Dozens of countries have become embroiled in a state-backed spat between Russian and Iranian hacking groups, security agencies have warned.

On Monday, the UK's National Cyber Security Centre (NCSC), together with the US National Security Agency (NSA), published [an advisory](https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims) warning that military establishments, government departments, scientific organizations, and universities are among victims of an ongoing hacking campaign undertaken by Turla.

**Security**

* [Microsoft Double Key Encryption enters public preview](https://www.zdnet.com/article/microsoft-double-key-encryption-enters-public-preview/)
* [University of York discloses data breach, staff and student records stolen](https://www.zdnet.com/article/university-of-york-discloses-data-breach-staff-and-student-records-stolen/)
* [Best security keys in 2020: Hardware-based two-factor authentication for online protection](https://www.zdnet.com/article/best-security-keys/)
* [Best password managers for business in 2020: 1Password, Keeper, LastPass, and more](https://www.zdnet.com/article/best-password-managers/)
* [Cyber security 101: Protect your privacy from hackers, spies, and the government](https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)
* [Phone privacy settings: Securing your iPhone and Android phone (ZDNet YouTube)](https://www.youtube.com/watch?v=92rC4x0D1B0)
* [Top 6 cheap home security devices in 2020 (CNET)](https://www.cnet.com/how-to/top-cheap-home-security-devices-in-2020-amazon-echo-smart-cam-wyze/?ftag=CMG-01-10aaa1b)
* [What are IT pros concerned about in the new normal? (TechRepublic)](https://www.techrepublic.com/article/what-are-it-pros-concerned-about-in-the-new-normal-security-and-flexibility/?ftag=CMG-01-10aaa1b)

Turla, also known as Snake, Uroburos, Waterbug or Venomous Bear, is believed to originate from Russia.

As an advanced persistent threat (APT), members of Turla have state backing, granting them [more resources](https://www.zdnet.com/article/turla-backdoors-compromise-two-european-government-offices-defense-contractor/) than your average cyberattackers -- and making them more dangerous as a result.

The joint report says that at least 35 countries have become targets, of which the majority are in the Middle East, and at least 20 have been successfully compromised over the past 18 months.

Believed to be sponsored by the Russian FSB security service, Turla has been active since at least 2008 and while constantly evolving its own toolkit, has also been turning its attention towards the infrastructure and resources of other APTs.

As [ZDNet previously reported](https://www.zdnet.com/article/russian-apt-hacked-iranian-apts-infrastructure-back-in-2017/) in June, the Russian threat actors have hijacked the systems of a rival APT. Hailing from Iran, APT34 -- also known as Oilrig or Crambus -- has been compromised and its "Poison Frog" command-and-control (C2) servers have been hijacked by Turla to drop its own brand of malware on PCs already infected by Oilrig.

Symantec researchers came to this conclusion after finding evidence of a Turla task scheduler on an Oilrig-compromised system. A Middle Eastern government entity was the victim of this specific attack.

**See also:**[Russian APT hacked Iranian APT's infrastructure back in 2017](https://www.zdnet.com/article/russian-apt-hacked-iranian-apts-infrastructure-back-in-2017/)

There is currently no evidence to suggest Oilrig has fought back against the exploitation of its systems by another attack group, a scenario that highlights what is becoming an increasingly inter-competitive arena -- and what Paul Chichester, NCSC director of operations [believes is now](https://www.bbc.co.uk/news/technology-50103378) a "very crowded space."

Turla's Snake toolkit has been used alongside Neuron and Nautilus malware implants, both of which have been connected to Iran. The agencies believe Turla first acquired access to these tools before testing them on victims already compromised via Snake.

In some cases, Oilrig-linked IP addresses would deploy these implants and Turla-based infrastructure would access the same payloads later on.

"Those behind Neuron or Nautilus were almost certainly not aware of, or complicit with, Turla's use of their implants," the agencies say. "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."

**TechRepublic:**[What is a zero-day vulnerability?](https://www.techrepublic.com/article/what-is-a-zero-day-vulnerability/?ftag=CMG-01-10aaa1b)

The Russian APT's main focus is often [data exfiltration](https://www.kaspersky.co.uk/resource-center/threats/epic-turla-snake-malware-attacks), and when the group focused its efforts on compromising Oilrig, keyloggers were also deployed to monitor the other APT's activities, techniques, and tactics -- alongside active victims and the credentials needed to access their systems. According to the agencies, the code required to lift the Iranian tools from the C2 for independent use.

Turla's [evolving toolset](https://www.zdnet.com/article/wav-audio-files-are-now-being-used-to-hide-malicious-code/) is being watched by cybersecurity firms with interest across the globe. LightNeuron, for example, is a new and [highly-complex backdoor](https://www.zdnet.com/article/russian-cyberspies-are-using-one-hell-of-a-clever-microsoft-exchange-backdoor/) spotted by ESET that works as a mail transfer agent on Microsoft Exchange email servers to intercept and tamper with messages.

**CNET:**[The best antivirus protection of 2019 for Windows 10](https://www.cnet.com/news/the-best-antivirus-protection-in-2019-for-windows-10/?ftag=CMG-01-10aaa1b)

The [use of Powershell](https://www.zdnet.com/article/turla-turns-powershell-into-a-weapon-in-attacks-against-eu-diplomats/) in attacks to load executables in memory has also been a new development, and earlier this month, Kaspersky said Turla was likely to blame for a campaign in which the internal mechanisms of browsers including Firefox and Chrome were being tampered with to [fingerprint traffic streams](https://www.zdnet.com/article/russian-hacker-group-patches-chrome-and-firefox-to-fingerprint-tls-traffic/).