FBI BUSTS THE GUY WHO SAVED THE WORLD FROM NSA'S MALWARE

Yesterday, the FBI arrested Marcus Hutchins as he was leaving Las Vegas after Black Hat/Defcon.

Hutchins is best known as the malware researcher, MalwareTechBlog, who inadvertently saved the world from NSA's repurposed hacking tools by registering what has been assumed to be the sand boxing domain, effectively turning it into a killswitch.

But the government accuses him of making the Kronos banking malware sold on AlphaBay. In an indictment signed July 11 (6 days after AlphaBay got seized and), the government asserts simply that Hutchins made the malware. Motherboard first reported the arrest.

a. Defendant MARCUS HUTCHINS created the Kronos malware.

It also accuses him of conspiring with a co-defendant whose name is redacted, going back to July 2014, of selling it.

There's a lot of skepticism about this indictment in the infosec community, in part because no one took Hutchins for a black hat, though others point to a past identity under which he may have engaged in carding. Plus, the timing is curious. The press release for the arrest notes "the Kronos banking Trojan … was first made available through certain internet forums in early 2014."

On July 13, 2014, Hutchins put out an ask for a sample of the malware.

That’s also the day the indictment describes an advertising video first being posted to AlphaBay on how Kronos worked.

In remarkably timed news, between 3:10 and 3:25 AM UTC this morning (8 PM last night Mountain Time), someone emptied out all the WannaCry accounts.