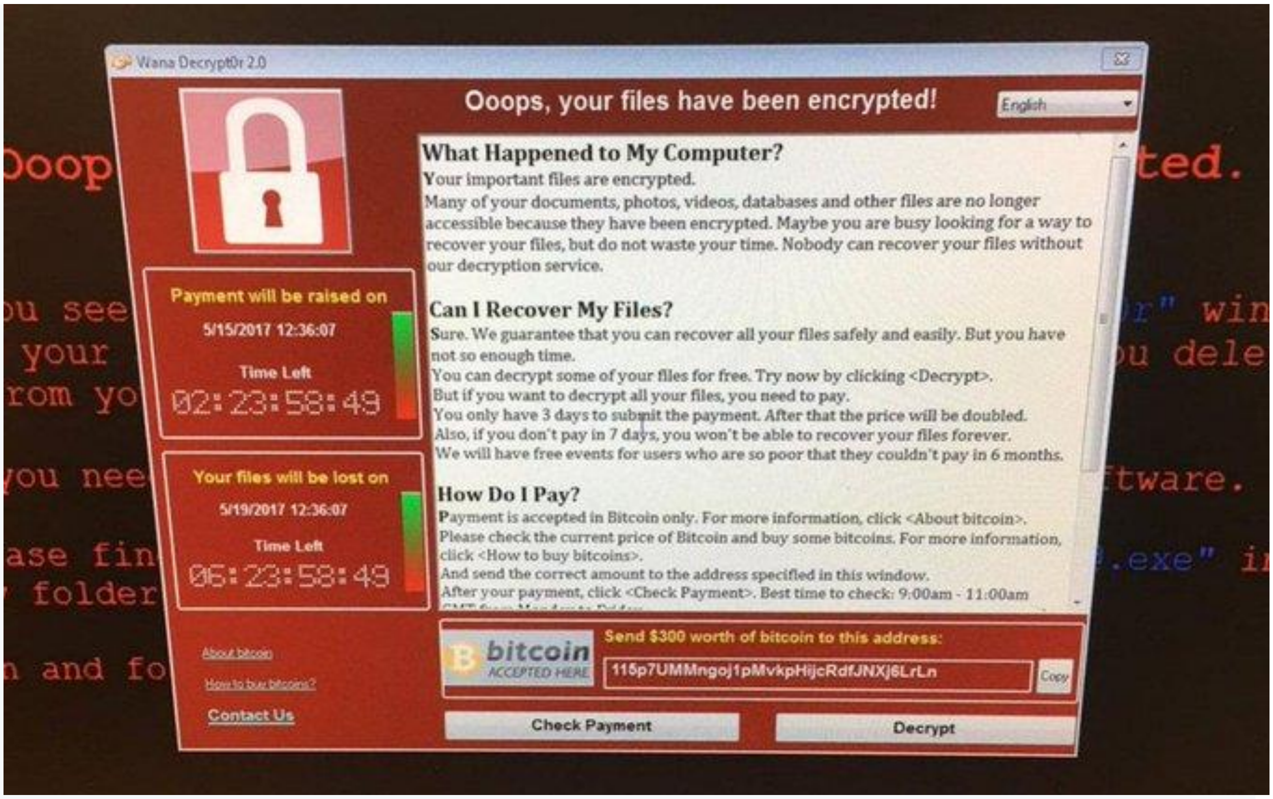
Vox

The ransomware outbreak that's sweeping the internet, explained

Timothy B. Lee

May 12, 2017

On Friday afternoon, Windows computers in some British hospitals displayed an ominous message that looked like this:



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

This is called ransomware, a relatively new form of malware that scrambles a victim’s files and then demands a payment to unscramble them.

Since then, the software has spread rapidly. In a matter of hours, it has infected thousands of computers in dozens of countries around the world. With millions of potentially vulnerable Windows computers out there, it could spread a lot further before IT security professionals get the infection under control.

According to **experts**, the software has spread by exploiting a **vulnerability** that was first revealed to the public in April. A hacking group called the Shadow Brokers posted a cache of hacking tools online that it hinted had been stolen from the National Security Agency.

