Dozens of countries hit by huge cyberextortion attack

May 13 2017, by Anick Jesdanun, Jill Lawless And Aritz Parra

Patrick Ward, 47, a sales director at Purbeck Ice Cream, from Dorset in England, poses for photographs after giving media interviews after his heart operation scheduled today was cancelled because of a cyberattack, outside St Bartholomew's Hospital in London, 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)

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.

It was believed to the biggest attack of its kind ever recorded.

The malicious software behind the onslaught appeared to exploit a vulnerability in Microsoft Windows that was supposedly identified by the National Security Agency for its own intelligence-gathering purposes and was later leaked to the internet.

Britain's [national health service](#) fell victim, its hospitals forced to close wards and emergency rooms and turn away patients. Russia appeared to be the hardest hit, according to [security experts](#), with the country's Interior Ministry confirming it was struck.

All told, several cybersecurity firms said they had identified the [malicious software](#), which so far has been responsible for tens of thousands of attacks, in more than 60 countries. That includes the United States, although its effects there didn't appear to be widespread, at least initially.

The attack infected computers with what is known as "ransomware"—software that locks up the user's data and flashes a message demanding payment to release it. In the U.S., FedEx reported that its Windows computers were "experiencing interference" from malware, but wouldn't say if it had been hit by ransomware.
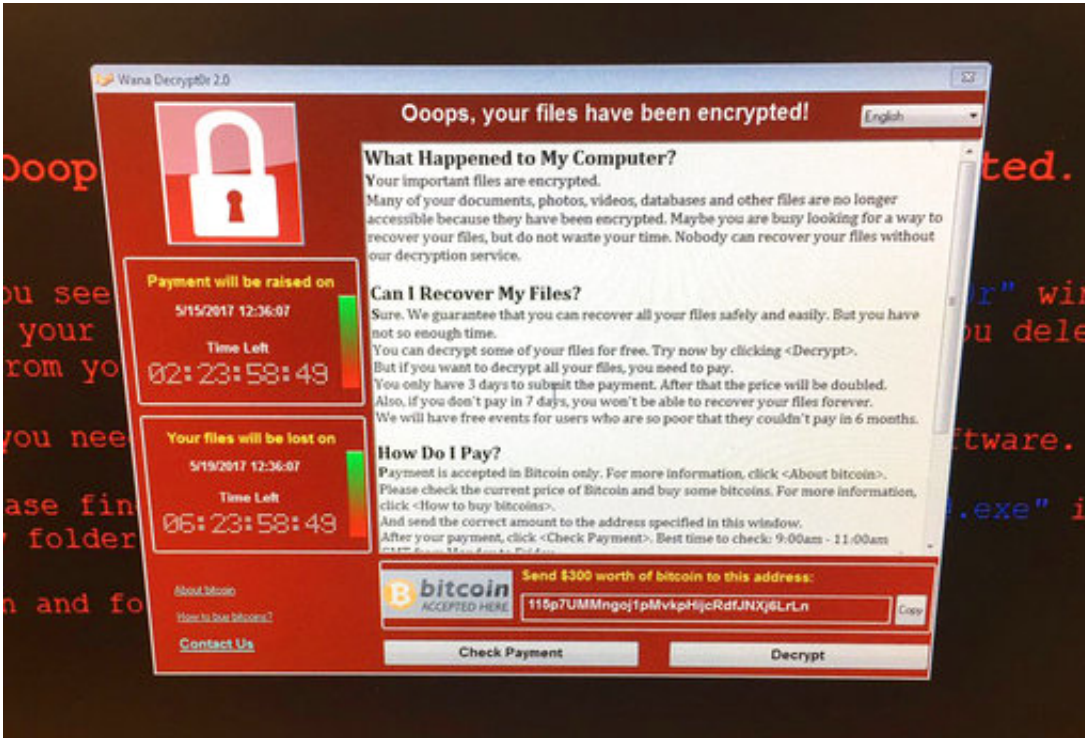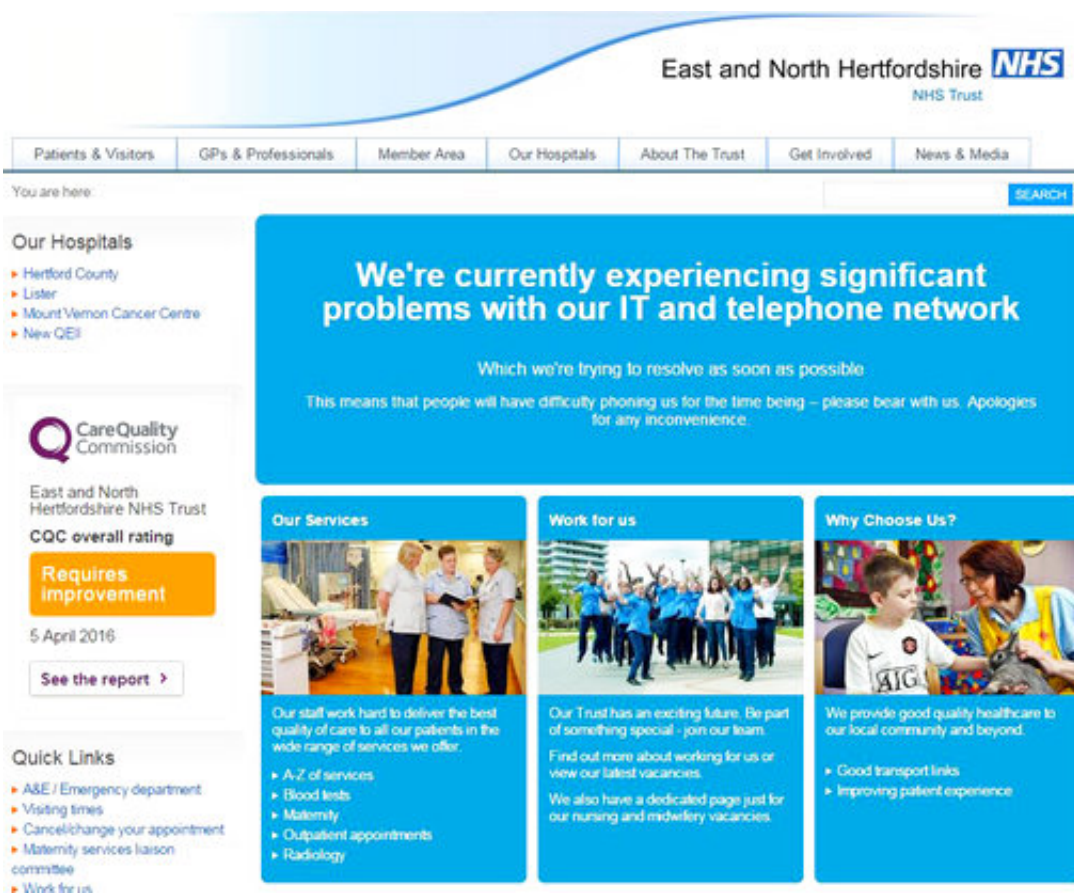
This image provided by the Twitter page of @fendifille shows a computer at Greater Preston CCG as Britain's National Health Service is investigating "an issue with IT" Friday May 12, 2017. Several British hospitals say they are having major computer problems Hospitals in London, northwest England and other parts of the country are reporting problems with their computer systems as the result of an apparent cyberattack. (@fendifille via AP)

