



What is WannaCry ransomware?

Published on 08 June 2020

Is your computer vulnerable to attack from WannaCry ransomware? Read on to find out as we explore all there is to know about the WannaCry ransomware attack.

In this article, you will learn:

- What WannaCry ransomware is
- How the WannaCry ransomware attack worked
- The impact of the WannaCry ransomware attack
- How to protect your computer from ransomware

WannaCry ransomware explained

WannaCry is an example of crypto ransomware, a type of malicious software (malware) used by cybercriminals to extort money.

Ransomware does this by either encrypting valuable files, so you are unable to read them, or by locking you out of your computer, so you are not able to use it.

Ransomware that uses encryption is called crypto ransomware. The type that locks you out of your computer is called locker ransomware.

Like other types of crypto-ransomware, WannaCry takes your data hostage, promising to return it if you pay a ransom.

WannaCry targets computers using Microsoft Windows as an operating system. It encrypts data and demands payment of a ransom in the cryptocurrency Bitcoin for its return.



What was the WannaCry ransomware attack?

The WannaCry ransomware attack was a global epidemic that took place in May 2017.

This ransomware attack spread through computers operating Microsoft Windows. User's files were held hostage, and a Bitcoin ransom was demanded for their return.

Were it not for the continued use of outdated computer systems and poor education around the need to update software, the damage caused by this attack could have been avoided.



Featured Articles



Coronavirus Charity Scams — What You Need to Know and How to Protect Yourself



Online Gaming Scams during Pandemic. How to Stay Safe



How Safe Are Money E-Transfers?



How to Keep Kids Safe Online During the Coronavirus Outbreak



Online Video Calls & Conferencing: How to Stay Safe from Hackers



How does a WannaCry attack work?

The cybercriminals responsible for the attack took advantage of a weakness in the Microsoft Windows operating system using a hack that was allegedly developed by the *United States National Security Agency*.

Known as EternalBlue, this hack was made public by a group of hackers called the *Shadow Brokers* before the WannaCry attack.

Microsoft released a security patch which protected user's systems against this exploit almost two months before the WannaCry ransomware attack began. Unfortunately, many individuals and organizations do not regularly update their operating systems and so were left exposed to the attack.

Those that had not run a Microsoft Windows update before the attack did not benefit from the patch and the vulnerability exploited by EternalBlue left them open to attack.

When it first happened, people assumed that the WannaCry ransomware attack had initially spread through a phishing campaign (a phishing campaign is where spam emails with infected links or attachments lure users to download malware). However, EternalBlue was the exploit that allowed WannaCry to propagate and spread, with DoublePulsar being the 'backdoor' installed on the compromised computers (used to execute WannaCry).

What happened if the WannaCry ransom was not paid?

The attackers demanded \$300 worth of bitcoins and then later increased the ransom demand to \$600 worth of bitcoins. If victims did not pay the ransom within three days, victims of the WannaCry ransomware attack were told that their files would be permanently deleted.

The advice when it comes to ransom payments is not to cave into the pressure. Always avoid paying a ransom, as there is no guarantee that your data will be returned and every payment validates the criminals' business model, making future attacks more likely.

This advice proved wise during the WannaCry attack as, reportedly, the coding used in the attack was faulty. When victims paid their ransom, the attackers had no way of associating the payment with a specific victim's computer.

There's some doubt about whether anyone got their files back. Some researchers claimed that no one got their data back. However, a company called F-Secure claimed that some did. This is a stark reminder of why it is never a good idea to pay the ransom if you experience a ransomware attack.



What impact did the WannaCry attack have?

The WannaCry ransomware attack hit around 230,000 computers globally.

One of the first companies affected was the Spanish mobile company, Telefónica. By May 12th, thousands of NHS hospitals and surgeries across the UK were affected.

A third of NHS hospital trusts were affected by the attack. Terrifyingly ambulances were reportedly rerouted, leaving people in need of urgent care in need. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were canceled as a result of the attack.

As the ransomware spread beyond Europe, computer systems in 150 countries were crippled. The WannaCry ransomware attack had a substantial financial impact worldwide. It is estimated this cybercrime caused \$4 billion in losses across the globe.

Ransomware protection

Now you understand how the WannaCry ransomware attack took place and the impact that it had, let's consider how you can protect yourself from ransomware.

Here are our top tips:

Update your software and operating system regularly

Computer users became victims of the WannaCry attack because they had not updated

Computer users became victims of the WannaCry attack because they had not updated their Microsoft Windows operating system.

Had they updated their operating systems regularly, they would have benefited from the security patch that Microsoft released before the attack.

This patch removed the vulnerability that was exploited by EternalBlue to infect computers with WannaCry ransomware.

Be sure to keep your software and operating system updated. This is an essential ransomware protection step.

