GlobalResearch
Center for Research on Globalization

Did the Russians Really Hack the DNC?

By Gregory Elich

Global Research, January 15, 2017
CounterPunch 13 January 2017

Region: USA
Theme: Intelligence

Russia, we are told, breached the servers of the Democratic National Committee (DNC), swiped emails and other documents, and released them to the public, to alter the outcome of the U.S. presidential election.

How substantial is the evidence backing these assertions?

Hired by the Democratic National Committee to investigate unusual network activity, the security firm Crowdstrike discovered two separate intrusions on DNC servers. Crowdstrike named the two intruders Cozy Bear and Fancy Bear, in an allusion to what it felt were Russian sources. According to Crowdstrike, "Their tradecraft is superb, operational security second to none," and "both groups were constantly going back into the environment" to change code and methods and switch command and control channels.

On what basis did Crowdstrike attribute these breaches to Russian intelligence services? The security firm claims that the techniques used were similar to those deployed in past security hacking operations that have been attributed to the same actors, while the profile of previous victims "closely mirrors the strategic interests of the Russian government. Furthermore, it appeared that the intruders were unaware of each other's presence in the DNC system. "While you would virtually never see Western intelligence agencies going after the same target without de-confliction for fear of compromising each other's operations," Crowdstrike reports, "in Russia this is not an uncommon scenario." [1]

Those may be indicators of Russian government culpability. But then again, perhaps not. Regarding the point about separate intruders, each operating independently of the other, that would seem to more likely indicate that the sources have nothing in common.

Each of the two intrusions acted as an advanced persistent threat (APT), which is an attack that resides undetected on a network for a long time. The goal of an APT is to exfiltrate data from the infected system rather than inflict damage. Several names have been given to these two actors, and most commonly Fancy Bear is known as APT28, and Cozy Bear as APT29.

The fact that many of the techniques used in the hack resembled, in varying degrees, past attacks attributed to Russia may not necessarily carry as much significance as we are led to believe. Once malware is deployed, it tends to be picked up by cybercriminals and offered for sale or trade on Deep Web black markets, where anyone can purchase it. Exploit kits are especially popular sellers. Quite often, the code is modified for specific uses. Security specialist Josh Pitts demonstrated how easy that process can be, downloading and modifying nine samples of the OnionDuke malware, which is thought to have first originated with the Russian government. Pitts reports that this exercise demonstrates "how easy it is to repurpose nation-state code/malware." [2]

In another example, when SentinalOne Research discovered the Gyges malware in 2014, it reported that it "exhibits similarities to Russian espionage malware," and is "designed to target government organizations. It comes as no surprise to us that this type of intelligence agency-grade malware would eventually fall into cybercriminals' hands." The security firm explains that Gyges is an "example of how advanced techniques and code developed by governments for espionage are effectively being repurposed, modularized and coupled with other malware to commit cybercrime." [3]

Attribution is hard, cybersecurity specialists often point out. "Once an APT is released into the wild, its spread isn't controlled by the attacker," writes Mark McArdle. "They can't prevent someone from analyzing it and repurposing it for their own needs." Adapting malware "is a well-known reality," he continues. "Finding irrefutable evidence that links an attacker to an attack is virtually unattainable, so everything boils down to assumptions and judgment." [4]

Security Alliance regards security firm FireEye's analysis that tied APT28 to the Russian government as based "largely on circumstantial evidence." FireEye's report "explicitly disregards targets that do not seem to indicate sponsorship by a nation-state," having excluded various targets because they are "not particularly indicative of a specific sponsor's interests." [5] FireEye reported that the APT28 "victim set is narrow," which helped lead it to the conclusion that it is a Russian operation. Cybersecurity consultant Jeffrey Carr reacts with scorn: "The victim set is narrow because the report's authors make it narrow! In fact, it wasn't narrowly targeted at all if you take into account the targets mentioned by other cybersecurity companies, not to mention those that FireEye deliberately excluded for being 'not particularly indicative of a specific sponsor's interests'." [6]

FireEye's report from 2014, on which much of the DNC Russian attribution is based, found that 89 percent of the APT28 software samples it analyzed were compiled during regular working hours in St. Petersburg and Moscow. [7]

