WHY IS CROWDSTRIKE CONFUSED(LYING) ON KEY DETAILS ABOUT THE DNC HACK?

by Larry C Johnson

Here is the bottom-line—despite being hired in late April (or early May) of 2016 to stop an unauthorized intrusion into the DNC, CrowdStrike, the cyber firm hired by the DNC's law firm to solve the problem, failed abysmally. More than 30,000 emails were taken from the DNC server between 22 and 25 May 2016 and given to Wikileaks. Crowdstrike blamed Russia for the intrusion but claimed that only two files were taken. And CrowdStrike inexplicably waited until 10 June 2016 to reboot the DNC network.

CrowdStrike, a cyber-security company hired by a Perkins Coie lawyer retained by the DNC, provided the narrative to the American public of the alledged hack of the DNC, But the Crowdstrike explanation is inconsistent, contradictory and implausible. Despite glaring oddities in the CrowdStrike account of that event, CrowdStrike subsequently traded on its fame in the investigation of the so-called Russian hack of the DNC and became a publicly traded company. Was CrowdStrike’s fame for “discovering” the alleged Russian hack of the DNC a critical factor in its subsequent launch as a publicly traded company?

The Crowdstrike account of the hack is very flawed. There are 11 contradictions, inconsistencies or oddities in the public narrative

about CrowdStrike's role in uncovering and allegedly mitigating a Russian intrusion (note--the underlying facts for these conclusions are found in Ellen Nakashima's Washington Post story, Vicki Ward's Esquire story, the Mueller Report and the blog of Crowdstrike founder Dmitri Alperovitch):

1. Two different dates—30 April or 6 May—are reported by Nakashima and Ward respectively as the date CrowdStrike was hired to investigate an intrusion into the DNC computer network.
2. There are on the record contradictions about who hired Crowdstrike. Nakashima reports that the DNC called Michael Sussman of the law firm, Perkins Coie, who in turn contacted Crowdtrike's CEO Shawn Henry. Crowdstrike founder Dmitri Alperovitch tells Nakashima a different story, stating our "Incident Response group, was called by the Democratic National Committee (DNC).
3. CrowdStrike claims it discovered within 24 hours the "Russians" were responsible for the "intrusion" into the DNC network.
4. CrowdStrike's installation of Falcon (its proprietary software to stop breaches) on the DNC on the 1st of May or the 6th of May would have alerted to intruders that they had been detected.
5. CrowdStrike officials told the Washington Post's Ellen Nakashima that they were, "not sure how the hackers got in" and didn't "have hard evidence."
6. In a blog posting by CrowdStrike's founder, Dmitri Alperovitch, on the same day that Nakashima's article was published in the Washington Post, wrote that the intrusion into the DNC was done by two separate Russian intelligence

organizations using malware identified as Fancy Bear (APT28) and Cozy Bear (APT29).

7. But, Alperovitch admits **his team found no evidence** the two Russian organizations were coordinating their "attack" or even knew of each other's presence on the DNC network.
8. There is great confusion over what the "hackers" obtained. DNC sources claim the hackers gained access to the entire database of opposition research on GOP presidential candidate Donald Trump. DNC sources and CrowdStrike claimed the intruders, "read all email and chat traffic." Yet, DNC officials insisted, "that no financial, donor or personal information appears to have been accessed or taken." However, CrowdStrike states, "The hackers stole two files."
9. Crowdstrike's Alperovitch, in his blog posting, does not specify whether it was Cozy Bear or Fancy Bear that took the files.
10. Wikileaks published DNC emails in July 2016 that show the last message taken from the DNC was dated 25 May 2016. This was much more than "two files."
11. CrowdStrike, in complete disregard to basic security practice when confronted with an intrusion, waited five weeks to disconnect the DNC computers from the network and sanitize them.

