Le 13 juillet 2026

Ciblage et compromission d'entités françaises au moyen du mode opératoire d'attaque Turla

Activités d'espionnage associées au 16ème Centre du FSB au moyen du MOA Turla depuis les années 2010

Les membres du Centre de Coordination des Crises Cyber (C4)[1] ont observé le ciblage et la compromission d'entités françaises au moyen du mode opératoire d'attaque (MOA[2]) Turla, opéré par le 16ème Centre du service fédéral de sécurité de la fédération de Russie (FSB). Ce MOA a également déjà fait l'objet d'attributions à la Russie par d'autres pays [1, 2, 3, 4]. Depuis au moins 2004, il a été mis en œuvre à des fins de collecte de renseignement contre des entités stratégiques et des personnes physiques à l'échelle mondiale, dont en France. Les campagnes d'espionnage associées au MOA Turla contre l'Ukraine, les pays de l'Organisation du Traité de l'Atlantique Nord et de l'Union européenne se poursuivent dans le contexte de la guerre d'agression déclenchée par la Russie contre l'Ukraine le 24 février 2022.

Les activités cyber-malveillantes du 16ème Centre du FSB à l'encontre de la France et de ses partenaires européens font l'objet ce jour (13 juillet 2026) de deux déclarations formelles d'attribution par le Ministre de l'Europe et des Affaires Étrangères, au nom de la France et par la Haute Représentante de l'UE pour les affaires étrangères et la politique de sécurité, au nom de l'UE et des Etats membres.

1. Le 16ème Centre du service fédéral de sécurité de la fédération de Russie (FSB)

Organisation et répartition géographique

Les membres du C4 ont identifié que le 16ème Centre du service fédéral de sécurité de la fédération de Russie (FSB), également connu sous les appellations « unité militaire 71330 » ou

[1] Le C4 est une instance interministérielle traitant de l'analyse de la menace informatique. Le C4 rassemble l'ANSSI, le COMCYBER, la DGA, la DGSE et la DGSI.

[2] Un mode opératoire d'attaque (MOA) est défini comme un ensemble de techniques, tactiques et procédures, codes et infrastructures, évolutifs mais cohérents dans le temps, qui est utilisé pour mener des attaques informatiques.

« Centre de renseignement radio-électronique des communications »[3] opère différents MOA pour cibler les intérêts français et européens, parmi lesquels le MOA Turla[4].

Pour conduire ces activités, le 16ème Centre du FSB peut s'appuyer sur les onze centres d'interception dont il dispose, répartis sur l'ensemble du territoire russe. Ces centres d'interception sont désignés sous des numéros d'unités militaires :

- l'unité militaire 03110, située à proximité de Sotchi ;
- l'unité militaire 11380, située à proximité de Temriouk dans la région de Krasnodar ;
- l'unité militaire 28735, située à proximité d'Alouchta en Crimée ;
- l'unité militaire 44231, située à proximité de Balachov dans la région de Saratov ;
- l'unité militaire 49911, située à proximité de Pskov dans la région de Pskov ;
- l'unité militaire 51952, située à proximité de Tchekhov dans la région de Moscou ;
- l'unité militaire 61240, située à proximité de Krasnoïe Selo dans la région de Saint-Pétersbourg ;
- l'unité militaire 61608, située dans le sud de Moscou ;
- l'unité militaire 70822, située à proximité de Khabarovsk dans la région de Khabarovsk ;
- l'unité militaire 83417, située à proximité de Chkotovo dans la région de Vladivostok ;
- l'unité militaire 83521, située à proximité de Zelenogradsk dans la région de Kaliningrad.

L'emplacement géographique des unités militaires et l'orientation des antennes sur les sites laissent envisager une répartition géographique du ciblage. Ainsi, les unités de Pskov, Krasnoïe Selo et Zelenogradsk sont orientées vers l'Europe et les Etats-Unis, tandis que Chkotovo et Khabarovsk ciblent plutôt l'Asie.

L'unité militaire 61240, chargée du ciblage de la France

L'unité militaire 61240 est chargée du ciblage de la France en termes de renseignement d'origine électromagnétique (ROEM) et d'activités cyber offensives. Elle se situe à proximité de Krasnoïe Selo, au sud-ouest de Saint-Pétersbourg.

En outre, cette unité entretient des relations étroites avec plusieurs entreprises russes telles que AO AST ou NPP Gamma, connues pour leur appui aux activités cyber offensives des services russes de renseignement.

Cette unité militaire serait donc fortement liée aux dispositifs d'interception ROEM et de LIA du FSB, constituant ainsi une menace réelle pour les intérêts français et européens.

2. Le MOA Turla

Actif depuis au moins 2004, le MOA Turla est notamment employé à des fins de collecte de renseignement contre des entités publiques et privées appartenant aux secteurs gouvernemental,

[3] Центр Радиоэлектронной Разведки Средств Связи ou TsRRSS.

