

APT group: Turla, Waterbug, Venomous Bear

Names	<p>Turla (<i>Kaspersky</i>) Waterbug (<i>Symantec</i>) Venomous Bear (<i>CrowdStrike</i>) Group 88 (<i>Talos</i>) SIG2 (<i>NSA</i>) SIG15 (<i>NSA</i>) SIG23 (<i>NSA</i>) Iron Hunter (<i>SecureWorks</i>) CTG-8875 (<i>SecureWorks</i>) Pacifier APT (<i>Bitdefender</i>) ATK 13 (<i>Thales</i>) ITG12 (<i>IBM</i>) Makersmark (<i>ESET</i>) Krypton (<i>Microsoft</i>) Belugasturgeon (<i>Accenture</i>) Popeye (?) Wraith (?) TAG-0530 (<i>Recorded Future</i>) UNC4210 (<i>Mandiant</i>) SUMMIT (<i>Google</i>) Secret Blizzard (<i>Microsoft</i>) Pensive Ursa (<i>Palo Alto</i>) Blue Python (<i>PWC</i>)</p>
Country	 Russia
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	1996
Description	Turla is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. Turla is known for conducting watering hole and spear-phishing campaigns and leveraging in-house tools and malware. Turla's espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines.
Observed	<p>Sectors: Aerospace, Defense, Education, Embassies, Energy, Government, High-Tech, IT, Media, NGOs, Pharmaceutical, Research, Retail.</p> <p>Countries: Afghanistan, Algeria, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bolivia, Botswana, Brazil, China, Chile, Denmark, Ecuador, Estonia, Finland, France, Georgia, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Iraq, Italy, Jamaica, Jordan, Kazakhstan, Kyrgyzstan, Kuwait, Latvia, Mexico, Netherlands, Pakistan, Paraguay, Poland, Qatar, Romania, Russia, Serbia, Spain, Saudi Arabia, South Africa, Sweden, Switzerland, Syria, Tajikistan, Thailand, Tunisia, Turkmenistan, UK, Ukraine, Uruguay, USA, Uzbekistan, Venezuela, Vietnam, Yemen.</p>
Tools used	<p>AdobeARM, Agent.BTZ, Agent.DNE, ASPXSpy, ATI-Agent, certutil, CloudDuke, Cobra Carbon System, COMpfun, ComRAT, Crutch, DoublePulsar, EmpireProject, Epic, EternalBlue, EternalRomance, Gazer, gpresult, HTML5 Encoding, HyperStack, IcedCoffee, IronNetInjector, Kazuar, KopiLuwak, KSL0T, LightNeuron, Maintools.js, Metasploit, Meterpreter, MiamiBeach, Mimikatz, Mosquito, Nautilus, nbtsan, nbstat, Neptun, NetFlash, NETVulture, Neuron, NewPass, Outlook Backdoor, Penguin Turla, PowerShellRunner-based RPC backdoor, PowerStallion, PsExec, pwdump, PyFlash, RocketMan, Satellite Turla, SScan, Skipper, SMBTouch, TinyTurla, TinyTurla-NG, Topinambour, Tunnus, TurlaChopper, Uroburos, Windows Credentials Editor, WhiteAtlas, WITCHCOVEN, Living off the Land.</p>
Operations performed	<p>1996 Operation "Moonlight Maze" That is why our experts, aided by researchers from King's College London, have carefully studied Moonlight Maze — one of the first widely known cyberespionage campaigns, active since at least 1996. It is of particular interest because several independent experts from countries have voiced the proposition that it is associated with a much more modern — and still active — group, the authors of the Turla APT attack. <https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/></p> <p>Nov 2008 Breach of the US Department of Defense <https://www.nytimes.com/2010/08/26/technology/26cyber.html> The investigation was called "Operation Buckshot Yankee" and led to the establishment of U.S. Cyber Command.</p> <p>2013 Operation "Epic Turla" Over the last 10 months, Kaspersky Lab researchers have analyzed a massive cyber-espionage operation which we call "Epic Turla". The attackers behind Epic Turla have infected several hundred computers in more than 45 countries, including government institutions, embassies, military, education, research and pharmaceutical companies. <https://securelist.com/the-epic-turla-operation/65545/></p>

