National Security Agency | National Cyber Security Centre
a part of GCHQ

# CYBERSECURITY ADVISORY

*Turla Group Exploits Iranian APT To Expand Coverage Of Victims*

## Introduction

The Turla group, also known as Waterbug or VENOMOUS BEAR, is widely reported to be associated with Russian actors. Turla uses a range of tools and techniques to target government, military, technology, energy and commercial organizations for the purposes of intelligence collection.

Previous advisories from NCSC detailed Turla's use of Neuron and Nautilus implants and an ASPX-based backdoor alongside the Snake rootkit. This document provides an update on the reported activity, with a particular focus on how those tools were used in the period leading up to, and following, the publication of those advisories.

Since those advisories were published, NCSC, NSA and partner-shared analysis of additional victims and infrastructure determined the Neuron and Nautilus tools were very likely Iranian in origin. Those behind Neuron or Nautilus were almost certainly not aware of, or complicit with, Turla's use of their implants.

After acquiring the tools – and the data needed to use them operationally – Turla first tested them against victims they had already compromised using their Snake toolkit, and then deployed the Iranian tools directly to additional victims. Turla sought to further their access into victims of interest by scanning for the presence of Iranian backdoors and attempting to use them to gain a foothold. The focus of this activity from Turla was largely in the Middle East, where the targeting interests of both Advanced Persistent Threats (APTs) overlap.

The timeline of incidents, and the behavior of Turla in actively scanning for Iranian backdoors, indicates that while Neuron and Nautilus tools were Iranian in origin, Turla were using these tools and accesses independently to further their own intelligence requirements. The behavior of Turla in scanning for backdoor shells indicates that although they had a significant amount of insight into the Iranian tools, they did not have full knowledge of where they were deployed.

While attribution of attacks and proving authorship of tools can be very difficult – particularly in the space of incident response on a victim network – the weight of evidence demonstrates that Turla had access to Iranian tools and the ability to identify and exploit them to further Turla's own aims.

## Background: Neuron and Nautilus Usage by Turla

The NCSC published two advisories on the use of Neuron and Nautilus tools by Turla in late 2017 and early 2018. These tools were observed in use alongside Snake on a number of victims.

Since publication of those advisories, further analysis by NCSC, the NSA and the wider Cybersecurity community determined Neuron and Nautilus tools were present on a range of victims, with a large cluster in the Middle East. Victims in this region included military establishments, government departments, scientific organizations and universities. Some of these victims, but not all, also had a Snake implant present.

## Victim Overlap

Investigation into these victims identified that while some implants had been deployed and administered from infrastructure associated with the Turla group, others had previously been connected to by Virtual Private Server (VPS) IP addresses associated in the Cybersecurity community with Iranian APT groups.

Interestingly, in some instances, it appeared an Iranian APT-associated IP address first deployed the implant, and later, Turla-associated infrastructure accessed the same implant.

In order to initiate connections with the implants, Turla must have had access to relevant cryptographic keys, and likely had access to controller software to produce legitimate tasking.

In other instances, Turla deployed Neuron to victims in which they already had access to via their Snake toolkit, all with observed connections from Turla-associated infrastructure.

## Scanning for Backdoors

Turla also made use of existing Snake victim networks to scan for the ASPX shell described in the initial advisory - attempting to identify the presence of, and access, the ASPX webshell on IP addresses in at least 35 countries, including Saudi Arabia, Kuwait, Qatar and UAE.

Commands were passed to the ASPX shell in encrypted HTTP Cookie values, requiring knowledge of the cryptographic keys to produce valid tasking and successfully interact with it.

From one Snake victim, a log file was recovered which recorded the output of Turla's scanning for these ASPX shells with the strings "!!!MAY BE SHELL!!! (check version)" and "!!!MAY BE SHELL!!! (100%)"; over 3500 unique IP addresses were scanned.

Once identified, Turla appeared to use these ASPX shells to gain an initial foothold into victims of interest, and then deploy further tools.

## Turla Compromise of Iranian C2 Infrastructure

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.

Reporting from Symantec®[1][2] details a specific victim in the Middle East where Turla was observed delivering their own malware via a Poison Frog panel, which Symantec and others in the Cybersecurity community attribute to APT34 (also known as OilRig/Crambus).

## Turla Compromise of Iranian Operational Infrastructure

The Turla group deployed their own implants against the operational infrastructure used by an Iranian APT actor and used this to further their own accesses into the Iranian APT's global infrastructure.

Exfiltration of data from Iranian APT infrastructure to Turla infrastructure took place.

Data exfiltrated from the Iranian infrastructure by Turla included directory listings and files, along with keylogger output containing operational activity from the Iranian actors, including connections to Iranian C2 domains. This access gave Turla unprecedented insight into the tactics, techniques and procedures (TTPs) of the Iranian APT, including lists of active victims and credentials for accessing their infrastructure, along with the code needed to build versions of tools such as

[1] *Waterbug: Espionage Group Rolls Out Brand New Toolset in Attacks Against Governments (*Blogpost), 20 June 2019

[2] *Symantec is a registered trademark of Symantec.*

Neuron for use entirely independently of Iranian C2 infrastructure.

## Indicators of Compromise (IOC)

As this advisory provides additional context around historical activity from the Turla group, these IOCs are provided for completeness. They may be useful to any investigator with historic data from a previous Turla (or Iranian APT) investigation.

### Indicators for Forensics Analysis

The following indicators can be used to search for the presence of Turla activity described in this document within forensic analysis tools.

!!!MAY BE SHELL!!! (check version)

!!!MAY BE SHELL!!! (100%)

## Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

## Notice

The information contained in this document was developed in the course of NSA's cybersecurity missions including its responsibilities to identify and disseminate threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-enabled products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders. It has been produced in collaboration and with the support of the United Kingdom's National Cyber Security Centre.

## Contact

For general cybersecurity inquiries and reporting, contact the NSA Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov, or the NCSC via their website.

For media inquiries, contact Press Desk: 443-634-0721   Email: MediaRelations@nsa.gov