THE MALWARETECH CASE RESETS TO ZERO: A DIALOGUE WHEREIN THE GOVERNMENT REPEATS "YOUTUBE" OVER AND OVER

Yesterday, the government responded to Marcus Hutchins (MalwareTech)'s renewed challenges, submitted two weeks ago, to the superseding indictment the government used to replace its previous crappy-ass indictment and thereby set the motions process almost back to zero. Here's my abbreviated summary of what Hutchins argues in the renewed motions, with the government response.

1) Motion for a Bill of Particulars with respect to CFAA charges

Hutchins: Name the 10 or more protected computers I allegedly damaged and the damage I did, because recording and exfiltrating data is not damaging a computer. Also, name the computers I allegedly tried to access without authorization.

Government: We're going to revert to the outdated definition of malware the Seventh Circuit has already rejected to claim it is damage. Also, we're going to pretend we used the word intent where you keep nagging us for not doing so.

2) Challenge to Seventh

Count (CFAA)

Hutchins: You've rewritten the CFAA language, "[K]nowingly cause[] the transmission of a program, information and command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer[.]," but not included the intentionality language.

Government: Correct! We've simply replaced the word "intentionally" with "attempted," so it's all good.

> [A]n attempt means to take a substantial step towards committing the offense, with the "intent to commit the offense." (emphasis added) Because Count Seven is charged as an attempt to violate section 1030, including the word "intentionally" before "attempted" (which Hutchins believes to be necessary) would be unnecessary and redundant. See United States v. Rutherford, 54 F.3d 370, 373 (7th Cir. 1995) (stating attempts are intentional acts; and under common law, "an attempt includes the specific intent to commit an unlawful act").

emptywheel: There are some cases where the government succeeded in convicting people of CFAA without the charged person causing the damage himself, but I'd have to look closer to see if this will fly under Seventh Circuit precedents.

3) Motion to dismiss the whole damn indictment

Hutchins: There was no damage in the damage charges, no wiretapping device in the wiretapping charges, nor did Marcus advertise any such device, and laying out how MalwareTech writes blog posts analyzing malware does not

mean he advertised a wiretapping device.

> The superseding indictment states that Mr. Hutchins "hacked control panels" associated with a so-called competing malware called Phase Bot and wrote a blog post about it. (First Superseding Indictment ¶ 4(h).) It does not appear that this allegation alone is the basis of any count, as Mr. Hutchins would presumably be charged with a direct—rather than inchoate—violation of § 1030(a)(2)(C) if that were the case. To the extent it is a basis for any count, however, the defense notes that analyzing malware is, in fact, what Mr. Hutchins does professionally. In total, Mr. Hutchins wrote a total of three lengthy blog posts to educate the public about Phase Bot's structure and functionality. These blog posts were based on Mr. Hutchins' analysis of Phase Bot installed on his own computers. Any attempt to punish or interfere with Mr. Hutchins' lawful security research and publishing activities would, of course, violate his First Amendment rights.

Government: We're going to define malware however we damn well please, even if we have to use a British dictionary rather than the American one the Seventh Circuit uses to throw a Brit in the pokey. Hell, we're willing to play word games with *four different* reference books if we need to! But if you use a dictionary to argue the law means what the law says, then you're cheating.

> Therefore, the Court should resist Hutchins's attempt to limit the scope of sections 2511 and 2512 based on a definition found in one online dictionary; or because "malware" or "spyware" or "software" is not specifically listed in the definition of "electronic, mechanical, or other device." The reference to "any device or

> apparatus" is written broadly in order to capture changes in technology.

Also, because Hutchins' co-conspirator showed a video of malware operating on a computer and both talked about malware operating on a computer in forums, that turns the malware into a device! Presto!

4) Motion to dismiss wiretapping because Congress never intended to charge foreigners with wiretapping and none of the rest of this happened in the United States

Hutchins: "A foreign defendant like Mr. Hutchins is not subject to the jurisdiction of the United States merely because someone else posted a video on the Internet." And "to the extent that Mr. Hutchins and Individual B interacted while Individual B was purportedly in the United States, that circumstance cannot, as the first superseding indictment tries to do, subject Mr. Hutchins' alleged dealings with Individual A to domestic prosecution."

Government: So what if Congress didn't intend wiretapping to apply extraterritorially? There's a YouTube! Also, you're being hypertechnical by arguing Congress' intent in passing a law. Besides, that was *so* long ago!

