Contents

[**G0010-Turla** 2](#_Toc179442367)

[**I. Introduction** 2](#_Toc179442368)

[**II. Tactics** 2](#_Toc179442369)

[**III. Techniques** 2](#_Toc179442370)

[**IV. Procedures** 3](#_Toc179442371)

[**V. Summary** 4](#_Toc179442372)

[**References** 6](#_Toc179442373)

## **G0010-Turla**

## **I. Introduction**

Turla, also known as Snake, Uroburos, and Venomous Bear, is a highly sophisticated and long-standing Russian-linked advanced persistent threat group. It has been active since at least 2008, Turla is renowned for its complex malware, its innovative tactics, and its high-profile targets. The group primarily focuses on espionage operations whereby they target government institutions, embassies, military organizations, research and academic institutions, and large corporations worldwide.

## **II. Tactics**

The approach that this group uses is characterized by

1. ***Sophisticated Malware***

Development and deployment of highly advanced, modular malware platforms.

1. ***Stealthy Operations***

Emphasis on remaining undetected in compromised networks for extended periods.

1. ***Strategic Intelligence Gathering***

Focus on collecting sensitive geopolitical, military, and scientific information.

1. ***Adaptive Techniques***

Continuous evolution of tactics to bypass security measures and avoid detection.

1. ***Satellite Hijacking***

Unique use of hijacked satellite connections for command and control.

## **III. Techniques**

Turla employs a wide array of sophisticated techniques

|  |  |
| --- | --- |
| Technique | Description |
| Spear-phishing Campaigns (T1566) | Use of meticulously crafted emails with malicious attachments or links. |
| Watering Hole Attacks (T1189) | Compromise of legitimate websites to distribute malware. |
| Custom Malware Suites | Deployment of complex malware families such as Snake, Turla Carbon, and Neuron. |
| Hijacked Satellite Connections (T1020) | Innovative use of satellite-based Internet connections for covert C2 communication |
| Living off the Land (T1059) | Extensive use of legitimate system tools and PowerShell for post-exploitation activities |
| Supply Chain Attacks (T1195) | Compromise of trusted third-party software to gain access to targets. |
| Rootkit Deployment | Use of sophisticated rootkits for deep system persistence and stealth |

## **IV. Procedures**

This group’s typical attack chain follows this sequence

***1. Initial Access***

a. Spear-phishing emails are sent to targeted individuals with malicious attachments or links.

b. Alternatively, watering hole attacks are set up on compromised legitimate websites.

***2. Execution and Persistence***

a. Upon successful compromise, Turla deploys its initial loader malware.

b. The loader then installs more sophisticated components of the Turla malware suite.

c. Multiple persistence mechanisms are established, often leveraging rootkit techniques.

***3. Privilege Escalation***

a. The group employs both public and custom exploits to elevate privileges.

b. Advanced rootkit capabilities are used to maintain high-level system access.

***4. Defense Evasion***

a. Turla uses sophisticated obfuscation and encryption techniques to avoid detection.

b. Their malware often mimics legitimate system processes and leverages valid digital signatures.

***5. Discovery and Lateral Movement***

a. Extensive network reconnaissance is conducted to map out the target's infrastructure.

b. Lateral movement is achieved using both stolen credentials and exploits.

***6. Collection and Exfiltration***

a. Sensitive data is identified and collected from compromised systems.

b. Data exfiltration often occurs through innovative channels, including hijacked satellite connections.

***7. Command and Control***

a. Turla employs a variety of C2 mechanisms, including the use of compromised websites and hijacked satellite links.

b. Communication is heavily obfuscated and often blended with legitimate traffic.

## **V. Summary**

Turla has gained its position in the list of one of the most successful groups in the sphere of cyber espionage. Their actions have aimed at major organizations such as the United States Department of State and Central Command establishing their reach and skill set.

It is the diverse approach that Turla took that really puts their tactics into a league of its own. Consider their employment of hijacked satellite internet connections for C2 – it is brilliant. C2 servers are usually very well hidden, by leveraging these downstream-only links, it has been very challenging for the other side, to track them or even try to shut them down. They also have an extensive set of malware, and the Snake / Uroburos platform is one of the best examples of its kind. This modular, multistage framework includes rootkit functionality and is nearly impossible to identify and eliminate for security personnel.

Turla’s targeting is broad, while at the same time specific with emphasis on foreign policy, defense, and scientific research. This combined with their constant adaptability toward the tactics and tools used all points towards state sponsorship and many have pointed towards Russian intelligence services as the source of these campaigns funding. Stealing software installers, compromising other actors’ infrastructure, Turla is one of the most innovative and flexible threats on the market. It’s not for nothing that these threats have stayed around for so long; it is indicative of how vibrant and complicated they remain for global cybersecurity.

## **References**

ESET Research. (2020). "Tracking Turla: New backdoor delivered via Armenian watering holes." <https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/>

Kaspersky Lab. (2015). "Satellite Turla: APT Command and Control in the Sky." <https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/>

Symantec Threat Hunter Team. (2019). "Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments." <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/waterbug-espionage-governments>

NCSC. (2018). "Turla group exploits Iranian APT to expand coverage of victims." <https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims>

MITRE ATT&CK. (2024). "Turla, G0010." <https://attack.mitre.org/groups/G0010/>