Worldwide ransomware cyberattacks: What we know

May 14 2017

A computer technician connects a computer into a network server in an office building in Washington, DC on May 13, 2017

Computers in more than 150 countries have been hit by what experts are calling an unprecedented mass cyberattack using ransomware.

Experts were scrambling to determine who was behind the attack, which exploited a security flaw in older versions of Microsoft's Windows

operating software.

Here is what we know so far about the cyber ransom attacks:

What happened?

Computers around the globe were hacked beginning on Friday using a security flaw in Microsoft's Windows XP operating system, an older version that was no longer given mainstream tech support by the US giant.

The so-called WannaCry ransomware locks access to user files and demands money—in the form of the virtual currency Bitcoin—in order to decrypt them.

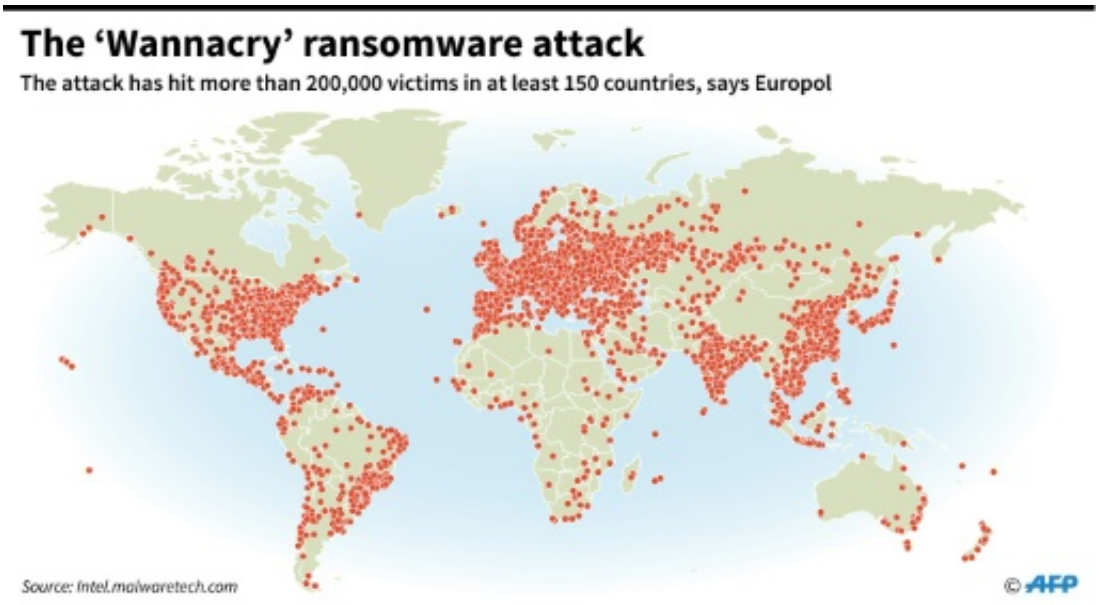
How many countries were affected?

Europol chief Rob Wainwright said more than 200,000 victims had been hit in more than 150 countries.

It is the largest ransomware attack observed in history.

High-profile victims include hospitals in Britain, the Spanish telecoms giant Telefonica, French carmaker Renault, US package delivery company FedEx, Russia's interior ministry and the German rail operator Deutsche Bahn.

How did the attack spread worldwide?



A computer technician connects a computer into a network server in an office building in Washington, DC on May 13, 2017

Experts said the ransomware programme appears to support dozens of languages, showing that the hackers wanted to corrupt networks worldwide.

The virus spread quickly because the culprits used a digital code believed to have been developed by the US National Security Agency—and subsequently leaked as part of a document dump, according to researchers at the Moscow-based computer security firm Kaspersky Lab.

The attack is unique, according to Wainwright, because it combines ransomware with a worm function, meaning once one machine is infected, the entire internal network is scanned and other vulnerable machines are infected.

The US security firm Symantec said the attack appeared to be

indiscriminate.

