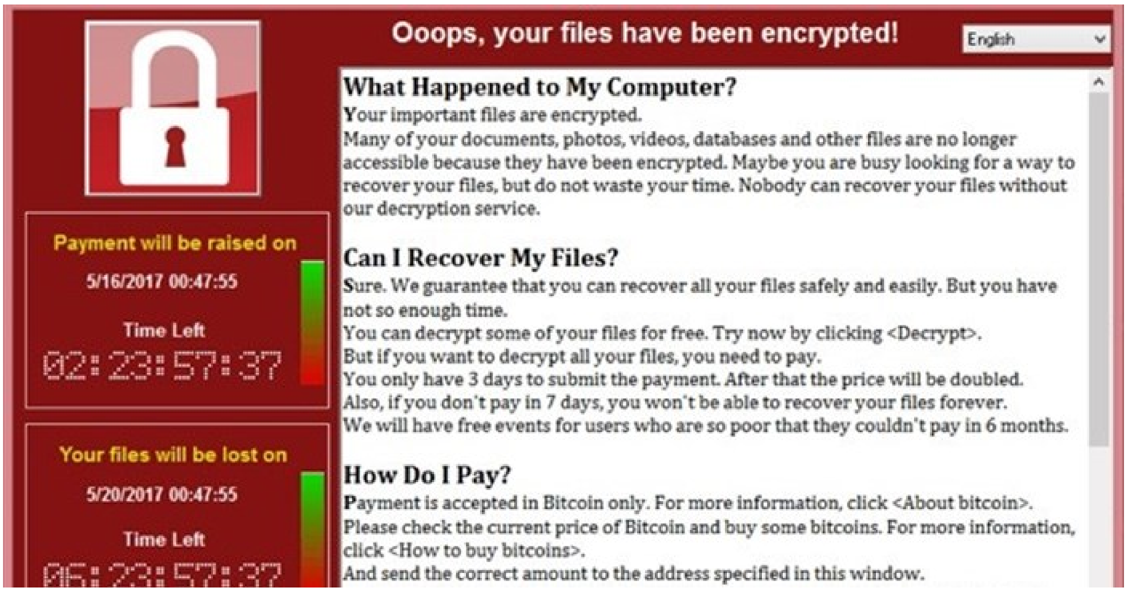
BIZCOMMUNITY

Fast-moving cyber attacks wreak havoc worldwide

WASHINGTON, US: A fast-moving wave of cyber attacks swept the globe on Friday, apparently exploiting a flaw exposed in documents leaked from the US National Security Agency.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Image via Wikimedia

The attacks - which experts said affected dozens of countries - 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 organizations.

"International attack"

Britain's National Cyber Security Centre and its National Crime Agency were looking into the UK incidents, which disrupted care at National Health Service facilities.

"This is not targeted at the NHS, it's an international attack and a number of countries and organisations have been affected," British Prime Minister Theresa May said.

Russia's interior ministry said that some of its computers had been hit by a "virus attack" and that efforts were underway to destroy it.

The US Department of Homeland Security's computer emergency response team said it was aware of ransomware infections "in several countries around the world."

"More than 75,000 detections"

Jakub Kroustek of the security firm Avast said in a blog post update around 2000 GMT, "We are now seeing more than 75,000 detections... in 99 countries."

Kaspersky researcher Costin Raiu cited 45,000 attacks in 74 countries, saying that the malware, a self-replicating "worm," was spreading quickly.

In a statement, Kaspersky Labs said it was "trying to determine whether it is possible to decrypt data locked in the attack -- with the aim of developing a decryption tool as soon as possible."

"Kill switch"

On Saturday, a cybersecurity researcher told AFP he had accidentally discovered a "kill switch" that can prevent the spread of the ransomware.

The researcher, tweeting as @MalwareTechBlog, said the discovery was accidental, but that registering a domain name used by the malware stops it from spreading. Computers already affected will not be helped by the solution.

However @MalwareTechBlog warned that the "crisis isn't over" as those behind it "can always change the code and try again".

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

"It's unequivocally scary," said John Dickson of the Denim Group, a US security consultancy.

Dickson said the malware itself, which exploits a flaw in Windows, was not new but that adding the ransomware "payload" made it especially dangerous.

"I'm watching how far this propagates and when governments get involved," he said.

Forcepoint Security Labs said in a 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."

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

Germany's Deutsche Bahn computers were also impacted, with the company reporting on Saturday morning that display panels in the stations were affected.

"Ooops, your files have been encrypted!"

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, Kaspersky said.

Although Microsoft released a security patch for the flaw earlier this year, many systems have yet to be updated, researchers said.

"Unlike most other attacks, this malware is spreading primarily by direct infection from machine to machine on local networks, rather than purely by email," Lance Cottrell, chief scientist at the US technology group Ntrepid.

"The ransomware can spread without anyone opening an email or clicking on a link."

Growing ransom demands

The sort of ransom demands have been growing precedent at medical facilities. In February 2016, a Los Angeles hospital, the Hollywood Presbyterian Medical Center, paid $17,000 in Bitcoin to hackers who took control of its computers for more than a week.

"Ransomware becomes particularly nasty when it infects institutions like hospitals, where it can put people's lives in danger," said Kroustek, the Avast analyst.

A spokesman for Barts Health NHS Trust in London said it was experiencing "major IT disruption" and delays at all four of its hospitals.

"Ambulances are being diverted to neighboring hospitals," the spokesman said.

Two employees at St Bartholomew's Hospital, which is part of Barts Health, told AFP that all the computers in the hospital had been turned off.

Some said the attacks highlighted the need for agencies like the NSA to disclose security flaws so they can be patched.

"These attacks underscore the fact that vulnerabilities will be exploited not just by our security agencies, but by hackers and criminals around the world," said Patrick Toomey of the American Civil Liberties Union.

Source: AFP