Let us start with the very contradictory public accounts attributed to Crowdstrke's founder, Dmitri Alperovitch. The 14 June 2016 story by Ellen Nakashima of the Washington Post and the October 2016 piece by Vicki Ward in Esquire magazine offer two different dates for the start of the investigation:

<u>When did the DNC learn of the "intrusion"?</u>

Ellen Nakashima claims it was the end of April:

> “DNC leaders were **tipped to the hack in late April**. Chief executive Amy Dacey got a call from her operations chief saying that their information technology team had noticed some unusual network activity. . . . That evening, she spoke with Michael Sussmann, a DNC lawyer who is a partner with Perkins Coie in Washington. Soon after, Sussmann, a former federal prosecutor who handled computer crime cases, called Henry, whom he has known for many years. Within 24 hours, CrowdStrike had installed software on the DNC’s computers so that it could analyze data that could indicate who had gained access, when and how.

Ward’s timeline, citing Alperovitch, reports the alert came later, on 6 May 2016:

> At six o'clock on the morning of May 6, Dmitri Alperovitch woke up in a Los Angeles hotel to an alarming email. . . . late the previous night, his company had been asked by the Democratic National Committee to investigate a possible breach of its network. A CrowdStrike security expert had sent the DNC a proprietary software package, called Falcon, that monitors the networks of its clients in real time. Falcon "lit up," the email said, within ten seconds of being installed at the DNC: Russia was in the network.

This is a significant and troubling discrepancy because it marks the point in time when CrowdStrike installed its Falcon software on the DNC server. It is one thing to confuse the 30th of April with the 1st of May. But Alperovitch gave two different reporters two different dates.

What did the “hackers” take from the DNC?

Ellen Nakashima's reporting is contradictory and wrong. Initially, she is told that the hackers got access to the entire Donald Trump database and that all emails and chats could be read. But then she is assured that only two files were taken. This was based on Crowdstrike's CEO's assurance, which was proven subsequently to be spectacularly wrong when Wikileaks published 35,813 DNC emails. How did Crowdstrike miss that critical detail? Here is Nakashima's reporting:

> Russian government hackers penetrated the computer network of the Democratic National Committee and gained access to the entire database of opposition research on GOP presidential candidate Donald Trump, according to committee officials and security experts who responded to the breach.
>
> The intruders so thoroughly compromised the DNC’s system that they also were able to read all email and chat traffic, said DNC officials and the security experts. . . .
>
> The DNC said that no financial, donor or personal information appears to have been accessed or taken, suggesting that the breach was traditional espionage, not the work of criminal hackers.
>
> One group, which CrowdStrike had dubbed Cozy Bear, had gained access last summer (2015) and was monitoring the DNC’s email and chat communications, Alperovitch said.
>
> The other, which the firm had named Fancy Bear, broke into the network in late April and targeted the opposition

> research files. It was this breach that set off the alarm. **The hackers stole two files,** Henry said. And they had access to the computers of the entire research staff — an average of about several dozen on any given day. . . .
>
> CrowdStrike is continuing the forensic investigation, said Sussmann, the DNC lawyer. “But at this time, it appears that no financial information or sensitive employee, donor or voter information was accessed by the Russian attackers,” he said.

The DNC emails that are posted on the Wikileaks website and the metadata shows that these emails were removed from the DNC server starting the late on the 22nd of May and continuing thru the 23rd of May. The last tranche occurred late in the morning (Washington, DC time) of the 25th of May 2016. Crowdstrike’s CEO, Shawn Henry, insisted on the 14th of June 2016 that “ONLY TWO FILES” had been taken. This is demonstrably not true. Besides the failure of Crowdstrike to detect the removal of more than 35,000 emails, there is another important and unanswered question—why did Crowdstrike wait until the 10th of June 2016 to start disconnecting the DNC server when they allegedly knew on the 6th of May that the Russians had entered the DNC network?

Crowdstrike accused Russia of the DNC breach but lacked concrete proof.

