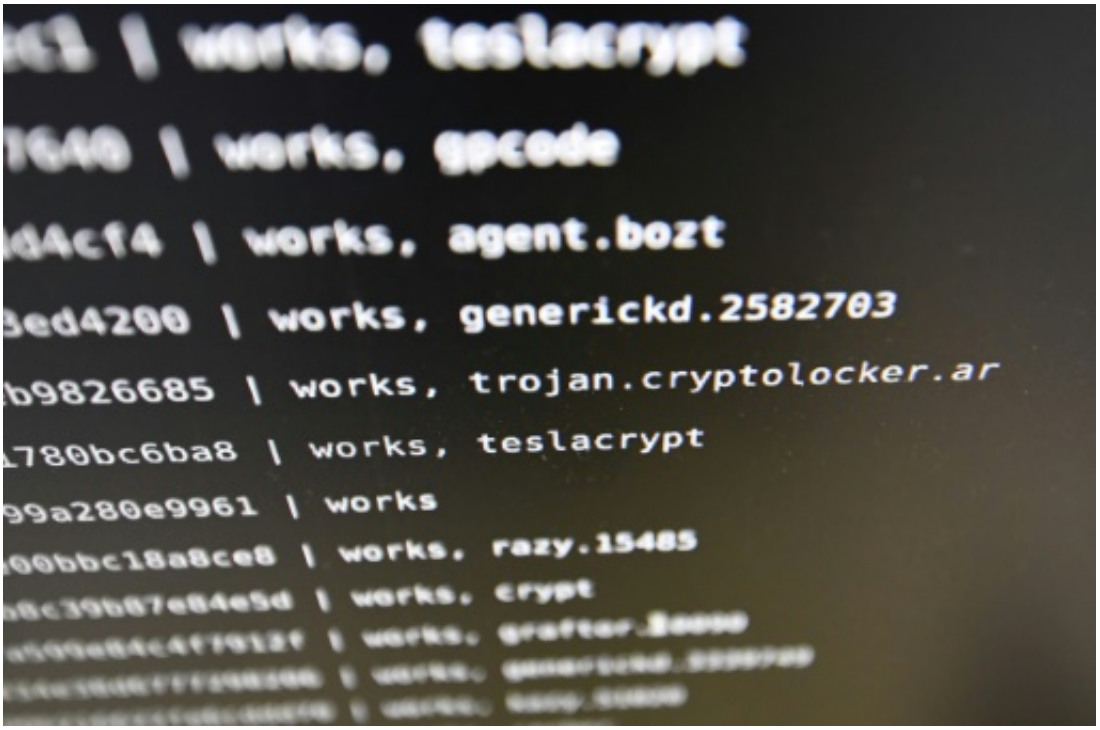
Another large-scale cyberattack underway: experts

May 17 2017



Adylkuzz is believed to have infected more computers than WannaCry, using the same vulnerabilities

Another large-scale, stealthy cyberattack is underway on a scale that could dwarf last week's assault on computers worldwide, a global cybersecurity firm told AFP on Wednesday.

The new attack targets the same vulnerabilities the WannaCry

ransomware worm exploited but, rather than freeze files, uses the hundreds of thousands of computers believed to have been infected to mine virtual currency.

Following the detection of the WannaCry attack on Friday, "researchers at Proofpoint discovered a new attack linked to WannaCry called Adylkuzz," said Nicolas Godier, a researcher at the computer security firm.

"It uses the hacking tools recently disclosed by the NSA and which have since been fixed by Microsoft in a more stealthy manner and for a different purpose," he said.

Instead of completely disabling an infected computer by encrypting data and seeking a ransom payment, Adylkuzz uses the machines it infects to "mine" in a background task a virtual currency, Monero, and transfer the money created to the authors of the virus.

Virtual currencies such as Monero and Bitcoin use the computers of volunteers for recording transactions. They are said to "mine" for the currency and are occasionally rewarded with a piece of it.

Proofpoint said in a blog that symptoms of the attack include loss of access to shared Windows resources and degradation of PC and server performance, effects which some users may not notice immediately.

"As it is silent and doesn't trouble the user, the Adylkuzz attack is much more profitable for the cyber criminals. It transforms the infected users into unwitting financial supporters of their attackers," said Godier.

Proofpoint said it has detected infected machines that have transferred several thousand dollars worth of Monero to the creators of the virus.

The firm believes Adylkuzz has been on the loose since at least May 2, and perhaps even since April 24, but due to its stealthy nature was not immediately detected.

"We don't know how big it is" but "it's much bigger than WannaCry", Proofpoint's vice president for email products, Robert Holmes, told AFP.

A US official on Tuesday put the number of computers infected by WannaCry at over 300,000.

"We have seen that before—malwares mining cryptocurrency—but not this scale," said Holmes.

The WannaCry attack has sparked havoc in computer systems worldwide.

Britain's National Health Service, US package delivery giant FedEx, Spanish telecoms giant Telefonica and Germany's Deutsche Bahn rail network were among those hit.