But compile times, like language settings, can be easily altered to mislead investigators. Mark McArdle wonders, "If we think about the very high level of design, engineering, and testing that would be required for such a sophisticated attack, is it reasonable to assume that the attacker would leave these kinds of breadcrumbs? It's possible. But it's also possible that these things can be used to misdirect attention to a different party. Potentially another adversary. Is this evidence the result of sloppiness or a careful misdirection?" [8]

"If the guys are really good," says Chris Finan, CEO of Manifold Technology, "they're not leaving much evidence or they're leaving evidence to throw you off the scent entirely." [9] How plausible is it that Russian intelligence services would fail even to attempt such a fundamental step?

James Scott of the Institute for Critical Infrastructure Technology points out that the very vulnerability of the DNC servers constitutes a muddied basis on which determine attribution. "Attribution is less exact in the case of the DNC breach because the mail servers compromised were not well-secured; the organization of a few hundred personnel did not practice proper cyber-hygiene; the DNC has a global reputation and is a valuable target to script kiddies, hacktivists, lone-wolf cyber-threat actors, cyber-criminals, cyber-jihadists, hail-mary threats, and nation-state sponsored advanced persistent threats; and because the malware discovered on DNC systems were well-known, publicly disclosed, and variants could be purchased on Deep Web markets and forums." [10]

Someone, or some group, operating under the pseudonym of Guccifer 2.0, claimed to be a lone actor in hacking the DNC servers. It is unclear what relation – if any – Guccifer 2.0 has to either of the two APT attacks on the DNC. In a PDF file that Guccifer 2.0 sent to Gawker.com, metadata indicated that it was it was last saved by someone having a username in Cyrillic letters. During the conversion of the file from Microsoft Word to PDF, invalid hyperlink error messages were automatically generated in the Russian language. [11]

This would seem to present rather damning evidence. But who is Guccifer 2.0? A Russian government operation? A private group? Or a lone hacktivist? In the poorly secured DNC system, there were almost certainly many infiltrators of various stripes. Nor can it be ruled out that the metadata indicators were intentionally generated in the file to misdirect attribution. The two APT attacks have been noted for their sophistication, and these mistakes – if that is what they are – seem amateurish. To change the language setting on a computer can be done in a matter of seconds, and that would be standard procedure for advanced cyber-warriors. On the other hand, sloppiness on the part of developers is not entirely unknown. However, one would expect a nation-state to enforce strict software and document handling procedures and implement rigorous review processes.

At any rate, the documents posted to the Guccifer 2.0 blog do not necessarily originate from the same source as those published by WikiLeaks. Certainly, none of the documents posted to WikiLeaks possess the same metadata issues. And one hacking operation does not preclude another, let alone an insider leak.

APT28 relied on XTunnel, repurposed from open source code that is available to anyone, to open network ports and siphon data. The interesting thing about the software is its failure to match the level of sophistication claimed for APT28. The strings in the code quite transparently indicate its intent, with no attempt at obfuscation. [12] It seems an odd oversight for a nation-state operation, in which plausible deniability would be essential, to overlook that glaring point during software development.

Command-and-control servers remotely issue malicious commands to infected machines. Oddly, for such a key component of the operation, the command-and-control IP address in both attacks was hard-coded in the malware. This seems like another inexplicable choice, given that the point of an advanced persistent threat is to operate for an extended period without detection. A more suitable approach would be to use a Domain Name System (DNS) address, which is a decentralized computer naming system. That would provide a more covert means of identifying the command-and-control server. [13] Moreover, one would expect that address to be encrypted. Using a DNS address would also allow the command-and-control operation to easily move to another server if its location is detected, without the need to modify and reinstall the code.

One of the IP addresses is claimed to be a "well-known APT 28" command-and-control address, while the second is said to be linked to Russian military intelligence. [14] The first address points to a server located in San Jose, California, and is operated by a server hosting service. [15] The second server is situated in Paris, France, and owned by another server hosting service. [16] Clearly, these are servers that have been compromised by hackers. It is customary for hackers to route their attacks through vulnerable computers.

