GlobalResearch
Center for Research on Globalization

New Russian Hacks? No, Old Ukrainian Malware Found

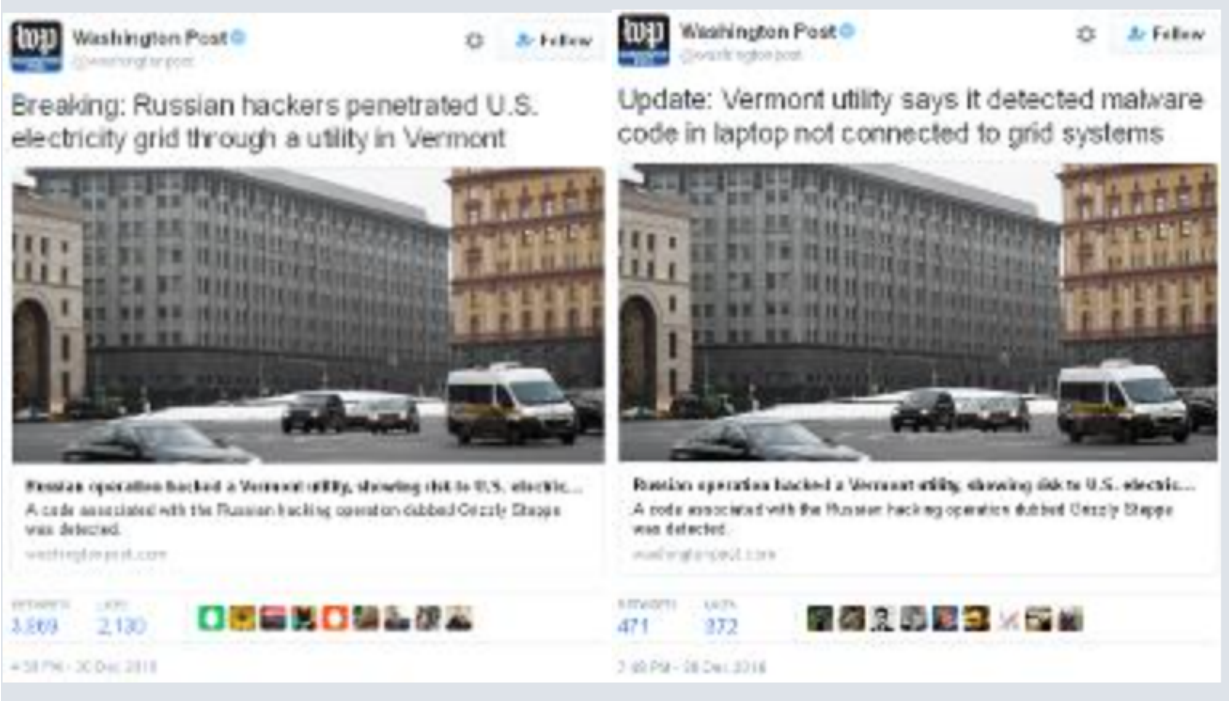
By Moon of Alabama
Global Research, January 01, 2017
Moon of Alabama 31 December 2016

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

All recent claims of "Russian hacking" are either outright false or are based on "evidence" that only shows run-of-the-mill attacks by some anonymous basement hacker.

The year 2016 saw the person elected U.S. president who the Washington Post, hated most. To celebrate the end of this very bad year its writers and editors decided to put more egg on their faces.

It first published the piece promoted on the left and some three hours later the fundamentally "corrected" one on the right.



The claim in the first piece, based on anonymous "officials", was that Russia hacked into the U.S. electricity grid through a utility company in Vermont. But then the utility companies in question, Burlington Electric, issued a statement that a recent scan of its IT systems had found only one laptop with some malware and that the laptop in questions was not connected to its networks at all. There was nothing found on any net-connected system. It had reported the find to the federal U.S. government. (Some very shortsighted "officials" immediately abused the confidential company information to miss-inform the Washington Post.) The utility company found the malware by scanning for a malware signature

published in a lame recent assessment by Homeland Security and the FBI.

Dubious claims of foreign hacking of the electricity grid have already been made in 2009. Its an old trick of the Obama administration to achieve some political aims.

The Washington Post was obviously so eager to publish another of its daily "Russian hacking" fakes that it did not even ask the two Vermont utilities in question before pushing the stenographed piece out of the door.

