MALWARETECH'S CASE GETS COMPLEX

Today, prosecutor Michael Chmelar and Marcus Hutchins' lawyers, Marcia Hofmann and Brian Klein, had a phone meeting with judge Nancy Johnson.

Hutchins' lawyers got the judge to agree to further loosen his bail terms (putting him on a curfew rather than house arrest, it appears). But, after agreeing willingly to most requests last week, the government is now objecting to the change, asking for a stay and reconsideration. Recall, too, that AUSA Michael Chmelar had tacitly agreed to have Hutchins taken off GPS monitoring. We will likely see the substance of their complaint in a motion in the coming days.

The other thing that happened — again, as I reported would happen here — the case got deemed complex, meaning the trial can be delayed without a violation of the Speedy Trial Act. The minutes describe the judge's approval of the motion for these reasons.

> Based on the information presented here, the nature of the charges, the nature and amount of the discovery, the fact that discovery is coming from multiple sources and the fact that some of the information may need independent testing/review, the court will designate this matter COMPLEX.

The most interesting detail here is that independent testing may be required. Probably — especially given researchers are already raising doubts — Hutchins' lawyers are going to get outside experts to check the government claims that the code sold in Kronos came from Hutchins.

Another detail from the minutes is that Hutchins' lawyers object to the redaction of the indictment.

> The Government gives background of this case and notes that defendant Hutchins is the only party to appear thus far.
>
> [snip]
>
> The defense notes that it objects to the redaction of the Indictment.

The WI courthouse already accidentally revealed the name of Hutchins' co-defendant, Tran.

In spite of some effort, no one I've seen has identified a likely (and sufficiently interesting) co-defendant whose last name is Tran — or a connection between that name and VinnyK, the name currently associated with selling the malware. Presumably, if the co-defendant's aliases were unsealed, it would be easier for researchers to understand what Hutchins has been accused of, and who he has been accused of conspiring with.

As for the discovery, some of that was provided in the minutes. As I noted, the government turned over Hutchins' custodial interview (curiously, the minutes don't specify that they were with the FBI) and the recordings of two calls.

> The government will be following its open file policy. To date, the defendant has provided the defense with the following:
>
> – 1 CD with post arrest statements
>
> – CD with 2 audio recordings from the county jail in Nevada. (The government is awaiting a written transcript from the FBI.)

Here's what's left to discovery, with my comments interspersed.

> In addition, there are:
>
> – 150 pages of Jabber chats between the defendant and an individual (somewhat

> redacted).

Were these encrypted or group chats? If the former, via what means did FBI decrypt them? Did someone hand them over to the FBI?

> – Business records from Apple, Google and Yahoo.

These would be accessible via Section 702 (though, given the lack of a FISA notice, would likely have been backstopped via subpoena if they were collected via 702).

> – Statements (350 pages) to the defendant from another internet forum which were seized by the government in another District.

The government provides no details on what the location (US or overseas) of this forum is – and they describe it as statements to Hutchins rather than statements by him. But their existence shows that another District had enough interest in some conversations Hutchins happened to be involved in that they collected – via whatever means – this forum.

> – 3-4 samples of malware

At a minimum, the government needs 3 pieces of malware: Kronos before Hutchins allegedly updated it, Kronos after he did, and the version of Kronos that got sold. Apparently, the government hasn't decided how many versions they'll give the defense. And all that still leaves the question of victims; to prove that anything Hutchins did affected any Americans they might need more malware.

In part for that reason, I suspect independent researchers will continue to look for their own publicly available samples.

> – A search warrant executed on a third party which may contain some privileged

> information.

As with the other forum, this suggests the FBI or some other agency was interested enough in another case — or a corporation — such that some kind of privilege might apply. This could, in fact, be a victim.

All of that is what led the defense to request (after the government already said it would do the same, having initially said this wouldn't be a complex case) that this should be deemed complex, in part so Hutchins' team can have a couple of months to review what they're looking at.

> The parties agree that the case should be designated as complex. Information is still being obtained from multiple sources. The issues are complex[.] The defendant requests 45-60 days in which to review the discovery. The government notes that it is in agreement with the request.

So it's a complex case and it'll drag on until such time as the government gets more coercive to get whatever it is they're after or they drop the case.