WannaCry ransomware attack

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#mw-head)[Jump to search](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#searchInput)

|  |  |
| --- | --- |
| **WannaCry** | |
| Screenshot of the ransom note left on an infected system | |
| **Date** | 12 May 2017 – 15 May 2017 (initial outbreak)[[1]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-1) |
| **Duration** | 4 days |
| **Location** | Worldwide |
| **Also known as** | Transformations: Wanna → Wana Cryptor → Crypt0r Cryptor → Decryptor Cryptor → Crypt → Cry Addition of "2.0" Short names: Wanna → WN → W Cry → CRY |
| **Type** | [Cyberattack](https://en.wikipedia.org/wiki/Cyberattack) |
| **Theme** | [Ransomware](https://en.wikipedia.org/wiki/Ransomware) encrypting files with $300 – $600 [USD](https://en.wikipedia.org/wiki/United_States_dollar) demand (via [bitcoin](https://en.wikipedia.org/wiki/Bitcoin)) |
| **Cause** | * WannaCry worm |
| **Outcome** | Over 200,000 victims and more than 300,000 computers infected[[2]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-2)[[3]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-3)[[4]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-threaten_release-4) |
| **Arrests** | None |
| **Suspects** | [Lazarus Group](https://en.wikipedia.org/wiki/Lazarus_Group) |
| **Accused** | Two North Koreans Indicted |
| **Convictions** | None |

|  |  |
| --- | --- |
| **WannaCry** | |
| **Subtype** | [Ransomware](https://en.wikipedia.org/wiki/Ransomware) |
| **Point of origin** | [Pyongyang](https://en.wikipedia.org/wiki/Pyongyang), [North Korea](https://en.wikipedia.org/wiki/North_Korea) |
| **Author(s)** | [Lazarus Group](https://en.wikipedia.org/wiki/Lazarus_Group) |

The **WannaCry ransomware attack** was a May 2017 [worldwide](https://en.wikipedia.org/wiki/Global_issue) [cyberattack](https://en.wikipedia.org/wiki/Cyberattack) by the WannaCry [ransomware](https://en.wikipedia.org/wiki/Ransomware) [cryptoworm](https://en.wikipedia.org/wiki/Cryptovirology), which targeted computers running the [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) [operating system](https://en.wikipedia.org/wiki/Operating_system) by encrypting data and demanding ransom payments in the [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency). It propagated through [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue), an exploit discovered by the United States [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called [The Shadow Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers) at least a year prior to the attack. While [Microsoft](https://en.wikipedia.org/wiki/Microsoft) had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their [end-of-life](https://en.wikipedia.org/wiki/End-of-life_(product)). These patches are imperative to an organization's cyber-security but many were not applied because of needing 24/7 operation, risking having applications that used to work break, inconvenience, or other reasons.

The attack was halted within a few days of its discovery due to emergency patches released by Microsoft and the discovery of a [kill switch](https://en.wikipedia.org/wiki/Kill_switch) that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of [dollars](https://en.wikipedia.org/wiki/United_States_dollar). Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.

In December 2017, the [United States](https://en.wikipedia.org/wiki/United_States), [United Kingdom](https://en.wikipedia.org/wiki/United_Kingdom) and [Australia](https://en.wikipedia.org/wiki/Australia) formally asserted that [North Korea](https://en.wikipedia.org/wiki/North_Korea) was behind the attack.[[5]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-5)

A new variant of WannaCry forced [Taiwan Semiconductor Manufacturing Company](https://en.wikipedia.org/wiki/Taiwan_Semiconductor_Manufacturing_Company) (TSMC) to temporarily shut down several of its chip-fabrication factories in August 2018. The virus spread to 10,000 machines in TSMC's most advanced facilities.[[6]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-6)



**Contents**

* [1Description](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Description)
* [2Attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Attack)
  + [2.1Defensive response](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Defensive_response)
* [3Attribution](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Attribution)
* [4Impact](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Impact)
  + [4.1Affected organizations](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Affected_organizations)
* [5Reactions](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Reactions)
  + [5.1United Kingdom](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#United_Kingdom)
* [62018 email scam](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#2018_email_scam)
* [7See also](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#See_also)
* [8References](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#References)
* [9External links](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#External_links)

