THE GOVERNMENT BUILT ITS CRIMINAL CASE AGAINST MALWARETECH OFF INCIDENTAL COLLECTION

The government has responded to MalwareTech's (Marcus Hutchins) demand for more evidence by refusing everything. Along the way, they reveal that the bulk of the case against Hutchins arises from him being incidentally collected off two other criminal suspects, Tran (his co-defendant) and Randy (an informant who provided testimony against him in conjunction with his own criminal exposure).

Twenty-somethings claiming they're not drunk occifer

As for rebuttals of the points made in his demand, the government has two rebuttals as to the substance of Hutchins' argument, versus the law. First, they claim that Hutchins told the FBI he wasn't drunk when they arrested him, contrary to the claim made to support a demand for materials on the surveillance of him leading up to his arrest.

> Before the interview started, Hutchins told agents that he was not under the influence of alcohol.

Apparently they made a separate 302 (of unknown date) to memorialize their claim he told them he wasn't drunk.

> In addition to those materials, the government recently disclosed an additional FBI 302 report memorializing the defendant's statement that he was

> not under the influence of alcohol at the time of his arrest,

The filing also reveals that there are,

> two reports detailing limited surveillance of the defendant on July 26, 2017, and August 2, 2017.

Note, while August 2 is the day Hutchins left Las Vegas, the 26th was not the day he arrived; that was July 21. So they conducted surveillance of him on at least one day while he was in the US hanging out with other hackers at Black Hat, but won't tell him if they conducted surveillance on the other days.

The government's "intentional" fuckups may lead to superseding indictments

The government seems to cede Hutchins' suggestion that it flubbed the language on "intention" versus "knowledge" on at least one and maybe a second charge against him.

> Hutchins claims that the indictment is defective because Count Two of the indictment states that the defendant acted "knowingly" instead of "intentionally." 3 Likewise, despite the fact that Count Six charges an attempt, Hutchins argues Count Six fails to allege that defendant "intentionally" attempted to cause damage to a protected computer.4 This, however is not an allegation of "error in the grand jury proceedings" under Rule 12(b)(3)(A)(v). It is an allegation of a defect in the indictment under Rule 12(b)(3)(B)(v). Thus, if Hutchins truly believes Counts Two and Six are facially defective, he can file a motion dismiss those counts

> under Rule 12(b)(3)(B)(v).
>
> 3 Count Two appears to contain a drafting error because Counts Three and Four, which also allege violations of 18 U.S.C. § 2512, state that the defendant acted "intentionally" rather than "knowingly." This further undermines Hutchins' speculation that the grand jury was erroneously instructed.
>
> 4 According to Seventh Circuit jury instructions, an attempt means to take a substantial step towards committing the offense, with the "intent to commit the offense." Therefore, because Count Six is charged as an attempt to violate section 1030, including the word "intentionally" before "attempted" would be unnecessary and redundant.

But they generously offer to fix that problem in a superseding indictment.

> The government has already explained to the defense that it will likely seek a superseding indictment in this case. That superseding indictment would address any possible drafting errors noted by the defense.

Given that elsewhere they say the informant, Randy, who provided information against Hutchins, discussed "involvement in creating the Kronos banking Trojan, *among other criminal conduct*" [my emphasis] with him in online chats, they seem to be suggesting that if the defense makes too big a deal about this they'll add charges against Hutchins.

Incidentally collected defendants get nothing

Perhaps most interesting, this filing demonstrates the degree to which Hutchins'

prosecution stems from his incidental collection in investigative efforts targeting Tran and Randy. In fact, precisely *because* he was incidentally collected and not personally targeted, the government claims it doesn't have to provide affidavits that might explain how — and more importantly, why — they decided to arrest Hutchins.

For example, the government argues Hutchins can't have the MLAT requests, which are used to ask other countries to provide information for a criminal prosecution. In this case, MLATs obtained information on Tran, the guy who sold the Kronos malware Hutchins is alleged to have helped write. The government refuses to hand these over, in part, because they don't get signed by FBI Agents, but instead get signed by lawyers.

