

Fast-moving cyberattacks wreak havoc worldwide (Update 3)

12 May 2017, by Rob Lever, With Robin Millard In London



Britain's National Health Service reported a cyber attack on a number of hospitals on May 12, 2017

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

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.

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 organizations 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."

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."

'Unequivocally scary'

"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.

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

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.

Message to users: 'Oops'

Pictures posted on social media showed screens of NHS computers with images demanding payment of \$300 (275 euros) in Bitcoin, saying: "Oops, 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."

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.

"We have activated our major incident plan to make sure we can maintain the safety and welfare of patients," the spokesman said. "Ambulances are being diverted to neighboring hospitals."

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.

Caroline Brennan, 41, went to the hospital to see her brother, who had open heart surgery.

"They told us there was a problem. They said the system was down and that they cannot transfer anyone till the computer system was back up," Brennan said.

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.

© 2017 AFP

APA citation: Fast-moving cyberattacks wreak havoc worldwide (Update 3) (2017, May 12) retrieved 13 April 2021 from <https://phys.org/news/2017-05-global-cyber-british-hospitals-spanish.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.