THE GOVERNMENT'S MALWARETECH CASE GOES (FURTHER) TO SHIT

MalwareTech's lawyers just submitted a motion to compel discovery in his case. It makes it clear his case is going to shit — and that's only the stuff that is public.

DOJ is hiding what drunken MalwareTech understood about un-common law

First, the motion reveals that even though the FBI recorded its interview with Marcus Hutchins at the Las Vegas airport, where Hutchins allegedly admitted to creating the Kronos malware (though in actuality Hutchins only admitted to creating that code), they somehow forgot to record (or even write down) the Miranda warning part.

> After Mr. Hutchins was taken into custody, two law enforcement agents interviewed him at the airport. The memorandum of that interview generically states: "After being advised of the identity of the interviewing Agents, the nature of the interview and being advised of his rights, HUTCHINS provided the following information . . ." A lengthy portion of Mr. Hutchins' interview with the agents was audio recorded. Importantly, however, the agents did not record the part of the interview in which they purportedly advised of him of his Miranda rights, answered any questions he might have had, and had him sign a Miranda waiver

> form.

This is important for several reasons. First, Hutchins is a foreign kid. And while I presume he has seen Miranda warnings a jillion times on the TV, those warnings are different in the US than they are in the UK, contrary to whatever else we might share as common law.

> Mr. Hutchins is a citizen of the United Kingdom, where a defendant's post-arrest rights are very different than in the United States.4 The United Kingdom's version of Miranda contains no mention of the right to counsel, and if a defendant does not talk, it may later be used against him under certain circumstances.5 Because of this, any government communications in advance of Mr. Hutchins' arrest and regarding how to advise him of his rights under Miranda are important to demonstrate that Mr. Hutchins would not have understood any purported Miranda warnings and that he was coerced to waive his rights.
>
> 4 United Kingdom law requires the following caution being given upon arrest (though minor wording deviations are allowed): "You do not have to say anything. But it may harm your defence if you do not mention when questioned something which you later rely on in Court. Anything you do say may be given in evidence."

So the specific wording of the warning he got would be especially important to understand whether he was told how things are different here in the former colonies, where you're always told you can have a lawyer.

Also Hutchins was drunk and — because he'd been at DefCon and Black Hat all week — exhausted. But the defense can't show that because the

government isn't turning over any of the surveillance materials from the week the FBI was surely following Hutchins in Las Vegas.

> The defense believes the requested discovery will show the government was aware of Mr. Hutchins' activities while he was in Las Vegas, including the fact that he had been up very late the night before his arrest, and the high likelihood that the government knew he was exhausted and intoxicated at the time of his arrest.

The government doesn't want you to know co-defendant Tran is just a convenient excuse to arrest MalwareTech

Next, the government is withholding both information about Hutchins' co-defendant, and the MLAT request the government used to get that information. The co-defendant's last name is Tran, but the government has been hiding that since it accidentally published the name when Hutchins' docket went live. Tran has not yet been arrested, but apparently there was evidence relating to him in a country that would respond to an American MLAT request. The government hasn't turned it over.

> [T]he government may be withholding information that could exculpate Mr. Hutchins. For example, any material showing that the codefendant operated independently of Mr. Hutchins' alleged conduct would tend to demonstrate that they did not conspire to commit computer fraud and abuse (Count 1). The indictment itself supports that notion: it alleges that the codefendant advertised and sold the Kronos malware

> independently of Mr. Hutchins. (Indictment at 3 ¶ 4(e)-(f).) Moreover, the indictment alleges that the malware was advertised on the AlphaBay market forum, which the Department of Justice seized and shut down on July 20, 2017 in cooperation with a number of foreign authorities.8 In connection with that case, the government likely has records of the co-defendant's activities on AlphaBay that it has not produced (e.g., records obtained through MLAT requests).

They also haven't turned over the MLAT application itself, which would explain why some country has turned over evidence on Tran, but not Tran himself.

> To date, the government has produced materials responsive to a single MLAT request, and has declined to produce the MLAT request itself. The MLAT request, however, surely contains information regarding the government's theory of the case and may have been signed by an agent who will testify at trial. MLAT requests vary from country to country, but they can be quite similar to search warrants, since they are often used to obtain documents.

DOJ won't tell you which ham sandwiches the grand jury ~~intended~~ knowed to indict

Hutchins' lawyers then ask for the grand jury instructions because the indictment as charged doesn't get the *mens rea* necessary for the underlying charges. Basically, two of the charges against Hutchins were laid out as if the only thing needed for a crime was to knowingly

do something, as opposed to intentionaly do it.

