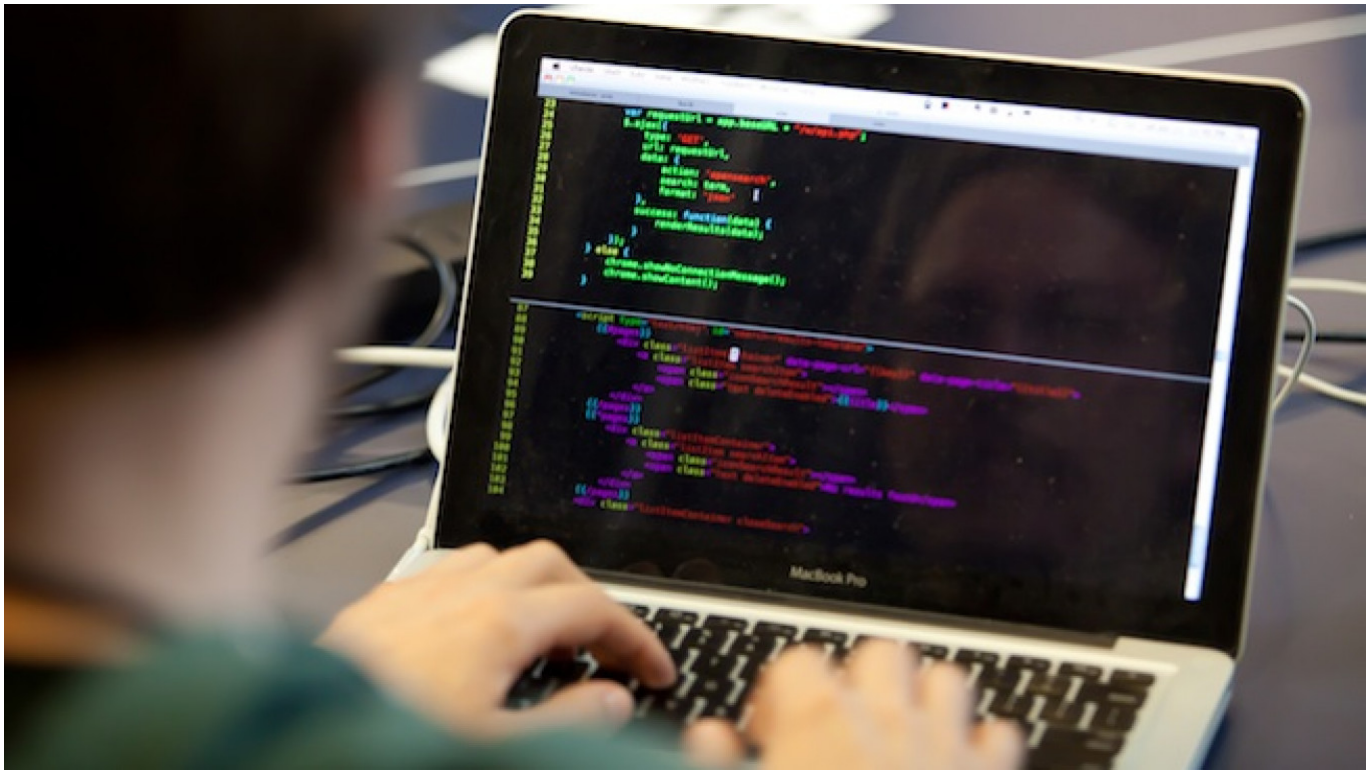
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Intelligence Firm Says Russian Hackers Target NATO, Ukraine, Others

By The Moscow Times

October 14, 2014



The five-year cyber espionage campaign is still going on, according to iSight.

BOSTON — Russian hackers exploited a bug in Microsoft Windows and other software to spy on computers used by NATO, the European Union, Ukraine and companies in the energy and telecommunications sectors, according to cyber intelligence firm iSight Partners.

ISight said it did not know what data had been found by the hackers, though it suspected they were seeking information on the Ukraine crisis, as well as diplomatic, energy and telecom issues, based on the targets and the contents of phishing e-mails used to infect computers with tainted files.

The five-year cyber espionage campaign is still going on, according to iSight, which dubbed the operation "Sandworm Team" because it found references to the "Dune" science fiction series in the software code used by the hackers.

The operation used a variety of ways to attack the targets over the years, iSight said, adding that the hackers began only in August to exploit a vulnerability found in most versions of Windows.

ISight said it told Microsoft Corp about the bug and held off on disclosing the problem so the software maker had time to fix it.

A Microsoft spokesman said the company plans to roll out an automatic update to affected versions of Windows on Tuesday.

There was no immediate comment from the Russian government, NATO, the EU or the Ukraine government.

Researchers with Dallas-based iSight said they believed the hackers are Russian because of language clues in the software code and because of their choice of targets.

"Your targets almost certainly have to do with your interests. We see strong ties to Russian origins here," said John Hulquist, head of iSight's cyber espionage practice. The firm plans to release a 16-page report on Sandworm Team to its clients on Tuesday.

While technical indicators do not indicate whether the hackers have ties to the Russian government, Hulquist said he believed they were supported by a nation state because they were engaging in espionage, not cyber crime.

For example, in December 2013, NATO was targeted with a malicious document on European diplomacy. Several regional governments in the Ukraine and an academic working on Russian issues in the U.S. were sent tainted e-mails that claimed to contain a list of pro-Russian extremist activities, according to iSight.

The firm said its researchers uncovered evidence that some Ukrainian government computer systems were infected, but they were unable to remotely confirm specific victims among those systems that had been targeted.

Still, researchers believe a large percentage of those targeted systems were infected because the malicious software used was very sophisticated, using a previously unknown attack method that enabled it to get past virtually all known security protections, said Drew Robinson, a senior technical analyst with iSight Partners.

ISight said it had alerted some victims of Sandworm Team, but declined to elaborate.

The iSight research is the latest in a series of private sector security reports that link Moscow to some of the most sophisticated cyber espionage uncovered to date.

Russia's Kaspersky Lab in August released details on a campaign that attacked two spy agencies and hundreds of government and military targets across Europe and the Middle East.

Original url:
https://www.themoscowtimes.com/2014/10/14/intelligence-firm-says-russian-hackers-target-nato-ukraine-others-a40358