# Advisory: Turla group exploits Iranian APT to expand coverage of victims

**A joint report from the NCSC and NSA highlighting Turla activity**

> This report draws on reported information and NCSC investigations into Turla activity in the UK alongside information shared by partners and industry sources. It has been produced in collaboration and with the support of the United States' National Security Agency (NSA).

## Introduction

The Turla group, also known as Waterbug or VENOMOUS BEAR, is suspected to be Russia-based. Turla uses a range of tools and techniques to target government, military, technology, energy and commercial organisations for the purposes of intelligence collection.

Previous advisories from the 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, the 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 behaviour of Turla in actively scanning for Iranian backdoors, indicates that whilst Neuron and Nautilus tools were Iranian in origin, Turla were using these tools and accesses independently to further their own intelligence requirements. The behaviour of Turla in scanning for backdoor shells indicates that whilst 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 the NCSC, the NSA and the wider cyber security community determined that 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 organisations 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 open source cyber security 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 key material, and likely had access to controller software in order to produce legitimate tasking.

In other instances, Turla deployed Neuron to victims in which they already had access to via their Snake toolkit, with all 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.

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 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 cyber security 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 exfiltration 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 Neuron for use entirely independently of Iranian C2 infrastructure.

---

## Indicators of Compromise (IOCs)

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. The most effective way to mitigate the risk of actors exploiting these vulnerabilities is to ensure that the affected products are patched with the latest security updates.

---

## Indicators for Forensic 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%)

---

## Reporting to the NCSC

Any current activity related to these threats should be reported via the NCSC website here where the NCSC can offer help and guidance.

The NCSC is also interested in receiving indicators of compromise and threat intelligence, even if the activity has already been remediated.

**PUBLISHED**

21 October 2019

**WRITTEN FOR**

Large organisations

Cyber security professionals

Public sector

**NEWS TYPE**

Alert