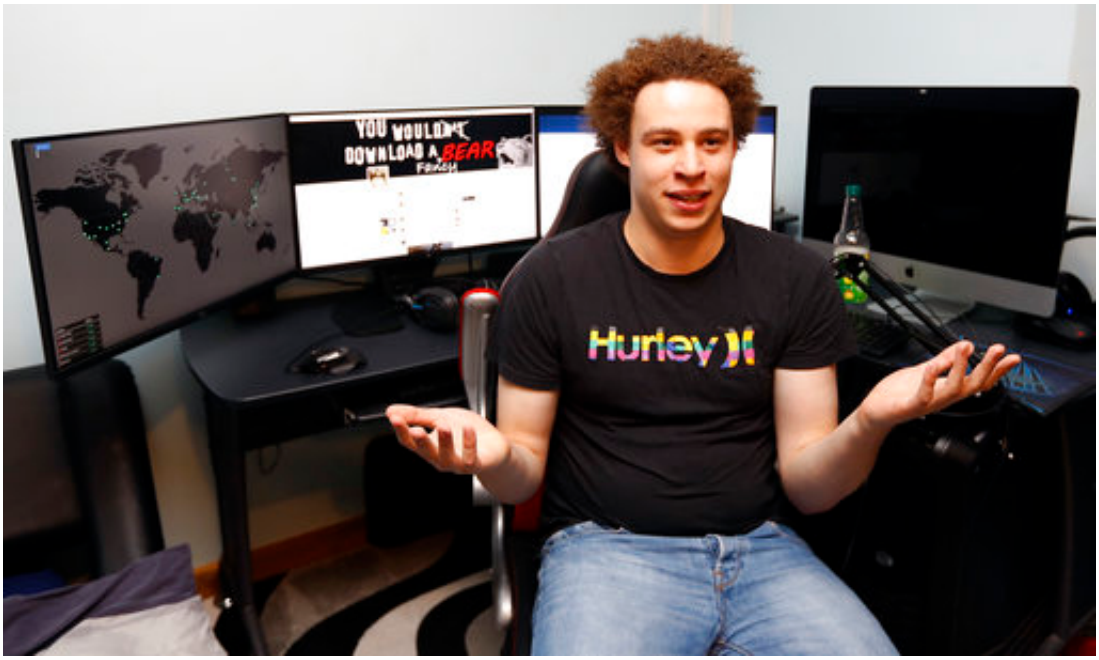
Hacker who helped stop global cyberattack arrested in US (Update)

August 4 2017, by Ken Ritter And Matt O'brien



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)

Marcus Hutchins, a young British researcher credited with derailing a

global cyberattack in May, was arrested for allegedly creating and distributing malicious software designed to collect bank-account passwords, U.S. authorities said Thursday.

News of Hutchins' detention came as a shock to the cybersecurity community. Many had rallied behind the researcher whose quick thinking helped control the spread of the WannaCry ransomware attack that crippled thousands of computers.

Hutchins was detained in Las Vegas on his way back to 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.

Authorities said the malware was first made available in early 2014, and "marketed and distributed through AlphaBay, a hidden service on the Tor network." The U.S. Department of Justice announced in July that the AlphaBay "darknet" marketplace was shut down after an international law enforcement effort.

Hutchins' arraignment was postponed Thursday in U.S. District Court in Las Vegas by a magistrate judge who gave him until Friday afternoon to

determine if he wants to hire his own lawyer.

Hutchins was in Las Vegas for Def Con, an annual cybersecurity conference that ended Sunday. On Wednesday, Hutchins madecomments on Twitter that suggested he was at an airport getting ready to board a plane for a flight home. He never left Nevada.

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."

A Justice Department spokesman confirmed the 22-year-old Hutchins was arrested Wednesday in Las Vegas. Officer Rodrigo Pena, a police spokesman in Henderson, near Las Vegas, said Hutchins spent the night in federal custody in the city lockup.

Andrew Mabbitt, a British digital security specialist who had been staying in Las Vegas with Hutchins, said he and his friends grew worried when they got "radio silence" from Hutchins for hours. The worries deepened when Hutchins' mother called to tell him the young researcher hadn't made his flight home.

Mabbitt said he eventually found Hutchins' name on a detention center website. News of his indictment Thursday left colleagues scrambling to understand what happened.

"We don't know the evidence the FBI has against him, however we do have some circumstantial evidence that he was involved in that community at the time," said computer security expert Rob Graham.

The big question is the identity of the co-defendant in the case, whose name is redacted in the indictment. Why was it blacked out? "Maybe the other guy testified against him," said Graham.

The co-defendant allegedly advertised the malware online. Hutchins is accused of creating and transmitting the program.

Williams, the president of Rendition Infosec, speculated that the co-defendant might have been caught up in the takedown of AlphaBay and framed Hutchins in exchange for a plea deal.

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

Williams pointed to a July 13, 2014 tweet by Hutchins, whose moniker is @MalwareTechBlog, asking if anyone had a sample of Kronos to share.

"I've written code that other people have injected malware into," said Graham. "We know that large parts of Kronos were written by other people."

One legal scholar who specializes in studying computer crime 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.

"This is the first case I know of where the government is prosecuting someone for creating or selling malware but not actually using it," said Orin Kerr, a law professor at George Washington University. Kerr said it will be difficult to prove criminal intent.

"It's a constant issue in criminal law—the helping of people who are committing a crime," Kerr said. "When is that itself a crime?"

Citation: Hacker who helped stop global cyberattack arrested in US (Update) (2017, August 4) retrieved 3 May 2024 from https://phys.org/news/2017-08-hacker-ransomware.html