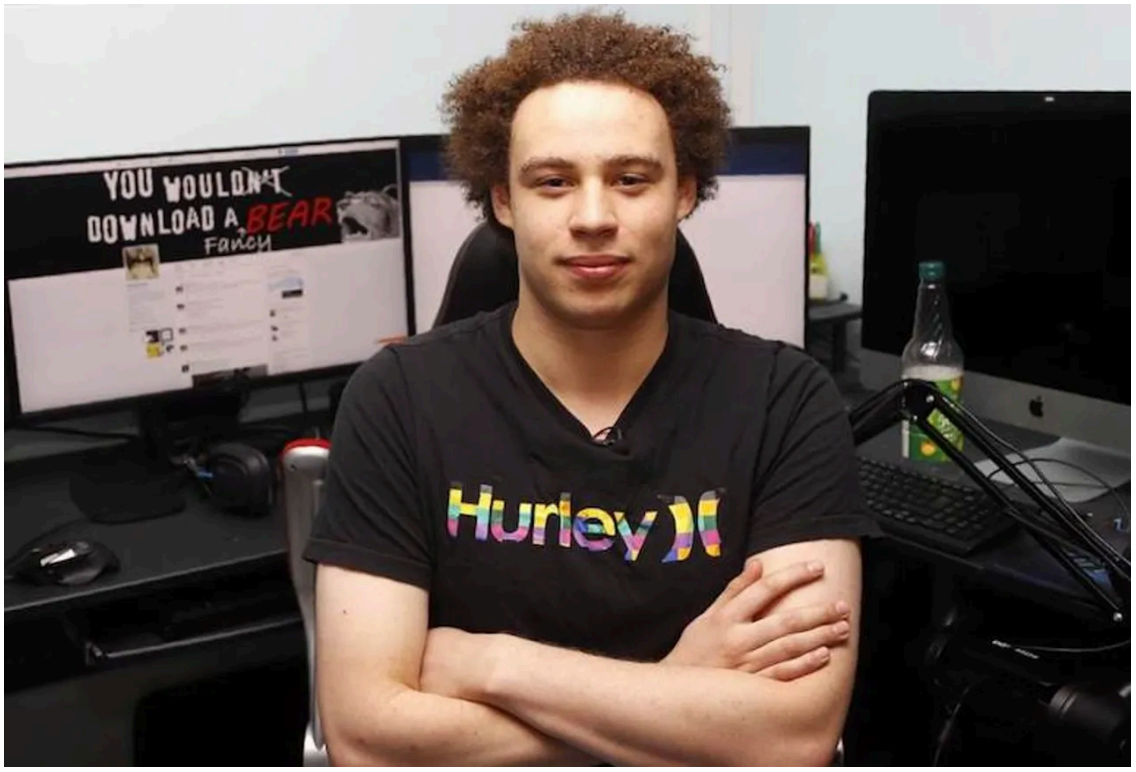
Security researcher MalwareTech pleads guilty

By Written by Catalin Cimpanu, ContributorContributor April 19, 2019 at 1:10 p.m. PT

Archived: 2026-04-05 16:36:01 UTC



Security

-
-
-
-

Marcus "MalwareTech" Hutchins, the British security researcher known for stopping the WannaCry ransomware outbreak, has pleaded guilty today to writing malware in the years prior to his prodigious career as a malware researcher.

"I regret these actions and accept full responsibility for my mistakes," Hutchins wrote in a statement posted on his website. "Having grown up, I've since been using the same skills that I misused several years ago for constructive purposes. I will continue to devote my time to keeping people safe from malware attacks."

Up to ten years in prison

According to court documents obtained by ZDNet, Hutchins pleaded guilty to two counts, and the government agreed to drop the other eight.

He pleaded guilty to entering a conspiracy to create and distribute malware, and in aiding and abetting its distribution.

For each count, Hutchins faces up to five years in prison, up to $250,000 in fines, and up to one year of supervised release.

US authorities arrested Hutchins at the Las Vegas international airport in August 2017, when the researcher was trying to return home to the UK after participating at the Black Hat and DEF CON security conferences.

Hutchins was charged with developing the Kronos and UPAS-Kit malware strains --two banking trojans.

He was also charged with working with a co-conspirator --identified only as "Vinny," "VinnyK," and "Aurora123"-- to advertise and sell the two malware strains online. This happened between July 2012 and September 2015, before Hutchins built a career as a talented security researcher.

Controversial case

Hutchins' arrest was controversial, and for many reasons. He argued that he was detained and interrogated while sleep-deprived and intoxicated, and that FBI agents misled him about the true intentions of the interrogation.

Further, his lawyers also argued that Hutchins' actions happened while he was still a minor, and outside the standard five-year statute of limitations.

The prosecution responded by piling new charges --such as developing the UPAS-Kit trojan (he was initially only charged with developing the Kronos malware) and with lying to the FBI during his interrogation. These later charges were deemed ludicrous by some US legal experts.

Ultimately, Hutchins' team failed in their attempt to suppress statements made during the FBI's interrogation following his arrest, and his case was locked for a jury trial in Madison, Wisconsin.

Hutchins' sentencing hearing has not been set.

See als

-

Helping the infosec community

After his arrest, Hutchins has been released on bail and has been living in Los Angeles while awaiting trial.

He was prohibited from working for his employer, US-based cyber-security firm Kryptos Logic, but Hutchins has turned his focus on sharing his malware analysis skills with the rest of the information security (infosec) community.

Over the course of the past one and a half year, Hutchins has been publishing written and video malware analysis tutorials. He is considered one of today's most talented security researchers.

> Hear! Hear! - Marcus has taught me a great deal during my journey with #emotet. I am still amazed that he has worked with me and the @Cryptolaemus1 team to help us with our battle. Without his help, we would still be in the stone age fighting this botnet!
>
> — Joseph Roosen (@JRoosen) April 19, 2019

Data leaks: The most common sources

Related malware and cybercrime coverage:

- Malvertising campaign abuses Chrome for iOS bug to target iPhone users
- Cyber-security firm Verint hit by ransomware
- Reveton ransomware distributor sentenced to six years in prison in the UK
- Scranos rootkit expands operations from China to the rest of the world
- Emotet hijacks email conversation threads to insert links to malware
- Source code of Iranian cyber-espionage tools leaked on Telegram
- How the United Nations helps fight global cybercrime **TechRepublic**
- Apple removed popular app that was secretly stealing your browser history **CNET**

Source: https://www.zdnet.com/article/security-researcher-malwaretech-pleads-guilty/