Swallowing the Snake's Tail: Tracking Turla Infrastructure

By Insikt Group®

Archived: 2026-04-06 01:48:31 UTC

Recorded Future's Insikt Group® has developed new detection methods for Turla malware and infrastructure as part of an in-depth investigation into recent Turla activities. Data sources included the Recorded Future® Platform, ReversingLabs, VirusTotal, Shodan, BinaryEdge, and various OSINT tools. The target audience for this research includes security practitioners, network defenders, and threat intelligence professionals who are interested in Russian nation-state computer network operations activity.

Executive Summary

Turla, also known as Snake, Waterbug, and Venomous Bear, is a well-established, sophisticated, and strategically focused cyberespionage group that has for over a decade been linked to operations against research, diplomatic, and military organizations worldwide, with an ongoing focus against entities within North Atlantic Treaty Organization (NATO) and Commonwealth of Independent States (CIS) nations in particular.

While many nation-state threat actor groups are becoming more reliant on open source and commodity software for operations, Turla continues to develop its own unique, advanced malware and tools and adopts new methods of attack and obfuscation. It uses these TTPs alongside older techniques and generic, open source tools. For these reasons, Insikt Group assesses that Turla Group will remain an active, advanced threat for years to come that will continue to surprise with unique operational concepts.

However, the group's consistent patterns and use of stable and periodically updated versions of unique malware for lengthy campaigns may allow defenders to proactively track and identify Turla's infrastructure and activities. This research examines the history of Turla's operations and provides our methodology for identifying infrastructure currently being used by Turla, focusing on several Turla-associated malware types. Details on two of them — the composite Mosquito backdoor and the hijacked Iranian TwoFace ASPX web shell — are provided in this report.

Recorded Future has provided a detailed report to our clients with further research and detections for additional Turla-related malware families, which is available in the Recorded Future platform.

Key Judgments

- Turla Group can be tracked based on unique features of their malware and C2 communication. Additionally, Turla's use of open source tools when avoiding detection and confusing attribution attempts also allows researchers to quickly analyze and build detections, as the source code is readily available for analysis and testing.
- In June 2019, Turla Group was found to have infiltrated the computer network operations infrastructure of APT34, an Iranian threat group. This amounted to the effective takeover of the computer network

operations of a nation-state group by state actors from another country — an unprecedented action. Insikt Group assesses that Turla Group's use of APT34 infrastructure was primarily opportunistic in nature and was not coordinated between Iranian and Russian organizations.

- Recorded Future assesses with high confidence that TwoFace is the Iranian APT34 ASPX shell Turla was scanning for to pivot to additional hosts, as documented in the NSA/NCSC report. We assess that any live TwoFace shells as of late January 2020 could also be potential operational assets of the Turla Group.
- In 2019, Turla began relying heavily on PowerShell scripts for malware installation. Previously, it had also heavily targeted Microsoft vulnerabilities as well as email servers. Turla also often uses compromised WordPress websites as the foundation of its C2 infrastructure.
- Among the malware that we researched, Turla mainly uses HTTP/S for their command and control (C2) communication.

Background

Turla has been attributed to operations targeting the Pentagon as early as 2008 and has continued targeting NATO nations to the present day. Primary targets of Turla include publishing and media companies, universities/academia, and government organizations, often specifically targeting scientific and energy research, remote and local diplomatic affairs, and military data. Turla actively targets European and CIS countries, historically focusing on ministries of foreign affairs or defense, as well as similar government organizations and affiliated research institutions.

Turla is known for its use of watering hole attacks (compromising websites to target visitors) and spearphishing campaigns to precisely attack specific entities of interest. Turla has also used inventive, out-of-the box techniques, including using satellites to exfiltrate data from remote areas in North Africa and the Middle East. The group is known for the use of both unaltered and customized versions of open source software such as Meterpreter and Mimikatz, as well as bespoke malware such as Gazer, IcedCoffee, Carbon, and Mosquito.

Turla operators have also commandeered third-party infrastructure or used false flags in order to further their purposes. In many cases, this group has used compromised websites (typically WordPress sites) as both an infection vector and as operational infrastructure for C2 communications.

In June 2019, Turla was identified by researchers at Symantec as having infiltrated the computer network operations infrastructure of APT34, an Iranian threat group, collecting and exfiltrating Iranian operational information, and simultaneously gaining access to active victims of the Iranians.

Turla's hijacking of Iranian APT34 operations in part consisted of scanning for and discovering their web shells using existing APT34 victim networks to scan for a specific web shell on IP addresses across at least 35 different countries. Once identified, Turla used these shells to gain an initial foothold into victims of interest and then deployed further tools.

TwoFace, first observed in 2015, is the primary APT34 web shell, and Recorded Future assesses with high confidence that TwoFace is the shell Turla was scanning for to pivot to additional hosts. We assess that any live TwoFace shells as of late January 2020 could also be potential operational assets of the Turla Group.

