

WannaCry slayer, malware author Marcus Hutchins sentenced to time served

Enlarge / Hutchins, right, walks to court with his lawyers in 2017.

Joshua Lott/Getty Images

reader comments

20 with 14 posters participating, including story author

Share this story

British security expert and onetime malware developer Marcus Hutchins has been sentenced to time served, he announced in a Friday tweet.

Hutchins became famous in the security world in 2017 after he inadvertently stopped the WannaCry malware outbreak by registering a domain name that served as a kill switch for the sophisticated malware. Yet Hutchins, now in his mid-20s, had a dark past, having developed banking malware earlier in his life. At the time of his WannaCry efforts, Hutchins was already under investigation by US authorities for creating two banking trojans in the early 2010s.

Hutchins was arrested in August 2017 during a visit to the United States. He initially denied any role in developing malware. However, during his detention, federal prosecutors intercepted phone conversations in which he reportedly made incriminating statements. Under pressure from the authorities, Hutchins eventually came clean, admitting to his role in developing the malware. He took a plea deal in April.

"I regret these actions and accept full responsibility for my mistakes," Hutchins wrote at the time. "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."

Hutchins could have been sentenced to as many as 10 years in prison for his crimes. Instead, he received the lightest possible sentence: time served.

"Incredibly thankful for the understanding and leniency of the judge, the wonderful character letter you all sent, and everyone who helped me through the past two years, both financially and emotionally," Hutchinson wrote after the sentence was announced.

Hutchins developed malware for stealing banking info

Hutchins has admitted to developing two pieces of malware known as UPAS Kit and Kronos. Both pieces of software were banking trojans—Kronos was an updated version of UPAS Kit with expanded capabilities.

According to the prosecutor's sentencing memo in the case, Kronos was "designed to give the attacker the ability to steal banking credentials from victims' computers using a process called keylogging." The software could also grab data from Web forms filled out by a victim and inject malicious code into a website visited by the victim. It also included virtual network connection capabilities, allowing a hacker to remotely control a victim's computer.

Prosecutors said that Hutchins developed the software and relied on a pseudonymous co-conspirator known as "Vinny" to market it to the hacking underworld.

"Since 2014, Kronos has been used to infect numerous computers

around the world and steal banking information," prosecutors wrote. Kronos usage continues today.

Hutchins hoped to earn more than \$100,000 per year from the software, but he reportedly once complained to a friend that he wasn't making as much money as he expected. Now, he says he's going to devote his career to fighting against malware instead of creating it.

<https://arstechnica.com/?p=1542417>