PROSECUTORS CITE OSIRIS IN AN ATTEMPT TO RESUSCITATE DEAD LAW AGAINST MARCUS HUTCHINS

I've been meaning to do an update on a series of filings in the MalwareTech (Marcus Hutchins') case in which his defense challenged the magistrate's recommendations, the government responded, and MalwareTech replied. As I'll get to, those filings reveal a bit more about what the government was really up to in their prosecution of Hutchins.

First, however, I want to look at something the government does in the first paragraph of their response. The paragraph starts with a succinct statement about the case that smooths over a lot of legally suspect moves they make in the case.

> Marcus Hutchins is charged with developing and distributing malware capable accessing and damaging computers without the owners' knowledge and stealing personal information. See Doc. #86. As set forth in the superseding indictment, he worked with others to sell this malware in online forums. Doc. #86. Hutchins did this to earn money for himself. He essentially admitted his crimes in online "chats" that were later obtained by law enforcement.

Effectively, this statement obscures all the problems with charging Hutchins for making malware that he never intended to use to damage computers as understood by the Computer Fraud and Abuse Act and which doesn't equate to a device that might amount to wiretapping.

Immediately after having done that, the government points to an entirely different

generation of malware than Hutchins wrote — which has since been dubbed Osiris — to suggest Hutchins' own work has led to damage.

> The malware developed and sold by Hutchins and his coconspirators, and variants of that malware, particularly Kronos, have been used to compromise computers around the world for years. See, e.g., "Kronos Reborn," Proofpoint, July 24, 2018, available at https://www.proofpoint.com/us/threat-insight/post/kronos-reborn (last visited November 30, 2018) (discussing 2018 campaigns involving Kronos variants).

The link describes a much later version of the underlying malware used in campaigns in Germany, Poland, and Japan.

> In April 2018, the first samples of a new variant of the banking Trojan appeared in the wild [2]. The most notable new feature is that the command and control (C&C) mechanism has been refactored to use the Tor anonymizing network. There is some speculation and circumstantial evidence suggesting that this new version of Kronos has been rebranded "Osiris" and is being sold on underground markets. In this blog, we present information on the German, Japanese, and Polish campaigns as well as a fourth campaign that looks to be a work in progress and still being tested.

Even if Hutchins' code formed a key part of this module (I'm sure if this ever gets to trial Hutchins' team will be able to mock this as a possibility), attacks in three other countries do not justify a prosecution of a British citizen in Milwaukee.

Remember, early on in this case, the government admitted they don't believe Hutchins continues to engage in criminal activity.

Effectively, Hutchins is on trial for code he wrote years ago, some of it while he was a minor. Because people associated with later generations of that code — with its literal rebirth as a new product — are causing havoc, the government is intent on holding him accountable.