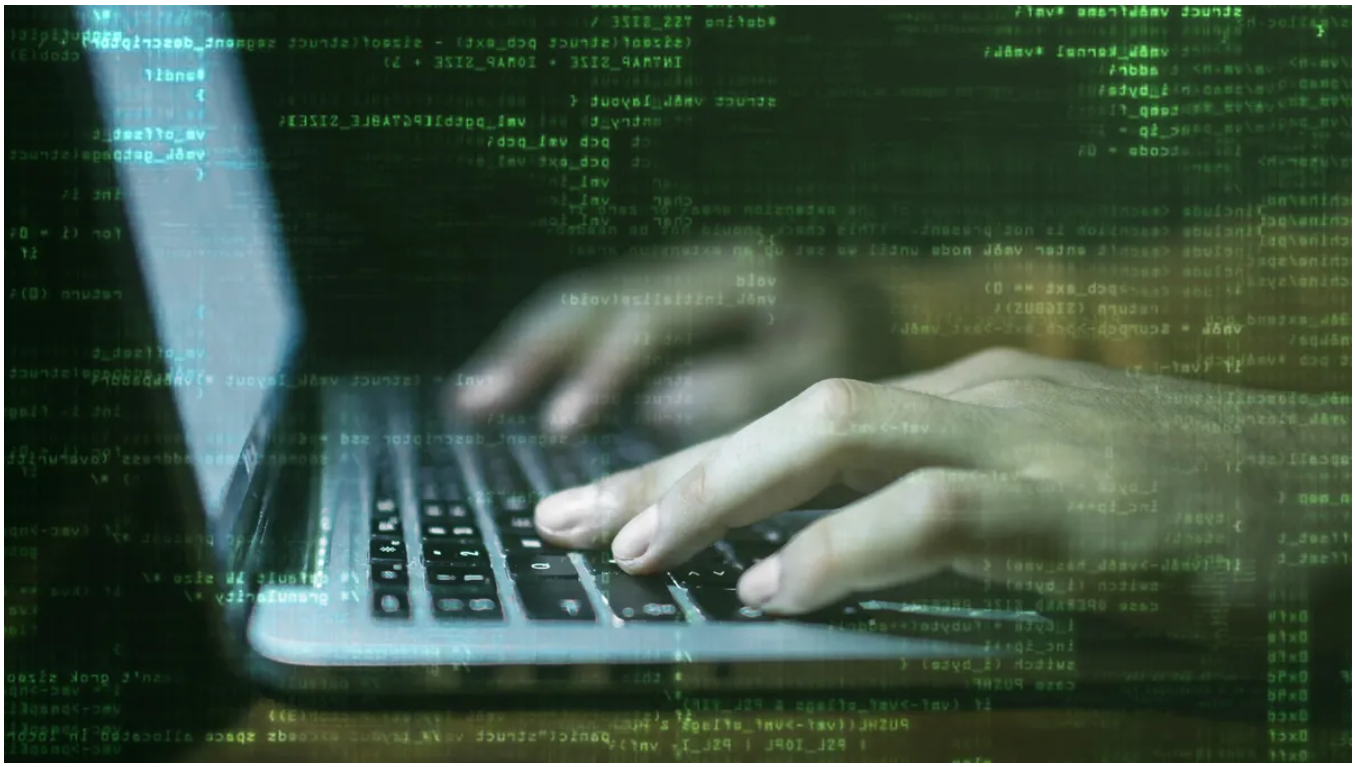
This hacking gang just updated the malware it uses against UK targets

zdnet.com/article/this-hacking-gang-just-updated-the-malware-it-uses-against-uk-targets/



Home Innovation Security

The National Cyber Security Centre issues a warning over updated Neuron malware attacks by the Turla hacking group.

Written by Danny Palmer, Senior Reporter on Jan. 22, 2018

-
-
-
-
-

Video: Gazer malware enables hacking group to spy on Europe's embassies

Security

- My Instagram account was hacked, and two-factor authentication didn't help
- The 5 best browsers for privacy: Secure web browsing
- Stop doing these 10 things that let hackers in, says FBI and NSA
- What is a cybersecurity degree?
- How to delete yourself from search results and hide your identity online

A notorious hacking group is targeting the UK with an updated version of malware designed to embed itself into compromised networks and stealthily conduct espionage.

Both the Neuron and Nautilus malware variants have previously been attributed to the Turla advanced persistent threat group, which regularly carries out cyber-espionage against a range of targets, including government, military, technology, energy, and other commercial organisations.

Within the last year, the group appears to have been particularly focusing on diplomatic targets, including consulates and embassies.

Primarily targeting Windows mail servers and web servers, the Turla group deploys specially-crafted phishing emails to compromise targets in attacks that deploy Neuron and Nautilus in conjunction with the Snake rootkit.

By using a combination of these tools, Turla is able to gain persistent network access on compromised systems, providing covert access to sensitive data or the ability to use the system as a gateway for carrying out further attacks.

The advanced nature of the group means Turla is continually updating and developing its attacks and now the UK's National Cyber Security Centre (NCSC) -- the cybersecurity arm of GCHQ -- has issued a warning that Turla is deploying a new version of Neuron which has been modified to evade discovery.

Alterations to the dropper and loading mechanisms of Neuron are designed to avoid the malware being detected, allowing its malicious activities to continue without being interrupted.

Hackers are using an updated version of Neuron malware to conduct espionage against UK targets, warns the NCSC.

Image: iStock

One of the ways this is achieved is using an in-memory payload, which is encrypted within the loader to ensure it never touches the disk in plaintext. This modification allows Neuron to evade detection during disk scans performed by antivirus software, although the NCSC say it's "likely" that AV suites which scan memory will still uncover the payload.

See also: The secret to being a great spy agency in the 21st century: Incubating startups

The authors of Neuron have also altered the encryption of the new version, now configuring multiple hardcoded keys rather than just using one. Like many of the other changes, it's most likely these have been implemented to make detection and decryption by network defenders more difficult.

The Turla group moves quickly: the compile times contained within the code show that the new version of the malware was compiled just five days after previous warnings about Neuron were made public in November.

Advice by the NCSC for organisations that have previously been targeted by Turla is to "be diligent in checking for the presence of these additional tools".

Download now: Intrusion detection policy (free PDF)

The National Cyber Security Centre doesn't point to the work of Turla being associated with any particular threat actor -- instead referring to it as "a prevalent cyber threat group targeting the UK".

However, cybersecurity researchers have previously argued that Turla is a state-sponsored operation which works to further the aims of the Russian government.

Recent and related coverage

> **Tracking Turla: Hackers abuse satellite signals high in the sky**
>
> A sophisticated hacking group is using satellites in a novel manner to disguise their tracks.
>
> **Stealthy malware targets embassies in snooping campaign**
>
> The Turla hacking group is using the new Gazer backdoor to conduct espionage, according to researchers at ESET.
>
> **Russian hacking campaign targets G20 attendees with booby-trapped invites**
>
> Turla APT group is sending out invites to a real G20 event in Hamburg, targeting politicians, policy makers and other experts for the purposes of espionage.

READ MORE ON CYBERCRIME