Description[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=1)]

WannaCry is a [ransomware](https://en.wikipedia.org/wiki/Ransomware) [cryptoworm](https://en.wikipedia.org/wiki/Cryptovirology), which targeted computers running the [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) [operating system](https://en.wikipedia.org/wiki/Operating_system) by encrypting data and demanding ransom payments in the [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency). The worm is also known as WannaCrypt,[[7]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-microsoftreleases-7) Wana Decrypt0r 2.0,[[8]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-8) WanaCrypt0r 2.0,[[9]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-:0-9) and Wanna Decryptor.[[10]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-auto-10) It is considered a network worm because it also includes a "transport" mechanism to automatically spread itself. This transport code scans for vulnerable systems, then uses the [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue) exploit to gain access, and the [DoublePulsar](https://en.wikipedia.org/wiki/DoublePulsar) tool to install and execute a copy of itself.[[11]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-talos-11) WannaCry versions 0, 1, and 2 were created using [Microsoft Visual C++ 6.0](https://en.wikipedia.org/wiki/Microsoft_Visual_C%2B%2B#vc6).[[12]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-doj-12)

EternalBlue, is an [exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)) of Windows' [Server Message Block](https://en.wikipedia.org/wiki/Server_Message_Block) (SMB) protocol released by [The Shadow Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers). Much of the attention and comment around the event was occasioned by the fact that the U.S. [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA) (from whom the exploit was likely stolen) had already discovered the vulnerability, but used it to create an exploit for its own [offensive work](https://en.wikipedia.org/wiki/National_Security_Agency#Hacking_operations), rather than report it to Microsoft.[[13]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-independent-13)[[14]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-telegraph-14) Microsoft eventually discovered the vulnerability, and on [Tuesday](https://en.wikipedia.org/wiki/Patch_Tuesday), 14 March 2017, they issued security bulletin MS17-010, which detailed the flaw and announced that [patches](https://en.wikipedia.org/wiki/Security_patch) had been released for all Windows versions that were currently supported at that time, these being [Windows Vista](https://en.wikipedia.org/wiki/Windows_Vista), [Windows 7](https://en.wikipedia.org/wiki/Windows_7), [Windows 8.1](https://en.wikipedia.org/wiki/Windows_8.1), [Windows 10](https://en.wikipedia.org/wiki/Windows_10), [Windows Server 2008](https://en.wikipedia.org/wiki/Windows_Server_2008), [Windows Server 2008 R2](https://en.wikipedia.org/wiki/Windows_Server_2008_R2), [Windows Server 2012](https://en.wikipedia.org/wiki/Windows_Server_2012), and [Windows Server 2016](https://en.wikipedia.org/wiki/Windows_Server_2016).[[15]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Ars_Technica-15)

DoublePulsar is a [backdoor](https://en.wikipedia.org/wiki/Backdoor_(computing)) tool, also released by [The Shadow Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers) on 14 April 2017. Starting from 21 April 2017, security researchers reported that there were tens of thousands of computers with the DoublePulsar backdoor installed.[[16]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-16) By 25 April, reports estimated that the number of infected computers could be up to several hundred thousand, with numbers increasing every day.[[17]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-17)[[18]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-18) The WannaCry code can take advantage of any existing DoublePulsar infection, or installs it itself.[[11]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-talos-11)[[19]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-19)[[20]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-20) On 9 May 2017, private cybersecurity company RiskSense released code on the website github.com with the stated purpose of allowing legal “white hat” penetration testers to test the CVE-2017-0144 exploit on unpatched systems.