Mikko Hypponen, chief research officer at the Helsinki-based cybersecurity company F-Secure, called the attack "the biggest ransomware outbreak in history."

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

Its ransom demands start at $300 and increase after two hours to $400, $500 and then $600, said Kurt Baumgartner, a security researcher at Kaspersky Lab. Affected users can restore their files from backups, if they have them, or pay the ransom; otherwise they risk losing their data entirely.

Chris Wysopal of the software security firm Veracode said criminal organizations were probably behind the attack, given how quickly the malware spread.

This is screengrab taken from the website of the East and North Hertfordshire NHS trust as Britain's National Health Service is investigating "an issue with IT" Friday May 12, 2017. Several British hospitals say they are having major computer problems Hospitals in London, northwest England and other parts of the country are reporting problems with their computer systems as the result of

an apparent cyberattack,.(PA via AP)

"For so many organizations in the same day to be hit, this is unprecedented," he said.

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 as part of its intelligence-gathering.

Shortly after that disclosure, Microsoft announced that it had already issued software "patches" for those holes. But many companies and individuals haven't installed the fixes yet or are using older versions of Windows that Microsoft no longer supports and didn't fix.

By Kaspersky Lab's count, the malware struck at least 74 countries. In addition to Russia, the biggest targets appeared to be Ukraine and India, nations where it is common to find older, unpatched versions of Windows in use, according to the security firm.

This Friday Aug. 14, 2009 file photo shows a sign outside one of London's National Health Service hospitals. Several British hospitals say they are having

Hospitals across Britain found themselves without access to their computers or phone systems. Many canceled all routine procedures and asked patients not to come to the hospital unless it was an emergency. Doctors' practices and pharmacies reported similar problems.

Patrick Ward, a 47-year-old sales director, said his heart operation, scheduled for Friday, was canceled at St. Bartholomew's Hospital in London.

Tom Griffiths, who was at the hospital for chemotherapy, said several cancer patients had to be sent home because their records or bloodwork couldn't be accessed.

"Both staff and patients were frankly pretty appalled that somebody, whoever they are, for commercial gain or otherwise, would attack a health care organization," he said. "It's stressful enough for someone going through recovery or treatment for cancer."

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)

British Prime Minister Theresa May said there was no evidence patient data had been compromised and added that the attack had not specifically targeted the National Health Service.

"It's an international attack and a number of countries and organizations have been affected," she said.

Spain, meanwhile, took steps to protect critical infrastructure in response to the attack. Authorities said they were communicating with more than 100 energy, transportation, telecommunications and financial services providers about the attack.

Spain's Telefonica, a global broadband and telecommunications company, was among the companies hit.

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)

Ransomware attacks are on the rise around the world. In 2016, Hollywood Presbyterian Medical Center in California said it had paid a $17,000 ransom to regain control of its computers from hackers.

Krishna Chinthapalli, a doctor at Britain's National Hospital for Neurology & Neurosurgery who wrote a paper on cybersecurity for the British Medical Journal, warned that British hospitals' old operating

systems and confidential patient information made them an ideal target for blackmailers.

He said many NHS hospitals in Britain use Windows XP software, introduced in 2001, and as government funding for the health service has been squeezed, "IT budgets are often one of the first ones to be reduced."

"Looking at the trends, it was going to happen," he said. "I did not expect an attack on this scale. That was a shock.

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)