GOVERNMENT AIMS TO PROTECT OTHER ONGOING INVESTIGATIONS IN MALWARETECH CASE

In its request for a protection order governing discovery materials turned over to the defense in the Marcus Hutchins/MalwareTech case, the government provided this explanation of things it needed to keep secret.

> The discovery in this matter may include information related to other ongoing investigations, malware, and investigative techniques employed by the United States during its investigation of Mr. Hutchins and others.

The government will always aim to protect investigative techniques — though in an international case investigating hackers, those techniques might well be rather interesting. Of particular interest, the government wants to hide techniques it may have used against Hutchins … and against others.

The government's claim it needs to hide information on malware will disadvantage researchers who are analyzing the Kronos malware in an attempt to understand whether any code Hutchins created could be deemed to be original and necessary to the tool. For example, Polish researcher hasherezade showed that the hooking code Hutchins complained had been misappropriated from him in 2015, when the government claims he was helping his co-defendant revise Kronos, was not actually original to him.

> The interesting thing about this part of Kronos is its similarity with a hooking engine described by MalwareTech on his

> blog in January 2015. Later, he complained in his tweet, that cybercriminals stolen and adopted his code. Looking at the hooking engine of Kronos we can see a big overlap, that made us suspect that this part of Kronos could be indeed based on his ideas. However, it turned out that this technique was described much earlier (i.e. here, *//thanks to @xorsthings for the link*), and both authors learned it from other sources rather than inventing it.

Hasherezade may well have proven a key part of the government's argument wrong here. Or she may be missing some other piece of code the government claims comes from Hutchins. By hiding any discussions about what code the government is actually looking at, though, it prevents the security community from definitely undermining the claims of the government, at least before trial.

Finally, there's the reference to other, ongoing investigations.

One investigation of interest might be the Kelihos botnet. In the April complaint against Pyotr Levashov, the government claimed that the Kelihos botnet had infected victims with Kronos malware.

> In addition to using Kelihos to distribute spam, the Defendant also profits by using Kelihos to directly install malware on victim computers. During FBI testing, Kelihos was observed installing ransomware onto a test machine, as well as "Vawtrak" banking Trojan (used to steal login credentials used at financial institutions), and a malicious Word document designed to infect the computer with the Kronos banking Trojan.

Unlike known uses of Kronos by itself, Kelihos *is* something that has victimized people in the United States; the government has indicted and is trying to extradite Pyotr Levashov in that case. So that may be one investigation the government is trying to protect.

It's also possible that, in an effort to pressure Hutchins to take a plea deal, the government is investigating allegations he engaged in other criminal activity, activity that would more directly implicate him in criminal hacking. There's little (aside from statutes of limitation) to prevent the government from doing that, and their decision to newly declare the case complex may suggest they're threatening more damaging superseding indictments against Hutchins, if they can substantiate those allegations, to pressure him to take a plea deal.

Finally, there's WannaCry. As I noted, while the government lifted some of the more onerous bail conditions on Hutchins, they added the restriction that he not touch the WannaCry sinkhole he set up in May. The reference to ongoing investigations may suggest the government will be discussing aspects of that investigation with Hutchins' defense team, but wants to hide those details from the public.

Update: I've corrected the language regarding Kelihos to note that this doesn't involve shared code. h/t ee for finding the reference.