# [SOME OF] WHERE TRUMP WANTS TO GO WITH THE SERVER IN UKRAINE STORY

As I emphasized in this post, before Trump pushed Volodymyr Zelensky to frame Hunter Biden, he first pressed Ukraine's president to "get to the bottom" of the "what happened with this whole situation with Ukraine."

> The President: I would like you to do us a favor though because our country has been through a lot and Ukraine knows a lot about it. I would like you to find out what happened with this whole situation with Ukraine, they say Crowdstrike … I guess you have one of your wealthy people… The server, they say Ukraine has it. There are a lot of things that went on, the whole situation. I think you are surrounding yourself with some of the same people. I would like to have the Attorney General call you or your people and I would like you to get to the bottom of it. As you saw yesterday, that whole nonsense ended with a very poor performance by a man named Robert Mueller, an incompetent performance, but they say a lot of it started with Ukraine. Whatever you can do, it's very important that you do it if that's possible.

Contrary to virtually all the coverage on this, there is reason to believe that Bill Barr can get information from Ukraine that will feed the disinformation about the Russian operation. Trump has obviously been told — and not just by Rudy Giuliani (as Tom Bossert believes) — to ask for this, but some of this is probably part of the disinformation that Russia built in to the operation.

# Rudy Giuliani wants to frame Alexandra Chalupa

This morning, Rudy Giuliani explained that he wants to know who in Ukraine provided information damning to Trump during the 2016 campaign.

> GIULIANI: I have never peddled it. Have you ever hear me talk about Crowdstrike? I've never peddled it. Tom Bossert doesn't know what he's talking about. I have never engaged in any theory that the Ukrainians did the hacking. In fact, when this was first presented to me, I pretty clearly understood the Ukrainians didn't do the hacking, but that doesn't mean Ukraine didn't do anything, and this is where Bossert…
>
> STEPHANOPOULOS: So, why does the president keep repeating it?
>
> GIULIANI: Let's get on to the point…
>
> STEPHANOPOULOS: Well, this was in the phone call.
>
> GIULIANI: I agree with Bossert on one thing, it's clear: there's no evidence the Ukrainians did it. I never pursued any evidence and he's created a red herring. What the president is talking about is, however, there is a load of evidence that the Ukrainians created false information, that they were asked by the Obama White House to do it in January of 2016, information he's never bothered to go read. There are affidavits that have been out there for five months that none of you have listened to about how there's a Ukrainian court finding that a particular individual illegally gave the Clinton campaign information. No one wants to investigate that. Nobody cared about it. It's a court opinion in the

> Ukraine. The Ukrainians came to me. I didn't go to them. The Ukrainians came to me and said…
>
> STEPHANOPOULOS: When did they first come to you?
>
> GIULIANI: November of 2016, they first came to me. And they said, we have shocking evidence that the collusion that they claim happened in Russia, which didn't happen, happened in the Ukraine, and it happened with Hillary Clinton. George Soros was behind it. George Soros' company was funding it.

This is an effort to frame Alexandra Chalupa, who while working as a DNC consultant in 2016 raised alarms about Paul Manafort. This is an effort that Trump has pursued since 2017 in part with a story first floated to (!!) Ken Vogel, an effort that key propagandist John Solomon was pursuing in May. Remember, too, that Chalupa was hacked separately in 2016, and believed she was being followed.

## Peter Smith's operation may have asked for help from a hacker in Ukraine

But per the transcript, this is not about Rudy, it's about Barr. And even leaving Rudy's antics aside, there is more that Trump may be after.

First, a fairly minor point, but possibly important. According to Charles Johnson, he advised Peter Smith to reach out to Weev for help finding Hillary's deleted emails.

> Johnson said he also suggested that Smith get in touch with Andrew Auernheimer, a hacker who goes by the alias "Weev" and has collaborated with Johnson in the past. Auernheimer—who was

> released from federal prison in 2014 after having a conviction for fraud and hacking offenses vacated and subsequently moved to Ukraine—declined to say whether Smith contacted him, citing conditions of his employment that bar him from speaking to the press.

At the time (and still, as far as I know), Weev was living in Ukraine. The Mueller Report says that his investigators never found evidence that Smith or Barbara Ledeen (or Erik Prince or Mike Flynn, who were also key players in this effort) ever contacted *Russian* hackers.

> Smith drafted multiple emails stating or intimating that he was in contact with Russian hackers. For example, in one such email, Smith claimed that, in August 2016, KLS Research had organized meetings with parties who had access to the deleted Clinton emails, including parties with "ties and affiliations to Russia."286 The investigation did not identify evidence that any such meetings occurred. Associates and security experts who worked with Smith on the initiative did not believe that Smith was in contact with Russian hackers and were aware of no such connection.287 The investigation did not establish that Smith was in contact with Russian hackers or that Smith, Ledeen, or other individuals in touch with the Trump Campaign ultimately obtained the deleted Clinton emails.

