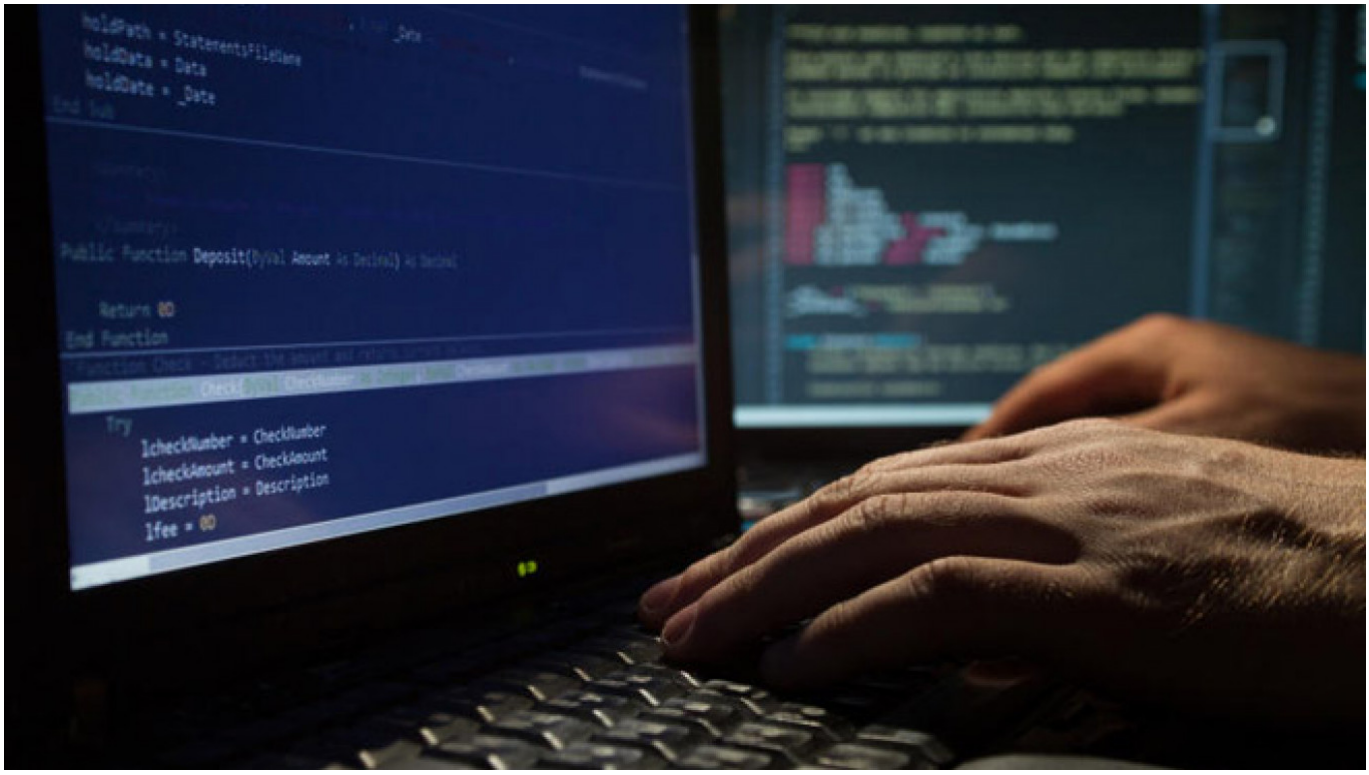
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Spy Malware Deployed Against Russia by Unknown Nation, Report Says

By Allison Quinn

November 24, 2014



The newly discovered Regin malware may serve as a reminder of how cyber warfare can be just as debilitating as physical attacks.

Russian and Saudi Arabian telecommunications and Internet firms are being targeted by highly advanced cyber espionage malware that is likely being controlled by a Western intelligence agency, The Financial Times reported Monday.

Leading computer security company Symantec issued a statement Sunday warning about a new piece of malware known as Regin. The advanced espionage tool "displays a degree of technical competence rarely seen and has been used in spying operations against governments, infrastructure operators, businesses, researchers and private individuals."

How Regin infects computer systems remains unclear, but it has primarily been deployed against telecommunications firms and Internet service providers in Russia and Saudi Arabia, and to a lesser extent in Mexico, Ireland and Iran, The Financial Times reported, citing

Symantec.

"Almost half of all infections targeted private individuals and small businesses. Attacks on telecoms companies appear to be designed to gain access to calls being routed through their infrastructure," Symantec wrote in its statement.

The warnings come amid a flurry of reports of increased cyber espionage as the ongoing crisis in Ukraine continues to pit Russia against many Western countries.

Concerns of cyber espionage prompted NATO to hold the world's biggest-ever cyber war games last week in Estonia, where hundreds of representatives from 28 countries tested their own ability to respond to new cyber threats, The Financial Times reported Thursday.

The newly discovered Regin malware may serve as a reminder of how cyber warfare can be just as debilitating as physical attacks. Regin, believed to have been in use since 2008, has been used for "systematic data collection or intelligence-gathering campaigns" since its creation, Symantec's statement said.

The malware's design "makes it highly suited for persistent, long-term surveillance operations against targets," the report said.

Symantec did not identify any possible culprits, but said the malware's "authors have gone to great lengths to cover its tracks," and the "capabilities and the level of resources behind Regin indicate that it is one of the main cyber espionage tools used by a nation state."

In mid-October, another cyber security company, iSIGHT Partners, released a report claiming that a large-scale cyber espionage campaign was under way against NATO, Ukrainian government agencies, Polish energy firms and American academic institutions, among others.

The so-called Sandworm malware at the center of that campaign was believed to have originated in Russia, the report said.

Meanwhile, just days after The Telegraph reported that British troops were told to be wary of Russian cyber spies using electronic devices in intelligence-gathering during upcoming drills in Poland, a spokesman for Russia's Defense Ministry denied a similar claim made in the Russian media.

Major General Igor Konashenkov refuted earlier media reports that Russian troops had been forbidden from using iPhones for fear that foreign spies could access them to monitor a soldier's location and activities at all times.

"There is no ban on using mobile telephones in Russia's armed forces, and certainly no ban on products from any specific manufacturer," Konashenkov said Monday in comments carried by state news agency RIA Novosti.

Contact the author at a.quinn@imedia.ru

Original url:
https://www.themoscowtimes.com/2014/11/24/spy-malware-deployed-against-russia-by-unknown-nation-report-says-a41660