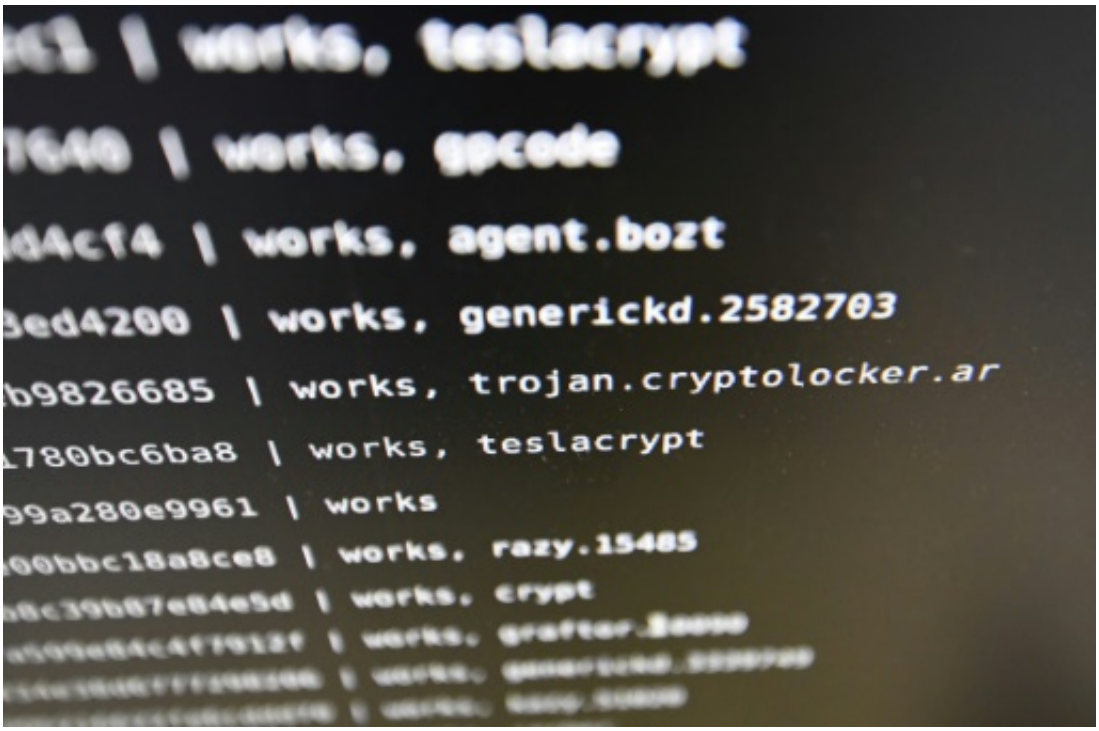
Who was behind the attack?

So far, the culprits are unknown, as is the motivation. Security agencies in affected countries were racing to find out.

Experts think it unlikely to have been one person, with criminally minded cyber crime syndicates nowadays going underground and using ever more sophisticated encryption to hide their activities.

How can people protect their computers?

Microsoft took the unusual step of reissuing security patches first made available in March for Windows XP and other older versions of its operating system.



The wave of attacks on May 12 hit Britain's health service, Russia's interior ministry and French carmaker Renault, along with many other organisations around the world

Kaspersky said it was seeking to develop a decryption tool "as soon as possible".

Europol provides free decryption downloads for most ransomware already detected, though not yet for this particular attack.

How much ransom was asked?

Victims were asked for payment of $300 (275 euros) in the virtual currency Bitcoin.

Payment is demanded within three days or the price is doubled, and if none is received within seven days, the files will be deleted, according to the screen message.

Given the attack's widespread nature, even such a small sum would stack up quickly, though few victims seem to be paying up so far.

Experts advise people not to pay, as it would only encourage the attackers, there is no guarantee that they will unblock files, and may result in them gaining access to victims' bank details.

Citation: Worldwide ransomware cyberattacks: What we know (2017, May 14) retrieved 19 September 2024 from https://phys.org/news/2017-05-worldwide-ransomware-cyberattacks.html