That may well have been because the lead editorial of that day was warning of Putin hacking the U.S. electricity network and (again) hitting at Trump:

> For any American leader, an attempt to subvert U.S. democracy ought to be unforgivable — even if he is the intended beneficiary. Some years ago, then-Defense Secretary Leon Panetta warned of a "cyber-Pearl Harbor," and the fear at the time was of a cyberattack collapsing electric grids or crashing financial markets. Now we have a real cyber-Pearl Harbor, though not one that was anticipated.

Pearl Harbor was followed by the U.S. entry into a world war. Do the editors want to repeat that when alluding to it?

The editorial also pushed a bunch of wholly invented conspiracy theories:

> Why is Mr. Trump so dismissive of Russia's dangerous behavior? Some say it is his lack of experience in foreign policy, or an oft-stated admiration for strongmen, or naivete about Russian intentions. But darker suspicions persist. Mr. Trump has steadfastly refused to be transparent about his multibillion-dollar business empire. Are there loans or deals with Russian businesses or the state that were concealed during the campaign? Are there hidden communications with Mr. Putin or his representatives? We would be thrilled to see all the doubts dispelled, but Mr. Trump's odd behavior in the face of a clear threat from Russia, matched by Mr. Putin's evident enthusiasm for the president-elect, cannot be easily explained.

During the election campaign WaPo was the news paper with the most anti-Trump screeds on its neoconned editorial page. That actually helped Trump by making him the obvious anti-Neocon candidate. But "Pearl Harbor" comparisons and "darker suspicions" beat even the most stupid earlier pieces on him.

I suspect that the pushing of the Vermont hack was also an attempted hit against Bernie Sanders, the Senator from Vermont who was scammed out of the Democratic candidacy by the Clinton aligned Democratic National Council. He would now either have to jump on the "Russian hacking->bad Putin->bad-Trump" train or could be blamed of pro-Russian, pro-Putin and pro-Trump tendencies. All such tendencies are of course bad in the view of the pseudo-liberal Washington establishment which is busy promoting the New Red Scare.

But back to that malware. DHS and FBI had published a "report" (pdf) which again attempted to blame Russia of hacking the Democratic National Council while again providing zero actual evidence of such a hack (hint: there is none). The 13 pages include 2 with amateur graphics of a trivial hack architecture and 7 with amateur advice on how to protect a network. Of interest in it were samples and checksums of moduls of the hacking software

it attributed to Russia and a list of IP addresses through which it claims the DNC hack was made. Of special interest is also what it does not say.

Several well known IT security experts have said earlier, like me, that such "reports" and claims are bullshit. A few more add to that:

Jonathon Zdziarski:

> Any antivirus company doing any amount of threat intelligence would be able to come up with more solid indicators than FBI released.

John McAfee (now often nutty but right in this):

> If it looks like the Russians did it I can guarantee you it wasn't the Russians.

Matt Tait:

> My money's on this all turns out to be commodity malware and not even APT28/APT29 and everyone jumping on the bandwagon will look v silly

All, and especially Matt Tait, are right.

Wordfence, also a reputed IT security company, took a detailed look at the samples and tables in the new DHS/FBI "report" and concludes:

> The IP addresses that DHS provided may have been used for an attack by a state actor like Russia. But they don't appear to provide any association with Russia. They are probably used by a wide range of other malicious actors, especially the 15% of IP addresses that are Tor exit nodes.The malware sample is old, widely used and appears to be Ukrainian. It has no apparent relationship with Russian intelligence and it would be an indicator of compromise for any website.

There is your "Russian hack" the DHS and FBI claim hit the DNC servers and WaPo falsely claimed hit the U.S. electricity grid. A run-of-the-mill hack through freely available servers with old Ukrainian malware just like the hundred-thousand others that happen each day.

Pic: Device not found in Vermont

(Putin though is likely to accept the "Russian Hack" claim if the U.S. helps Russia to annex the source country of the identified malware. "If you give me Ukraine we will also call it 'a Russian hack'. We will even take responsibility!")

But if you, like me, believe the word of former British ambassador Craig Murray who works with Wikileaks, there was no hack at all. The DNC data came via an insider who had direct access to them. They were handed to Craig for publishing by Wikileaks.

The whole bogus "Russian hacking" and "Putin did it" claims are issued to lock the coming President Trump into an anti-Russian position. Peace with Russia means less plausible "imminent threat" claims and thereby lower budgets and management prestige for the defense and cybersecurity industry and government organizations. That again would mean lower advertisement income for the Washington Post and less money for its staff, editors and owner.

These people would rather have Word War III than to endure that.