Ellen Nakashima’s report reveals that Crowdstrike relied exclusively on circumstantial evidence for its claim that the Russian Government hacked the DNC server. According to Nakashima:

> CrowdStrike is not sure how the hackers got in. The firm suspects they may have targeted DNC employees with “spearphishing” emails. These are communications that appear legitimate — often made to look like they came from a colleague or someone trusted — but that contain links or attachments that when clicked on deploy malicious software that enables a hacker to gain access to a computer. “**But we don’t have hard evidence,**” Alperovitch said.

There is a word in English for the phrases, "Not sure" and "No hard evidence”--that word is, "assumption." Assuming that the Russians did it is not the same as proving, based on evidence, that the Russians were culpable. But that is exactly what CrowdStrike did.

The so-called "proof" of the Russian intrusions is the presence of Fancy Bear and Cozy Bear?

At first glance, Dmitri Alperovitch’s blog posting describing the Fancy Bear and Cozy Bear “intrusions” appears quite substantive. But cyber security professionals quickly identified a variety of shortcomings with the Alperovitch account. For example, this malware is not unique nor proprietary to Russia. Other countries and hackers have access to APT28 and have used it.

Skip Folden offers one of the best comprehensive analyses of the problems with the Alperovitch explanation:

> **No basis whatsoever**:
>
> APT28, aka Fancy Bear, Sofacy, Strontium, Pawn Storm, Sednit, etc., and APT29, aka Cozy Bear, Cozy Duke, Monkeys, CozyCar,The Dukes, etc., are used as ‘proof’ of Russia

‘hacking’ by Russian Intelligence agencies GRU and FSB respectively.

There is no basis whatsoever to attribute the use of known intrusion elements to Russia, not even if they were once reverse routed to Russia, which claim has never been made by NSA or any other of our IC.

On June 15, 2016 Dmitri Alperovitch himself, in an Atlantic Council article, gave only “medium-level of confidence that Fancy Bear is GRU” and “low-level of confidence that Cozy Bear is FSB.” These assessments, from the main source himself, that either APT is Russian intelligence, averages 37%-38% [(50 + 25) / 2].

Exclusivity:

None of the technical indicators, e.g., intrusion tools (such as X-Agent, X-Tunnel), facilities, tactics, techniques, or procedures, etc., of the 28 and 29 APTs can be uniquely attributed to Russia, even if one or more had ever been trace routed to Russia. Once an element of a set of intrusion tools is used in the public domain it can be reverse-engineered and used by other groups which precludes the assumption of exclusivity in future use. The proof that any of these tools have never been reverse engineered and used by others is left to the student - or prosecutor.

Using targets:

Also, targets have been used as basis for attributing

intrusions to Russia, and that is pure nonsense. Both many state and non-state players have deep interests in the same targets and have the technical expertise to launch intrusions. In Grizzly Steppe, page 2, second paragraph, beginning with, “Both groups have historically targeted …,” is there anything in that paragraph which can be claimed as unique to Russia or which excludes all other major state players in the world or any of the non-state organizations? No.

Key Logger Consideration:

On the subject of naming specific GRU officers initiating specific actions on GRU Russian facilities on certain dates / times, other than via implanted ID chips under the finger tips of these named GRU officers, the logical assumption would be by installed key logger capabilities, physical or malware, on one or more GRU Russian computers.

The GRU is a highly advanced Russian intelligence unit. It would be very surprising were the GRU open to any method used to install key logger capabilities. It would be even more surprising, if not beyond comprehension that the GRU did not scan all systems upon start-up and in real time, including key logger protection and anomalies of performance degradation and data transmissions.

Foreign intelligence source:

Other option would be via a foreign intelligence unit source with local GRU access. Any such would be quite anti-Russian

> and be another nail in the coffin of any chain of evidence / custody validity at Russian site.

Stated simply, Dmitri Alperovitch's conclusion that "the Russians did it" are not supported by the forensic evidence. Instead, he relies on the assumption that the presence of APT28 and APT29 prove Moscow's covert hand. What is even more striking is that the FBI accepted this explanation without demanding forensic evidence.

