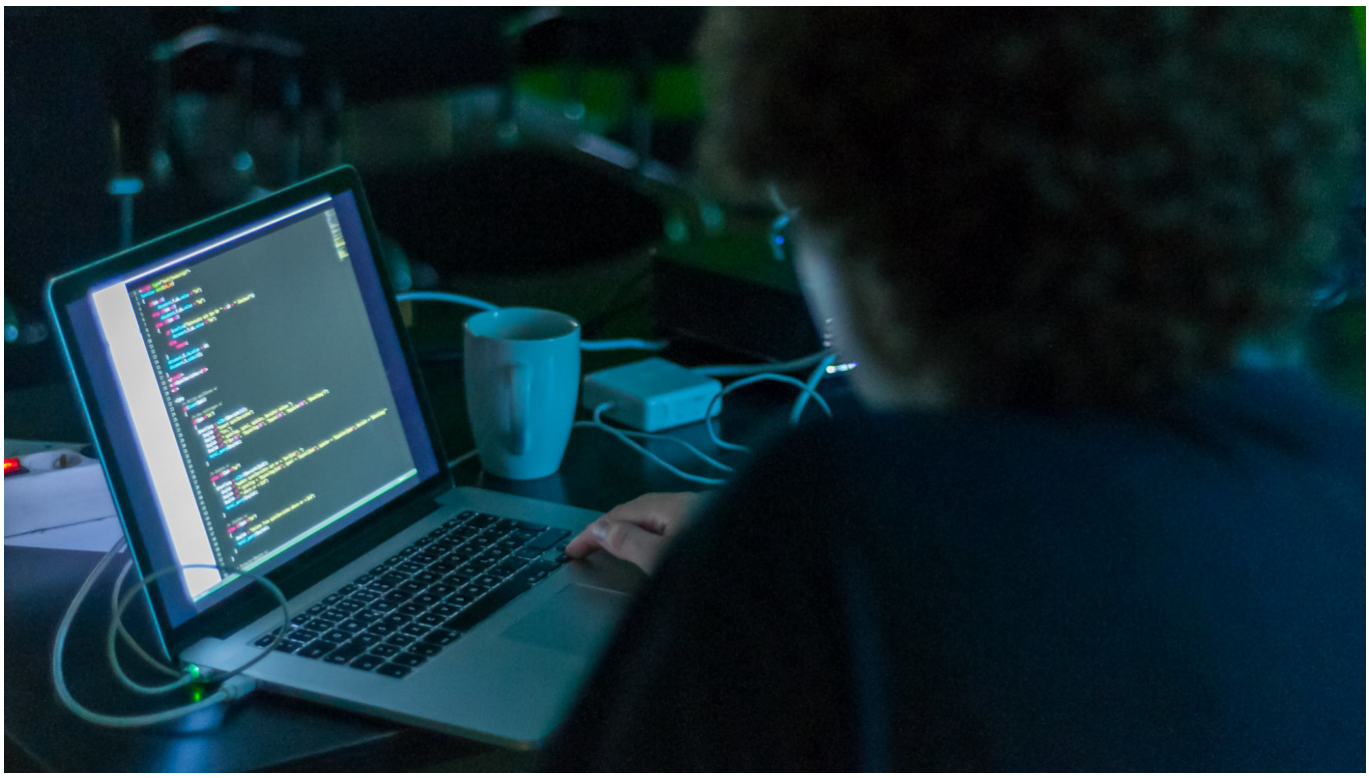
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

# Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say

By Reuters

October 21, 2019



**Marco Verch / Flickr (CC BY 2.0)**

Russian hackers piggy-backed on an Iranian cyber-espionage operation to attack government and industry organizations in dozens of countries while masquerading as attackers from the Islamic Republic, British and U.S. officials said on Monday.

The Russian group, known as "Turla" and accused by Estonian and Czech authorities of operating on behalf of Russia's FSB security service, has used Iranian tools and computer infrastructure to successfully hack in to organizations in at least 20 different countries over the last 18 months, British security officials said.

The hacking campaign, the extent of which has not been previously revealed, was most active in the Middle East but also targeted organizations in Britain, they said.

Paul Chichester, a senior official at Britain's GCHQ intelligence agency, said the operation shows state-backed hackers are working in a "very crowded space" and developing new attacks and methods to better cover their tracks.

**Related article**: Russian Hackers Stole U.S. Evidence to Discredit Mueller Probe — Court Filing

In a statement accompanying a joint advisory with the U.S. National Security Agency (NSA), GCHQ's National Cyber Security Center said it wanted to raise industry awareness about the activity and make attacks more difficult for its adversaries.

"We want to send a clear message that even when cyber actors seek to mask their identity, our capabilities will ultimately identify them," said Chichester, who serves as the NCSC's director of operations.

Officials in Russia and Iran did not immediately respond to requests for comment sent on Sunday. Moscow and Tehran have both repeatedly denied Western allegations over hacking.

### Global hacking campaigns

Western officials rank Russia and Iran as two of the most dangerous threats in cyberspace, alongside China and North Korea, with both governments accused of conducting hacking operations against countries around the world.

Intelligence officials said there was no evidence of collusion between Turla and its Iranian victim, a hacking group known as "APT34" which cybersecurity researchers at firms including FireEye say works for the Iranian government.

Rather, the Russian hackers infiltrated the Iranian group's infrastructure in order to "masquerade as an adversary which victims would expect to target them," said GCHQ's Chichester.

Turla's actions show the dangers of wrongly attributing cyberattacks, British officials said, but added that they were not aware of any public incidents that had been incorrectly blamed on Iran as a result of the Russian operation.

**Related article**: Anonymous Hackers Hijack Russian Government Website, Issuing 'Last Warning'

The United States and its Western allies have also used foreign cyberattacks to facilitate their own spying operations, a practice referred to as "fourth party collection," according to documents released by former U.S. intelligence contractor Edward Snowden and reporting by German magazine Der Spiegel.

GCHQ declined to comment on Western operations.

By gaining access to the Iranian infrastructure, Turla was able to use APT34's "command and control" systems to deploy its own malicious code, GCHQ and the NSA said in a public advisory.

The Russian group was also able to access the networks of existing APT34 victims and even access the code needed to build its own "Iranian" hacking tools.

Original url:
https://www.themoscowtimes.com/2019/10/21/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-a67815