When executed, the WannaCry malware first checks the "[kill switch](https://en.wikipedia.org/wiki/Kill_switch#Software)" domain name; if it is not found, then the ransomware [encrypts](https://en.wikipedia.org/wiki/Encryption_software) the computer's data,[[21]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-:1-21)[[22]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-syma-22)[[23]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-23) then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet,[[24]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-mbytes-24) and "laterally" to computers on the same network.[[25]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-mcafee-25) As with other modern ransomware, the [payload](https://en.wikipedia.org/wiki/Payload_(computing)) displays a message informing the user that files have been encrypted, and demands a payment of around US$300 in [bitcoin](https://en.wikipedia.org/wiki/Bitcoin) within three days, or US$600 within seven days.[[22]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-syma-22)[[26]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-26) Three [hardcoded](https://en.wikipedia.org/wiki/Hard_coding) bitcoin addresses, or "wallets", are used to receive the payments of victims. As with all such wallets, their transactions and balances are publicly accessible even though the [cryptocurrency wallet](https://en.wikipedia.org/wiki/Cryptocurrency_wallet) owners remain unknown.[[27]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-27)

Several organizations released detailed technical writeups of the malware, including a senior security analyst at RiskSense,[[28]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-28)[[29]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-29) Microsoft,[[30]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-30) [Cisco](https://en.wikipedia.org/wiki/Cisco_Systems),[[11]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-talos-11) [Malwarebytes](https://en.wikipedia.org/wiki/Malwarebytes),[[24]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-mbytes-24) [Symantec](https://en.wikipedia.org/wiki/NortonLifeLock) and [McAfee](https://en.wikipedia.org/wiki/McAfee).[[25]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-mcafee-25)

Attack[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=2)]

The attack began on Friday, 12 May 2017,[[31]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-naked-31)[[32]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-32) with evidence pointing to an initial infection in Asia at 07:44 UTC.[[31]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-naked-31)[[33]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-33) The initial infection was likely through an exposed [vulnerable](https://en.wikipedia.org/wiki/Vulnerability_(computing)) SMB port,[[34]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-34) rather than email phishing as initially assumed.[[31]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-naked-31) Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.[[35]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-:3-35)[[36]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-cnbc1-36)

Organizations that had not installed Microsoft's security update from April 2017 were affected by the attack.[[37]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-exploit-37) Those still running [unsupported](https://en.wikipedia.org/wiki/End-of-life_(product)) versions of [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows), such as [Windows XP](https://en.wikipedia.org/wiki/Windows_XP) and [Windows Server 2003](https://en.wikipedia.org/wiki/Windows_Server_2003)[[38]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-vicexp-38)[[39]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-unsupported-39) were at particularly high risk because no security patches had been released since April 2014 for Windows XP (with the exception of one emergency patch released in May 2014) and July 2015 for Windows Server 2003.[[7]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-microsoftreleases-7) A [Kaspersky Lab](https://en.wikipedia.org/wiki/Kaspersky_Lab) study reported however, that less than 0.1 percent of the affected computers were running Windows XP, and that 98 percent of the affected computers were running Windows 7.[[7]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-microsoftreleases-7)[[40]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-:2-40) In a controlled testing environment, the cybersecurity firm Kryptos Logic found that it was unable to infect a Windows XP system with WannaCry using just the exploits, as the payload failed to load, or caused the operating system to crash rather than actually execute and encrypt files. However, when executed manually, WannaCry could still operate on Windows XP.[[41]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-verge-xpimpact-41)[[42]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-kl-twoweekslater-42)[[43]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-43)

**Defensive response**[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=3)]

Experts quickly advised affected users against paying the ransom due to no reports of people getting their data back after payment and as high revenues would encourage more of such campaigns.[[44]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-NS-44)[[45]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-BBC-45)[[46]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-46) As of 14 June 2017, after the attack had subsided, a total of 327 payments totaling US$130,634.77 (51.62396539 XBT) had been transferred.[[47]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-47)

The day after the initial attack in May, Microsoft released out-of-band security updates for end of life products [Windows XP](https://en.wikipedia.org/wiki/Windows_XP), [Windows Server 2003](https://en.wikipedia.org/wiki/Windows_Server_2003) and [Windows 8](https://en.wikipedia.org/wiki/Windows_8); these patches had been created in February of that year following a tip off about the vulnerability in January of that year.[[48]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-48)[[39]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-unsupported-39) Organizations were advised to patch Windows and plug the vulnerability in order to protect themselves from the cyber attack.[[49]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-49) The head of Microsoft's Cyber Defense Operations Center, Adrienne Hall, said that “Due to the elevated risk for destructive cyber-attacks at this time, we made the decision to take this action because applying these updates provides further protection against potential attacks with characteristics similar to WannaCrypt [alternative name to WannaCry]”.[[50]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-50)[[51]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-51)

