A NEW FORM OF VICTIM BLAMING: DEMANDING THAT RAT-FUCKER ROGER STONE GET TO LEARN THE DEFENSIVE MEASURES DNC IMPLEMENTED IN 2016

Roger Stone's ongoing effort to float hoaxes rather than mount a credible defense has gotten the left and right denialists into a tizzy about CrowdStrike again. But this time it's not just an effort to raise doubts about whether Russia hacked the DNC, but an effort to suggest that Democrats can only obtain law enforcement help in response to being hacked if they're willing to share their own network defenses with the FBI, and do so while their candidate is under active investigation by the FBI.

As I noted back in May, Stone demanded unredacted CrowdStrike reports in the guise of challenging warrants based off a claim that Russia didn't actually hack the DNC. In the latter motion, Stone claimed to have received three redacted CrowdStrike reports (though as is typical of the sloppy work his lawyers do, they can't even get that citation correct).

> CrowdStrike's three draft reports are dated [sic] August 8 and August 24, 2016. The Mueller Report states Unit 26165 officers also hacked into a DNC account hosted on a cloud-computing service on September 20, 2016, thereby illustrating the government's reliance on CrowdStrike even though the DNC suffered another attack under CrowdStrike's watch. (See Mueller Report at 49-50). [my emphasis]

The government's response to the Fourth Amendment challenge notes that the fourteen warrant affidavits for hacking (Computer Fraud and Abuse Act) violations don't rely on Russian attribution to establish probable cause, but instead point to Stone's, WikiLeaks', Guccifer 2.0's, and Jerome Corsi's communications to establish *that* a hack was committed and Stone's facilities likely had evidence about it.

> In brief, each of these affidavits (at a minimum) states that Stone communicated with the Twitter account Guccifer 2.0 about hacked materials Guccifer had posted. Each affidavit states that on June 15, 2016, Guccifer 2.0 publicly claimed responsibility for the hack of the computer systems of the Democratic National Committee ("DNC"). Each affidavit states that Organization 1 published materials stolen from the DNC in the hack. Each affidavit describes Stone's communications (including his own public statements about them) with Guccifer 2.0, Organization 1, and the head of Organization 1. Each affidavit submits that, based on those communications, there was probable cause to believe that evidence related to the DNC hack would be found in the specified location.
>
> [snip]
>
> On the contrary, the 1030 warrant affidavits contain detailed descriptions of Stone's communications with Guccifer 2.0, Organization 1, and the head of Organization 1, and, in some cases, detailed descriptions of witness tampering and false statements. See, e.g., Doc 109, Ex. 10 at ¶¶ 35-40 (discussing Stone's communications with Organization 1 and the head of organization 1), Ex. 11 at ¶ 24 (discussing private Twitter message between Stone and Guccifer 2.0); Ex. 18

> at ¶¶ 64-77 (relating to Stone's conversations with Person 2).
>
> [snip]
>
> The various showings of probable cause in the 1030 warrant affidavits did not depend on the identity of the hacker, but rather were based on evidence showing that Stone communicated with a Twitter account that publicly claimed responsibility for the DNC hack, and that Stone communicated with the very organization that was disseminating materials from the DNC computers in the months after the hack. This evidence established probable cause that searches of the target locations would yield evidence of a violation of 18 U.S.C. § 1030, regardless of whether the Russian state was involved.

If Judge Amy Berman Jackson agrees that those warrant affidavits establish probable cause independent of any attribution, then then entire question of CrowdStrike reports is moot.

Yet the government still had to explain why the CrowdStrike demand was frivolous. In the response to the CrowdStrike demand, then, the government noted that these reports are unrelated to the false statements charges Stone is facing.

> The defendant is not charged with conspiring to hack the DNC or DCCC. Cf. Netyksho, Doc. 1. The defendant is charged with making false statements to Congress regarding his interactions with Organization 1 and the Trump Campaign and intimidating a witness to cover up his criminal acts. Any information regarding what remediation steps CrowdStrike took to remove the Russian threat from the system and strengthen the DNC and DCCC computer systems against subsequent attacks is not

> relevant to these charges. And, in any case, the government does not need to prove at the defendant's trial that the Russians hacked the DNC in order to prove the defendant made false statements, tampered with a witness, and obstructed justice into a congressional investigation regarding election interference.

But along with that, the government also provides some details about how it came into possession of the CrowdStrike reports — which basically amounts to the Democrats sharing them with the FBI when they informed the FBI of a crime. The government describes that the redacted materials don't actually pertain to evidence about the hack, but instead pertain to what CrowdStrike did — while their client was trying to win a presidential election, remember, and while the party's presidential candidate was being investigated by the FBI — to protect the Democrats against further hacking. The government also demonstrates that Stone exaggerates when he claims these are "heavily" redacted.

