

US Cyberwar on Russia?

By [Stephen Lendman](#)

Global Research, August 01, 2016

Region: [Russia and FSU](#)

Theme: [Intelligence](#)

On Saturday, [Tass](#) reported what looks like Washington's dirty handiwork, perhaps complicit with its NATO allies, saying:

Russia's "Federal Security Service (FSB) revealed virus software for cyber-spying in computer networks of about 20 organizations located in Russia."

The attack targeted "information resources of the state authorities, scientific and defense companies, enterprises of the defense industry and other objects of the country's critically important infrastructures."

(C)learly, it was a targeted virus spread, planned and made professionally. Specialists say the malicious software, judging by the style of programming, names of files, parameters of their use and by methods, is similar to the software, which was used in much-spoken-about earlier revealed cyber-spying, revealed both in territory of the Russian Federation and around the globe.

The newest sets of the said software are made individually for every 'victim,' on the basis of unique features of attacked machines.

The virus is spread by target attacks on computers by sending an electronic message, containing a malicious attachment.

As the software gets inside the system, it launches necessary modules and becomes able to intercept the network traffic, listen to it, make screenshots, turn on web cameras and PC microphones, mobile devices, to record audio and video files, reports on use of keys and so forth.

Russia's Federal Security Service (FSB), ministries and authorities are taking all necessary steps to minimize damage and restore targeted agencies to proper working order.

An FSB statement said operations infected include "IT assets of government offices, scientific and military organizations, defense companies, and other parts of the nation's crucial infrastructure..."

Cyberattacking Russia followed hacked DNC emails, revealing electoral rigging to anoint Hillary party nominee - Moscow baselessly blamed, no evidence presented suggesting its involvement.

An attack this sophisticated and extensive had to have been planned long before DNC emails were hacked, a convenient pretext to launch it.

Provocative US anti-Russian policies perhaps now include cyberwar. Did Washington declare war on Russia (as well as China) without anyone noticing, paying attention or reporting it?

Will things turn red hot if Hillary succeeds Obama?

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net.

His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

<http://www.claritypress.com/LendmanIII.html>

Visit his blog site at sjlendman.blogspot.com.

Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network.

The original source of this article is Global Research
Copyright © [Stephen Lendman](#), Global Research, 2016

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Stephen Lendman](#)

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

<http://www.claritypress.com/LendmanIII.html> Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca
www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca