WHY DID GUCCIFER 2.0 KEEP HARPING ON VAN?

One problem with the skeptics' claims that Guccifer 2.0 is not Russian, but instead a Democrat or Crowdstrike blaming Russia, is they misread how his original post responded to the WaPo article announcing the hack. The assumption at the time was that Guccifer 2.0 was disinformation to disclaim the attack. But it more immediately discredited the claims the Democrats and Crowdstrike made to WaPo.

There's Shawn Henry's claim the hackers took just two documents.

> 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.

In response Guccifer 2.0 posted eleven documents and taunted Crowdstrike.

> Shame on CrowdStrike: Do you think I've been in the DNC's networks for almost a year and saved only 2 documents? Do you really believe it?
>
> [snip]
>
> I guess CrowdStrike customers should think twice about company's competence.
>
> Fuck the Illuminati and their conspiracies!!!!!!!!! Fuck CrowdStrike!!!!!!!!!

There's the bizarre pitch suggesting that only documents affecting Trump had been stolen, describing it as typical foreign espionage

(which APT 29 might have been doing).

> the entire database of opposition research on GOP presidential candidate Donald Trump
>
> [snip]
>
> 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.
>
> [snip]
>
> "It's the job of every foreign intelligence service to collect intelligence against their adversaries," said Shawn Henry, president of CrowdStrike, the cyber firm called in to handle the DNC breach and a former head of the FBI's cyber division.

Guccifer 2.0 did post a Trump document. But the DNC, Hillary, and Crowdstrike should have known that (even if there had been one stolen) it wasn't the one they had in mind. That was a document stolen from Podesta, not the DNC.

Which would have been a response — one her aides might understand, but the rest of us would not — to this claim by Hillary.

> Clinton called the intrusion "troubling" in an interview with Telemundo. She also said, "So far as we know, my campaign has not been hacked into," and added that cybersecurity is an issue that she "will be absolutely focused on" if she becomes president.

Because it would have been a sign that, indeed, her campaign had been hacked.

Similarly, by posting documents that dated from months earlier, Guccifer 2.0 would have made it clear to DWS that her lie — that the DNC

responded quickly — could be exposed.

> "The security of our system is critical to our operation and to the confidence of the campaigns and state parties we work with," said Rep. Debbie Wasserman Schultz (Fla.), the DNC chairwoman. "When we discovered the intrusion, we treated this like the serious incident it is and reached out to CrowdStrike immediately. Our team moved as quickly as possible to kick out the intruders and secure our network."

Finally, there's Michael Sussman's claim that no donor or voter information was stolen.

> 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.

Guccifer 2.0 proved that wrong by posting a number of financial documents.

In other words, the initial post was designed to discredit anything Crowdstrike and Democrats said. More importantly, it included a number of threats that Hillary and her aides should have recognized: Guccifer 2.0 had more, had more of the stuff closer to Hillary.

This was dick-waving, not obfuscation (which is consistent with what we see in the documents, and consistent with what I understand was left in some of the servers). It's just that most of the public wouldn't have seen that dick-waving; just the Democrats and Crowdstrike would.

Which is why I want to return to something that commentators have long been hung up on: Guccifer 2.0's claim to have gotten in through VAN.

> The DNC had NGP VAN software installed on their system so I used the 0-day

> exploit and then deployed my backdoor.

I suspect his reference to zero-days was actually a further taunt to Dmitri Alperovitch, who had fluffed up the Russians in the original WaPo.

> The two crews have “superb operational tradecraft,” he said. They often use previously unknown software bugs — known as “zero-day” vulnerabilities — to compromise applications.

But why did dick-wagging Guccifer 2.0 focus on VAN? One obvious reason is that it invoked the events of December, when a Bernie staffer got fired for having saved Hillary files when the wall between the two campaigns in VAN came down, literally at the moment the Sanders campaign finished their best fundraiser to date. That is, it might be that VAN just invoked a really sore subject between the two sides.

Guccifer 2.0 may have raised it because Crowdstrike was brought in and did a cursory review to endorse the official view. Had Crowdstrike done more at the time, it they might have discovered the Russians.

The reason I ask, though, is that Guccifer 2.0 kept harping on VAN. A big file that has been the focus of recent attention — in the last few days credibly shown to come from the same file set as the documents later released falsely labeled as Clinton Foundation documents — was called NGP VAN, even though the file has nothing to do with VAN.

Notably, too, some of the last files stolen and shared with WikiLeaks included a series providing VAN access to the finance team. That is, one of the last things that happened before Russia got dumped from the system is a new set of VAN passwords got set up.

Amid the discussion of how the Russians got targeting data, I think it worth noting that

having VAN access would have provided a lot of the information the Russians would have wanted.