GOVERNMENT WON'T BE ABLE TO HIDE ITS INFORMANT IN MALWARETECH CASE

While Paul Manafort was busy getting charged with 32 new charges (more on that tomorrow), I was in Milwaukee at a motion hearing in MalwareTech (Marcus Hutchins') case.

Hutchins was asking for five things from the government:

1. More information on his surveillance in Vegas, partly to challenge the claim he wasn't drunk or exhausted when he waived Miranda rights, partly to understand whether he really understood how Miranda works in the US, and partly for probably unstated other reasons
2. Information on Tran, his co-defendant, who remains at large in some other country, that he would have gotten if Tran were in custody facing the same charges with Hutchins
3. More information on "Randy," the informant who provided chat logs and a copy of the Kronos malware while trying to proffer his way out of his own cyber-crimes

4. The instructions provided to the grand jury, to see if the importance of intentionality to the charges was properly emphasized
5. Both the MLAT request used to get information on Tran and the search warrant used to search Randy's home

Here are my pieces on the motion, the government's response, and Hutchins' reply.

At Thursday's hearing, Judge Nancy Johnson made the following decisions:

1. Based on the government's representation that it had no more information on surveillance of Hutchins, she denied that motion barring any further evidence that it exists (though she did make the prosecution check again to make sure there weren't text messages between Agents)
2. Based on the government's representation that there was nothing Hutchins would get about Tran were he in custody that he hasn't already gotten, she denied that without prejudice
3. Required the government to provide "Randy's" identity 30 days before trial
4. Took the request for grand

jury instructions under advisement

5. Denied the request for the search warrant for "Randy's" house, but asked for more briefing on other cases pertaining to MLAT requests

While the discussion about materials pertaining to Tran were uninteresting, my comments about the other requests follow:

What surveillance happens in Vegas stays in Vegas

Much of this discussion pertained to clarifications that the defense wasn't looking for the FBI Agents' lunch place recommendations, though Hutchins' lawyer Brian Klein said he'd take them if he got them. Klein admitted, however, that they want the surveillance materials, in part, because they think the government intentionally waited to arrest Hutchins until after he had been partying with other hackers for a week. "[W]e have our reasons to believe they arrested him at very end of Vegas trip, there was maybe a very pointed reason to believe they chose to wait until the end." Note, I'm not sure they're after (just) the exhaustion of DefCon, or even the government's desire to hold off on a real rebellion if they had arrested Hutchins just as everyone was arriving to Las Vegas.

The government claims it only has active surveillance from July 26, and August 2, as he headed for the airport. Prosecutor Michael Chmelar described the July 26 date as Hutchins' arrival, though I think that's incorrect as I noted here.

> 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.

Chmelar also seemed to describe a discussion about "certain preparations put in place if he did travel to the US," which is curious given that Hutchins was publicly talking about his trip to Vegas for some time, and given the apparently weird start date of the surveillance. Chmelar also described, for the first time, a 302 on his unrecorded comments on the way to the detention facility. Chmelar made it clear that they want to force Hutchins to take the stand if he's going to challenge his Miranda warning.

One more comment about this: Black Hat and DefCon are among the most spooked up conventions going. There would have been tons of law enforcement types wandering around unassociated with Hutchins, specifically. Would he get any surveillance from those guys?

FBI finally dug through its AlphaBay loot to find materials supporting a six month old arrest

Hutchins' co-defendant, Tran, allegedly sold the Kronos malware at issue on AlphaBay. FBI, working with international partners (and probably using the Tor exception), took AlphaBay down on July 20, even before Hutchins' arrest, and immediately started using those materials to prosecute crimes that, unlike Hutchins' alleged crime, have actual American victims.

