AFTER REITERATING ORIN KERR'S ARGUMENTS, MALWARETECH ASKS FOR THE INDICTMENT TO BE DISMISSED WITH PREJUDICE

In a post explaining that MalwareTech (Marcus Hutchins) had gotten a last minute continuance before an evidentiary hearing last month, I linked to my thread on the government's weak responses to a bunch of motions he had submitted. Here's how I described the original motions:

> The five filings are:
>
> 1. *A motion for a bill of particulars, basically demanding that the government reveal what 10 computers Hutchins and his alleged co-conspirator conspired and intended to damage*
> 2. *A motion to suppress the statements Hutchins made after he was arrested, requesting an evidentiary hearing, based on the fact that Hutchins was high and exhausted and didn't know US law about Miranda warnings*

3. *A motion to dismiss the indictment, arguing on three different grounds that,*
    - *The CFAA charges (one and six) don't allege any intent to cause damage to a protected computer (because the malware in question steals data, but doesn't damage affected computers)*
    - *The Wiretapping charges (two through five) don't allege the use of a device as defined under the Wiretap Act, but instead show use of software*
    - *The sales-related charges (one, five, and six) conflate the sale of malware with the ultimate effect of it*
4. *A motion to dismiss the indictment for improper extraterritorial application and venue, effectively because*

> *this case should never have been charged in the US, much less Milwaukee*
>
> 5. *A motion to dismiss charges two and six based on suspected improper grand jury instruction failing to require intentionality*

Yesterday, Hutchins submitted his replies to the government's arguments, in which he argues:

> 1.The government needs to explain what kind of proof of damage to 10 computers that Hutchins and his co-defendant conspired to damage it will offer and provide discovery on it.
>
> 2. [Hutchins offered no new response to the government's Miranda response]
>
> 4. Because the government didn't include the legitimate (purchase by an FBI Agent of the malware) and specious (sharing a binary with someone in CA and discussing the malware in online forums) bases that tie Hutchins' activities to Eastern District of Wisconsin or even the US in the indictment itself, the indictment is an improper extraterritorial application of the law and lack venues in EDWI.
>
> 5. Because the government doesn't include intentionality where the statute requires it, it should dismiss the related counts with prejudice (note, this argument has evolved from a grand jury error to a more fundamental problem assault on the indictment).

While I'm not sure all of these will succeed on their own (indeed, I think the motion on venue

with respect to CFAA might fail in the absence of the rest of this), these motions form an interlocking argument that there's no there there.

Which the defense argues at most length is the motion reiterating that selling software does not amount to either CFAA (damaging 10 computers) or wiretapping (which requires a device), an argument Orin Kerr made just after the charges were released in August. I get the feeling the defense thought that, having had access to Kerr's argument all these months, the government might have responded better. The two substantive parts of their argument are here, addressing the point that CFAA violations require doing (or attempting to do) actual damage to computers, not just code that has the ability to damage them.

> [T]he government suggests that its characterization of Kronos as "malware" should satisfy the pleading standard, claiming that it is "common knowledge" that malware is "written with the intent of being disruptive or damaging." (Gov't Response at 4 (citing Oxford English Dictionary 2018).) But the CFAA does not make so-called malware illegal—it is not some form of contraband. In fact, the term "malware" does not appear anywhere in the statute. The CFAA is not concerned with what software is called, but what an actor uses it to do. Artificial labels aside, the question before the Court is whether the indictment adequately pleads a case that Mr. Hutchins and his co-defendant conspired or attempted to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer." 18 U.S.C. §§ 371 & 1030(a)(5)(A).
>
> The only definition of "malware"

> relevant to that question is one offered in the indictment. The indictment, at paragraph 3(d), defines "malware" as "malicious computer code installed on protected computers without authorization that allowed unauthorized access to the protected computer." Nothing in this definition involves "intentionally caus[ing] damage without authorization, to a protected computer," which is necessary to violate § 1030(a)(5)(A). The indictment's "unauthorized access" language seems to be borrowed from other provisions of the CFAA that have not been charged in this case, such as §§ 1030(a)(2), (5)(B), and (5)(C)—all of which include additional elements beyond "unauthorized access." Even if Kronos precisely meets the definition of "malware" offered by the government in the indictment, that functionality alone would not constitute a violation of § 1030(a)(5)(A) or any other provision of the CFAA.

There are, I think, cases where malware sellers have been convicted — but only after their customers were busted doing damage. Here, the only customer mentioned in the legal case thus far was an FBI Agent that no one has alleged actually used the malware (the malware was used in other countries, including Hutchins' home in the UK, about which the government has been completely silent since the initial indictment).

Here's the language arguing that software, sold without a computer, is not a device as defined in the wiretapping statute charged.

> [T]hose cases all involved claims that the defendants acquired communications using software running on a computer. Under those circumstances, a court has no reason to draw a distinction between the two because the software and computer are working together: the operation of one depends on the other.

> Indeed, the cases cited by the government discuss computers and the software installed on them as one unit. See, e.g., Zang, 833 F.3d at 633 ("[O]nce installed on a computer, WebWatcher automatically acquires and transmits communications to servers"); Klumb, 884 F. Supp. 2d at 661 ("The point is that a program has been installed on the computer which will cause emails sent at some time in the future through the internet to be re-routed[.]"); see also Shefts, 2012 WL 4049484, **6-10 (variously referring to servers, email accounts, software, and BlackBerry smartphones as interception devices).
>
> For purposes of the § 2512 charges in this case, however, the distinction between software and computer is important. In Counts Two through Four, there is no computer, which would not be true in any scenario involving an actual interception. As noted in Potter, software alone is incapable of intercepting anything. 2008 WL 2556723, at *8. "It must be installed in a device, such as a computer, to be able to do so." protected computer," which is necessary to violate § 1030(a)(5)(A).

In both cases, the defense is basically arguing that not only do Hutchins' actions not meet the terms of the statute, but the indictment was also badly written in an unsuccessful attempt to make those statutes apply.

These are alleged crimes for which the government has refused to identify victims, provided none of the requisite evidence of intentionality, applied to software that doesn't obviously qualify under either of the charged laws. Some of that is a problem with the indictment, as written. Much about this case suggests the government assumed Hutchins would plead quickly, obviating the need to write an

indictment that could hold up to a trial. As I noted, in its response a few weeks ago, the government claimed (after threatening that it might) it was planning on obtaining a superseding indictment.

> The government plans to seek a superseding indictment in this case, and in doing so will correct this drafting error and moot Hutchins's argument.

Two weeks later, there's still no sign of the indictment that fixes the aspects the government admits are flawed, much less the other scope issues. And so now Hutchins is asking for the indictment — all counts of it, between one challenge or another — be dismissed with prejudice.

I'm not sure that will happen — judges have proven the ability to interpret CFAA to include all manner of bad hacker stuff. But an outright dismissal might put the government out of the misery it brought on itself with a case it should never have charged.