[4] Les activités et techniques, tactiques et procédures (TTP) associées au MOA Turla se recoupent avec celles documentées par des éditeurs de sécurité sous les noms de Secret Blizzard, Venomous Bear, Pensive Ursa, Pacifier ou encore Waterbug. Les membres du C4 considèrent donc que ces alias renvoient au même MOA.

diplomatique, de la défense, de la recherche, des technologies, de l'éducation, des médias, ou encore de l'énergie ainsi que des personnes physiques à l'échelle mondiale [1, 4, 5, 6].

Des attaques informatiques notables associées au MOA Turla ont été menées contre des entités européennes et américaines parmi lesquelles la compromission de réseaux militaires américains en 2008, de l'entreprise de défense suisse RUAG en 2016 ou encore de réseaux gouvernementaux allemands en 2018 [7, 8, 9].

Depuis le début de la guerre d'agression déclenchée par la Russie contre l'Ukraine le 24 février 2022, le MOA Turla est utilisé pour participer à l'effort de guerre russe à travers la collecte de renseignements sur l'Ukraine et ses alliés. Il est notamment mis en œuvre dans le cadre d'activités de reconnaissance et d'espionnage informatique contre des entités gouvernementales, du secteur de la défense ou encore des technologies en Ukraine ainsi que dans plusieurs pays alliés européens [4, 10, 11, 12].

Codes malveillants et infrastructures d'attaque

Les membres du C4 considèrent que le MOA Turla est à la fois associé à l'utilisation d'outils disponibles en source ouverte comme Mimikatz ou Metasploit, et à un ensemble défini de codes malveillants parfois complexes, propres au MOA[5] et dont l'origine remonte aux codes Agent.BTZ et Uroburos, également connus sous les noms Turla et Snake. Ces codes malveillants ont été utilisés pour cibler des systèmes d'exploitation Windows, notamment des solutions de messagerie telles que Outlook et Microsoft Exchange, ainsi que Linux et macOS. Ils ont également été utilisés contre des navigateurs, des applications métier et des serveurs Web [1, 4, 13, 14, 15, 16, 17, 18, 19, 20, 21].

Depuis 2016, les campagnes d'attaque associées au MOA Turla se sont régulièrement appuyées sur le code malveillant Kazuar, qui a connu plusieurs évolutions au fil des années et est toujours utilisé en 2026 [22, 23, 24, 25].

Pour compromettre des systèmes d'information, les opérateurs du MOA Turla ont déjà employé des techniques d'accès initial telles que l'hameçonnage ciblé et les attaques par points d'eau, visant par exemple à inciter des cibles à télécharger des fichiers malveillants usurpant des logiciels légitimes. Les attaquants ont également déjà compromis des équipements réseaux, des applications métier et exploité des vulnérabilités, y compris jour-zéro. Dans certaines campagnes, ils ont combiné l'exploitation de plusieurs vulnérabilités dans une même chaine de compromission [26, 27, 28].

En outre, de l'accès initial à l'exfiltration de données, les opérateurs du MOA Turla s'appuient sur des infrastructures d'attaque visant à assurer leur sécurité opérationnelle et à limiter leur détection. Ils utilisent des ressources louées ou compromises, telles que des serveurs et sites Internet, notamment des systèmes de gestion de contenu comme WordPress. Ils ont également recours à des moyens satellitaires, par exemple pour administrer leur infrastructure d'attaque en assurant leur anonymisation, pour des activités de commande et de contrôle ou encore pour le rapatriement des données collectées. Par ailleurs, ils ont déjà utilisé des outils communiquant de pair-à-pair composés de machines compromises dans leur infrastructure d'attaque [15, 18, 26, 29].

Le MOA est également associé à la compromission et la réutilisation de capacités offensives rattachées à d'autres menaces, dont des MOA réputés étatiques et des acteurs cybercriminels [6, 30, 31, 32].

[5] Ces codes malveillants incluent Epic, ComRAT, Carbon, Mosquito, Penquin, Gazer, Crutch, TinyTurla, LightNeuron ou encore Capibar et Kazuar. Cette liste n'est pas exhaustive.

3. Victimologie française

Les membres du C4 distinguent deux types de victimes du MOA Turla[6] :

- des **victimes finales**, compromises à des fins d'espionnage ;
- des **victimes intermédiaires**, de secteurs variés, dont les systèmes d'information sont compromis de manière opportuniste afin d'être intégrés en tant que relais dans les infrastructures malveillantes du MOA et faciliter la conduite d'attaques ultérieures menées contre des victimes finales.

Depuis les années 2010, les victimes françaises intermédiaires et finales du MOA Turla incluent notamment des **ministères, des entités du secteur diplomatique, de la défense, de la justice et des technologies.** Parmi les victimes intermédiaires du MOA, les membres du C4 ont également identifié des **associations, des particuliers, et des entreprises diverses**.

