《近百国遭黑客攻击 英国小哥意外阻止勒索病毒蔓延》

近百国遭黑客攻击 英国小哥意外阻止勒索病毒蔓延

??????????????????????—???MalwareTech?????????????????????“????”??12???1400?????????????8.29??:“????????????????????????????????????”??twitter?????“??” MalwareTech?????“????”

An anonymous internet blogger, who asked to be known only by his online alias Malware Tech, stumbled on the "off switch" that halted an attack by a ransomware virus that affected computer systems in over 100 countries, the BBC reported, citing an interview with the man.

His discovery halted the virus, which freezes computer systems and access to files unless a cash ransom is paid, but will not repair any damage already done, he said.

The blogger, who works for a UK Internet security company, was on a week's holiday when he heard about the virus and decided to check it out.

He told the BBC he saw that each time the virus entered a new computer system, it would try and contact a specific web address, which he discovered was unregistered. He immediately acquired it for eight pounds.

His ownership of the site meant his investigations accidentally triggered the "off switch" and halted the further spread of the virus, which hit Britain's National Health Service, Nissan's car plant in northern England, Spanish telecoms giant Telefonica, Spanish energy company Iberdrola and Russian government ministries, the BBC reported.

MalwareTech now thinks the code was originally designed to thwart researchers trying to investigate the ransomware, but it backfired by letting them remotely disable it.

"It was actually partly accidental," he told the BBC, after spending the night investigating. "I have not slept a wink."

He added that his boss had given him an extra week off to recover from what he called "a train wreck of a holiday."

Security experts said that new variants of the malware that ignore the "kill switch" will appear.

"This variant shouldn't be spreading any further, however there'll almost certainly be copycats," said security researcher Troy Hunt, according to the BBC.

MalwareTech warned: "We have stopped this one, but there will be another one coming and it will not be stoppable by us.

"There's a lot of money in this, there is no reason for them to stop. It's not much effort for them to change the code and start over."

简答网 —jiandongshicai.cn—