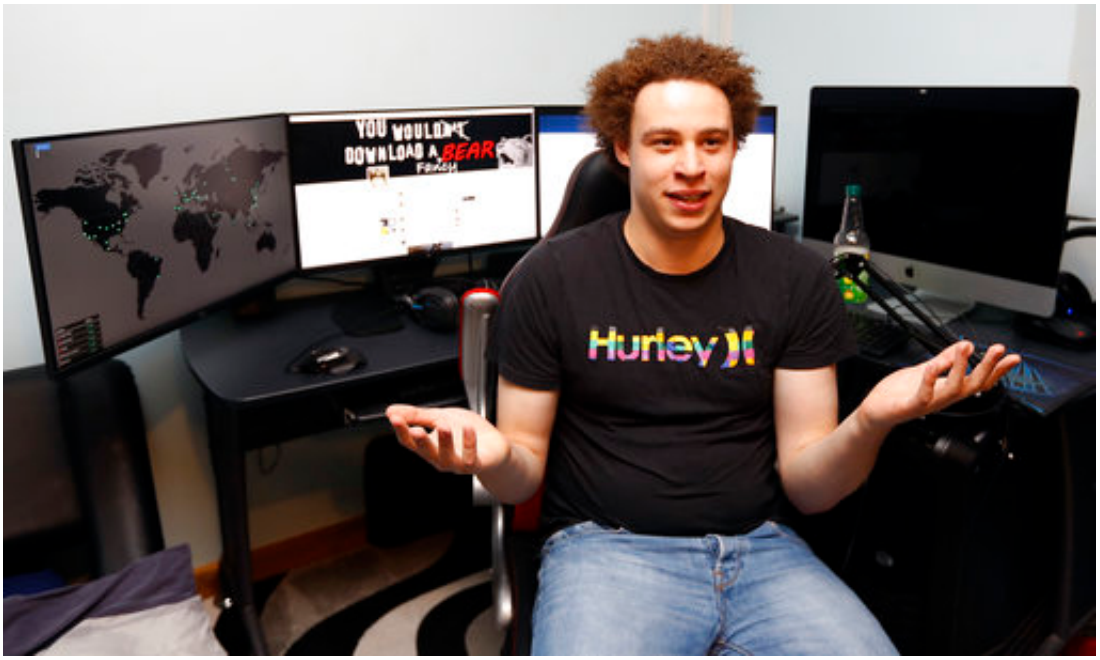
Computer law expert says British hacker arrest problematic

August 4 2017, by Danica Kirka And Ken Ritter



In this Monday, May 15, 2017, file photo, British IT expert Marcus Hutchins speaks during an interview in Ilfracombe, England. Hutchins, a young British researcher credited with derailing a global cyberattack in May, has been arrested for allegedly creating and distributing banking malware, U.S. authorities say. Hutchins was detained in Las Vegas on Wednesday, Aug. 2, 2017, while flying back to Britain from Defcon, an annual gathering of hackers of IT security gurus. A grand jury indictment charges Hutchins with "creating and distributing" malware known as the Kronos banking Trojan. (AP Photo/Frank Augstein, File)

A computer law expert on Friday described the evidence so far

presented to justify the U.S. arrest of a notorious British cybersecurity researcher as being problematic—an indictment so flimsy that it could create a climate of distrust between the U.S. government and the community of information-security experts.

News of Marcus Hutchins' arrest in the United States for allegedly creating and selling malicious software able to collect bank account passwords has shocked the cybersecurity community. Many had rallied behind the British hacker, whose quick thinking helped control the spread of the WannaCry ransomware attack that crippled thousands of computers in May.

Attorney Tor Ekeland told The Associated Press that the facts in the indictment fail to show intent.

"This is a very, very problematic prosecution to my mind, and I think it's bizarre that the United States government has chosen to prosecute somebody who's arguably their hero in the WannaCry malware attack and potentially saved lives and thousands, hundreds of thousands, if not millions, of dollars over the sale of alleged malware," Ekeland said. "This is just bizarre, it creates a disincentive for anybody in the information security industry to cooperate with the government."

Hutchins was detained in Las Vegas as he was returning to his home in southwest Britain from an annual gathering of hackers and information security gurus. A grand jury indictment charged Hutchins with creating and distributing malware known as the Kronos banking Trojan.

Such malware infects web browsers, then captures usernames and passwords when an unsuspecting user visits a bank or other trusted location, enabling cybertheft.

The indictment, filed in a Wisconsin federal court last month, alleges

that Hutchins and another defendant—whose name was redacted—conspired between July 2014 and July 2015 to advertise the availability of the Kronos malware on internet forums, sell the malware and profit from it. The indictment also accuses Hutchins of creating the malware.

The problem with software creation, however, is that often a program can include code written by multiple programmers. Prosecutors might need to prove that Hutchins wrote code with specific targets.

Ekeland said that what is notable to him from the indictment is that it doesn't allege any financial loss to any victims—or in any way identify them. Besides that, laws covering aspects of computer crime are unclear, often giving prosecutors broad discretion.

"The only money mentioned in this indictment is ... for the sale of the software," he said. "Which again is problematic because in my opinion of this, if the legal theory behind this indictment is correct, well then half of the United States software industry is potentially a bunch of felons."

Another expert in computer crime, Orin Kerr from George Washington University's law school, also took aim at the charges. Kerr said it's unusual, and problematic, for prosecutors to go after someone simply for writing or selling malware—as opposed to using it to further a crime.

"The indictment is pretty bare bones, and we don't have all the facts or even what the government thinks are the facts," Kerr wrote in an opinion piece in the Washington Post. "So while we can't say that this indictment is clearly an overreach, we can say that the government is pushing the envelope in some ways and may or may not have the facts it needs to make its case."

Jake Williams, a respected cybersecurity researcher, said he found it difficult to believe Hutchins is guilty. The two men have worked on various projects, including training material for higher education for which the Briton declined payment.

"He's a stand-up guy," Williams said in a text chat. "I can't reconcile the charges with what I know about him."

Hutchins, who lives with his family in the town of Ilfracombe, England, and worked out of his bedroom, has until Friday afternoon to determine if he wants to hire his own lawyer. The Electronic Frontier Foundation, a San Francisco-based digital rights group, said Friday it was "deeply concerned" about Hutchins' arrest and was attempting to help him "obtain good legal counsel."

Hutchins' mother, Janet, who has been frantically trying to reach her son, said she was "outraged" by the arrest and that it was "hugely unlikely" her son was involved because he spends much of his time combatting such attacks.

The curly-haired computer whiz and surfing enthusiast discovered a so-called "kill switch" that slowed the unprecedented WannaCry outbreak. He then spent the next three days fighting the worm that crippled Britain's hospital network as well as factories, government agencies, banks and other businesses around the world.

Though he had always worked under the moniker of MalwareTech, cracking WannaCry led to the loss of his anonymity and propelled him to cyber stardom. There were appearances and a $10,000 prize for cracking WannaCry. He planned to donate the money to charity.

"I don't think I'm ever going back to the MalwareTech that everyone knew," he told The Associated Press at the time.