> Here, the defendant relies on Rule 16(a)(1)(E)(i) in seeking disclosure of MLATs and search warrant applications. But that Rule is inapplicable. With regard to MLATs, they are not signed or attested to by law enforcement agents. Instead, they are signed by an attorney representing the United States. Information received in response to an MLAT that is subject to disclosure under Rule 16 has been, and will continue to be, turned over to the defense in this case. Indeed, the defendant acknowledges that he has received materials responsive to an MLAT request. Doc. #44 at 17. The MLAT request itself, however, is not subject to production. In fact, MLAT requests (rather than the responsive materials) are explicitly excluded from production under Rule 16(a)(2).

Moreover, because the MLAT was targeted at Hutchins' co-defendant, and not him, he doesn't get it.

> Moreover, the MLAT request submitted in

> this case related to Hutchins's codefendant and not Hutchins. As noted above, the government has disclosed materials received in response to the MLAT, but the MLAT itself is not subject to production under Rule 16, Giglio, Brady, or § 3500.

There is one still undisclosed search warrant affidavit in the case. But because that was used to incriminate Randy, the informant, Hutchins won't get that either.

> With regard to search warrant materials, the government has explained to Hutchins that no search warrants were executed that focused on Hutchins' activities. There was a search warrant executed in an unrelated case that revealed statements made by Hutchins to CS-1, and those statements were turned over in discovery under Rule 16. But, there is no authority supporting the production of that search warrant affidavit or other documents relating to that warrant. The warrant was executed at a residence in the United States and did not involve Hutchins' property or privacy interests. The affidavit is not subject to disclosure under 18 U.S.C. § 3500 because it was made in connection with an unrelated investigation. Given the separation between this case and the other investigation, the government does not believe at this time that the affiant's statements in the affidavit supporting that warrant "relate to the subject matter of the testimony" to be presented in this case. 18 U.S.C. § 3500.

The government seems

pretty lackadaisical towards Hutchins' co-defendant

The government's unwillingness to turn over information on the other alleged criminals in this case is particularly interesting given how uninterested they seem in him. The filing reveals that someone working undercover for the FBI did have discussions with Tran about Kronos (again, this is malware that had no significant US victims in the form Hutchins is alleged to have been involved in it), and they collected postings on it off the Darkode forum.

> In support of this request, Hutchins asserts that such items "must be material to preparing Mr. Hutchins' defense" because the indictment alleges a conspiracy; that "the government may be withholding information that could exculpate Mr. Hutchins"; and that he has a right to "locate the codefendant." Doc. #44 at 8-9. Because the government has disclosed information relating to the codefendant, and there is no authority supporting the defendant's request for additional information, his motion to compel the production of this information should be denied.
>
> Of note, Hutchins' codefendant has not yet been arrested in connection with this case. And, the government has disclosed certain information relating to the codefendant to Hutchins. This includes (1) the codefendant's name; (2) materials responsive to an MLAT request that included a redacted copy of the codefendant's passport; (3) undercover chats between the codefendant and the FBI related to the marketing, sale, and distribution of Kronos; and (4) various Internet postings related to Kronos that are attributable to one of the aliases

> used by the codefendant, including on the now shuttered Darkode forum.

But the government hasn't obtained any information about the other things Tran was selling on dark markets.

> Hutchins' speculation that "the government must be withholding substantial additional information in its possession," including information that may show the codefendant acted independently of Hutchins, is not supported. Doc. #44 at 8. While it might be true that the codefendant was involved in criminal activity in addition to distributing Kronos with Hutchins, the government is not suppressing that information. It simply does not possess such information. If additional records in the government's possession are identified and deemed material, the government will provide those records to the defendant.1

That suggests he's not really the target here.

More interesting still, the government claims it hasn't yet identified *any* records from its AlphaBay seizure pertaining this malware they claim is so important they've arrested the guy who stopped the WannaCry malware attack.

> 1 In his motion, Hutchins states that "the government likely has records of the codefendant's activities on AlphaBay." Doc. #44 at 9. The government is still pursing information from the AlphaBay marketplace, but it has not yet located any materials subject to disclosure.

It seems virtually impossible that they wouldn't find information in the seized servers, if it was, at all, a priority. Which seems to suggest the opposite — not finding anything — may be a

priority.

By providing evidence that suggests the government simply isn't all that interested in Tran (if, as his name suggests, he's Vietnamese, he may be beyond any extradition treaty), the government dismisses the possibility that Hutchins or his friends could find Tran (not an unreasonable possibility, because that's how hackers roll).

