ON THE DNC-FBI SPAT OVER THE DNC SERVER

The Ukrainian Ministry of Defense issued a statement in response to the media coverage following the CrowdStrike claim that malware in an artillery app had a role in massive casualties among Ukraine's howitzer units. The Google translation (note, it has not yet been translated into English, which itself may say something about intended audience) of it reads,

> In connection with the emergence in some media reports which stated that the alleged "80% howitzer D-30 Armed Forces of Ukraine removed through scrapping Russian Ukrainian hackers software gunners," Land Forces Command of the Armed Forces of Ukraine informs that the said information is incorrect .
>
> According Command Missile Forces and Artillery Land Forces of Ukraine, artillery weapons lost during the time of ATO times smaller than the above and are not associated with the specified cause. Currently, troops Missile Forces and Artillery Army Forces of Ukraine fully combat-ready, staffed and able to fulfill the missions.
>
> Ministry of Defence of Ukraine asks journalists to publish only verified information received from the competent official sources. Spreading false information leads to increased social tension in society and undermines public confidence in the Armed Forces of Ukraine.

Understand what this is: it is in no way a denial that malware infected the artillery app (though it's also, given that it comes from a country at war with Russia that wants people to stop using this to implicate Russia, not confirmation the malware is Russian). Rather, it is a correction for local journalists to an avowedly pro-Russian source used by Crowdstrike claiming that Ukraine faced 80% losses. And it is a statement that artillery losses from the period in question are due to something else (perhaps the drones that Crowdstrike admitted were involved in the fighting).

Mostly, it's a complaint that Crowdstrike's speculative report made Ukraine look bad. As I've noted, the report was released before Crowdstrike had spoken to the app developer (and as this statement makes clear, to Ukraine's MOD), to explain why its previously "medium" confidence that GRU had hacked the DNC was now "high."

I raise all that as background to the spat Buzzfeed's Ali Watkins reported on yesterday between the DNC and FBI. In the morning, she reported the DNC claim that the FBI had inexplicably never, itself, accessed the DNC servers.

> Six months after the FBI first said it was investigating the hack of the Democratic National Committee's computer network, the bureau has still not requested access to the hacked servers, a DNC spokesman said. No US government entity has run an independent forensic analysis on the system, one US intelligence official told BuzzFeed News.
>
> "The DNC had several meetings with representatives of the FBI's Cyber Division and its Washington (DC) Field Office, the Department of Justice's National Security Division, and U.S. Attorney's Offices, and it responded to a variety of requests for cooperation, but *the FBI never requested access to the DNC's computer servers,"* Eric Walker, the DNC's deputy communications director, told BuzzFeed News in an email.

Over the course of the day, many people explained that that's fairly normal. Crowdstrike would have imaged the server, which would provide FBI what it needed.

But the snipe to Watkins was not the first time DNC has presented their case in a light that makes FBI look as bad as possible — they did that with the NYT, too. And so it was inevitable that the FBI would eventually push back, as they did later in the day with Watkins.

> "The FBI repeatedly stressed to DNC officials the necessity of obtaining direct access to servers and data, only to be rebuffed until well after the initial compromise had been mitigated. This left the FBI no choice but to rely upon a third party for information," a senior law enforcement official told BuzzFeed News in a statement. "These actions caused significant delays and inhibited the FBI from addressing the intrusion earlier."

Which promptly led the same DNC that originally leaked a claim making the FBI look bad to bitch about "haters."

> A DNC source familiar with the investigation tried to downplay that report on Thursday, hours before the FBI statement was issued. The fact that the FBI didn't have direct access to the servers was not "significant," the source said.
>
> "I just don't think that that's really material or an important thing," the source continued. "They had what they needed. There are always haters out here."

In general, I think people are right that you can learn what you need to about a typical breach from an imaged server and the server logs. Indeed, the FBI rebuttal here doesn't even address whether they needed to get the server. Rather, they just said that there was a delay in their access to the data, not that they didn't eventually get the data they needed.

And it's true that there was a delay.

FBI gave the DNC the information they needed to start responding to the FSB hack in September 2015, but the FBI wasn't brought in formally until maybe June 2016. That doesn't necessarily excuse that they didn't escalate sooner (the FBI may have had other reasons not to and I expect we may one day learn that the FBI contacted people beyond just the contractor IT guy), but it does mean that the FBI repeatedly tried to help and the DNC did not accept that help until months later.

Underlying all this is surely the distrust that stems from a political party believing the FBI was conducting a witch hunt of its principal (they'd be proven right a month after the breach became public), though the FBI agents investigating the DNC hack were surely different than the ones investigating Hillary's server. There may have even been other reasons the DNC didn't want the FBI nosing around their servers.

Still, we now know they did not ever access DNC's servers themselves.

And I think *in this case* they should have, for two reasons.

The Hill story covering this bickering includes this quote from a former FBI agent describing one reason why.

> "In nine out of 10 cases, we don't need access, we don't ask for access, we don't get access. That's the normal [procedure]," Leo Taddeo, a former special agent in charge of the cyber division of the FBI's New York office, told The Hill.
>
> "It's extraordinarily rare for the FBI to get access to the victim's

> infrastructure because we could mess it up," he added. "We usually ask for the logs and images, and 99 out of a hundred times, that's sufficient."
>
> Asking for direct access to a server wouldn't be necessary, Taddeo said, "unless there was a reason to think the victim was going to alter the evidence in some way."

You don't need access to the server itself unless you've got reason to believe the victim altered the evidence. From the very first, you had an entity, Guccifer 2.0, challenging the attribution Crowdstrike made on the server. Abundant analysis has proven that Guccifer is a liar, but Chinese and Iranians and Americans lie just as often as Russians do.

Plus, months after the hack, people started claiming that the source for the files that got to Wikileaks came from an insider. Which, if true (I don't think it is, but nevertheless it is a competing theory, one that given the animosity within the Democratic party last year is not impossible), would mean that the *victim might have altered the evidence*.

There's another reason why the FBI should have double checked the forensics, if they hadn't already: because (we learned six months after the fact) Crowdstrike *only ever had medium confidence* that GRU had hacked the DNC based on the forensics they examined.

> While CrowdStrike, which was hired by the DNC to investigate the intrusions and whose findings are described in a new report, had always suspected that one of the two hacker groups that struck the DNC was the GRU, Russia's military intelligence agency, it had only medium confidence.
>
> Now, said CrowdStrike co-founder Dmitri Alperovitch, "we have high confidence" it was a unit of the GRU. CrowdStrike

> had dubbed that unit “Fancy Bear.”

And Crowdstrike only came to have high confidence in that attribution by writing a paper that multiple Ukrainian sources (not exactly Russian shills) have now pushed back on. That is, nothing in the original forensics changed, as far as we know; external evidence, of whatever quality, led to a change in confidence.

Which means the forensics itself is not a slam dunk.

I’m beginning to see a hole in all the other security firms’ validation of Crowdstrike’s original attribution, which I hope to return to (though not before next week). In any case, it’d be useful for FBI to have really vetted this work, given that we’ve turned this into an international incident.

So, yeah, the FBI never obtained the DNC server full of political information the government really shouldn’t possess, particularly not an agency perceived to be really hostile to that political party.

But maybe, in this case, they should have.