The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

2nd Russian Hacker Group Accused of Targeting NATO

By Matthew Bodner

October 28, 2014

A U.S. security firm has claimed that a Russia-based hacker group is spying on NATO.

A U.S. security firm has claimed that a sophisticated, Russia-based hacker group is spying on NATO and former Soviet member states, most likely on the orders of the Russian government.

In a report issued Tuesday, security firm FireEye said the group, which the firm dubbed APT28, has since 2007 conducted "long-standing, focused operations that indicate a government sponsor — specifically, a government based in Moscow."

"APT28 targets insider information related to governments, militaries and security organizations that would likely benefit the Russian government," the report says. These targets include the Georgian Defense and Interior ministries, post-Soviet governments in Eastern Europe that are now members of NATO, and the NATO alliance itself.

Russian cyber espionage efforts have long been considered unrivaled in skill and scope, but the difficulty of identifying attacks and tracing them to an identifiable source has prevented cyber security investigators from pinning any activity directly on a single Russian entity.

But evidence of a wide-ranging cyber espionage campaign is mounting. Earlier in October, another U.S. cyber security firm said that a group of Russian hackers with suspected government backing had used a previously unknown backdoor in Microsoft Windows operating systems to spy on NATO and several Western governments.

APT28 does not appear to be stealing intellectual property or directly profiting from stolen financial information, as is characteristic of China-based actors tracked by FireEye, the report said. Instead, the hackers focus on defense and geopolitical intelligence-gathering.

The sophistication of APT28's malware indicates that the group is state-sponsored, the report said. Samples of the group's coding show that work on the group's cyber weapons corresponds to a normal working week in the St. Petersburg and Moscow time zone almost 90 percent of the time.

FireEye's report also mentions that the language settings on the coding are Russian, rather than English or language-neutral settings.

Contact the author at m.bodner@imedia.ru

Original url:
https://www.themoscowtimes.com/2014/10/28/2nd-russian-hacker-group-accused-of-targeting-nato-a40826