> At the direction of the DNC and DCCC's legal counsel, CrowdStrike prepared three draft reports.1 Copies of these reports were subsequently produced voluntarily to the government by counsel for the DNC and DCCC. 2 At the time of the voluntary production, counsel for the DNC told the government that the redacted material concerned steps taken to remediate the attack and to harden the DNC and DCCC systems against future attack. According to counsel, no redacted information concerned the attribution of the attack to Russian actors. The government has also provided defense counsel the opportunity to review additional reports obtained from CrowdStrike related to the hack.
>
> [snip]

> As the government has advised the defendant in a letter following the defendant's filing, the government does not possess the material the defendant seeks; the material was provided to the government by counsel for the DNC with the remediation information redacted. However, the government has provided defense counsel the opportunity to review additional unredacted CrowdStrike reports it possesses, and defense counsel has done so. 3
>
> 1 Although the reports produced to the defendant are marked "draft," counsel for the DNC and DCCC informed the government that they are the last version of the report produced.
>
> 2 The defendant describes the reports as " heavily redacted documents," Doc. 103, at 1. One report is thirty-one pages; only five lines in the executive summary are redacted. Another runs sixty-two pages, and redactions appear on twelve pages. The last report is fifty-four pages, and redactions appear on ten pages.
>
> 3 These materials are likewise not covered by Brady, but the government produced them for defense counsel review in an abundance of caution.

This makes it clear that, on top of being totally irrelevant to the probable cause consideration of the warrants for Stone's communications, Stone is basically arguing that as part of asking the FBI to investigate a crime targeting them — at a time when the FBI was actively investigating Hillary!!! — the Democrats should have had to share the new network security measures installed in response to the crime. This amounts to demanding that a crime victim who might also be under FBI investigation provide the FBI with investigative benefit — the equivalent of handing over their

passwords — just to report the crime.

But what Stone has done is worse. He has demanded that he — modern America's greatest rat-fucker, and someone against whom the FBI was able to show probable cause for hacking crimes — be informed of the opposing party's defenses against being hacked for no good reason at all.

And a bunch of chumps are magnifying Stone's demand, as if it has credibility, because they're still clinging to some kind of hope that Russia didn't hack the DNC.

Below, I've put a list of all the obvious investigative sources cited in the GRU indictment (cited by paragraph number) and the Mueller Report (cited as MR and page number) aside from CrowdStrike reports on the server activity and the witness reports of Democratic employees (hoaxsters often assume that no one in the Democratic Party conducted their own investigation, which is false). This is a fairly conservative list, and primarily consists of stuff the FBI would obtain from subpoenas for third party records. There are *twenty-nine* sources of information totally independent of CrowdStrike, and those sources include Google, Facebook, Microsoft, and AWS — all of which have global visibility and conduct their own tracking of GRU's hacking for their own security purposes, plus Twitter and WordPress (the latter of which also has superb security resources). The list also includes a server in AZ that I assume the FBI seized; it does not include a server in TX that I've also been told got seized in the FBI's investigation.

And that's just the unclassified stuff.

The notion that the attribution of the DNC hack to the GRU relies on CrowdStrike reports or FBI possession of the alleged single DNC server has always been nonsense. But that nonsense is now being wielded to demand that victims of a crime turn over to their political adversaries — and not just any adversary but an epic rat-fucker — details of what they did to make sure they would

not be victimized in the next election. As Rayne explained in May, this is not just an attempt to obfuscate what happened in 2016; it's an attempt to continue to damage the Democrats going forward.

And left and right wing denialists are playing along like chumps.

Update: I should have noted something that is obvious to anyone who follows cybersecurity but which hoaxsters pretend not to know: CrowdStrike gave the FBI forensic images of the servers and other affected hardware and software. That is the norm for computer investigations.

1. URL-shortening service (WADA hack used bit.ly) [Indictment ¶21a]
2. Gmail, including accounts of victims [Indictment ¶21b, MR 37]; accounts used by GRU [MR 47]; and their own security
3. Linked In [Indictment 21c]
4. Probe of DNC's IP address
5. Search on open source info on DNC [MR 37]
6. AZ server – FBI with direct access, possible seizure [Indictment ¶24c, ¶58, MR 39]
7. Malaysian server [Indictment ¶25, MR 39]
8. Other redacted servers [MR 39]
9. Microsoft [MR 41]
10. Romanian domain registration site [Indictment ¶¶33b, 35, 58]
11. ActBlue [Indictment ¶33b]

12. AWS [personal reporting, ¶34, MR 49]
13. Smartech Corporation [¶37, MR 42]
14. Facebook [¶38, MR 42]
15. Twitter [¶¶39, 44, MR 44]
16. WordPress [¶¶42-43, 46]
17. BTC exchanges [¶63]
18. VPN purchase [¶45a]
19. gfade147 email account [¶60]
20. US payment processor [¶62]
21. Forensic images of DNC servers and traffic logs [MR 40]
22. Stolen document forensics [MR 47]
23. Aaron Nevins [MR 43]
24. AOL [MR 43]
25. Online archives [MR 46]
26. Ecuadorian Embassy network [MR 46]
27. Guccifer@mail.com email [MR 46]
28. WikiLeaks email [MR 47]
29. Clinton personal office domain [MR 49]

As I disclosed last July, I provided information to the FBI on issues related to the Mueller investigation, so I'm going to include disclosure statements on Mueller investigation posts from here on out. I will include the disclosure whether or not the stuff I shared with the FBI pertains to the subject of the post.