Whiz kid who foiled cyberattack

May 16 2017, by Julie Charpentrat

The young cyber security researcher known only by his Twitter handle @MalwareTechBlog, says he found a way of slowing the spread of WannaCry by chance

They are called white hats—the good guys in the Wild West of the internet—and they ride to the rescue as in the case of the 22-year-old British expert who helped stop the WannaCry cyberattack.

The young cyber security researcher, known only by his Twitter handle @MalwareTechBlog, says he found a weakness by chance that allowed

slowing the spread of WannaCry, a type of malware called ransomware that encrypts files on an infected computer and demands money to unlock them.

Britain's National Cyber Security Centre (NCSC) published his discovery, but also noted he was not an employee.

British media reported that he is employed in a cyber security firm and that he wishes to remain anonymous.

"He clearly succeeded in halting the spread" of WannaCry, said cyber security expert Marco Cova at Lastline.

According to Europol, the situation is now stable in Europe.

In China, which was also hard hit, the spread of the malware has slowed considerably according to authorities.

@MalwareTechBlog "stopped WannaCry by finding the 'kill switch' that the hackers introduced into the virus themselves to stop it if necessary," said Nicolas Godier, a cyber security expert at Proofpoint.

Godier said the British researcher worked closely with cyber security company Proofpoint expert Darien Huss over the weekend.

Contrary to the image of solitary hackers conversing through encrypted messages, the computer experts communicate most often through Twitter, according to Godier.

"All day long they analyse strains of computer viruses to see how they function" and find ways to stop them, said Godier.

"If each works in his own corner, it isn't effective, so they share their

research. And with social networks, it moves quickly."

In this case it only took them several hours to find a weakness, said Godier.

'White hat' vs 'Black hat'

The hackers who launch attacks and the cyber security experts who parry them have largely the same skills.

"In a certain way there are white knights and black knights" in cyber security, said Godier.

More often the terms are drawn from Westerns.

"The white hat is a researcher that does work for the good of the industry/society, the black hat's motivation is more nefarious in nature," said Raj Samani, Chief Scientist at McAfee, a leading producer of antivirus software.

They are in a perpetual race to discover vulnerabilities in software, which hackers will exploit to profit from while cyber security experts will develop solutions to protect their clients and the public.

In addition to the pride of a job well done, good publicity that comes from foiling a massive cyberattack can boost the reputation of white hats such as @MalwareTechBlog.

It can help them increase their circle of collaborators, thus improving their work.

The attention can also help a researcher get a job in a cyber security firm, if they don't already have one.

The same can be true for negative publicity, providing some hackers the opportunity to switch sides and join reputable firms.

Sued by Sony for hacking the PlayStation 3 games console, George Hotz was later recruited by Facebook in 2011.

Citation: Whiz kid who foiled cyberattack (2017, May 16) retrieved 28 April 2024 from https://phys.org/news/2017-05-whiz-kid-foiled-cyberattack.html