The IP addresses of compromised computers are widely available on the Deep Web, and typically a hacked server will be used by multiple threat actors. These two particular servers may or may not have been regularly utilized by Russian Intelligence, but they were not uniquely so used. Almost certainly, many other hackers would have used the same machines, and it cannot be said that these IP addresses uniquely identify an infiltrator. Indeed, the second IP address is associated with the common Trojan viruses Agent-APPR and Shunnael. [17]

"Everyone is focused on attribution, but we may be missing the bigger truth," says Joshua Croman, Director of the Cyber Statecraft Initiative at the Atlantic Council. "[T]he level of sophistication required to do this hack was so low that nearly anyone could do it." [18]

In answer to critics, the Department of Homeland Security and the FBI issued a joint analysis report, which presented "technical details regarding the tools and infrastructure used" by Russian intelligence services "to compromise and exploit networks" associated with the U.S. election, U.S. government, political, and private sector entities. The report code-named these activities "Grizzly Steppe." [19]

For a document that purports to offer strong evidence on behalf of U.S. government allegations of Russian culpability, it is striking how weak and sloppy the content is. Included in the report is a list of every threat group ever said to be associated with the Russian government, most of which are unrelated to the DNC hack. It appears that various governmental organizations were asked to send a list of Russian threats, and then an official lacking IT background compiled that information for the report, and the result is a mishmash of threat groups, software, and techniques. "PowerShell backdoor," for instance, is a method used by many hackers, and in no way describes a Russian operation.

Indeed, one must take the list on faith, because nowhere in the document is any evidence provided to back up the claim of a Russian connection. Indeed, as the majority of items on the list are unrelated to the DNC hack, one wonders what the point is. But it bears repeating: even where software can be traced to Russian origination, it does not necessarily indicate exclusive usage. Jeffrey Carr explains: "Once malware is deployed, it is no longer under the control of the hacker who deployed it or the developer who created it. It can be reverse-engineered, copied, modified, shared and redeployed again and again by anyone." Carr quotes security firm ESET in regard to the Sednit group, one of the items on the report's list, and which is another name for APT28: "As security researchers, what we call 'the Sednit group' is merely a set of software and the related infrastructure, which we can hardly correlate with any specific organization." Carr points out that X-Agent software, which is said to have been utilized in the DNC hack, was easily obtained by ESET for analysis. "If ESET could do it, so can others. It is both foolish and baseless to claim, as Crowdstrike does, that X-Agent is used solely by the Russian government when the source code is there for anyone to find and use at will." [20]

The salient impression given by the government's report is how devoid of evidence it is. For that matter, the majority of the content is taken up by what security specialist John Hinderaker describes as "pedestrian advice to IT professionals about computer security." As for the report's indicators of compromise (IoC), Hinderaker characterizes these as "tools that are freely available and IP addresses that are used by hackers around the world." [21]

In conjunction with the report, the FBI and Department of Homeland Security provided a list of IP addresses it identified with Russian intelligence services. [22] Wordfence analyzed the IP addresses as well as a PHP malware script provided by the Department of Homeland Security. In analyzing the source code, Wordfence discovered that the software used was P.A.S., version 3.1.0. It then found that the website that manufactures the malware had a site country code indicating that it is Ukrainian. The current version of the P.A.S. software is 4.1.1, which is much newer than that used in the DNC hack, and the latest version has changed "quite substantially." Wordfence notes that not only is the software "commonly available," but also that it would be reasonable to expect "Russian intelligence operatives to develop their own tools or at least use current malicious tools from outside sources." To put it plainly, Wordfence concludes that the malware sample "has no apparent relationship with Russian intelligence." [23]

Wordfence also analyzed the government's list of 876 IP addresses included as indicators of compromise. The sites are widely dispersed geographically, and of those with a known location, the United States has the largest number. A large number of the IP addresses belong to low-cost server hosting companies. "A common pattern that we see in the industry," Wordfence states, "is that accounts at these hosts are compromised and those hacked sites are used to launch attacks around the web." Fifteen percent of the IP addresses are currently Tor exit nodes. "These exit nodes are used by anyone who wants to be anonymous online, including malicious actors." [24]