En 2014, les membres du C4 ont identifié le ciblage et la compromission d'**entités ministérielles** au moyen du code malveillant Uroburos, probablement à des fins d'espionnage.

En particulier, depuis au moins 2017, des comptes de messagerie Internet du **ministère des Armées** ont été compromis par les opérateurs du MOA Turla. Ces attaques ont visé des comptes de messagerie de cadres du ministère. Au-delà de cette campagne, cette menace reste active à l'encontre du ministère des Armées et des entités sous sa tutelle.

En 2018, le réseau du **ministère de l'Europe et des Affaires étrangères à l'ambassade de France à Moscou** a été compromis au moyen du MOA Turla. Les attaquants auraient notamment effectué des activités de balayage réseau et d'exfiltration de données sur le réseau de l'ambassade.

Commentaire : cet incident fait écho à une campagne rapportée récemment par l'éditeur de sécurité MICROSOFT et portant sur le ciblage informatique d'ambassades étrangères localisées à Moscou depuis au moins 2024. L'éditeur de sécurité a associé cette campagne au MOA Turla, ce qui témoigne de l'intérêt constant des opérateurs de ce MOA pour les cibles diplomatiques [33, 34].

Toujours au cours de l'année 2018, les membres du C4 ont également identifié la compromission de plusieurs machines appartenant à une **entité française du secteur des technologies** au moyen du code malveillant Uroburos. Les investigations des membres du C4 ont permis d'observer que les machines compromises étaient utilisées comme relais dans l'infrastructure d'attaque des opérateurs du MOA.

En 2019, les membres du C4 ont eu connaissance de la compromission d'un serveur appartenant à **une entité du secteur de la justice** et hébergeant un service au bénéfice de la formation continue de personnels. Dans le cadre de cette attaque, les opérateurs du MOA Turla ont exploité une vulnérabilité liée à SHAREPOINT pour installer un code malveillant. Les investigations des membres du C4 ont démontré que les attaquants ont potentiellement eu accès aux informations de plusieurs milliers de comptes utilisateurs.

Entre 2019 et 2025, les membres du C4 ont observé la compromission de **plusieurs victimes intermédiaires** françaises par les opérateurs du MOA Turla.

Au cours de l'année 2025, les membres du C4 ont également été informés d'activités malveillantes potentiellement liées au MOA Turla menées contre une **entité travaillant sur des technologies avancées**.

[6] Cette typologie repose sur l'observation du comportement des attaquants et la déduction de leurs objectifs.

Références

[1] CISA et al. Hunting Russian Intelligence "Snake" Malware. 9 mai 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. 15 septembre 2017. URL : https://www.valisluureamet.ee/doc/raport/2018-en.pdf.

[3] BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Annual Report of the Security Information Service for 2017. 29 novembre 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). 31 juillet 2023. URL : https://csirt.csi.cip.gov.ua/en/posts/uac-0024-uac.

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

[6] NCSC-UK. Turla Group Exploits Iranian APT to Expand Coverage of Victims. 21 octobre 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. 28 novembre 2008. URL : https://www.latimes.com/archives/la-xpm-2008-nov-28-na-cyberattack28- story.html.

[8] GOVCERT.CH. APT Case RUAG. 23 mai 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. 1er mars 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. 15 mars 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. 23 mai 2022. URL : https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/.

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

[13] KASPERSKY. The 'Penquin' Turla. 8 décembre 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. 21 septembre 2021. URL : https://blog.talosintelligence.com/tinyturla/.

[15] ESET. Turla Mosquito : A Shift towards More Generic Tools. 22 mai 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. 31 août 2017. URL : https://www.welivesecurity.com/2017/08/30/eset-research-cyberespionage-gazer/.

[17] ESET. Turla Crutch : Keeping the "Back Door" Open. 2 décembre 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. 12 mars 2020. URL : https://www.recordedfuture.com/fr/research/turla-apt-infrastructure.

[19] FOX IT. Snake : Coming Soon in Mac OS X Flavour. 3 mai 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. 6 juin 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. 1er septembre 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. 19 septembre 2025. URL : https://www.welivesecurity.com/en/eset-research/gamaredon-x-turla-collab/.

[23] PALO ALTO. Kazuar : Multiplatform Espionage Backdoor with API Access. 3 mai 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). 31 octobre 2023. URL : https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/.

[25] R136A1. COMmand & Evade : Turla's Kazuar v3 Loader. 14 janvier 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. 22 septembre 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. 14 janvier 2016. URL : docs.broadcom.com/doc/waterbug-attack-group.

[28] ESET. Tracking Turla : New Backdoor Delivered Via Armenian Watering Holes. 12 mars 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. 9 septembre 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. 20 juin 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. 11 décembre 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. 1er mai 2023. URL : https://cloud.google.com/blog/topics/threat-intelligence/turla-galaxy-opportunity.

[33] ESET. Diplomats in Eastern Europe Bitten by a Turla Mosquito. 9 janvier 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. 31 juillet 2025. URL : https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/.