Do not click on suspicious links

If you open an unfamiliar email or visit a website, you do not trust, do not click on any links. Clicking on unverified links could trigger a ransomware download.

Never open untrusted email attachments

Avoid opening any email attachments unless you are sure they are safe. Do you know and trust the sender? Is it clear what the attachment is? Were you expecting to receive the attached file?

If the attachment asked you to enable macros to view it, stay well clear. Do not enable macros or open the attachment as this is a common way ransomware and other types of malware are spread.

Do not download from untrusted websites

Downloading files from unknown sites increases the risk of downloading ransomware. Only download files from websites you trust.

Avoid unknown USBs

Do not insert USBs or other removal storage devices into your computer, if you do not know where they came from. They could be infected with ransomware.



Use a VPN when using public Wi-Fi

Exercise caution when using public Wi-Fi as this makes your computer system more vulnerable to attack.

Use a secure VPN to protect yourself from the risk of malware when using public Wi-Fi.

Install internet security software

Keep your computer protected and prevent ransomware by installing internet security software. Go for a comprehensive solution that protects against multiple complex threats, like [Kaspersky's System Watcher](#).

Update your internet security software

To ensure you receive the maximum protection your internet security has to offer (including all the latest patches) keep it updated.

Back up your data

Be sure to back up your data regularly using an external hard drive or cloud storage. Should you become victimized by ransomware hackers, your data will be safe if it is backed up. Just remember to disconnect your external storage device from your computer once you've backed up your data. Keeping your external storage routinely connected to your PC will potentially expose it to ransomware families that can encrypt data on these devices as well.

Want to sleep easy with maximum ransomware protection? Protect yourself with free [Kaspersky Anti-Ransomware Tool](#) or [Premium Kaspersky Anti-Ransomware Products](#)

Related articles:

- [Data Theft and Data Loss](#)
- [The Biggest Ransomware Threats](#)
- [WannaCry: Not Dead Yet](#)

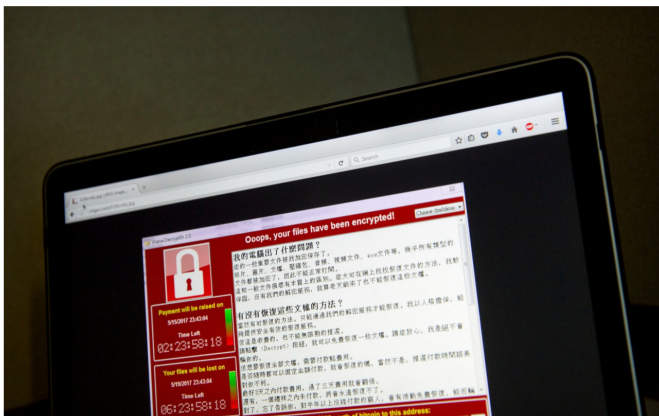
Technology Intelligence

WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled



FOLLOW THE TELEGRAPH

- Follow on Facebook
- Follow on Twitter
- Follow on Instagram
- Follow on LinkedIn



A computer hit by the WannaCry attack CREDIT: AP

By **Matthew Field**

11 OCTOBER 2018 • 6:05PM

A devastating global cyber attack that crippled computers in hospitals across the UK has cost the NHS £92m, a report from the Department of Health has found.

The so-called **WannaCry hack**, which shut down hundreds of thousands of computers around the world with messages from hackers demanding ransom payments, hit a third of hospital trusts and 8pc of GP practices. Around 1pc of all NHS care was disrupted over the course of a week.

The hack caused more than 19,000 appointments to be cancelled, costing the NHS £20m between 12 May and 19 May and £72m in the subsequent cleanup and upgrades to its IT systems.

The cyber attack caused 200,000 computers to lock out users with red-lettered error messages demanding the cryptocurrency Bitcoin. The attack was blamed on elite North Korean hackers after a year-long investigation.

At the time of the attacks, the NHS was criticised for using outdated IT systems, including Windows XP, a 17 year-old operating system that could be vulnerable to cyber attacks.

In a report from the Department of Health, the Government said it had continued to invest in its cyber security and infrastructure to prevent similar attacks.

The NHS has increased infrastructure investment of £60m this year to the most vulnerable services, such as major trauma centres and ambulance services. The Government said it had committed £150m to upgrading its technology systems over the next three years.

The NHS also this year signed a new deal to upgrade local NHS computers to Microsoft's Windows 10.

The report **said**: "The results have shown that organisations have made good progress in implementing the data security standards related to people and process, but that those relating to technology continue to be challenging."

The WannaCry cyber attack hit businesses around the world, including Renault and FedEx and crashed thousands of ordinary peoples' computers.

Last month, US prosecutors pinned blame for the attacks on North Korean hackers the Lazarus Group. While the attack didn't specifically target the NHS, it spread over the internet using a leaked hacking tool developed by the US spy agency the NSA.