Turla also directly accessed C2 panels of the APT34 Poison Frog tool from their own infrastructure and used this access to task victims with downloading Turla tools.

Threat Analysis

To date, Turla Group's hijacking of Iranian computer network operations resources has been unique among known threat actors; this action amounted to the effective takeover of the computer network operations of a nation-state group by state actors from another country.

Although it is possible that the Iranian and Russian organizations were cooperating in some manner, the evidence available to Insikt Group does not support this theory. For example, while Turla had significant insight into APT34 tools and operations, they were required to scan for Iranian web shells in order to find where these tools were deployed. We assess that Turla's interposition into Iranian operations was likely an uncoordinated, and thus hostile, act.

While Insikt Group assesses that Turla Group's use of APT34 infrastructure was primarily opportunistic in nature, an added benefit for the operators was likely the deception of incident responders who would potentially identify the tools as Iranian in origin. Turla has reused malware from other threat actors prior to their use of Iranian tools, including the use of Chinese-attributed Quarian malware in 2012. In that instance, Kaspersky researchers assessed that Turla actors downloaded, then uninstalled, the Quarian malware in an attempt to divert and deceive incident responders post-discovery.

Outside of their bold Iranian venture, Turla has concurrently conducted other operational and development activities. In 2019, Turla started heavily using PowerShell scripts, likely in an effort to avoid discovery of malicious files on disk. Over the course of the year, they have increased their use of PowerShell scripts, using PowerSploit and PowerShell Empire, as well as developing their own Powershell backdoor, PowerStallion.

While Turla most often targets Microsoft Windows operating systems, they have also purposely exploited email servers. The LightNeuron backdoor is specifically designed to function on Microsoft Exchange mail servers, and the Outlook backdoor is designed to operate on Exchange and The Bat! (popular in Eastern Europe) email servers. Compromising mail servers provides Turla control of email traffic on a target network, including the ability to not only monitor email, but create, send, and even block email.

Turla relies on compromised WordPress sites as C2s. They also have regularly used WordPress-focused URL names for payload delivery since 2014 and possibly earlier. This tendency enables the profiling of their C2s and payload URLs to discover new Turla infrastructure.

Turla operations have been associated with a variety of custom malware. Insikt Group performed deeper analysis on several of these malware types in an effort to create scanning rules to detect live Turla-associated infrastructure active from December 2019 to January 2020.

Turla Advanced Detection Analysis

The focus of our analysis was the development of identification methods for Turla, focusing on several Turla-associated malware types. Details of our analysis of both the composite Mosquito backdoor and the hijacked Iranian TwoFace web shell are provided in this report.

Mosquito Controller Detection

In January 2018, ESET reported on a newer backdoor named Mosquito that they observed Turla using during intrusion analysis. There were multiple components to the Mosquito delivery and installation, such as:

- Use of a trojanized Adobe installer
- Use of Metasploit shellcode to download a legitimate copy of the Adobe Flash installer and a copy of Meterpreter in order to enable the download and installation of the Mosquito installer
- Installer with encrypted payload
- Launcher which executes the primary backdoor, "Commander"

Mosquito is a Win32 remote access trojan (RAT). The malware includes three primary components: an installer, launcher, and the backdoor component sometimes called CommanderDLL. The Mosquito malware has been dropped after the initial use of Metasploit shellcode and installation of Meterpreter to gain control of the victim. It has the following capabilities:

- Download file
- Create process
- Delete file
- Upload file
- Execute shell commands
- Execute PowerShell commands
- Add C2 server
- Delete C2 server

Commander is the main component of the Mosquito backdoor. In this research, we focused our analysis primarily on the C2 communication of Commander. For details on the other aspects of the Mosquito package, a thorough analysis was conducted by researchers at ESET.
ESET's analysis of the communication from Commander to its C2 shows that communication to and from the controller is sent via HTTP or HTTPS. On the client side, data can be sent as a parameter in the GET request, as a cookie, or as the parameter and payload of a POST (as shown in the image below). On the controller side, responses and commands are sent as an HTTP payload.

Beacon from the Mosquito "Commander" backdoor with encrypted data sent in the POST parameter and payload.

As shown above, the data sent to the controller is not in clear text. It is first protected with an encryption routine that uses a Blum Blum Shub pseudo-random number generator to create a stream of bytes that are used to XOR encode the cleartext data. The resulting data is then Base64 encoded.

To encrypt or decrypt, a key and modulus are required by the encryption process. As ESET reported, and as Insikt Group observed during its analysis, the modulus of "0x7DFDC101" is hardcoded. The key is not hardcoded and is randomly generated at each exchange between the client and controller so the key is different for each transmission. This randomized key is sent as a part of the C2 communication and can be easily extracted. Insikt Group analysts have reversed this pseudo-random number generator implementation and have created a decoder script in Python that can be found in our GitHub repository.

Mirroring analysis from ESET, Insikt Group found there is header information prepended to the data being sent. The header, when decrypted, consists of the following fields:
