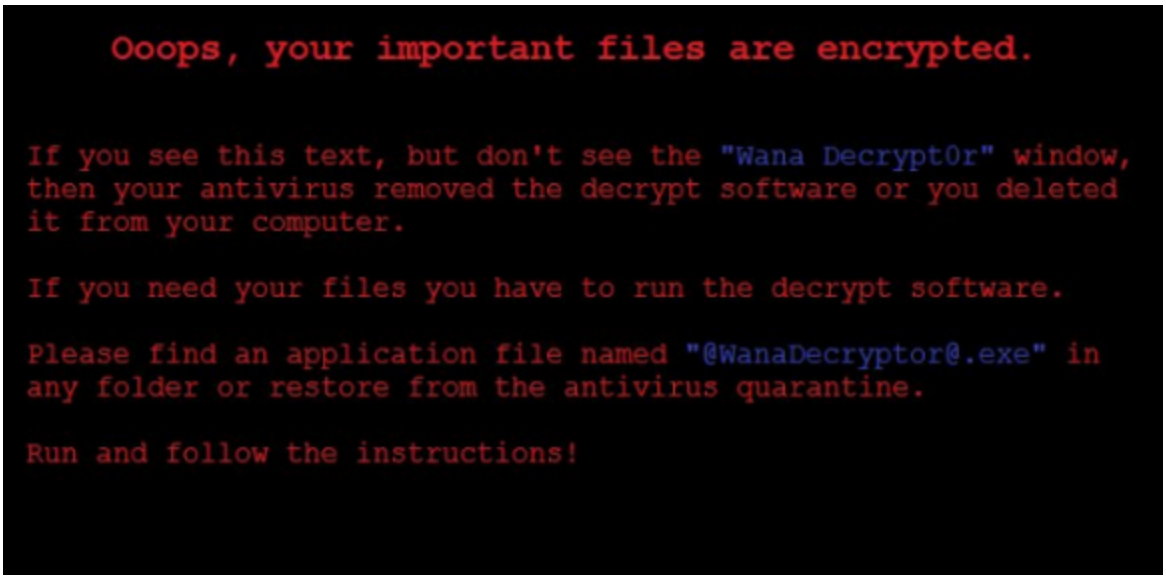
U.K. Hospitals Hit in Widespread Ransomware Attack

krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/

At least 16 hospitals in the United Kingdom are being forced to divert emergency patients today after computer systems there were infected with ransomware, a type of malicious software that encrypts a victim's documents, images, music and other files unless the victim pays for a key to unlock them.

It remains unclear exactly how this ransomware strain is being disseminated and why it appears to have spread so quickly, but there are indications the malware may be spreading to vulnerable systems through a security hole in **Windows** that was recently patched by **Microsoft**.



The ransom note left behind on computers infected with the Wanna Decryptor ransomware strain. Image: BleepingComputer.

In a statement, the U.K.'s **National Health Service** (NHS) said a number of NHS organizations had suffered ransomware attacks.

"This attack was not specifically targeted at the NHS and is affecting organizations from across a range of sectors," the NHS said. "At this stage we do not have any evidence that patient data has been accessed."

According to Reuters, hospitals across England are diverting patients requiring emergency treatment away from the affected hospitals, and the public is being advised to seek medical care only for acute medical conditions.

NHS said the investigation is at an early stage but the ransomware that hit at least 16 NHS facilities is a variant of **Wana Decryptor** (a.k.a. "**WannaCry**"), a ransomware strain that surfaced roughly two weeks ago.

Lawrence Abrams, owner of the tech-help forum BleepingComputer, said Wana Decryptor wasn't a big player in the ransomware space until the past 24 hours, when something caused it to be spread far and wide very quickly.

"It's been out for almost two weeks now, and until very recently it's just been sitting there," Abrams said. "Today, it just went nuts. This is by far the biggest outbreak we have seen to date."

For example, the same ransomware strain apparently today also hit **Telefonica**, one of Spain's largest telecommunications companies. According to an article on BleepingComputer, Telefonica has responded by "desperately telling employees to shut down computers and VPN connections in order to limit the ransomware's reach."

An alert published by Spain's national computer emergency response team (**CCN-CERT**) suggested that the reason for the rapid spread of Wana Decryptor is that it is leveraging a software vulnerability in Windows computers that **Microsoft** patched in March.

According to CCN-CERT, that flaw is MS17-010, a vulnerability in the Windows Server Message Block (SMB) service, which Windows computers rely upon to share files and printers across a local network. Malware that exploits SMB flaws could be extremely dangerous inside of corporate networks because the file-sharing component may help the ransomware spread rapidly from one infected machine to another.

That SMB flaw has enabled Wana Decryptor to spread to more than 36,000 Windows computers so far, according to **Jakub Kroustek**, a malware researcher with **Avast**, a security firm based in the Czech Republic.

"So far, Russia, Ukraine, and Taiwan leading," the world in new infections, Kroustek wrote in a tweet. "This is huge."

Abrams said Wana Decryptor — like many ransomware strains — encrypts victim computer files with extremely strong encryption, but the malware itself is not hard to remove from infected computers. Unfortunately, removing the infection does nothing to restore one's files to their original, unencrypted state.

"It's not difficult to remove, but it also doesn't seem to be decryptable," Abrams said. "It also seems to be very persistent. Every time you make a new file [on an infected PC], it encrypts that new file too."

Experts may yet find a weakness in Wana that allows them to way to decode the ransomware strain without paying the ransom. For now, however, victims who don't have backups of their files have one option: Pay the $300 Bitcoin ransom being demanded by the program.

Wana Decryptor is one of hundreds of strains of ransomware. Victims who are struggling with ransomware should pay a visit to BleepingComputer's ransomware help forum, which often has tutorials on how to remove the malware and in some cases unlock encrypted files without paying the ransom. In addition, the No More Ransom Project also includes an online tool that enables ransomware victims to learn if a free decryptor is available by uploading a single encrypted file.

Update, May 13, 9:33 a.m.: Microsoft today took the unusual step of releasing security updates to fix the SMB flaw in unsupported versions of Windows, including Windows XP, Windows 8, and Windows Server 2003. See this post for more details.