

Huge cyberattack forces Microsoft to offer free tech fix

May 13 2017, by Sylvia Hui And Jim Heintz



An exterior view shows the main entrance of St Bartholomew's Hospital, in London, one of the hospitals whose computer systems were affected by a cyberattack, Friday, May 12, 2017. A large cyberattack crippled computer systems at hospitals across England on Friday, with appointments canceled, phone lines down and patients turned away. (AP Photo/Matt Dunham)

Teams of technicians worked "round the clock" Saturday to [restore hospital computer systems](#) in Britain and check bank or transport

services in other nations after a global cyberattack hit dozens of countries and crippled the U.K.'s health system.

The worldwide attack was so unprecedented that Microsoft quickly changed its policy and announced that it will make security fixes available for free for older Windows systems, which are still used by millions of individuals and smaller businesses.

In Russia, where a wide array of systems came under attack, officials said services had been restored or the virus contained.

The extortion attack, which locked up computers and held users' files for ransom, is believed to be the biggest of its kind ever recorded, disrupting services in nations as diverse as the U.S., Russia, Ukraine, Spain and India.

Europol, the European Union's police agency, said the onslaught was at "an unprecedented level and will require a complex international investigation to identify the culprits."

The ransomware appeared to exploit a vulnerability in Microsoft Windows that was purportedly identified by the U.S. National Security Agency for its own intelligence-gathering purposes and was later leaked to the internet.

Before Friday's attack, Microsoft had made fixes for older systems, such as 2001's Windows XP, available only to mostly larger organizations that paid extra for extended technical support. Microsoft says now it will make the fixes free for everyone.

It was not yet known who perpetrated Friday's [attacks](#). Two security firms—Kaspersky Lab and Avast—said they had identified the malicious software behind the attack in over 70 countries, although both

said the attack had hit Russia the hardest.

In Britain, the National Cyber Security Center said it is "working round the clock" with experts to restore vital health services.



A security guard stands outside the Telefonica headquarters in Madrid, Spain, Friday, May 12, 2017. The Spanish government said several companies including Telefonica had been targeted in ransomware cyberattack that affected the Windows operating system of employees' computers. (AP Photo/Paul White)

British Home Secretary Amber Rudd—who was chairing a government emergency security meeting Saturday in response to the attack—said 45 [public health organizations](#) were hit, though she stressed that no patient data had been stolen. The attack froze computers at hospitals across the country, with some canceling all routine procedures. Patients were asked

not to go to hospitals unless it was an emergency and even some key services like chemotherapy were canceled.

Security officials in Britain urged organizations to protect themselves from ransomware by updating their security software fixes, running anti-virus software and backing up data elsewhere.

The Russian Interior Ministry, which runs the country's police, confirmed it was among those that fell victim to the ransomware, which typically flashes a message demanding a payment to release the user's own data.

Ministry spokeswoman Irina Volk was quoted by the Interfax news agency Saturday as saying the problem had been "localized" and that no information was compromised. But the ministry's website still carried a banner on Saturday afternoon saying that technical work was continuing.

A spokesman for the Russian Health Ministry, Nikita Odintsov, said on Twitter that the cyberattacks on his ministry were "effectively repelled."

