/business/security- insider/wp-content/uploads/2023/03/A- year- of- Russian- hybrid- warfare- in- Ukraine_MS- Threat- Intelligence-1.pdf.

[11] SEKOIA. Turla's New Phishing-Based Reconnaissance Campaign in Eastern Europe. May 23, 2022. URL : https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/.

[12] GOOGLE TAG. Update on Cyber Activity in Eastern Europe. May 3, 2022. URL : https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/.

[13] KASPERSKY. The 'Penquin' Turla. December 8, 2014. URL : https://securelist.com/the-penquin-turla-2/67962/.

[14] CISCO TALOS. TinyTurla - Turla Deploys New Malware to Keep a Secret Backdoor on Victim Machines. September 21, 2021. URL : https://blog.talosintelligence.com/tinyturla/.

[15] ESET. Turla Mosquito : A Shift towards More Generic Tools. May 22, 2018. URL : https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/.

[16] ESET. New ESET Research Uncovers Gazer, the Stealthy Backdoor That Spies on Embassies. August 31, 2017. URL : https://www.welivesecurity.com/2017/08/30/eset-research-cyberespionage-gazer/.

[17] ESET. Turla Crutch : Keeping the "Back Door" Open. December 2, 2020. URL : https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/.

[18] RECORDED FUTURE. Swallowing the Snake's Tail : Tracking Turla Infrastructure. March 12, 2020. URL : https://www.recordedfuture.com/fr/research/turla-apt-infrastructure.

[19] FOX IT. Snake : Coming Soon in Mac OS X Flavour. May 3, 2017. URL : https://blog.fox-it.com/2017/05/03/snake-coming-soon-in-mac-os-x-flavour/.

[20] ESET. Turla's Watering Hole Campaign : An Updated Firefox Extension Abusing Instagram. June 6, 2017. URL : https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/.

[21] BITDEFENDER. New Pacifier APT Components Point to Russian-Linked Turla Group. September 1, 2017. URL : https://download.bitdefender.com/resources/files/News/CaseStudies/study/170/Bitdefender-Whitepaper-Pacifier2-A4-en-EN.pdf.

[22] ESET. Gamaredon X Turla Collab. September 19, 2025. URL : https://www.welivesecurity.com/en/eset-research/gamaredon-x-turla-collab/.

[23] PALO ALTO. Kazuar : Multiplatform Espionage Backdoor with API Access. May 3, 2017. URL : https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/.

[24] PALO ALTO. Over the Kazuar's Nest : Cracking Down on a Freshly Hatched Backdoor Used by Pensive Ursa (Aka Turla). October 31, 2023. URL : https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/.

[25] R136A1. COMmand & Evade : Turla's Kazuar v3 Loader. January 14, 2026. URL : https://r136a1.dev/2026/01/14/command-and-evade-turlas-kazuar-v3-loader/.

[26] TREND MICRO. Examining the Activities of the Turla APT Group. September 22, 2023. URL : https://www.trendmicro.com/fr_fr/research/23/i/examining-the-activities-of-the-turla-group.html.

[27] SYMANTEC. The Waterbug Attack Group. January 14, 2016. URL : docs.broadcom.com/doc/waterbug-attack-group.

[28] ESET. Tracking Turla : New Backdoor Delivered Via Armenian Watering Holes. March 12, 2020. URL : https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/.

[29] KASPERSKY. Satellite Turla : APT Command and Control in the Sky. September 9, 2015. URL : https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

[30] SYMANTEC. Waterbug : Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments. June 20, 2019. URL : https://www.security.com/threat-intelligence/waterbug-espionage-governments.

[31] MICROSOFT THREAT INTELLIGENCE. Frequent Freeloader Part II : Russian Actor Secret Blizzard Using Tools of Other Groups to Attack Ukraine. December 11, 2024. URL : https://www.microsoft.com/en- us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/.

[32] GTI. Turla : A Galaxy of Opportunity. May 1, 2023. URL : https://cloud.google.com/blog/topics/threat-intelligence/turla-galaxy-opportunity.

[33] ESET. Diplomats in Eastern Europe Bitten by a Turla Mosquito. January 9, 2018. URL : https://web-assets.esetstatic.com/wls/2018/01/ESET_Turla_Mosquito.pdf.

[34] MICROSOFT THREAT INTELLIGENCE. Frozen in Transit : Secret Blizzard's AiTM Campaign against Diplomats. July 31, 2025. URL : https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/.