Researcher [Marcus Hutchins](https://en.wikipedia.org/wiki/Marcus_Hutchins)[[52]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-52)[[53]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-MalwareTech-53) discovered the kill switch domain [hardcoded](https://en.wikipedia.org/wiki/Hard_coding) in the malware.[[54]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-54)[[55]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-55)[[56]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-56) Registering a [domain name](https://en.wikipedia.org/wiki/Domain_name) for a [DNS sinkhole](https://en.wikipedia.org/wiki/DNS_sinkhole) stopped the attack spreading as a worm, because the ransomware only encrypted the computer's files if it was unable to connect to that domain, which all computers infected with WannaCry before the website's registration had been unable to do. While this did not help already infected systems, it severely slowed the spread of the initial infection and gave time for defensive measures to be deployed worldwide, particularly in North America and Asia, which had not been attacked to the same extent as elsewhere.[[57]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-57)[[58]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-58)[[59]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-59)[[60]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-60)[[61]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-61) On 14 May, a first variant of WannaCry appeared with a new and second[[62]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-62) kill-switch registered by [Matt Suiche](https://en.wikipedia.org/wiki/Matt_Suiche) on the same day. This was followed by a second variant with the third and last kill-switch on 15 May, which was registered by [Check Point](https://en.wikipedia.org/wiki/Check_Point) threat intelligence analysts.[[63]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-63)[[64]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-64) A few days later, a new version of WannaCry was detected that lacked the kill switch altogether.[[65]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-spiegel1-65)[[66]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-66)[[67]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-67)[[68]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-68)

On 19 May, it was reported that hackers were trying to use a [Mirai](https://en.wikipedia.org/wiki/Mirai_(malware)) botnet variant to effect a [distributed attack](https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack) on WannaCry's kill-switch domain with the intention of knocking it offline.[[69]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-69) On 22 May, Hutchins protected the domain by switching to a cached version of the site, capable of dealing with much higher traffic loads than the live site.[[70]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-70)

Separately, researchers from [University College London](https://en.wikipedia.org/wiki/University_College_London) and [Boston University](https://en.wikipedia.org/wiki/Boston_University) reported that their *PayBreak* system could defeat WannaCry and several other families of ransomware by recovering the keys used to encrypt the user's data.[[71]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-71)[[72]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-72)

It was discovered that Windows encryption APIs used by WannaCry may not completely clear the [prime numbers](https://en.wikipedia.org/wiki/Prime_number) used to generate the payload's private keys from the memory, making it potentially possible to retrieve the required key if they had not yet been overwritten or cleared from resident memory. The key is kept in the memory if the WannaCry process has not been killed and the computer has not been rebooted after being infected.[[73]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-73) This behaviour was used by a French researcher to develop a tool known as WannaKey, which automates this process on Windows XP systems.[[74]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-zdnet-xpwannakey-74)[[75]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-ars-wannakey-75)[[76]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-76) This approach was iterated upon by a second tool known as Wanakiwi, which was tested to work on Windows 7 and Server 2008 R2 as well.[[77]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-ars-wanakiwi-77)

Within four days of the initial outbreak, new infections had slowed to a trickle due to these responses.[[78]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Volz-78)

Attribution[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=4)]

Linguistic analysis of the ransom notes indicated the authors were likely fluent in Chinese and proficient in English, as the versions of the notes in those languages were probably human-written while the rest seemed to be [machine-translated](https://en.wikipedia.org/wiki/Machine_translation).[[79]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-register-language-79)[[80]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-80) According to an analysis by the FBI's Cyber Behavioral Analysis Center, the computer that created the ransomware language files had [Hangul](https://en.wikipedia.org/wiki/Hangul) language fonts installed, as evidenced by the presence of the "\fcharset129" [Rich Text Format](https://en.wikipedia.org/wiki/Rich_Text_Format) tag.[[12]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-doj-12) Metadata in the language files also indicated that the computers that created the ransomware were set to [UTC+09:00](https://en.wikipedia.org/wiki/UTC%2B09:00), used in [Korea](https://en.wikipedia.org/wiki/Korea).[[12]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-doj-12)