> Out of the "several hundred" investigations cited by Phirippidis,

> other publicly known active US prosecutions arising out of AlphaBay sales involve clear American victims and perpetrators: a person in California suspected of paying an Israeli teenagerto phone and email bomb threats to Jewish Community Centers around the country;a group that fulfilled over 78,000 marijuana orders over the last two yearsmaking them largest vendor on AlphaBay; a transaction that led to the fentanyl overdose death of an 18-year old girl in Oregon; another transaction that led to a fentanyl overdose death, this time of a 24-year old Orlando woman; a fentanyl vendor suspected of making over $120,000 in profits who is tied to a non-lethal overdose; an investigation out of Atlanta into a still unidentified American who worked for AlphaBay. Other, earlier prosecutions, include the sales of heroin,fentanyl, and marijuana laid out in the indictment of AlphaBay's head, Alexandre Cazes.

In Chmelar's explanation that the government really doesn't have any materials on Tran, he revealed what he (incorrectly) thought had been revealed in the government response: an unencrypted copy of AlphaBay material pertaining to the Kronos sale "just became available," and they have put in a request for the material. "If anything is produced in that request," Chmelar said he'd turn it over.

Again, the lackadaisical approach to establishing evidence of the sale of Kronos as compared to other AlphaBay prosecutions suggests the sale of Kronos really wasn't that big of a priority.

As Klein noted, the government had spent three pages of their response arguing that Hutchins couldn't have any material pertaining to Tran; at the hearing Chmelar represented nothing existed. Based on that representation, Johnson

denied any further discovery.

“Randy” is not just a tipster

Michael Chmelar is a well-spoken guy. But he stumbled a lot, umming and uhing, during his discussion of “Randy,” the government informant who reportedly had chats with Hutchins about Kronos.

> He received Kronos from Mr. Hutchins, before he was acting as a government , um um source, we’ve produced the malware that was received. As Mr. [Benjamin] Proctor and I noted, if we determine that uh this individual would be called as a witness, we would disclose him as district court requires.

The government really, really wants to hide certain details about “Randy” (and as Chmelar admitted, the 302 in which he proffered up Hutchins and others includes pages and pages of redacted details of “Randy’s” own crimes.

As Johnson pointed out, even if the government uses Hutchins’ own statements to admit “Randy’s” testimony, Hutchins’s team can decide to call “Randy” themselves.

In any case, while she said “Randy” wasn’t fully a transactional witness, he is closer to that than to the tipster the government is claiming. So while the defense won’t get his identity, yet, they will before trial.

The government seems to have dropped its enthusiasm for a superseding indictment

Hutchins wants the instructions given to the grand jury because two of the charges don’t

include the necessary language about the required intentionality. Chmelar used one of the charges, where in parallel ones in the indictment the intentionality language is correct, to suggest this was just a scrivener's error — something he could disappear away with a stipulation — to suggest both were. But Klein argued "These are not just little nits or typos, it goes to mens rea, [Hutchins'] alleged mental state."

There was also an interesting subtext about whether the grand jury instructions exist. Chmelar claimed that normally he doesn't instruct the grand jury. Klein noted the government had claimed, 'We're not required to instruct them.' "Well, they did." And it seems that Chmelar did, indeed, admit that the jury had gotten instructions on this point (I'd have to look at the transcript to make sure).

Ultimately, Johnson said she'd take the request under advisement and do more research on what constituted a compelling need to obtain grand jury instructions, but wouldn't rule until the defense submitted their challenges to the indictment.

But what was just as interesting about this discussion is that, whereas previously there had been discussion about the government obtaining a superseding indictment (perhaps to lard on charges that might be easier to defend), Chmelar seemed unenthused about doing so here.

The government continues to insist documents sent to other countries are internal documents

Because privacy rights are not transitive in the United States (meaning, the Fourth Amendment only protects the privacy of the person whose

premise is being searched, not those who might be implicated by the search), Hutchins is not going to get the search warrant for “Randy’s” house that led to chat logs involving Kronos to be discovered.

But the question of whether he’ll get the MLAT request to whatever foreign country had information on his co-defendant, Tran (but may not be arresting him), is still a matter Johnson is weighing. The government at first argued that they didn’t have to turn over the request because it was written by lawyers, not law enforcement officers. In the hearing, Chmelar defended withholding the request because the request, which was sent to a foreign country, was an internal document.

Both sides will submit more caselaw on when and whether such requests get turned over (and the open file discovery here may make turning it over more likely).