Weev is a hacker, but not Russian. So if Smith had reached out to Weev — and if Weev had given him any reason for optimism in finding the emails or even the alleged emails that Ledeen obtained — it might explain why Trump would believe there was information in Ukraine that would help him.

# CrowdStrike once claimed its certainty on Russian attribution related to a problematic report on Ukraine

But that's not the CrowdStrike tie.

At least part of the CrowdStrike tie — and what Zelensky actually could feed to Trump — pertains to a report they did in December 2016. They concluded that one of the same tools that was used in the DNC hack had been covertly distributed to Ukrainian artillery units, which (CrowdStrike claimed) led to catastrophic losses in the Ukranian armed forces. When the report came out — amid the December 2016 frenzy as President Obama tried to figure out what to do with Russia given the Trump win — CrowdStrike co-founder Dmitri Alperovitch pitched it as further proof that GRU had hacked the DNC. In other words, according to CrowdStrike, their high confidence on the DNC attribution was tied to their analysis of the Ukrainian malware.

In a now deleted post, infosec researcher Jeffrey Carr raised several problems with the CrowdStrike report. He correctly noted that CrowdStrike vastly overstated the losses to the Ukranian troops, which both an outside analyst and then the Ukranian Defense Ministry corrected. CrowdStrike has since updated its report, correcting the claim about Ukrainian losses, but standing by its analysis that GRU planted this malware as a way to target Ukrainian troops.

Carr also claimed to know of two instances — one, another security company, and the other, a Ukrainian hacker — where the tool was found in the wild.

> Crowdstrike, along with FireEye and

> other cybersecurity companies, have long propagated the claim that Fancy Bear and all of its affiliated monikers (APT28, Sednit, Sofacy, Strontium, Tsar Team, Pawn Storm, etc.) were the exclusive developers and users of X-Agent. We now know that is false.
>
> ESET was able to obtain the complete source code for X-Agent (aka Xagent) for the Linux OS with a compilation date of July 2015. [5]
>
> A hacker known as RUH8 aka Sean Townsend with the Ukrainian Cyber Alliance has informed me that he has also obtained the source code for X-Agent Linux. [11]

Carr argued that since CrowdStrike's attribution of the DNC hack assumed that only GRU had access to that tool, their attribution claim could no longer be trusted. At the time I deemed Carr's objections to be worthwhile, but not fatal for the CrowdStrike claim. It was, however, damning for CrowdStrike's public crowing about attribution of the DNC hack.

Since that time, the denialist crowd has elaborated on theories about CrowdStrike, which BuzzFeed gets just parts of here. Something that will be very critical moving forward but which BuzzFeed did not include, is that the president of CrowdStrike, Shawn Henry, is the guy who (while he was still at FBI) ran the FBI informant who infiltrated Anonymous, Sabu. Because the FBI reportedly permitted Sabu to direct Antisec to hack other countries as a false flag, the denialist theory goes, Henry and CrowdStrike must be willing to launch false flags for their existing clients. [See update below, which makes it clear FBI did not direct this.] The reason I say this will be important going forward is that these events are likely being reexamined as we speak in the grand jury that has subpoenaed both Chelsea Manning and Jeremy Hammond.

So Trump has an incentive to damage not just CrowdStrike's 2016 reports on GRU, but also CrowdStrike generally. In 2017, Ukraine wanted to rebut the CrowdStrike claim because it made it look bad to Ukranian citizens. But if Trump gives Zelensky reason to revisit the issue, they might up the ante, and claim that CrowdStrike's claims did damage to Ukraine.

I also suspect Trump may have been cued to push the theory that the GRU tool in question may, indeed, have been readily available and could have been used against the DNC by someone else, perhaps trying to frame Russia.

As I've noted, the GRU indictment and Mueller Report list 30 other named sources of evidence implicating the GRU in the hack. That list doesn't include Dutch hackers at AIVD, which provided information (presumably to the Intelligence Community generally, including the FBI). And it doesn't include NSA, which Bossert suggested today attributed the hack without anything from CrowdStrike. In other words, undermining the CrowdStrike claims would do nothing to undermine the overall attribution to Russia (though it could be useful for Stone if it came out before his November 5 trial, as the four warrants tied to his false statements relied on CrowdStrike). But it would certainly feed the disinformation effort that has already focused on CrowdStrike.

That's just part of what Trump is after.

Update: Dell Cameron, who's one of the experts on this topic, says that public accounts significantly overstate how closely Sabu was being handled at this time. Nevertheless, the perception that FBI (and Henry) encouraged Sabu's attacks is out there and forms a basis for the claim that CrowdStrike would engage in a false flag attack. Here's the chatlog showing some of this activity. Hammond got to the Brazilian target by himself.