Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Man Who Stopped WannaCry Won't Cop To Kronos Malware

By **Allison Grande**

Law360, New York (August 14, 2017, 9:21 PM EDT) -- The British cybersecurity researcher who is credited with halting the global WannaCry ransomware attack pled not guilty Monday in Wisconsin federal court to charges that he helped to create and spread the Kronos banking Trojan malware, which harvested the private information of online banking users.

The plea entered by Marcus Hutchins at a hearing before U.S. Magistrate Judge William E. Duffin came less than two weeks after Hutchins was arrested on Aug. 2 in Las Vegas at the conclusion of Defcon, a popular annual international hacking conference that drew scores of security researchers, including Hutchins, to town.

Prosecutors claim that Hutchins was involved in the creation and dissemination of the Kronos banking Trojan that has been used since its creation in 2014 to harvest information related to banking systems in Canada, Germany, Poland, France and the United Kingdom. The 23-year-old gained notoriety in May after he inadvertently discovered and activated the "kill switch" that staunched the spread of the WannaCry malware that locked British hospitals, FedEx and scores of other global entities out of their data.

Brian Klein of Baker Marquart LLP, who is representing Hutchins, in a statement provided to Law360 Monday afternoon called his client "a brilliant young man and a hero."

"He plans to vigorously defend himself against these charges, and we are confident that when the evidence comes to light, he will be completely vindicated," Klein added.

Both Klein and co-counsel Marcia C. Hoffman of Zeitgeist Law PC said Monday on Twitter that they were "proud" and "delighted" to represent Hutchins.

Hutchins, who was released on a $30,000 secured cash bond, also took to Twitter following his court appearance Monday morning.

"I'm still on trial, still not allowed to go home, still on house arrest; but now i am allowed online," Hutchins wrote. "Will get my computers back soon."

Hutchins also expressed gratitude in one of his tweets for the "amazing support" he has received since

his arrest, which happened nearly a month after a grand jury returned a sealed indictment on July 11 that charged him with one count of conspiracy to commit computer fraud and abuse, three counts of distributing and advertising an electronic communication interception device, one count of endeavoring to intercept electronic communications, and one count of attempting to access a computer without authorization.

The charges are related to the spread of the Kronos banking Trojan, which prosecutors claim was built to yield and distribute the usernames and passwords for bank websites as they are entered into computers that have been infected with the virus. The information is then sent to a control panel operated by the hacker.

According to the U.S. Department of Justice, the virus surfaced on internet forums in early 2014, and Hutchins was allegedly involved with its creation and dissemination from July 2014 to July 2015.

Kronos was marketed through AlphaBay, a hidden service on the Tor network, which was shuttered after an investigation led by the U.S, the DOJ announced July 20, just nine days after the sealed Hutchins indictment.

Hutchins' arrest sent shock waves through the security research community, with participants expressing concerns over the lack of details in the indictment and the ripple effect the charges could have on those who work to find vulnerabilities in corporate systems to help companies and capitalize on bug bounty programs offered by Facebook, Google and a slew of other businesses.

Ron Austin, an associate professor at the School of Computing and Digital Technology at Birmingham City University, wrote in an Aug. 7 blog post that the Hutchins indictment "raises a number of issues between where the cybersecurity community is and where the law is in relation to researching and stopping attacks."

"Ethical hacking and bug hunting are required to keep the public safe," he continued. "If we are to start legal proceedings for researchers, then it’s a dark day for the industry. Being able to share information and code in good faith by helping other researchers is important for everyone."

Marcus Christian, a Mayer Brown LLP cybersecurity and data privacy partner and former federal prosecutor, told Law360 on Monday that the indictment indicates that the federal government is "certainly taking an increasingly assertive approach in the cybercrime area" and may serve to caution researchers that "if they are going to be engaged in behavior that arguably could be characterized as an offense, it's better to do that with a certain amount of forethought and planning rather than allow that behavior to be interpreted by people who don't understand or know your motives."

He also noted that the conduct attributed to Hutchins in the indictment dates back several years, and that both prosecutors and the court were likely to take into account his work in recent years, most notably his discovery of the WannaCry kill switch that likely shielded a multitude of companies from being infected.

"What the court is going to have to do is look at where we are now and the significant impact of his work with WannaCry, and I think the government will be amenable to that, too," Christian said, adding that developments in the case already, such as the relatively low bond amount and Hutchins' being allowed to access his computer again, show that the court likely "isn't concerned about his current conduct or worried that he poses a threat to society."

As the case moves forward, Christian said it will be important to watch whether the government tries to elicit help from Hutchins, given his reputation as a "clearly talented" security researcher.

"The ideas that one person can be committing crimes in one year and be helpful to prosecutors and law enforcement in the pursuit of justice the next are not incompatible," he said. "This is an area of a fast pace of change, so we'll have to hold onto our seats and watch what happens next."

Austin added that it was likely that the case would hinge on whether the FBI could prove that Hutchins wrote the code and if he intended to use it for material gain.

"The indictment has not provided many details and this may come out later if and when it proceeds to trial," Austin said. "However from what has been released at this time, it seems to be an odd case of a researcher being between a rock and a hard place, or as they say, no good deed goes unpunished."

Hutchins is represented by Brian E. Klein of Baker Marquart LLP and Marcia C. Hoffman of Zeitgeist Law PC.

The government is represented by Assistant U.S. Attorneys Michael J. Chmelar and Benjamin W. Proctor.

The case is U.S. v. Tran et al., case number 2:17-cr-00124, in the U.S. District Court for the Eastern District of Wisconsin.

--Editing by Breda Lund.