Related Topics


Cyber attacks NHS Department for Health & Social Care Health



Technology latest



Live | Drivers 'overjoyed' at victory over Uber in six year battle - live updates
19 Feb 2021, 2:12pm



India and Canada set to join fight with Facebook over Australian news block
19 Feb 2021, 12:57pm

MPs should decide the gig economy's future - not judges
ROBIN PAGNAMENTA
19 Feb 2021, 12:05pm




Uber drivers are 'workers' and entitled to holiday pay and minimum wage, Supreme Court rules
19 Feb 2021, 9:58am



British Summer Time 2021: When do the clocks change?
19 Feb 2021, 9:32am



Meet the Frenchman who wants to put mealworms on our dinner plates
19 Feb 2021, 8:08am



Robinhood boss fails to convince that he is the prince of thieves
19 Feb 2021, 6:00am



UK's secretive £800m tech research agency to launch next year
19 Feb 2021, 12:01am



Robinhood boss apologises over 'black swan' GameStop stock frenzy
18 Feb 2021, 10:32pm



WhatsApp changes plan for controversial privacy policy rollout
18 Feb 2021, 9:00pm

Britain must hold firm against Facebook's dangerous ban on news
DAMIAN COLLINS
18 Feb 2021, 5:59pm



Dogecoin surge leaves mystery holder with \$2.1bn
18 Feb 2021, 5:54pm



'Arrogant' Facebook is trying to intimidate us over news ban, says Australian PM Scott Morrison
18 Feb 2021, 5:03pm



'It's time Facebook was taken to task': Telegraph readers on its Australian news ban
18 Feb 2021, 4:57pm



GameStop saga's key players prepare to face US lawmakers
18 Feb 2021, 1:10pm




Ford goes electric – but Big Tech still holds the car keys
ROBIN PAGNAMENTA
18 Feb 2021, 6:00am



Tesla UK sales spike almost 90pc to £590m as more Britons go electric

18 Feb 2021, 11:56am



Facebook's Australia news ban will test how powerful the firm really is

18 Feb 2021, 6:43am



Facebook bans all news for Australian users amid government spat

18 Feb 2021, 5:50am



Only 1pc of Britain's start-up bailout money went to female founders







17 Feb 2021, 8:00pm



Texas power crisis threatens world microchip supply as plants shut down

17 Feb 2021, 7:01pm

[Voucher Codes](#) > The latest offers and discount codes from popular brands on Telegraph Voucher Codes

 <p>Amazon promo code</p>	 <p>Vodafone deals</p>	 <p>Argos promo code</p>	 <p>Currys discount code</p>	 <p>NOW TV Offers</p>	 <p>Dell discount codes</p>
--	---	---	---	---	--

Protecting You, Your Family & More

Get the Power to Protect. Discover how our award-winning security helps protect what matters most to you.

Get FREE Tools

There's a wide range of FREE Kaspersky tools that can help you to stay safe – on PC, Mac, iPhone, iPad & Android devices.

Contact Us

Helping you stay safe is what we're about – so, if you need to contact us, get answers to some FAQs or access our technical support team.

Who We Are

Find out why we're so committed to helping people stay safe... online and beyond.

Get Your Free Trial

Try Before You Buy. In just a few clicks, you can get a FREE trial of one of our products – so you can put our technologies through their paces.

Stay in Touch



Home Products

- [Kaspersky Anti-Virus](#)
- [Kaspersky Android Antivirus](#)
- [Kaspersky Internet Security](#)
- [Kaspersky Total Security](#)
- [Kaspersky Security Cloud](#)
- [Kaspersky VPN Secure Connection](#)
- [Free Antivirus](#)
- [All Products](#)

Small Business Products

(1-50 EMPLOYEES)

- [Kaspersky Small Office Security](#)
- [Kaspersky Endpoint Security Cloud](#)
- [All Products](#)

Medium Business Products

(51-999 EMPLOYEES)

- [Kaspersky Endpoint Security Cloud](#)
- [Kaspersky Endpoint Security for Business Select](#)
- [Kaspersky Endpoint Security for Business Advanced](#)
- [All Products](#)

Enterprise Solutions

(1000+ EMPLOYEES)

- [Cybersecurity Services](#)
- [Threat Management and Defense](#)
- [Endpoint Security](#)
- [Hybrid Cloud Security](#)
- [Cybersecurity Training](#)
- [Threat Intelligence](#)
- [All Solutions](#)

© 2021 AO Kaspersky Lab. All Rights Reserved. • [Privacy Policy](#) • [Cookies](#) • [Anti-Corruption Policy](#) • [Licence Agreement B2C](#) • [Licence Agreement B2B](#) • [Terms of Use](#) • [Refund Policy](#)