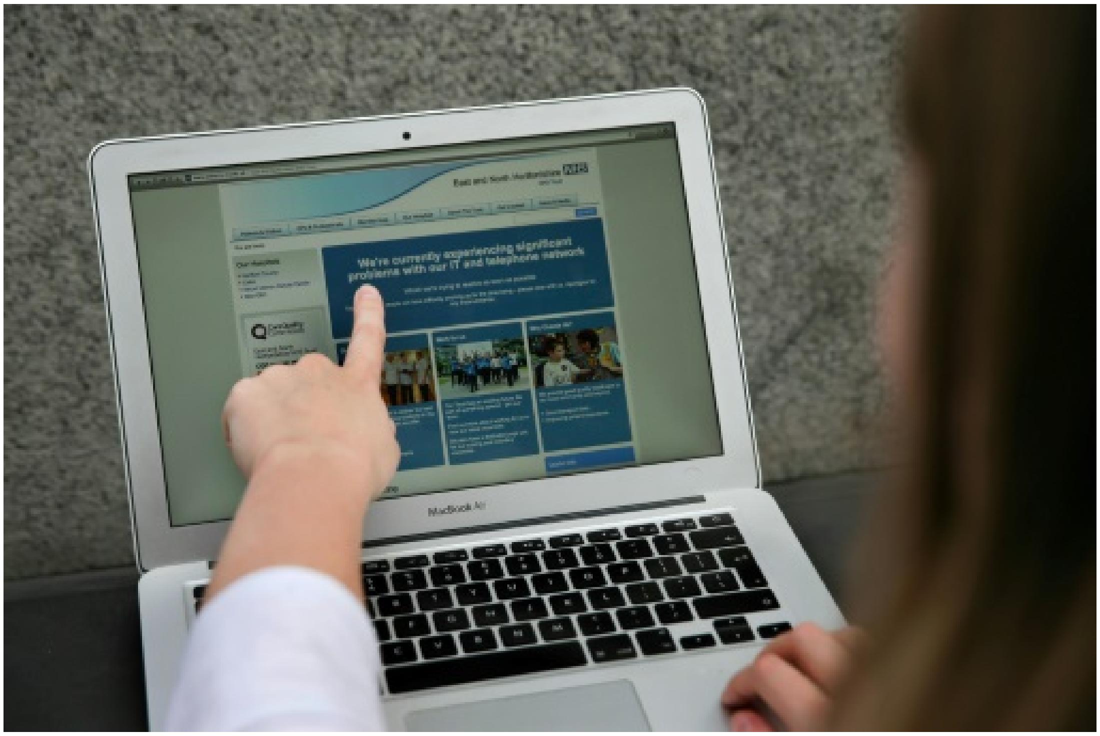
# Researcher finds 'kill switch' for cyberattack ransomeware

May 13 2017, by Kate Bartlett



We're currently experiencing significant problems with our IT and telephone network

A cybersecurity researcher appears to have discovered a "kill switch" that can prevent the spread of the WannaCry ransomware—for now—that has caused the cyberattacks wreaking havoc globally

A cybersecurity researcher appears to have discovered a "kill switch" that can prevent the spread of the WannaCry ransomware—for now—that has caused the cyberattacks wreaking havoc globally, they told AFP Saturday.

The researcher, tweeting as @MalwareTechBlog, said the discovery was accidental, but that registering a domain name used by the malware stops it from spreading.

"Essentially they relied on a domain not being registered and by registering it, we stopped their malware spreading," @MalwareTechBlog told AFP in a private message on Twitter.

The researcher warned however that people "need to update their systems ASAP" to avoid attack.

"The crisis isn't over, they can always change the code and try again," @MalwareTechBlog said.

