PHYS.ORG

Arrest shines light on shadowy community of good, bad hackers (Update)

August 4 2017

```
  | VirusShare_2a3ac47662b55
  | VirusShare_a60f66d3470bfb
1 | VirusShare_fed774bd34f2f2
2 | VirusShare_3062a78971f05f
3 | VirusShare_5ef1fdd422951c
     VirusShare_
                 4799dfefb83a
```

The arrest of a security researcher by the FBI after the Def Con gathering of hackers has delivered a shock to the computer security community

Two months ago, Marcus Hutchins was an "accidental hero," a young computer whiz living with his parents in Britain who found the "kill switch" to the devastating WannaCry ransomware.

Today, the 23-year-old is in a US federal prison, charged with creating and distributing malicious software designed to attack the banking system.

His arrest this week stunned the computer security community and shines a light on the shadowy world of those who sometimes straddle the line between legal and illegal activities.

Hutchins' arrest following Def Con in Las Vegas, one of the world's largest gathering of hackers, delivered "an extreme shock," according to Gabriella Coleman, a McGill University professor who studies the hacker community.

"The community at Def Con would not admire a hacker who was doing hard-core criminal activity for profit or damage—that is frowned upon," Coleman told AFP.

"But there are people who do security research... who understand that sometimes in order to improve security, you have to stick your nose in areas that may break the law. They don't want to hurt anyone but they are doing it for research."

Hackers are generally classified as "white hats" if they stay within the law and "black hats" if they cross the line.

At gatherings like Def Con, "you have people who dabble on both sides of the fence," said Rick Holland, vice president at the security firm Digital Shadows.

An indictment unsealed by US authorities charges Hutchins and a second individual—whose name was redacted—of making and distributing in 2014 and 2015 the Kronos "banking Trojan," a reference to malicious software designed to steal user names and passwords used at online banking sites.

Hacker mindset

James Scott, a senior fellow who follows cybersecurity at the Institute for Critical Infrastructure Technology, said it is sometimes difficult to separate the white hats from the black hats.

The hacker mindset includes "an insatiable need to satisfy their intellectual curiosity," Scott said.

"Hackers have that thing, they can't sleep. It's persistent and it's constant and it can drive you nuts."

Scott said he did not know details of the Hutchins case but that it is possible he wrote code that someone else "weaponized."

Rob Graham of Errata Security said he came to a similar conclusion, that Hutchins "wrote some code, but everything else was done by the other guy... As a writer of code sometimes used in viruses, this worries me."

Members of the hacker community may "dabble on both sides of the fence," one analyst says

Friends and collaborators of Hutchins—known by his online moniker "Malwaretech"—said they found the allegations hard to believe.

"He worked with me on a project in 2014 he refused payment for," said a tweet from Jake Williams of Rendition InfoSec. "This is incongruous with a black hat writing code for money at the same time."

Security researcher Andrew Mabbitt tweeted that Hutchins "spent his career stopping malware, not writing it."

'More circumspect'

Regardless of the outcome of the case, some security professionals said the arrest could erode trust between the hacker community and law enforcement.

Coleman said hackers and researchers already tread carefully in light of the Computer Fraud and Abuse Act, a law that makes it illegal to access a computer system without authorization and has been roundly criticized by some security professionals.

"The statute is very broad and it can be wielded as a tool against researchers," Coleman said.

She noted that many in the hacker community are still reeling over the 2013 suicide of activist Aaron Swartz, who was charged under the same law for illegally downloading academic journals.

Hutchins' arrest "might actually drive certain security researchers further underground," said John Dickson of Denim Group, a security consultancy.

"I know several security researchers from Europe, whom I consider on the 'white hat' side of the house, who will no longer travel to the US to be on the safe side."

Holland of Digital Shadows added that the news "could make people more circumspect about who they may collaborate with."

Scott said the arrest may be counterproductive for cybersecurity because hackers like Hutchins help expose security flaws in order to fix them.

"The establishment needs hackers more than hackers need the establishment," he said.

Scott added that Hutchins' obvious talents could make him an asset for national security instead of a liability.

"I wouldn't be surprised if a federal agency made him an offer he can't refuse," Scott said.

"A guy like that should be at Fort Meade," he added, referring to the headquarters of the National Security Agency.

Citation: Arrest shines light on shadowy community of good, bad hackers (Update) (2017, August 4) retrieved 25 April 2024 from https://phys.org/news/2017-08-shadowy-good-bad-hackers.html