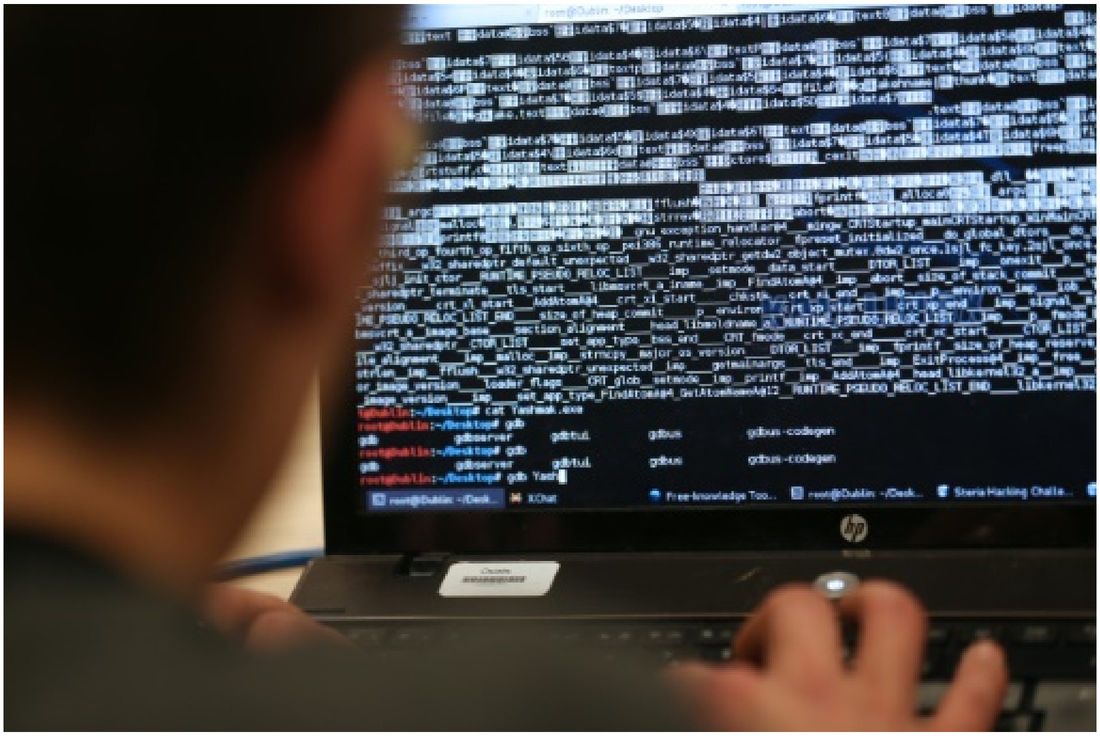
PHYS.ORG

Police, cyber firms tackle 'ransomware' hacking threat

July 25 2016, by Jan Hennop



The website www.nomoreransom.org offers advice on how to avoid data being taken hostage by ransomware, as well as more than 160,000 decryption keys in the event of a computer being infected

Dutch police, Europol and a coalition of cyber security firms launched a new website Monday to fight a surge in "ransomware" which locks users' data until they pay criminals to retrieve it.

The "No More Ransom" initiative is the new online portal "aimed at informing the public about the dangers of ransomware and helping victims to recover their data without having to pay ransoms to cyber criminals," said a combined statement, issued from Europol's Hague-based headquarters.

The website www.nomoreransom.org offers advice on how to avoid data being taken hostage by ransomware, as well as more than 160,000 decryption keys in the event of a computer being infected.

Hackers have been stepping up efforts to turn their exploits into hard cash in recent years by locking unsuspecting computer users' data after infecting their computers with malicious software.

Kaspersky Lab, one of the tech firms supporting the project, said the number of victims attacked by so-called crypto-ransomware was growing by an alarming rate—rising from 131,000 in 2014-15 to 718,000 in 2015-16.

"Ransomware is a top threat for EU law enforcement," added Monday's statement. "Almost two-thirds of EU member states are conducting investigations into this form of attack."

'Supporting the criminals' business'

Chief technical officer Steve Grobman from Intel Security, one of the other tech firms involved in the scheme, said in March the practice is growing due to several factors—easy access to necessary software, criminal networks which offer the service, and the difficulty of tracking down the culprits who are able to hide in anonymous networks.

One of the latest malicious programmes targeted by the combined law enforcement and the coalition of tech firms is the so-called "Shade" ransomware.

"Shade" is spread via malicious websites and infected email attachments and uses a strong algorithm for each encrypted file, encrypting not only the file's content, but the file name as well.

Kaspersky Lab and Intel Security prevented more than 27,000 attempts since 2014 to attack users with "Shade" ransomware.

"Most infections occurred in Russia, Ukraine, Germany, Austria and Kazakhstan. Shade activity was also registered in France, the Czech Republic, Italy and the United States," the statement added.

It warns victims not to pay ransoms should their computers become infected with ransomware but to immediately report it to the authorities.

"By making the payment you will be supporting the criminals' business. Plus, there is no guarantee that paying the fine will give you back access to the encrypted data," it said.

Citation: Police, cyber firms tackle 'ransomware' hacking threat (2016, July 25) retrieved 25 April 2024 from https://phys.org/news/2016-07-police-cyber-firms-tackle-ransomware.html