> [B]ecause the conduct charged in Counts Two and Three occurred in the U.S. there is no extraterritorial application of U.S. law to foreign conduct. This is true even if Hutchins and Individual A were abroad when the conduct occurred in the U.S.

Also, there's a YouTube!

emptywheel: One interesting aspect of the government's desperate attempt to claim the actions of two people outside of the US took place in the US is that the malware in question was sold on location obscuring sites, Darkode and AlphaBay. That doesn't change that an officer in Easter (as the government calls it at least twice) District of WI bought the malware in WI. But it will do interesting things to the government's claim that Hutchins and VinnyK "directed" such sales at the US. It all seems to come down to the YouTube.

5) Motion to compel the identity of Randy

Hutchins: In order to shore up your dodgy indictment, you've made Randy into an uncharged co-conspirator. Now you *really* have to give us his ID.

Government: Sure, sure, we've included Randy in overt acts to get around the fact that Randy, but not you, intended to steal data so we can argue you're guilty. But that doesn't change his role in the *investigation*. You're just using a local rule against us. Plus, you were mean to Sabu once on Twitter so obviously you just want to call for reprisal against Randy.

emptywheel: As far as I know MalwareTech has not called for reprisal *against me* for cooperating

with the government against a cybercriminal. Maybe he's just opposed to cybercriminals blaming others for their own crimes, as Randy appears to have done?

More seriously, I'm going to pull out two more things.

First, here's some language from the government response in 4 that pretty much sums up their argument.

> Second, Hutchins misunderstands the nature of the charges in Count One and Seven and the government's burden at trial. Conspiracy punishes an illegal agreement. United States v. Read, 658 F.2d 1225, 1240 (7th Cir. 1981) (describing liability for a conspiracy and mail fraud). And it is well established that under conspiracy law, the object of the conspiracy does not need to be achieved for liability to attach. United States v. Donner, 497 F.2d 184, 190 (7th Cir. 1974). Therefore, the government only needs to prove Hutchins conspired to damage computers, not the actual damage he intended.
>
> The same is true for Count Seven. An attempt is a substantial step towards completing the crime with the intent to complete the crime. United States v. Sanchez, 615 F.3d 836, 843-44 (7th Cir. 2010). As with Count One, the government does not have a burden to prove damage; only an attempt to damage.

What the government has done has charged crimes that permit Hutchins to be held liable for criminal acts his co-conspirator maybe possibly intended, even though it's not clear he had the same intent as his co-conspirator, even if neither had the intent to facilitate wiretapping or damage to computers (depending on what

dictionary you use). I make light above, but this is a very powerful aspect of US law, and it shouldn't be dismissed outright.

Finally, the only place either side addresses false statements (one of the two new charges that's not just smearing old charges more thinly and using the part of CFAA they should have charged under in the first place, the other being wire fraud) is in argument 4. Hutchins says that because everything else is bunk there are not false statements that can be charged.

> If the Court grants this motion as to Counts One Through Eight and Ten, it should also dismiss Count Nine. That count charges a violation of 18 U.S.C. § 1001 and flows from an allegedly false statement Mr. Hutchins made to law enforcement during a post-arrest interrogation focusing on the conduct charged in the broader indictment. Section 1001 is violated only when a false statement is made about a "matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States." 18 U.S.C. § 1001(a). This motion asserts a lack of domestic jurisdiction over the alleged offenses such that any false statement made by Mr. Hutchins about those offenses is not subject to prosecution under § 1001.

The government (predictably) doesn't agree. It says jurisdiction doesn't matter, what matters is that the FBI was investigating.

> In this case, the FBI was conducting a criminal investigation which falls within the meaning of "any matter" as used in 18 U.S.C. § 1001. United States v. Rogers, 466 U.S. 475, 476-484 (1984); see also 28 U.S.C. § 533; 28 C.F.R. § 0.85. Additionally, the term "jurisdiction" as used in section 1001 "merely differentiates the official,

> authorized functions of an agency or department from matters peripheral to the business of that body." United States v. Rogers, 466 U.S. 475, 476- 484 (1984). Therefore, even if all the other counts of the superseding indictment were dismissed, Count Nine would survive. Hutchins's motion should therefore be denied.

I fear this argument might well work: that because the FBI was investigating something mostly in a poorly executed attempt to strand Hutchins here so they could make him inform on others, he can be charged with false statements. That's crazy. But that's also the way false statements may work.

All of which is to say, a great deal of the government's argument boils down to, "YouTube! Try this dictionary! YouTube! Or maybe this dictionary! YouTube!" But that doesn't mean it won't all work.