THE CONVERSATION
Academic rigor, journalistic flair

MalwareTech’s arrest sheds light on the complex culture of the hacking world

August 9, 2017 8.10pm EDT

Which hat would you wear? crystalfoto/Shutterstock.com

The arrest of a British cybersecurity researcher on charges of disseminating malware and conspiring to commit computer fraud and abuse provides a window into the complexities of hacking culture.

In May, a person going by the nickname “MalwareTech” gained international fame – and near-universal praise – for figuring out how to slow, and ultimately effectively stop, the worldwide spread of the WannaCry malware attack. But in August, the person behind that nickname, Marcus Hutchins, was arrested on federal charges of writing and distributing a different malware attack first spotted back in 2014.

The judicial system will sort out whether Hutchins, who has denied wrongdoing and pleaded not guilty, will face as much as 40 years in prison. But to me as a sociologist studying the culture and social patterns of cybercrime, Hutchins’ experience is emblematic of the values, beliefs and practices of many hackers.

The hacker ethic

The term “hacking” has its origins in the 1950s and 1960s at MIT, where it was used as a positive label to describe someone who tinkers with computers. Indeed, the use of the word “hack,” signifying a clever or innovative use of something, is derived from this original meaning. Although the term may have originated at MIT, young people interested in computer technology were tinkering across the country. Technology journalist Steven Levy, in his well-regarded history of that period, writes that these early tinkerers were influenced by the countercultural milieu of the 1960s.

They developed a shared subculture, combining a disdain for tradition, a desire for an open society and optimistic views of how technology could transform people’s lives. Levy encapsulated this subculture into a series of beliefs he labeled the “hacker ethic.”

People who subscribe to the hacker ethic commonly have a disregard for traditional status markers,

Author

Roderick S. Graham
Assistant Professor of Sociology, Old Dominion University

like class, age or educational credentials. In this sense, hacking is open, democratic and based on ability. This particular belief has come under scrutiny as some scholars have argued that hacker culture discourages women from joining in. However, many hackers have taken nontraditional career paths, including Hutchins, whose computer skills are self-taught.

Another aspect of hacker subculture is interest in tinkering, changing, modifying and making things work differently or better. This has led to a great deal of innovation, including open-source programs being maintained by collections of coders and programmers – for free.

It is also this tinkering that allows hackers to find vulnerabilities in computers and software. It was through tinkering that Hutchins found a way to slow the WannaCry attack.

Different-colored hats

Members of the hacker subculture don't all agree on what they should do with those ideas. Typically, they're divided into three categories, with names inspired by the tropes of Western movies.

"Black hat" hackers are the bad guys. They find vulnerabilities in software and networks and exploit them to make money, whether by stealing data or encrypting data and holding the decryption key for ransom. They also create mischief and havoc, defacing websites and taking over Twitter feeds. The person, or people, who did what Hutchins is charged with – writing and distributing the Kronos malware – sought to hijack victims' banking information, break into their accounts and steal their money. That's a clear black hat activity.

"White hat" hackers are the good guys. They often work for technology companies, cybersecurity firms or government agencies, seeking to identify technological flaws and fix them. Some of them also use their skills to catch black hat hackers and shut down their operations, and even identify them so they can face legal repercussions. Hutchins, in his work as a researcher for the Kryptos Logic cybersecurity firm, was a white hat hacker.

A third group occupies a middle ground, that of the "gray hats." They are often freelancers looking to

identify exploits and vulnerabilities in systems for a varying range of purposes. Sometimes they may submit their findings to corporate or government programs intended to identify and fix problems; other times the same person may sell a new finding to a criminal.

What separates these three groups is not their actions – all three groups find weaknesses and tell someone else about them – but their motives. This makes hacking distinct from other types of criminal behavior: There are no “white hat” burglars or “gray hat” money launderers.

The importance of motivation is why many people are skeptical of the charges against Hutchins, at least at the moment. To hackers, whether someone is doing something wrong depends on what hat or hats he is wearing.

Is hacking a crime?

Prosecutions under the Computer Fraud and Abuse Act are not simple, mainly because the law addresses only actions, not motives. As a result, many things that white hat hackers do, such as public interest research reported in scholarly journals, may be illegal, if prosecutors decide to charge the people involved.

Hutchins’ arrest for his alleged association with the Kronos banking Trojan carries the clear suggestion that he’s a black hat. The charges say that in 2014 an as-yet-unnamed person allegedly posted a YouTube video showing how the attack worked, and then offered it for sale. Hutchins is linked because he and that other person allegedly updated the malware’s code sometime in 2015, after which the other person allegedly sold the malware at least once.

But Hutchins’ white hat job is to find vulnerabilities. Just as he tinkered with the WannaCry code – and found the way to slow it down – he could have been tinkering with the Kronos code. And even if he wrote Kronos – which the government alleges but has not yet proven – that’s not necessarily illegal: Orin Kerr, a George Washington University professor who studies the law of computer crimes, told the Guardian, “It’s not a crime to create malware. It’s not a crime to sell malware. It’s a crime to

sell malware with the intent to further someone else's crime."

Kerr's comments suggest a third explanation – that Hutchins may have been wearing a gray hat, creating malware for a criminal to use. But we're missing two key elements: proof of Hutchins' actions and any understanding of what his motives might have been. It's especially hard to be sure about his motives without knowing the details of any connection between Hutchins and the unnamed individual, nor even that person's identity.

It is too early to know what will happen to Marcus Hutchins. But there are precedents. In 1988, Robert Morris wrote the first worm malware while he was a graduate student at Cornell, and earned the dubious distinction of becoming the first person convicted under the Computer Fraud and Abuse Act. He is now a tenured professor at MIT.

Kevin Mitnick served five years in prison for various types of hacking. He now switches between white and gray hats – he is a security consultant and sells zero-day exploits to the highest bidder. And Mustafa Al-Bassam was once a member of the infamous LulzSec hacking group that hacked into the CIA and Sony. After serving a prison sentence, he completed a computer science degree and is now a security adviser. Hackers, unlike other criminals, can doff one hat and don another.

Hackers **Malware** **Ransomware** **Hacker**