If one also takes into account the IP addresses that not only point to current Tor exits, but also those that once belonged to Tor exit nodes, then these comprise 42 percent of the government's list. [25] "The fact that so many of the IPs are Tor addresses reveals the true sloppiness of the report," concludes network security specialist Jerry Gamblin. [26]

Cybersecurity analyst Robert Graham was particularly blistering in his assessment of the government's report, characterizing it as "full of garbage." The report fails to tie the indicators of compromise to the Russian government. "It contains signatures of viruses that are publicly available, used by hackers around the world, not just Russia. It contains a long list of IP addresses from perfectly normal services, like Tor, Google, Dropbox, Yahoo, and so forth. Yes, hackers use Yahoo for phishing and maladvertising. It doesn't mean every access of Yahoo is an 'indicator of compromise'." Graham compared the list of IP addresses against those accessed by his web browser, and found two matches. "No," he continues. "This doesn't mean I've been hacked. It means I just had a normal interaction with Yahoo. It means the Grizzly Steppe IoCs are garbage." Graham goes on to point out that "what really happened" with the supposed Russian hack into the Vermont power grid "is that somebody just checked their Yahoo email, thereby accessing one of the same IP addresses I did. How they get from the facts (one person accessed Yahoo email) to the story (Russians hacked power grid)" is U.S. government "misinformation." [27]

The indicators of compromise, in Graham's assessment, were "published as a political tool, to prove they have evidence pointing to Russia." As for the P.A.S. web shell, it is "used by hundreds if not thousands of hackers, mostly associated with Russia, but also throughout the rest of the world." Relying on the government's sample for attribution is problematic: "Just because you found P.A.S. in two different places doesn't mean it's the same hacker." A web shell "is one of the most common things hackers use once they've broken into a server," Graham observes. [28]

Although cybersecurity analyst Robert M. Lee is inclined to accept the government's position on the DNC hack, he feels the joint analysis report "reads like a poorly done vendor intelligence report stringing together various aspects of attribution without evidence." The report's list "detracts from the confidence because of the interweaving of unrelated data." The information presented is not sourced, he adds. "It's a random collection of information and in that way, is mostly useless." Indeed, the indicators of compromise have "a high rate of false positives for defenders that use them." [29]

Among the government's list of Russian actors are Energetic Bear and Crouching Yeti, two names for the same threat group. In its analysis, Kaspersky Lab found that most of the group's victims "fall into the industrial/machinery building sector," and it is "not currently possible to determine the country of origin." Although listed in the government's report, it is not suggested that the group played a part in the DNC hack. But it does serve as an example of the uncertainty surrounding government claims about Russian hacking operations in general. [30]

CosmicDuke is one of the software packages listed as tied to Russia. SecureList, however, finds that unlike the software's predecessor, CosmicDuke targets those who traffic in "controlled substances, such as steroids and hormones." One possibility is that CosmicDuke is used by law enforcement agencies, while another possibility "is that it's simply available in the underground and purchased by various competitors in the pharmaceutical business to spy on each other." In either case, whether or not the software is utilized by the Russian government, there is a broader base for its use. [31]

The intent of the joint analysis report was to provide evidence of Russian state responsibility for the DNC hack. But nowhere does it do so. Mere assertions are meant to persuade. How much evidence does the government have? The Democratic Party claims that the FBI never requested access to DNC servers. [32] The FBI, for its part, says it made "multiple requests" for access to the DNC servers and was repeatedly turned down. [33] Either way, it is a remarkable admission. In a case like this, the FBI would typically conduct its own investigation. Was the DNC afraid the FBI might come to a different conclusion than the DNC-hired security firm Crowdstrike? The FBI was left to rely on whatever evidence Crowdstrike chose to supply. During its analysis of DNC servers, Crowdstrike reports that it found evidence of APT28 and APT29 intrusions within two hours. Did it stop there, satisfied with what it had found? Or did it continue to explore whether additional intrusions by other actors had taken place?