> [Hutchins] told agents that he knew his codefendant only by various online aliases; his dealings with his codefendant were all online; and he has never met his codefendant in person or even seen a photograph of the codefendant. It therefore makes no sense for Hutchins to claim that, if provided the requested "materials and communications," he will be able to locate the fugitive codefendant and obtain exculpatory information from that individual.

But along the way, this prevents Hutchins from arguing that this case is all trumped up to go after him, for some reason.

Hiding Randy and the carding charges he's working off

More interesting, still, the government is going to some lengths to hide Randy, the informant they call CS-1 who provided information on Hutchins.

The list of what they have provided in discovery provides some outline of how they got to Randy.

> In reality, the government has produced the following materials related to CS-1: (1) A redacted proffer letter between the government and CS-1; (2) undercover chats between a government cooperator

> and CS-1 regarding the sale of stolen credit card numbers; (3) chats between CS-1 and Hutchins regarding Hutchins' involvement in creating the Kronos banking Trojan, among other criminal conduct; and (4) a redacted FBI 302 report (which Hutchins refers to in his motion) memorializing a FBI interview of CS-1 regarding Hutchins and others.

It seems that a third part (the "government cooperator," who himself may be an informant working off criminal charges) provided the FBI chats showing discussions with Randy of carding activity. This led to the FBI to go after Randy. He, in turn, made a proffer to the government offering to cooperate, presumably in exchange for leniency in his own case. That led to an interview with the FBI where Randy provided information on Hutchins "and others."

Note that the government doesn't tell us when all this happened?

The government argues that Randy is a mere tipster who wasn't (yet) being controlled by the FBI at the time, and so they won't have to let Hutchins question Randy about these underlying circumstances unless they put Randy on the stand, even though they concede he might (as someone working off his own criminal exposure) might actually be a transactional witness.

> CS-1's position in this case is more of a like a "mere tipster" than a transactional confidential informant. Hutchins sent a copy of the Kronos malware to CS-1 in 2015, but CS-1 was not acting as an agent for the government at that time. If the government called CS-1 as a witness at trial, his/her primary role would be to testify about the third-party admissions Hutchins made during chats with CS-1. Even if the Court found CS-1 acted more like a transactional witness, that finding does not automatically justify

> disclosure of CS-1's identity. United States v. McDowell, 687 F.3d 904, 911 (7th Cir. 2012). The defendant would still need to establish that knowing CS-1's identity is "relevant and helpful to his defense or is essential to a fair determination of a cause," Wilburn, 581 F.3d at 623. Here, his request for disclosure of CS-1's identity is based on speculation, which is insufficient. See Valles, 41 F.3d at 358 ("The confidential informant privilege 'will not yield to permit a mere fishing expedition, nor upon bare speculation that the information may possibly prove useful.'" (quoting Dole, 870 F.2d at 373)).

The government argues that Hutchins is only speculating that learning who Randy is would be material to his defense, and uses that to argue that they don't have to reveal Randy's name so Hutchins can test whether it's material to his defense.

The government generously agrees to give Hutchins Randy's real name if they call him to testify, but then boast that Hutchins' jail phone calls mitigate the need to put Randy on the stand.

> Nonetheless, the government agrees to disclose CS-1's identity to the defense if it determines that CS-1 will be a testifying witness at trial.2
>
> 2 To be sure, it might not be necessary to call CS-1 as a witness at trial because the defendant was shown the chats he had with CS-1 during his post-arrest interview and the defendant admitted that he was one of the parties in those conversations. Later, the defendant made phone call from jail in which he described the chats as "undeniable." Therefore, the admissions Mr. Hutchins made to CS-1 are admissible

> non-hearsay statements, which Mr. Hutchins previously identified as accurate.

There are a slew of reasons Randy's identity is of particular interest. Not least, that unknown entities engaged in serial credit card fraud to try to disrupt Hutchins' defense fundraisers. As I've suggested, that means that entities engaged in probable criminal credit card fraud made a concerted effort to thwart Hutchins' ability to mount the most robust defense.

Is the FBI even investigating who disrupted Hutchins' defense fundraising efforts? Would they do so if it would hurt their case?

All of which leaves the distinct impression that the government isn't all that interested in the two suspected criminals implicated in the case against him, but are very interested in ratcheting up the pressure on Hutchins himself.

And because they got to Hutchins via incidental collection — and not direct targeting — they might succeed in doing so.