> The defense needs the legal instructions for an anticipated motion to dismiss the indictment. One ground for that motion is that at least two of the charged counts are defective on their face, failing to include the appropriate *mens rea*. Since the two counts deviate materially from the required and heightened mental states set forth in the operative statutes, this demonstrates likely irregularities in how the grand jury was instructed on the law.
>
> [snip]
>
> Count 6 suffers from a similar defect. It charges that the defendants:
>
> > [K]nowingly caused the transmission of a program, information and command and as a result of such conduct, attempted to cause damage without authorization, to 10 or more protected computers during a 1-year period. In violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B)(i) and (ii), (c)(4)A(i)(VI), 1030(b), and 2.
>
> (Indictment at 8 (emphasis added).)
>
> But 1030(a)(5)(A) states it is illegal to:
>
> > [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[.] (Emphasis added.)
>
> Likewise, the Seventh Circuit Pattern Jury Instructions state the elements of the offense are:

> 1. The defendant knowingly caused the transmission of a [program; information; code; command]; and
>
> 2. By doing so, the defendant intentionally caused damage to a protected computer without authorization. (Emphasis added.)
>
> The plain text of 1030(a)(5)(A) and the Pattern Jury Instructions leave no doubt that Count 6, as it is pleaded, does not include the requisite "intentional" mens rea for causing damage without authorization, again failing to allege an essential element of the offense.

Effectively, they're arguing that the government has charged Hutchins for knowingly done something when they had to charge him for intentionally doing something. Which, given that his code was probably used without his knowledge, is going to present difficulties. And so Hutschins' team is going to attack the indictment itself.

> Considering that Counts 2 and 6 misstate the required mental states specified in the statutes, there is a high likelihood the government did not properly instruct the grand jury on the law, and the grand jury returned a legally defective indictment, as a result of improper legal instructions.

What about "Randy"?

But the thing that intrigues me the most about this case is that some guy the government is naming "Randy" — because they don't want to actually reveal *anything about this dude — is a key witness against Hutchins.*

> The defense expects "Randy" to testify at trial because he is alleged to have had extensive online chats with Mr.

> Hutchins around the time of the purported crimes in which Mr. Hutchins discussed his purported criminal activity. Any communications and materials relating to "Randy" are therefore material to defense preparations.

The defense argues that the government is treating Randy like a tipster rather than a witness as a way to hide who he is. This is worth citing at length (also note Marcia Hofmann and Brian Klein added local lawyer Daniel Stiller, who — I presume — is Seventh Circuit citing with great abandon).

> The informant privilege does not permit the government to conceal a witness when, as here, disclosure "is relevant and helpful" to a defendant's defense "or is essential to a fair determination of a cause." United States v. McDowell, 687 F.3d 904, 911 (7th Cir. 2012) (quoting Roviaro v. United States, 353 U.S. 53, 60-61 (1957)). Indeed, the Seventh Circuit's treatment of the privilege indicates that its reach is typically limited to background sources of information, as in a tipster who furnishes details that commence an investigation resulting in a prosecution premised on the fruits of the investigation, not the details of the background tip.
>
> A mere tipster, according to the Seventh Circuit, is "someone whose only role was to provide the police with the relevant information that served as the foundation to obtaining a search warrant." Id. Tipsters differ from what the Seventh Circuit terms "transactional witnesses," who are individuals "who participated in the crime charged . . . or witnessed the event in question." Id. For tipsters, "the rationale for the privilege is strong and the case for

> overriding it is generally weak." Id. In contrast, "the case for overriding the privilege and requiring disclosure tends to be stronger" for transactional witnesses. Id.
>
> Here, the government's refusal to disclose even the identity of "Randy's" attorney is apparently the result of miscategorizing an important witness as a mere tipster. "Randy" is a cooperating witness, one whose provision of information to law enforcement was facilitated by consideration—proffer immunity, at the least—from the government. This circumstance alone weighs against continuing confidentiality because "Randy" surely knows his cooperation will be revealed.

The government won't even give the defense the name of this dude's lawyer so the lawyer can tell them his client doesn't want to talk to them.

Me? I'm guessing if the government were required to put "Randy" on the stand they'd contemplate dismissing the charges against Hutchins immediately. I'm guessing the government now realizes "Randy" took them for a ride — perhaps an enormous one. And given how easy it is to reconstitute chat logs — but here, it's not even clear "Randy" has the chat logs, but just claimed to have been a part of them, in an effort to incriminate him — I'm guessing this part of the case against Hutchins won't hold up.

It'd probably be a good time for the government to dismiss the charges against Hutchins and give him an H1B for his troubles so he can surf off the last 6 months of stress. But that's not how the government works, when they realize they really stepped in a load of poo.