Turla Compromises, Infiltrates Iranian APT Infrastructure

By Tara Seals

Published: 2019-10-21 · Archived: 2026-04-05 19:23:20 UTC

The Russian-speaking APT stole the Neuron and Nautilus implants and accessed the Iranian APT's C2 infrastructure.

The Turla APT group has been spotted co-opting two cyberweapons from an Iranian APT (APT 34, according to one set of researchers), known as the Nautilus and Neuron implants, and deploying them against targets in the Middle East. The group also infiltrated the global operational infrastructure used by the Iranian APT.

Turla, also known as Venomous Bear, Waterbug and Uroboros, is a Russian-speaking threat actor known since 2014, but with roots that go back to 2004 and earlier, according to previous research from Kaspersky. "It is a complex cyberattack platform focused predominantly on diplomatic and government-related targets, particularly in the Middle East, Central and Far East Asia, Europe, North and South America, and former Soviet bloc nations," according to the firm.

According to the U.S. National Security Agency (NSA) and the UK's National Cyber Security Centre (NCSC), Turla had been seen using Neuron and Nautilus alongside its own Snake rootkit in 2017 and 2018. However, new intelligence shows that this was merely a testing stage. It turns out that the tools are Iranian in origin and "borrowed" from another APT – and Turla was merely trying them out on victims they had already infiltrated with Snake.

Most recently, the agencies observed Turla scanning for victims that are already compromised with the two implants, by looking for the presence of a specific ASPX webshell on IP addresses in at least 35 countries (more than 3,500 different IP addresses were scanned). If found, the group then attempted to use the backdoors to gain a foothold into those organizations and deploy more tools.

"Those behind Neuron or Nautilus were almost certainly not aware of, or complicit with, Turla's use of their implants," according to a notice on Monday from the NCSC. "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 whilst they had a significant amount of insight into the Iranian tools, they did not have full knowledge of where they were deployed."

The analysis also shows that Neuron and Nautilus tools are now present on a range of victims, with a large cluster in the Middle East. Some of the infections are the work of the Iranian APT (identified because the implants connect via Virtual Private Server IP addresses known to be associated with the group); and some appear to be Turla's efforts, (identified by their being administered from known Turla infrastructure).

"Victims in this region included military establishments, government departments, scientific organizations and universities," according to the NCSC.

Stealing Tools

The NSA and NCSC said that in order to make use of the existing Nautilus and Neuron infections that it scanned for, Turla's commands were passed to the ASPX shell in encrypted HTTP Cookie values. This means that Turla must have had access to the Iranian APT's relevant cryptographic keys, and "likely had access to controller software in order to produce legitimate tasking."

As for how Turla got ahold of the keys, the agencies also discovered that the APT directly accessed and used the command-and-control (C2) infrastructure the Iranian APT (known as "Poison Frog" C2 panels). A separate analysis by Symantec on one of these efforts determined the Iranian APT target was APT34 (also known as OilRig/Crambus/Helix Kitten).

From there, Turla exfiltrated a range of data, including the Iranian APT's directory listings and files, along with keylogger output containing operational activity from the Iranian actors.

"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," according to the NCSC.

"NCSC released an assessment in January 2018 pertaining to the Nautilus implant, tying it to Venomous Bear," said Adam Meyers, vice president of intelligence at CrowdStrike, via email. "They have issued a new assessment that the implant is actually from Helix Kitten, who's operation was penetrated by Venomous Bear. This is generally significant because we have one nation-state threat actor hijacking a second nation-state threat actors infrastructure and tools to target a third nation-state. This is like the cuckoo egg — where the cuckoo can get another species to hatch its egg."

Paul Chichester, the NCSC's director of operations, said that the agencies have a high degree of confidence that Turla is the actor behind the campaign.

"Identifying those responsible for attacks can be very difficult, but the weight of evidence points towards the Turla group being behind this campaign," he said in a media statement. "We want to send a clear message that even when cyber-actors seek to mask their identity, our capabilities will ultimately identify them. Turla acquired access to Iranian tools and the ability to identify and exploit them to further their own aims."
