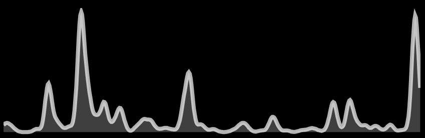
THREAT ACTOR FROM RUSSIAN FEDERATION 🇷🇺

Turla

28 mentions in the last 2 weeks



468 articles in the last 12 months

Using open-source data collected by Feedly AI.

Overview

Turla, also known as Pensive Ursa, Uroburos, Snake, Venomous Bear, and Waterbug, is a highly sophisticated Russian-based advanced persistent threat (APT) group linked to the Federal Security Service (FSB) of Russia. Active since at least 2004, Turla primarily targets government entities, militaries, and embassies, but has also expanded its operations to include sectors such as education, pharmaceu...

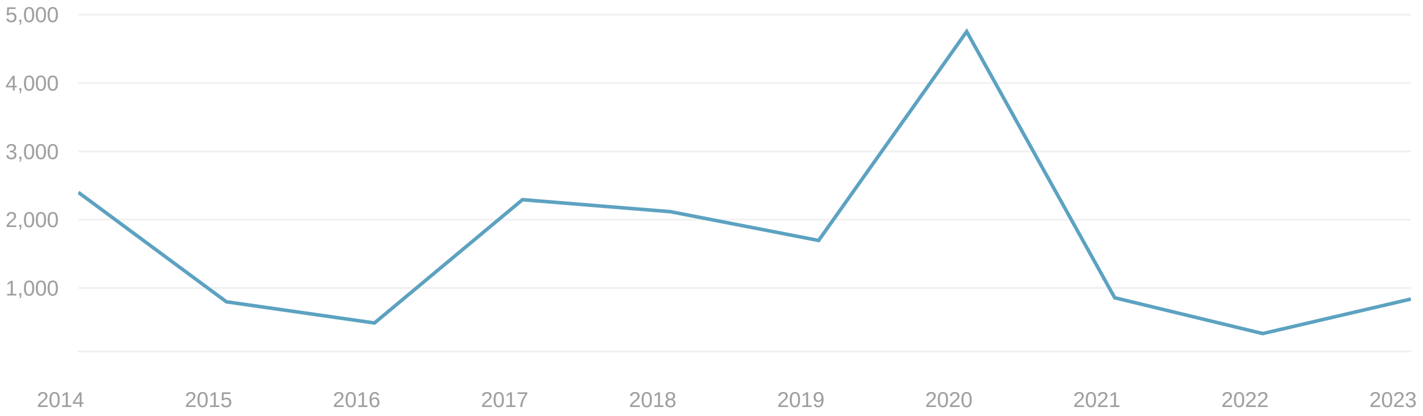
See More

Aliases

- ATK 13
- Blue Python
- G0010
- Group 88

See 23 more aliases

Article count



Targets

No targeted countries have been identified by MISP

Top targeted industries and organizations

INDUSTRIES	ORGANIZATIONS	ARTICLES	ATTACK REPORTED

No attack has been detected in the time frame selected

Top malware families associated with this threat actor

Loading...

Tactics, Techniques, and Procedures

Last mentioned

Loading...

Exploited vulnerabilities

Loading...

Detection Rules

RULE	ARTICLES	COUNT	ACTION
Sigma rules	0	2	Download
YARA rules	7	13	Download

Threat intelligence reports

Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage

AI Threat Actors • Threat intelligence by Microsoft Threat Intelligence / 4d • Threat Actors • Threat Intelligence Reports • IoC > 3 domains, 21 IPs, and 9 hashes

Secret Blizzard overlaps with the threat actor tracked by other security vendors as Turla , Waterbug, Venomous Bear, Snake, Turla Team, and Turla APT Group.... One of these CrimsonRAT deployments was configured with a C2 server at…

Also in Patrick C Miller, Techmeme, +81 feeds

Snowblind: The Invisible Hand of Secret Blizzard

AI Threat Actors • by Black Lotus Labs / 5d • Threat Actors • Threat Intelligence Reports • IoC > 39 IPs

submitted by /u/digicat [link] [comments]

Snowblind: The Invisible Hand of Secret Blizzard

IoC > 39 IPs • Lumen Blog by Black Lotus Labs / 5d • 12 TTPs • Turla exploits Pakistani hackers' servers

Executive Summary Lumen's Black Lotus Labs has uncovered a longstanding campaign orchestrated by the Russian-based threat actor known as "Secret Blizzard" (also referred to as Turla).

Also in Patrick C Miller, Techmeme, +84 feeds

Threat Hunting Case Study: Uncovering Turla

by netbiosX / 26d

submitted by /u/netbiosX [link] [comments]

News

9th December – Threat Intelligence Report

3 CVEs • Check Point Research by hagarb / 11h • 12 TTPs

Researchers report on Russian nation-state actor known as Secret Blizzard (Turla) leveraging the infrastructure of six other threat actors, both state-sponsored and cybercriminals, for facilitating their espionage operations.

⚡ THN Recap: Top Cybersecurity Threats, Tools and Tips (Dec 2 - 8)

AI New Malware > DroidBot •

27 The Hacker News by info@thehackernews.com (The Hacker News) / 11h • 18 CVEs • 22 TTPs

"This phase is crucial for attackers to achieve their ultimate objectives, which might include data exfiltration, persistence or further system compromise." The disclosure comes as new research has revealed how the legitimate Windows…

Andromeda Malware Resurfaces: Targeting APAC Manufacturing and Logistics Industries

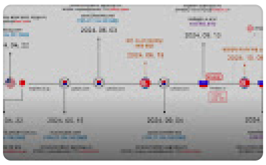
IoC > 1 domain •

CySecurity News - Latest Information Sec... by Shivani Tiwari / 1d •

10 TTPs • New Andromeda malware C2 cluster discovered

During Cybereason’s investigation, one such C2 domain, suckmycocklameavindustry[.]in, demonstrated agility by resolving to multiple IP addresses, ensuring constant communication between infected systems and th…

Also in IT Security News, NetmanageIT CTO Corn..., +8 feeds



CTO at NCSC Summary: week ending December 8th

Threat Actors • by Ollie Whitehouse / 2d • Threat Intelligence Reports • 2 CVEs • 27 TTPs

submitted by /u/digicat [link] [comments]

Also in r/cybersecurity, CTO at NCSC, +4 feeds

US Officials Recommend Encryption Apps Amid Chinese Telecom Hacking

US recommends encryption amid hacking •

37 Security Latest by Andy Greenberg, Lily Hay Newman / 2d

In a briefing with reporters about the breach of no fewer than eight phone companies by the Chinese state-sponsored espionage hackers known as Salt Typhoon, officials from the Cybersecurity and Infrastructure Security Agency…

Also in #cybersecurity, IT Industry News, +9 feeds

Russian Hackers Hijacked Pakistani Actor Servers For C2 Communication

AI New Malware > Waiscot • GBHackers Security by Aman Mishra / 3d • Command and Control (Enterprise TA0011) • Russian hackers exploit Pakistani servers

Secret Blizzard, a Russian threat actor, has infiltrated 33 command-and-control (C2) servers belonging to the Pakistani group Storm-0156, which allows Secret Blizzard to access networks of Afghan government entities and Pakistani…

Also in Cyberattacks News, RSS reader not yet w..., +85 feeds

See 29 more articles and social media posts