Former FBI Director James Comey and former NSA Director Mike Rogers testified under oath before Congress that neither agency ever received access to the DNC server. All information the FBI used in its investigation was supplied by CrowdStrike. The Hill reported:

> The FBI requested direct access to the Democratic National Committee's (DNC) hacked computer servers but was denied, Director James Comey told lawmakers on Tuesday.
>
> The bureau made "multiple requests at different levels," according to Comey, but ultimately struck an agreement with the DNC that a "highly respected private company" would get access and share what it found with investigators.

The foregoing facts raise major questions about the validity of the Crowdstrike methodology and conclusions with respect to what happened on the DNC network. This is not a conspiracy theory. It is a set of facts that, as of today, have no satisfactory explanation. The American public deserve answers.

Posted at 06:56 AM in Larry Johnson, Russiagate | Permalink

Reblog (0)

Comments

Feed You can follow this conversation by subscribing to the comment feed for this post.

Deap

Gut says lifting the CROWDSTRIKE rock will finally release the deep state Russia Gate creepy-crawlies. Thanks for keeping the flame burning bright on this topic.

Posted by: Deap | 17 March 2020 at 11:54 AM

Paul Merrell, J.D.

And on the Russia-gate election interference front, the DoJ has just moved to dismiss the criminal charges against the two Russian corporations in the IRA troll farm case. https://www.lawfareblog.com/us-moves-dismiss-case-against-company-linked-ira-troll-farm

If you read the motion, you see that a government decision to classify much of the evidence played a major role in the DoJ decision. Wasn't that convenient?

The Court in that case had already castigated Robert Mueller for making public statements that linked the Russian corporate defendants to the Russian government and expressed an opinion that they were guilty of election interference:

"In short, the Court concludes that the government violated Rule 57.7 by making or authorizing the release of public statements

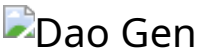
that linked the defendants' alleged activities to the Russian government and provided an opinion about the defendants' guilt and the evidence against them."
https://assets.documentcloud.org/documents/6185644/Sealed-Order.pdf

Now the government will never have to show that evidence (if it actually exists).

Posted by: Paul Merrell, J.D. | 17 March 2020 at 12:14 PM

Going public with what agreement to assuming legal liabilities for the officers of the company in its prior legal status (llc?)? There was certainly the benefit of cashing in on going public.

Posted by: Fred | 17 March 2020 at 04:43 PM



Larry, thank you for this enlightening article. Are you aware that Dmitri Alperovitch resigned from Crowdstrike for "personal reasons" on or around Feb.19?
https://www.crn.com/news/security/crowdstrike-co-founder-dmitri-alperovitch-leaves-to-launch-nonprofit

However, Alperovitch's motive for resigning his good job with Crowdstrike may be more complex, since Crowdstrike now seems to be separating itself from Alperovitch's claims. In response to an inquiry, Gateway Pundit received the following message from Goldin Solutions, Crowdstrike's Broadway PR firm:

"Now after three and a half years of the fraudulent Russia

collusion scam being repeated so often that half of America believes that Russia hacked the DNC and gave their emails to WikiLeaks, Crowdstrike announces that it had nothing to do with assessing that Russians gave the emails to WikiLeaks??!!"

It seems unlikely that the final question marks are in the original message, but I quote it as is. The quote can be found at the end of the following article: "BREAKING EXCLUSIVE: Crowdstrike and Their PR Firm Now Distance Themselves from Russia's Link to Wikileaks — HUGE DEVELOPMENT," by Joe Hoft (March 6, 2020). See: https://www.thegatewaypundit.com/2020/03/breaking-exclusive-crowdstrike-and-their-pr-firm-now-distance-themselves-from-russias-link-to-wikileaks-huge-development/

Posted by: Dao Gen | 17 March 2020 at 06:24 PM

Did I just hear the ghost of Seth Rich say "No justice -no peace"?