By the time the Shadow Brokers released the sensitive information, Microsoft had already released a software upgrade fixing the issue (experts think the NSA may have tipped Microsoft off). The problem is that in many cases, IT professionals failed to install the upgrade, leaving many computers vulnerable to the attack.

The incident highlights a big downside to the NSA's practice of collecting libraries of security vulnerabilities in popular consumer software rather than notifying software companies about them. Keeping flaws secret makes it easier for the NSA to spy on foreign adversaries by hacking into their computers. But it also creates a risk that the information could leak, making millions of ordinary internet users vulnerable to hacking.

"To the extent they're going to do that, it's critical that this stuff be secure," says Julian Sanchez, a civil liberties advocate at the Cato Institute. "The NSA's inability to keep their own hacking tools secure has — at least indirectly — led to a catastrophic cybersecurity outcome."

Ransomware forces people to pay to get their own files back

The basic idea behind ransomware is simple: A criminal hacks into your computer, scrambles your files with unbreakable encryption, and then demands that you pay for the encryption key needed to unscramble the files. If you have important files on your computer, you might be willing to pay a lot to avoid losing them.

Ransomware schemes have become a lot more effective since the invention of Bitcoin in 2009. Conventional payment networks like Visa and Mastercard make it difficult to accept payments without revealing your identity. Bitcoin makes that a lot easier. So the past four years have seen a surge in ransomware schemes striking unsuspecting PC users.

Some ransomware schemes are so sophisticated that they even **invest in customer service**, helping victims who want to pay their ransoms navigate the complexities of obtaining bitcoins and making bitcoin payments.

The best way to safeguard your computer against ransomware is to do regular backups. The malware can only encrypt and delete files that are on your computer. If you regularly backup your files — either to an external hard drive or using an online service — then you can simply wipe your ransomware-infected computer, reinstall its software, and then restore your files from the backup copy. Unfortunately, many people don't keep adequate backups, so they're vulnerable to this kind of extortion.

The latest ransomware is having serious human consequences. Hospitals in the UK are struggling to treat their patients with many of their computers inoperative:

Hackers appear to have exploited a vulnerability from the NSA

The ransomware is spread by an internet worm, software that spreads copies of itself by hacking into other computers on a network. In this case, the worm appears to be exploiting a vulnerability in Windows that was first revealed to the public by the Shadow Brokers. The group's exact identity isn't known, but Sanchez says the group is widely suspected to be connected to the Russian government. It leaked a cache of hacking tools in April that it said had been stolen from the NSA.

It's not surprising that the NSA knew about software vulnerabilities that were not known to the general public. There's a thriving underground market for software exploits. When independent hackers discover a flaw in popular software like Windows, they can often sell the information for thousands of dollars. Most intelligence agencies participate in this underground market, as do some criminal organizations. Many major software companies also participate, offering cash "bug bounties" to researchers who tell companies about flaws in their own products instead of selling the information to a third party.

We've **known since at least 2013** that the NSA participates heavily in this underground market. And the NSA's participation is controversial. **Critics argue** that if the spy agency discovers a flaw in a popular consumer software product, it should promptly notify the software's manufacturer so that the flaw can be fixed. Instead, the NSA often keeps the vulnerability secret to avoid tipping off potential hacking targets.

This works fine so long as the NSA is able to keep the information to itself. The problem is that a vulnerability might become more widely known — either because it's independently discovered or because someone steals the information from the NSA. In that case, the NSA's decision not to report the vulnerability can expose the computers of millions of ordinary users to hacking by criminals and foreign intelligence agencies.

In this case, Microsoft actually **released a software update** to fix the problem a month before the Shadow Brokers leaked it, so users who applied security patches regularly weren't put in danger. The problem is that Windows users — and their IT professionals — don't always apply security upgrades promptly. So many computers were still vulnerable two months after Microsoft released its upgrade.

Sanchez believes that the NSA likely could have done more to secure innocent peoples' computers. He noted that the Shadow Brokers first began leaking NSA files way back in August 2016. Sanchez argues the NSA should have anticipated that more files would be released and gone to Microsoft earlier, allowing Microsoft to release a software update in the fall of 2016 instead of March 2017. With more lead time, IT professionals might have had a long enough window to update their systems.