In an attempt to further inflame the hysteria generated from accusations of Russian hacking, the Office of the Director of National Intelligence published a declassified version of a document briefed to U.S. officials. The information was supplied by the CIA, FBI, and National Security Agency, and was meant to cement the government's case. Not surprisingly, the report received a warm welcome in the mainstream media, but what is notable is that it offers not a single piece of evidence to support its claim of "high confidence" in assessing that Russia hacked the DNC and released documents to WikiLeaks. Instead, the bulk of the report is an unhinged diatribe against Russian-owned RT media. The content is rife with inaccuracies and absurdities. Among the heinous actions RT is accused of are having run "anti-fracking programming, highlighting environmental issues and the impacts on health issues," airing a documentary on Occupy Wall Street, and hosting third-party candidates during the 2012 election.[34]

The report would be laughable, were it not for the fact that it is being played up for propaganda effect, bypassing logic and appealing directly to unexamined emotion. The 2016 election should have been a wake-up call for the Democratic Party. Instead, predictably enough, no self-examination has taken place, as the party doubles down on the neoliberal policies that have impoverished tens of millions, and backing military interventions that have sown so much death and chaos. Instead of thoughtful analysis, the party is lashing out and blaming Russia for its loss to an opponent that even a merely weak candidate would have beaten handily.

Mainstream media start with the premise that the Russian government was responsible, despite a lack of convincing evidence. They then leap to the fallacious conclusion that because Russia hacked the DNC, only it could have leaked the documents.

So, did the Russian government hack the DNC and feed documents to WikiLeaks? There are really two questions here: who hacked the DNC, and who released the DNC documents? These are not necessarily the same. An earlier intrusion into German parliament servers was blamed on the Russians, yet the release of documents to WikiLeaks is thought to have originated from an insider. [35] Had the Russians hacked into the DNC, it may have been to gather intelligence, while another actor released the documents. But it is far from certain that Russian intelligence services had anything to do with the intrusions. Julian Assange says that he did not receive the DNC documents from a nation-state. It has been pointed out that Russia could have used a third party to pass along the material. Fair enough, but former UK diplomat Craig Murray asserts: “I know who the source is… It’s from a Washington insider. It’s not from Russia.” [36]

There are too many inconsistencies and holes in the official story. In all likelihood, there were multiple intrusions into DNC servers, not all of which have been identified. The public ought to be wary of quick claims of attribution. It requires a long and involved process to arrive at a plausible identification, and in many cases the source can never be determined. As Jeffrey Carr explains, “It’s important to know that the process of attributing an attack by a cybersecurity company has nothing to do with the scientific method. Claims of attribution aren’t testable or repeatable because the hypothesis is never proven right or wrong.” [37]

Russia-bashing is in full swing, and there does not appear to be any letup in sight. We are plunging headlong into a new Cold War, riding on a wave of propaganda-induced hysteria. The self-serving claims fueling this campaign need to be challenged every step of the way. Surrendering to evidence-free emotional appeals would only serve those who arrogantly advocate confrontation and geopolitical domination.

Notes.

[1] Dmitri Alperovitch, “Bears in the Midst: Intrusion into the Democratic National Committee,” Crowdstrike blog, June 15, 2016.

[2] Josh Pitts, “Repurposing OnionDuke: A Single Case Study Around Reusing Nation-state Malware,” Black Hat, July 21, 2015.

[3] Udi Shamir, “The Case of Gyges, the Invisible Malware,” SentinelOne, July 2014.

[4] Mark McArdle, “’Whodunnit?’ Why the Attribution of Hacks like the Recent DNC Hack is so Difficult,” Esentire, July 28, 2016.

[5] “The Usual Suspects: Faith-Based Attribution and its Effects on the Security Community,” October 21, 2016.

[6] Jeffrey Carr, “The DNC Breach and the Hijacking of Common Sense,” June 20, 2016.

[7] “APT28: A Window into Russia’s Cyber Espionage Operations?” FireEye, October 27, 2014.

[8] Mark McArdle, “’Whodunnit?’ Why the Attribution of Hacks like the Recent DNC Hack is so Difficult,” Esentire, July 28, 2016.

[9] Patrick Howell O’Neill, “Obama’s Former Cybersecurity Advisor Says Only ‘Idiots’ Want to Hack Russia Back for DNC Breach,” The Daily Dot, July 29, 2016.

[10] Janes Scott, Sr., “It’s the Russians! … or is it? Cold War Rhetoric in the Digital Age,” ICIT, December 13, 2016.

[11] Sam Biddle and Gabrielle Bluestone, “This Looks like the DNC’s Hacked Trump Oppo File,” Gawker, June 15, 2016.

Dan Goodin, “’Guccifer’ Leak of DNC Trump Research Has a Russian’s Fingerprints on It,” Ars Technica, June 16, 2016.

[12] Pat Belcher, “Tunnel of Gov: DNC Hack and the Russian XTunnel,” Invincea, July 28, 2016.

[13] Seth Bromberger, “DNS as a Covert Channel within Protected Networks,” National Electric Sector Cyber Security Organization, January 25, 2011.

[14] Thomas Rid, “All Signs Point to Russia Being Behind the DNC Hack,” Motherboard, July 25, 2016.

[15] https://www.threatminer.org/host.php?q=45.32.129.185

[16] https://www.threatminer.org/host.php?q=176.31.112.10

[17] https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Agent-APPR/detailed-analysis.aspx

https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2015-062518-5557-99

[18] Paul, “Security Pros Pan US Government Report on Russian Hacking,” The Security Ledger, December 30, 2016.

[19] “Grizzly Steppe – Russian Malicious Cyber Activity,” JAR-16-20296, National Cybersecurity & Communications Integration Center, Federal Bureau of Investigation, December 29, 2016.

[20] Jeffrey Carr, “FBI/DHS Joint Analysis Report: A Fatally Flawed Effort,” Jeffrey Carr/Medium, December 30, 2016.

[21] John Hinderaker, “Is “Grizzly Steppe’ Really a Russian Operation?” Powerline, December 31, 2016.

[22] https://www.us-cert.gov/sites/default/files/publications/JAR-16-20296A.csv

[23] Mark Maunder, “US Govt Data Shows Russia Used Outdated Ukrainian PHP Malware,” Wordfence, December 30, 2016.

[24] Mark Maunder, “US Govt Data Shows Russia Used Outdated Ukrainian PHP Malware,”

Wordfence, December 30, 2016.

[25] Micah Lee, “The U.S. Government Thinks Thousands of Russian Hackers May be Reading my Blog. They Aren’t,” The Intercept, January 4, 2017.

[26] Jerry Gamblin, “Grizzly Steppe: Here’s My IP and Hash Analysis,” A New Domain, January 2, 2017.

[27] Robert Graham, “Dear Obama, from Infosec,” Errata Security, January 3, 2017.

[28] Robert Graham, “Some Notes on IoCs,” Errata Security, December 29, 2016.

[29] Robert M. Lee, “Critiques of the DHS/FBI’s Grizzly Steppe Report,” Robert M. Lee blog, December 30, 2016.

[30] “Energetic Bear – Crouching Yeti,” Kaspersky Lab Global Research and Analysis Team, July 31, 2014.

[31] “Miniduke is back: Nemesis Gemina and the Botgen Studio,” Securelist, July 3, 2014.

[32] Ali Watkins, “The FBI Never Asked for Access to Hacked Computer Servers,” Buzzfeed, January 4, 2017.

[33] “James Comey: DNC Denied FBI Direct Access to Servers During Russia Hacking Probe,” Washington Times, January 10, 2017.

[34] “Assessing Russian Activities and Intentions in Recent Activities and Intentions in Recent US Elections,” Office of the Director of National Intelligence, January 6, 2017.

[35] “Quelle für Enthüllungen im Bundestag Vermutet,” Frankfurter Allgemeine Zeitung, December 17, 2016.

[36] RT broadcast, January 7, 2017. https://www.youtube.com/watch?v=w3DvaVrRweY

[37] Jeffrey Carr, “Faith-based Attribution,” Jeffrey Carr/Medium, July 10, 2016.

Gregory Elich is on the Board of Directors of the Jasenovac Research Institute and the Advisory Board of the Korea Policy Institute. He a member of the Solidarity Committee for Democracy and Peace in Korea, a columnist for Voice of the People, and one of the co-authors of Killing Democracy: CIA and Pentagon Operations in the Post-Soviet Period, published in the Russian language. He is also a member of the Task Force to Stop THAAD in Korea and Militarism in Asia and the Pacific. His website is https://gregoryelich.org

The original source of this article is CounterPunch

Articles by: Gregory Elich

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