

# Digital Warfare: Stuxnet and Flame Viruses could have Three “Sister Viruses”

By [Global Research News](#)

Global Research, June 28, 2013

[Tech Blorge](#) 18 September 2012

Region: [USA](#)

Theme: [Intelligence](#), [US NATO War Agenda](#)

In-depth Report: [IRAN: THE NEXT WAR?](#)

*This article originally published by Global Research in September 2012 sheds light on recent revelations concerning the Stuxnet virus following the alleged leak of classified information about a covert cyberattack on Iran's nuclear facilities.*

“Retired Marine Gen. James “Hoss” Cartwright has been told he is a target of the probe, NBC News and The Washington Post reported Thursday. A “target” is someone a prosecutor or grand jury has substantial evidence linking to a crime and who is likely to be charged.”

Global Research, June 28, 2013

Two major security firms say the people behind the Flame virus may have already developed three similar viruses that haven't yet been discovered in action. The claims will raise more questions about the involvement of the US government in cyber-warfare. Flame shared code with the Stuxnet virus, which appeared to have been developed specifically to physically damage equipment used in Iran's controversial nuclear program. That, and the sheer complexity of the viruses, has often prompted speculation that the US was behind them. Major US newspapers and news agencies have since quoted anonymous sources suggesting the viruses were part of an operation authorized at the highest level.

Now both Russia's Kaspersky and the US-based Symantec have produced reports suggesting similar viruses created by the same hands (though they don't say who the responsible party is.) The two security firms worked separately on their research but appear to have coordinated the releases. The key is “Newsforyou”, a piece of software that appears to be a website content management tool but is actually a way of managing the command and control servers that issue instructions to infected machines. That's particularly important as Flame worked in a sophisticated modular manner, such that each infected machine could have a particular combination of spying tools, making detection and cleaning more difficult. According to Kaspersky and Symantec, Newsforyou dealt with four programs. One is known to be Flame, while the others are simply codenamed IP, SP and SPE. At least one of the programs is already active on infected machines in Iran and Lebanon and is trying to communicate with the command and control servers.

To add to the intrigue, the researchers say they can access some data on one of the command and control servers but cannot read it because its encryption is simply too tough to crack. That's yet another hint to military or government involvement.

The original source of this article is [Tech Blorge](#)  
Copyright © [Global Research News](#), [Tech Blorge](#), 2013

---

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

[Become a Member of Global Research](#)

Articles by: [Global Research](#)  
[News](#)

**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](mailto:publications@globalresearch.ca)  
[www.globalresearch.ca](http://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](mailto:publications@globalresearch.ca)