GlobalResearch
Center for Research on Globalization

CIA Leak: “Russian Election Hackers” May Work at Langley (i.e. CIA Headquarters)

By Moon of Alabama
Global Research, March 08, 2017
Moon of Alabama

Region: Russia and FSU, USA
Theme: Intelligence, Media Disinformation

Attribution of cyber-intrusions and attacks is nearly impossible. A well executed attack can not be traced back to its culprit. If there are some trails that seem attributable one should be very cautions following them. They are likely faked.

Hundreds if not thousands of reports show that this lesson has not been learned. Any attack is attributed to one of a handful of declared “enemies” without any evidence that would prove their actual involvement. Examples:

- Russian Hackers Blackmail US Liberal Groups After Stealing Emails And Documents, Report Says
- US officially accuses Russia of hacking DNC and interfering with election
- Iran hacked an American casino, U.S. says
- Iran suspected for the attack on the Saudi Aramco
- North Korea ‘hacks South’s military cyber command’
- Official: North Korea behind Sony hack

In June 2016 we warned The Next “Russian Government Cyber Attack” May Be A Gulf of Tonkin Fake:

> All one might see in a [cyber-]breach, if anything, is some pattern of action that may seem typical for one adversary. But anyone else can imitate such a pattern as soon as it is known. That is why **there is NEVER a clear attribution** in such cases. Anyone claiming otherwise is lying or has no idea what s/he is speaking of.

There is now public proof that this lecture in basic IT forensic is correct.

Wikileaks acquired and published a large stash of documents from the CIA’s internal hacking organization. Part of the CIA hacking organization is a subgroup named UMBRAGE:

> The CIA’s Remote Devices Branch‘s UMBRAGE group collects and maintains a substantial library of **attack techniques ‘stolen’ from malware produced in other states including the Russian Federation**.
>
> With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also **misdirect attribution by leaving behind the “fingerprints” of the groups that the attack techniques were stolen from.**

> UMBRAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques.

Hacking methods are seldom newly developed. They are taken from public examples and malware, from attacks some other organization once committed, they get bought and sold by commercial entities. Many attacks use a recombined mix of tools from older hacks. Once the NSA's STUXNET attack on Iran became public the tools used in it were copied and modified by other such services as well as by commercial hackers. Any new breach that may look like STUXNET could be done by anyone with the appropriate knowledge. To assert that the NSA must have done the new attack just because the NSA did STUXNET would be stupid.

The CIA, as well as other services, have whole databases of such 'stolen' tools. They may combine them in a way that looks attributable to China, compile the source code at local office time in Beijing or "forget to remove" the name of some famous Chinese emperor in the code. The CIA could use this to fake a "Chinese hacking attack" on South Korea to raise fear of China and to, in the end, sell more U.S. weapons.

Russia did not hack and leak the DNC emails, Iran did not hack American casinos and North Korea did not hack Sony.

As we wrote: "there is NEVER a clear attribution". Don't fall for it when someone tries to sell one.

(PS: There is a lot more in the new Wikileaks CIA stash. It seems indeed bigger than the few items published from the Snowden NSA leak.)

The original source of this article is Moon of Alabama

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Moon of Alabama**

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

For media inquiries: publications@globalresearch.ca