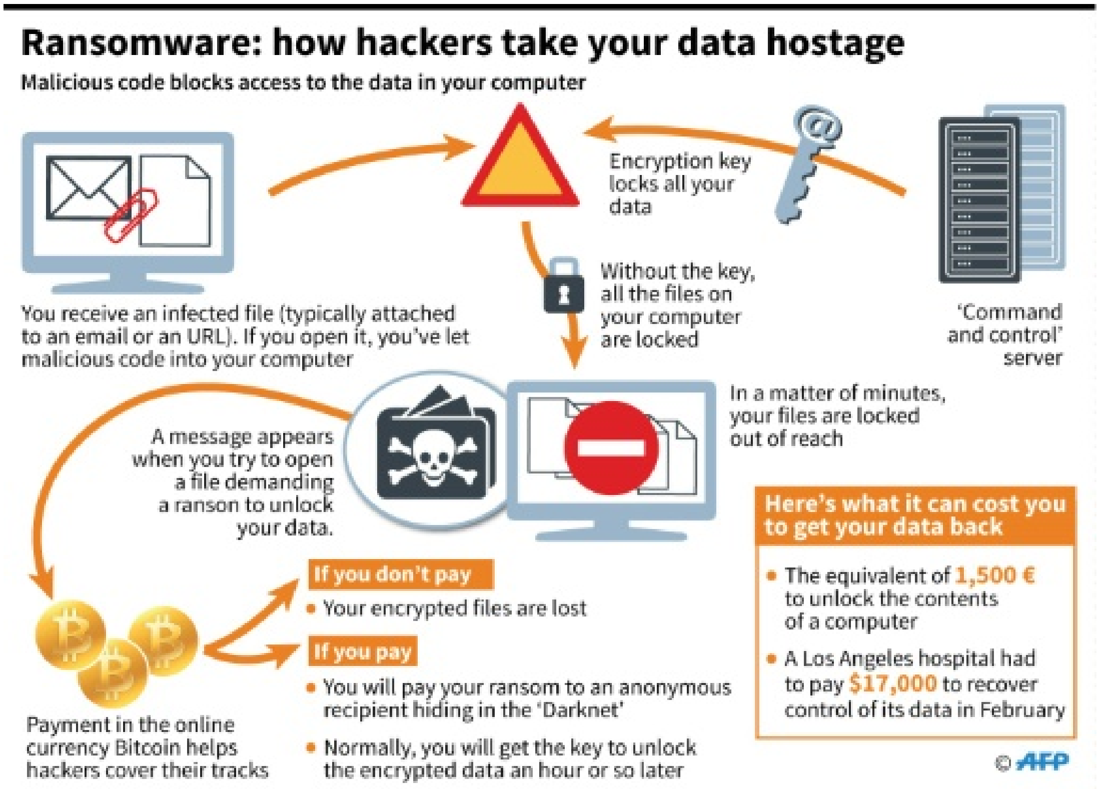
Friday's wave of cyberattacks, which affected dozens of countries, apparently exploited a flaw exposed in documents leaked from the US National Security Agency.

The attacks used a technique known as ransomware that locks users' files unless they pay the attackers a designated sum in the virtual currency Bitcoin.

Affected by the onslaught were computer networks at hospitals in Britain, Russia's interior ministry, the Spanish telecom giant Telefonica and the US delivery firm FedEx and many other organisations.

French carmaker Renault also announced it was attacked. A spokeswoman said the company was "doing what is needed to counter this attack."

"I will confess that I was unaware registering the domain would stop the malware until after I registered it, so initially it was accidental," @MalwareTechBlog tweeted.


Ransomware: how hackers take your data hostage
Malicious code blocks access to the data in your computer
You receive an infected file (typically attached to an email or an URL). If you open it, you've let malicious code into your computer
Encryption key locks all your data
'Command and control' server
Without the key, all the files on your computer are locked
In a matter of minutes, your files are locked out of reach
A message appears when you try to open a file demanding a ranson to unlock your data.
Payment in the online currency Bitcoin helps hackers cover their tracks
If you don't pay
• Your encrypted files are lost
If you pay
• You will pay your ransom to an anonymous recipient hiding in the 'Darknet'
• Normally, you will get the key to unlock the encrypted data an hour or so later
Here's what it can cost you to get your data back
• The equivalent of 1,500 € to unlock the contents of a computer
• A Los Angeles hospital had to pay $17,000 to recover control of its data in February
© AFP

Ransomware: how hackers take your data hostage

Unfortunately however, computers already affected will not be helped by the solution.

"So long as the domain isn't revoked, this particular strain will no longer cause harm, but patch your systems ASAP as they will try again."

The malware's name is WCry, but analysts were also using variants such as WannaCry.

Forcepoint Security Labs said in a Friday statement that the attack had "global scope" and was affecting networks in Australia, Belgium, France, Germany, Italy and Mexico.

In the United States, FedEx acknowledged it had been hit by malware and was "implementing remediation steps as quickly as possible."

Also badly hit was Britain's National Health Service, which declared a "major incident" after the attack, which forced some hospitals to divert ambulances and scrap operations.

Pictures posted on social media showed screens of NHS computers with images demanding payment of $300 (275 euros) in Bitcoin, saying: "Ooops, your files have been encrypted!"

It demands payment in three days or the price is doubled, and if none is received in seven days, the files will be deleted, according to the screen message.

A hacking group called Shadow Brokers released the malware in April claiming to have discovered the flaw from the NSA, according to Kaspersky Lab, a Russian cybersecurity provider.

Kaspersky researcher Costin Raiu cited 45,000 attacks in 74 countries as of Friday evening.

Citation: Researcher finds 'kill switch' for cyberattack ransomeware (2017, May 13) retrieved 3 May 2024 from https://phys.org/news/2017-05-cyberattack-ransomeware.html