2014	Breach of the Swiss military firm RUAG < https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html >
Dec 2014	Operation "Penguin Turla" The Turla APT campaigns have a broader reach than initially anticipated after the recent discovery of two modules built to infect servers running Linux. Until now, every Turla sample in captivity was designed for either 32- or 64-bit Windows systems, but researchers at Kaspersky Lab have discovered otherwise. < https://threatpost.com/linux-modules-connected-to-turla-apt-discovered/109765/ >
2015	Operation "Satellite Turla" Obviously, such incredibly apparent and large-scale attacks have little chance of surviving for long periods of time, which is one of the key requirements for running an APT operation. It is therefore not very feasible to perform the attack through MitM traffic hijacking, unless the attackers have direct control over some high-traffic network points, such as backbone routers or fiber optics. There are signs that such attacks are becoming more common, but there is a much simpler way to hijack satellite-based Internet traffic. < https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/ >
2015	Operation "WITCHCOVEN" When an unsuspecting user visits any of the over 100 compromised websites, a small piece of inserted code—embedded in the site's HTML and invisible to casual visitors—quietly redirects the user's browser to a second compromised website without the user's knowledge. This second website hosts the WITCHCOVEN script, which uses profiling techniques to collect technical information on the user's computer. As of early November 2015, we identified a total of 14 websites hosting the WITCHCOVEN profiling script. < https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf >
2015	ESET researchers found a previously undocumented backdoor and document stealer. Dubbed Crutch by its developers, we were able to attribute it to the infamous Turla APT group. According to our research, it was used from 2015 to, at least, early 2020. < https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/ >
Nov 2016	Operation "Skipper Turla" On 28 January 2017, John Lambert of Microsoft (@JohnLaTWC) tweeted about a malicious document that dropped a "very interesting .JS backdoor". Since the end of November 2016, Kaspersky Lab has observed Turla using this new JavaScript payload and specific macro variant. < https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/ > < https://securelist.com/introducing-whitebear/81638/ >
2017	Operation "Turla Mosquito" ESET researchers have observed a significant change in the campaign of the infamous espionage group < https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/ >
Mar 2017	New versions of Carbon The Turla espionage group has been targeting various institutions for many years. Recently, we found several new versions of Carbon, a second stage backdoor in the Turla group arsenal. < https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/ >
May 2017	New backdoor Kazuar < https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/ >
Jun 2017	Some of the tactics used in APT attacks die hard. A good example is provided by Turla's watering hole campaigns. Turla, which has been targeting governments, government officials and diplomats for years – see, as an example, this recent paper – is still using watering hole techniques to redirect potentially interesting victims to their C&C infrastructure. In fact, they have been using them since at least 2014 with very few variations in their modus operandi. < https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/ >
Jul 2017	Russian malware link hid in a comment on Britney Spears' Instagram The Slovak IT security company ESET Security released a report yesterday detailing a cleverly hidden example of such a post. And its hideout? A Britney Spears photo. Among the nearly 7,000 comments written on the performer's post (shown below) was one that could easily pass as spam. < https://www.engadget.com/2017/06/07/russian-malware-hidden-britney-spears-instagram/ >
Aug 2017	New backdoor Gazer < https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf >
Aug 2017	In this case, the dropper is being delivered with a benign and possibly stolen decoy document inviting recipients to a G20 task force meeting on the "Digital Economy". The Digital Economy event is actually scheduled for October of this year in Hamburg, Germany. < https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack >

Jan 2018	<p>A notorious hacking group is targeting the UK with an updated version of malware designed to embed itself into compromised networks and stealthily conduct espionage. Both the Neuron and Nautilus malware variants have previously been attributed to the Turla advanced persistent threat group, which regularly carries out cyber-espionage against a range of targets, including government, military, technology, energy, and other commercial organisations.</p> <p><https://www.zdnet.com/article/this-hacking-gang-just-updated-the-malware-it-uses-against-uk-targets/></p>
Jan 2018	<p>Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments</p> <p>Waterbug may have hijacked a separate espionage group's infrastructure during one attack against a Middle Eastern target.</p> <p><https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments></p>
Mar 2018	<p>Starting in March 2018, we observed a significant change in the campaign: it now leverages the open source exploitation framework Metasploit before dropping the custom Mosquito backdoor.</p> <p><https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/></p>
2018	<p>Much of our 2018 research focused on Turla's KopiLuwak javascript backdoor, new variants of the Carbon framework and meterpreter delivery techniques. Also interesting was Mosquito's changing delivery techniques, customized PoshSec-Mod open-source powershell use, and borrowed injector code. We tied some of this activity together with infrastructure and data points from WhiteBear and Mosquito infrastructure and activity in 2017 and 2018.</p> <p><https://securelist.com/shedding-skin-turlas-fresh-faces/88069/></p>
Early 2019	<p>2019 has seen the Turla actor actively renew its arsenal. Its developers are still using a familiar coding style, but they're creating new tools. Here we'll tell you about several of them, namely "Topinambour" (aka Sunchoke - the Jerusalem artichoke) and its related modules. We didn't choose to name it after a vegetable; the .NET malware developers named it Topinambour themselves.</p> <p><https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/></p>
Apr 2019	<p>COMpfun successor Reductor infects files on the fly to compromise TLS traffic</p> <p><https://securelist.com/compfun-successor-reductor/93633/></p>
May 2019	<p>Turla, also known as Snake, is an infamous espionage group recognized for its complex malware. To confound detection, its operators recently started using PowerShell scripts that provide direct, in-memory loading and execution of malware executables and libraries. This allows them to bypass detection that can trigger when a malicious executable is dropped on disk.</p> <p><https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/></p>
2019	<p>Turla accessed and used the Command and Control (C2) infrastructure of Iranian APTs to deploy their own tools to victims of interest. Turla directly accessed 'Poison Frog' C2 panels from their own infrastructure and used this access to task victims to download additional tools.</p> <p><https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims></p>
Sep 2019	<p>ESET researchers found a watering hole (aka strategic web compromise) operation targeting several high-profile Armenian websites. It relies on a fake Adobe Flash update lure and delivers two previously undocumented pieces of malware we have dubbed NetFlash and PyFlash.</p> <p><https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/></p>
Nov 2019	<p>COMpfun authors spoof visa application with HTTP status-based Trojan</p> <p><https://securelist.com/compfun-http-status-based-trojan/96874/></p>
Jan 2020	<p>During our investigation, we were able to identify three different targets where ComRAT v4 has been used:</p> <ul style="list-style-type: none"> • Two Ministries of Foreign Affairs in Eastern Europe • One national parliament in the Caucasus region <p><https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf></p>
Jun 2020	<p>At the best of our knowledge, this time the hacking group used a previously unseen implant, that we internally named "NewPass" as one of the parameters used to send exfiltrated data to the command and control.</p> <p><https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/></p>
Jun 2020	<p>Accenture Cyber Threat Intelligence researchers identified a Turla compromise of a European government organization. During this compromise Turla utilized a combination of remote procedure call (RPC)-based backdoors, such as HyperStack and remote administration trojans (RATs), such as Kazuar and Carbon, which ACTI researchers analyzed between June and October 2020.</p> <p><https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity></p>
Jan 2021	<p>In January 2021, ESET Research uncovered a new backdoor on a server belonging to a Ministry of Foreign Affairs in Eastern Europe.</p> <p><https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_threat_report_t12021.pdf></p>
Feb 2021	<p>IronNetInjector: Turla's New Malware Loading Tool</p> <p><https://unit42.paloaltonetworks.com/ironnetinjector/></p>


	Sep 2021	TinyTurla - Turla deploys new malware to keep a secret backdoor on victim machines < https://blog.talosintelligence.com/2021/09/tinyturla.html >
	Mar 2022	Turla, a group publicly attributed to Russia's Federal Security Service (FSB), recently hosted Android apps on a domain spoofing the Ukrainian Azov Regiment. < https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/ >
	Apr 2022	Turla, a group TAG attributes to Russia FSB, continues to run campaigns against the Baltics, targeting defense and cybersecurity organizations in the region. < https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/ >
	May 2022	TURLA's new phishing-based reconnaissance campaign in Eastern Europe < https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/ >
	Sep 2022	Turla: A Galaxy of Opportunity < https://www.mandiant.com/resources/blog/turla-galaxy-opportunity >
	Jul 2023	Microsoft: Hackers turn Exchange servers into malware control centers < https://www.bleepingcomputer.com/news/security/microsoft-hackers-turn-exchange-servers-into-malware-control-centers/ >
	Jul 2023	Over the Kazuar's Nest: Cracking Down on a Freshly Hatched Backdoor Used by Pensive Ursa (Aka Turla) < https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/ >
	Dec 2023	TinyTurla Next Generation - Turla APT spies on Polish NGOs < https://blog.talosintelligence.com/tinyturla-next-generation/ >
Information		< https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf > < https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/ > < https://www.recordedfuture.com/turla-apt-infrastructure/ > < https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf > < https://interaktiv.br.de/elite-hacker-fsb/en/index.html > < https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf > < https://unit42.paloaltonetworks.com/turla-pensive-ursa-threat-assessment/ > < https://www.trendmicro.com/en_us/research/23/i/examining-the-activities-of-the-turla-group.html >
MITRE ATT&CK		< https://attack.mitre.org/groups/G0010/ >

Card date: 10 March 2024

TLP: WHITE

This document has been created from the "Threat Group Cards: A Threat Actor Encyclopedia" portal, on a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License, by Digital Service Security Center
Electronic Transactions Development Agency

Report incidents

 **+66 (0)2-123-1227**

 **helpdesk@etda.or.th**

Follow us on

