New American

Written by **C. Mitchell Shaw** on January 6, 2017

When Politics Trumps National Security: Was Russia Behind the DNC/Clinton Hacks?

When President Obama used the waning days of his presidential power to expel 35 Russian intelligence operatives as well as sanctioning five Russian entities and four individuals last week, he said his actions were "a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior." His claim that "Russia's actions" were planned and executed to "interfere with the U.S. election process" was based on a Joint Analysis Report (JAR) by DHS and the FBI released the day before Obama's sanctions of Russia. But is that report correct?

There is little doubt that Russian hackers have been involved in both cyber-espionage and cyber-sabotage against the United States in the past and probably in the present. In early November 2014, *The New American* reported on Russian hackers — likely state-sponsored — hacking the systems of the White House itself. That hack — which was discovered by an unnamed "ally" of the United States — resulted in many computer systems in the White House being offline for days while the software used in the attack was removed and passwords were reset.

A week after reporting on that hack, *The New American* reported that Russian hackers — again, likely state-sponsored — had penetrated critical systems in the United States that control vital parts of the nation's infrastructure, including "complex industrial operations such as oil and gas pipelines, power transmission grids, water distribution and filtration systems, wind turbines and even some nuclear plants" and infected those systems with a piece of malware dubbed "BlackEnergy." As we reported then, the malware would allow hackers to remotely shut down or destroy these vital systems, creating chaos and causing untold damage to not only our infrastructure, but also our economy.

What is interesting in comparing those two cases to the claims of the recent JAR that Russia attempted to "interfere with the U.S. election process" by hacking the DNC and Clinton campaign is that in neither of those previous cases were any sanctions issued nor was anyone expelled from the country. To make that comparison stand out in sharper contrast, it should be noted that one of the tools the JAR claims was used in the alleged "election hack" was Advanced Persistent Threat (APT) 28, the very same same tool that was used in the White House hack.

As this writer wrote about the White House hack at the time:

> This is not an isolated incident. Over the past several years, Russia has been responsible for multiple, sustained attacks on computer systems belonging to governments and security firms with government contracts, according to a report by FireEye Inc. From the *Wall Street Journal*, "The

> report is one of four recent assessments by cybersecurity companies, buttressed by reports from Google Inc. and U.S. intelligence agencies, pointing to Russian sponsorship of a skilled hacking campaign dating back to 2007. Targets included NATO, governments of Russia's neighbors, and U.S. defense contractors Science Applications International Corp. and Academi LLC, the U.S. security firm previously known as Blackwater." FireEye has dubbed the cyber-weapon used by the Russians "APT28."

And:

> The types of information Russia is targeting would give it a military advantage in the case of conflict. The FireEye report states, "since at least 2007, APT28 has been targeting insider information related to governments, militaries, and security organisations that would likely benefit the Russian government." It's much like the old strategy of football teams trying to get their hands on a rival's playbook. If Russia knows the strengths and weaknesses of other nations, it would be in a better position to act aggressively.

APT28 is a "Spear Phishing" tool which, as the JAR explains, "is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials." The JAR goes on to say, "APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns" and that the hackers using APT28 (along with another tool known as APT29) "set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets." Spear Phishing is a more focused form of Phishing (an e-mail attack used to fool people into clicking a link they believe to be legitimate, but which leads to a fake address).

The gist of the report is that Russian hackers working under orders from the Kremlin used APT28 and APT29 to direct a Spear Phishing attack on both the DNC and the Clinton campaign for the purpose of leaking the stolen data in an effort to discredit Clinton. The implication, though it is not clearly stated in the report, is that Putin wanted Trump in the White House.

Left out of the JAR (and the reporting of it by the liberal mainstream media) is the simple fact that software is duplicable. Even *if* APT28 was used in a Spear Phishing attack — *which is not certain* — it would not prove that Russia was behind the attack. It would prove only that a tool sometimes used by Russians was used in the attack. Software is often left behind on systems after an attack. That software is then analyzed by computer security experts who are capable of copying it. The likelihood that both APT28 and APT29 are in the hands of nearly every tech-savvy government on the planet (including the United States) is very good. Not to mention the fact that hackers often "borrow" tools from other hackers. The mere presence (or alleged presence) of the tool is not a smoking gun.

Not only that, but both Julian Assange and former British ambassador Craig Murray of WikiLeaks deny that Russia was the source of the leaked DNC and Clinton documents published by the whistleblower website. Casting further doubt on the veracity of the JAR, Mark Maunder, CEO and founder of WordFence, said the PHP code sample listed in the JAR is called "P.A.S. 3.1.0." and is not only outdated, but is readily available to download from the Internet. WordFence designed a WordPress plugin to protect users of the blogging platform.

In a blog post after the release of the report, Maunder wrote, "Our security analysts spend a lot of time analyzing PHP malware, because WordPress is powered by PHP." He added:

> The PHP malware sample they have provided appears to be P.A.S. version 3.1.0 which is commonly available and the website that claims to have authored it says they are Ukrainian. It is also several versions behind the most current version of P.A.S which is 4.1.1b. One might reasonably expect Russian intelligence operatives to develop their own tools or at least use current malicious tools from outside sources.

And Jeffrey Carr, who is the founder and principal investigator of Project Grey Goose, which has investigated other Russian attacks on computer systems, also dismisses the claims that Russia was behind the leaked e-mails and documents that were so damning to the DNC and Clinton campaign. He drew special attention to the fact that documents leaked by the hacker known as Guccifer 2.0 were supposedly stamped with metadata showing they were doctored by someone with the username Felix Dzerzhinsky (the founder of the Soviet Secret Police). He wrote:

> OK. Raise your hand if you think that a GRU or FSB officer would add Iron Felix's name to the metadata of a stolen document before he released it to the world while pretending to be a Romanian hacker. Someone clearly had a wicked sense of humor.

The JAR makes big waves, but proves nothing it claims. One is expected to accept it on good faith; but people who lie and manipulate data for political purposes don't garner very much good faith. As President-elect Trump pointed out in a press conference after the JAR was made public, "I just want them to be sure, because it's a pretty serious charge, and I want them to be sure. And if you look at the weapons of mass destruction, that was a disaster, and they were wrong." It is now known that when the intelligence community stated that Saddam Hussein had weapons of mass destruction, it was a political ploy to involve the U.S. in a war in Iraq, which the American people did not support.

This appears to be more of that.

Remember that when Russia was the prime and obvious suspect in both the White House cyber-espionage attack and the "BlackEnergy" cyber-sabotage attack, nothing was done. And yet now with little more than a veneer-thin film of evidence to point to Russia, President Obama is bringing the full weight of his waning presidential power to bear against Russia. It is apparent that this is purely political. Even the way it has been reported has served those political purposes.

While the intelligence community has only claimed that Russia was behind the leaked e-mails and documents, the reporting of the liberal mainstream media has created an impression that has caused 50 percent of those polled who say they voted for Clinton to believe that "Russia tampered with vote tallies in order to get Donald Trump elected president." Going a step further than even other media outlets, the *Washington Post* got caught up in the Russian feeding frenzy and found itself in the position of having to retract a story about Russia hacking a Vermont utility.

Riding the mendacity of the pseudo-reporting of the left-wing media and the weak assumptions of the JAR, President Obama's issuing of sanctions and expulsion of Russian intelligence operatives appears to be designed to strangle Trump's presidency while it is still in the cradle. By taking such audacious action with less than one month left before he turns the keys of the White House over to Trump, Obama puts Trump in the position to either reverse that action or let it stand. Either way, Trump may appear to "confirm" the accusations of Clinton and others in the DNC that he is Putin's puppet.