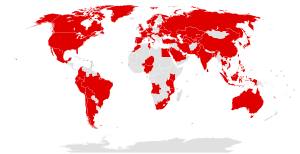
A [Google](https://en.wikipedia.org/wiki/Google) security researcher[[81]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-81)[[82]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-82) initially posted a tweet[[83]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-83) referencing code similarities between WannaCry and previous malware. Then cybersecurity companies[[84]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-84) [Kaspersky Lab](https://en.wikipedia.org/wiki/Kaspersky_Lab) and [Symantec](https://en.wikipedia.org/wiki/NortonLifeLock) have both said the code has some similarities with that previously used by the [Lazarus Group](https://en.wikipedia.org/wiki/Lazarus_Group)[[85]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-attrib-1-85) (believed to have carried out [the cyberattack on Sony Pictures](https://en.wikipedia.org/wiki/Sony_Pictures_hack) in 2014 and [a Bangladesh bank heist](https://en.wikipedia.org/wiki/Bangladesh_Bank_heist) in 2016—and linked to [North Korea](https://en.wikipedia.org/wiki/North_Korea)).[[85]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-attrib-1-85) This could also be either simple re-use of code by another group[[86]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-86) or an attempt to shift blame—as in a [cyber false flag](https://en.wikipedia.org/wiki/Cyber_false_flag) operation;[[85]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-attrib-1-85) but a leaked internal NSA memo is alleged to have also linked the creation of the worm to North Korea.[[87]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-washpo-nsa-dprk-87) [Brad Smith](https://en.wikipedia.org/wiki/Brad_Smith_(American_lawyer)), the president of Microsoft, said he believed North Korea was the originator of the WannaCry attack,[[88]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-88) and the UK's National Cyber Security Centre reached the same conclusion.[[89]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-89)

On 18 December 2017, the [United States Government](https://en.wikipedia.org/wiki/United_States_Government) formally announced that it publicly considers North Korea to be the main culprit behind the WannaCry attack.[[90]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-90) [President](https://en.wikipedia.org/wiki/U.S._President) [Trump](https://en.wikipedia.org/wiki/Donald_Trump)'s [Homeland Security Advisor](https://en.wikipedia.org/wiki/Homeland_Security_Advisor), [Tom Bossert](https://en.wikipedia.org/wiki/Tom_Bossert), wrote an [op-ed](https://en.wikipedia.org/wiki/Op-ed) in [*The Wall Street Journal*](https://en.wikipedia.org/wiki/The_Wall_Street_Journal) about this charge, saying "We do not make this allegation lightly. It is based on evidence."[[91]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-91) In a press conference the following day, Bossert said that the evidence indicates that [Kim Jong-un](https://en.wikipedia.org/wiki/Kim_Jong-un) had given the order to launch the malware attack.[[92]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-92) Bossert said that Canada, New Zealand and Japan agree with the United States' assessment of the evidence that links the attack to North Korea,[[93]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-93) while the United Kingdom's [Foreign and Commonwealth Office](https://en.wikipedia.org/wiki/Foreign_and_Commonwealth_Office) says it also stands behind the United States' assertion.[[94]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-94)

North Korea, however, denied being responsible for the cyberattack.[[95]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-95)[[96]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-96)

On 6 September 2018, the US Department of Justice (DoJ) announced formal charges against Park Jin-hyok for involvement in the [Sony Pictures hack](https://en.wikipedia.org/wiki/Sony_Pictures_hack) of 2014. The DoJ contended that Park was a North Korean hacker working as part of a team of experts for the North Korean [Reconnaissance General Bureau](https://en.wikipedia.org/wiki/Reconnaissance_General_Bureau). The Department of Justice asserted this team also had been involved in the WannaCry attack, among other activities.[[97]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-97)[[98]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-98)

Impact[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=5)]

[](https://en.wikipedia.org/wiki/File:Countries_initially_affected_in_WannaCry_ransomware_attack.svg)

Map of the countries initially affected[[99]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-99)