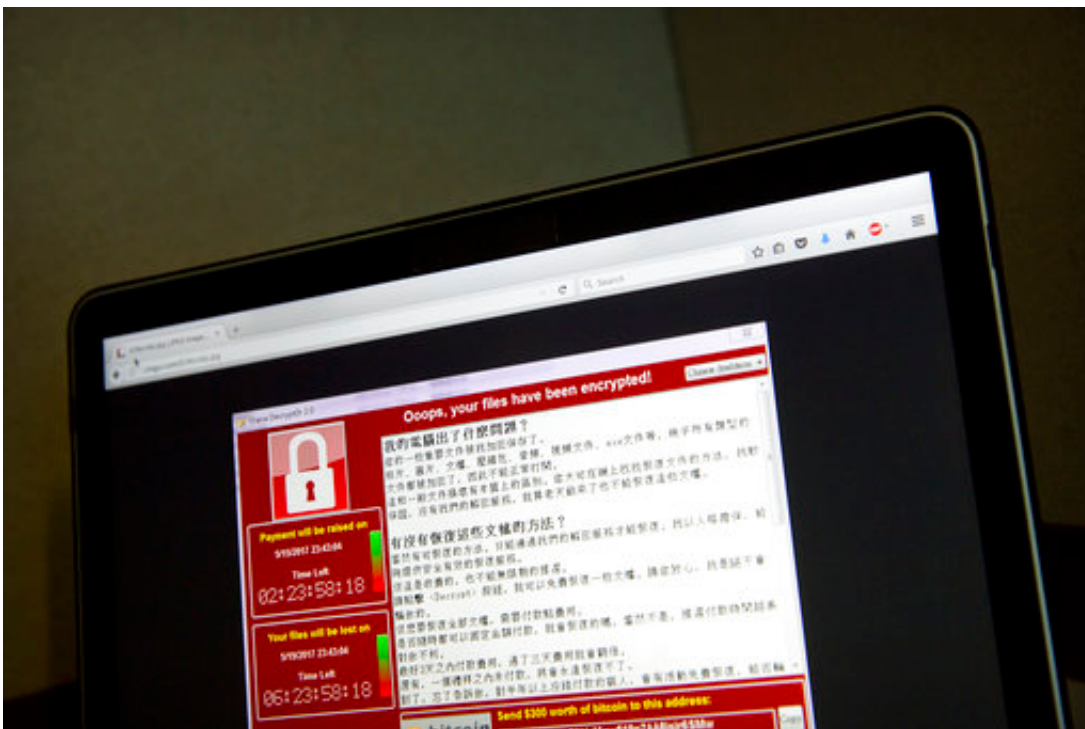
"When we say that the health ministry was attacked you should understand that it wasn't the main server, it was local computers ... actually nothing serious or deadly happened yet," German Klimenko, a presidential adviser, said on Russian state television.

Russian cellular phone operators Megafon and MTS said some of their computers were hit and the Russian national railway system said although it was attacked, rail operations were unaffected.

Russia's central bank said Saturday that no incidents had "compromising the data resources" of Russian banks, state news agency Tass reported.

French carmaker Renault's assembly plant in Slovenia halted production

after it was targeted in the global cyberattack. Radio Slovenia said Saturday the Revoz factory in the southeastern town of Novo Mesto stopped working Friday evening to stop the malware from spreading—and was working with the central office in France to resolve the problem.



A screenshot of the warning screen from a purported ransomware attack, as captured by a computer user in Taiwan, is seen on laptop in Beijing, Saturday, May 13, 2017. Dozens of countries were hit with a huge cyberextortion attack Friday that locked up computers and held users' files for ransom at a multitude of hospitals, companies and government agencies. (AP Photo/Mark Schiefelbein)

Krishna Chinthapalli, a doctor at Britain's National Hospital for Neurology & Neurosurgery who wrote a paper on cybersecurity for the British Medical Journal, said many British hospitals still use Windows

XP software, introduced in 2001.

Security experts said the attack appeared to be caused by a self-replicating piece of software that enters companies when employees click on email attachments, then spreads quickly internally from computer to computer when employees share documents.

The security holes it exploits were disclosed several weeks ago by TheShadowBrokers, a mysterious group that has published what it says are hacking tools used by the NSA. Shortly after that disclosure, Microsoft announced that it had already issued software "patches," or fixes, for those holes—but many users haven't yet installed the fixes or are using older versions of Windows.

In the U.S., FedEx Corp. reported that its Windows computers were "experiencing interference" from malware, but wouldn't say if it had been hit by ransomware.

Elsewhere in Europe, the attack hit companies including Spain's Telefonica, a global broadband and telecommunications company.

Germany's national railway said Saturday departure and arrival display screens at its train stations were affected, but there was no impact on actual train services. Deutsche Bahn said it deployed extra staff to busy stations to help customers, and recommended that they check its website or app for information on their connections.

Other European organizations hit by the massive cyberattack included soccer clubs in Norway and Sweden, with IF Odd, a 132-year-old Norwegian soccer club, saying its online ticketing facility was down.

© 2017 The Associated Press. All rights reserved.

Citation: Huge cyberattack forces Microsoft to offer free tech fix (2017, May 13) retrieved 23 September 2024 from <https://phys.org/news/2017-05-huge-cyberattack-microsoft-free-tech.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.