The ransomware campaign was unprecedented in scale according to [Europol](https://en.wikipedia.org/wiki/Europol),[[35]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-:3-35) which estimates that around 200,000 computers were infected across 150 countries. According to [Kaspersky Lab](https://en.wikipedia.org/wiki/Kaspersky_Lab), the four most affected countries were [Russia](https://en.wikipedia.org/wiki/Russia), [Ukraine](https://en.wikipedia.org/wiki/Ukraine), [India](https://en.wikipedia.org/wiki/India) and [Taiwan](https://en.wikipedia.org/wiki/Taiwan).[[100]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Jones-100)

One of the largest agencies struck by the attack was the [National Health Service](https://en.wikipedia.org/wiki/National_Health_Service) hospitals in England and Scotland,[[101]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-101)[[102]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-102) and up to 70,000 devices – including computers, [MRI scanners](https://en.wikipedia.org/wiki/Magnetic_resonance_imaging), blood-storage refrigerators and theatre equipment – may have been affected.[[103]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-14MaySunTim-103) On 12 May, some NHS services had to turn away non-critical emergencies, and some ambulances were diverted.[[104]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-BBC_news-104)[[105]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-105) In 2016, thousands of computers in 42 separate [NHS trusts](https://en.wikipedia.org/wiki/NHS_trust) in England were reported to be still running Windows XP.[[38]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-vicexp-38) In 2018 a report by Members of Parliament concluded that all 200 NHS hospitals or other organizations checked in the wake of the WannaCry attack still failed cyber security checks.[[106]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-106)[[107]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-107) NHS hospitals in Wales and Northern Ireland were unaffected by the attack.[[108]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-guardian-nhs-108)[[104]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-BBC_news-104)

[Nissan Motor Manufacturing UK](https://en.wikipedia.org/wiki/Nissan_Motor_Manufacturing_UK) in [Tyne and Wear](https://en.wikipedia.org/wiki/Tyne_and_Wear), England, halted production after the ransomware infected some of their systems. [Renault](https://en.wikipedia.org/wiki/Renault) also stopped production at several sites in an attempt to stop the spread of the ransomware.[[109]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-109)[[110]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-110) Spain's [Telefónica](https://en.wikipedia.org/wiki/Telef%C3%B3nica), [FedEx](https://en.wikipedia.org/wiki/FedEx) and [Deutsche Bahn](https://en.wikipedia.org/wiki/Deutsche_Bahn) were hit, along with many other countries and companies worldwide.[[111]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-cnn99countries-111)[[112]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-verge1-112)[[113]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-113)

The attack's impact is said to be relatively low compared to other potential attacks of the same type and could have been much worse had [Marcus Hutchins](https://en.wikipedia.org/wiki/Marcus_Hutchins) not discovered that a kill-switch had been built in by its creators[[114]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-chica1-114)[[115]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-guard1-115) or if it had been specifically targeted on highly [critical infrastructure](https://en.wikipedia.org/wiki/Critical_infrastructure), like [nuclear power plants](https://en.wikipedia.org/wiki/Nuclear_safety_and_security), dams or railway systems.[[116]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-116)[[117]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-117)

According to cyber-risk-modeling firm Cyence, economic losses from the cyber attack could reach up to US$4 billion, with other groups estimating the losses to be in the hundreds of millions.[[118]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-118)

**Affected organizations**[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=6)]

The following is an alphabetical list of organisations confirmed to have been affected:

* [Andhra Pradesh Police](https://en.wikipedia.org/wiki/Andhra_Pradesh_Police), India[[119]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-119)
* [Aristotle University of Thessaloniki](https://en.wikipedia.org/wiki/Aristotle_University_of_Thessaloniki), Greece[[120]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-120)
* [Automobile Dacia](https://en.wikipedia.org/wiki/Automobile_Dacia), Romania[[121]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-121)
* [Boeing Commercial Airplanes](https://en.wikipedia.org/wiki/Boeing_Commercial_Airplanes)[[122]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-122)
* [Cambrian College](https://en.wikipedia.org/wiki/Cambrian_College), Canada[[123]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-123)
* [Chinese public security bureau](https://en.wikipedia.org/wiki/Chinese_public_security_bureau)[[124]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-scmp-124)
* [CJ CGV](https://en.wikipedia.org/wiki/CJ_CGV) (a cinema chain)[[125]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-125)
* [Dalian Maritime University](https://en.wikipedia.org/wiki/Dalian_Maritime_University)[[126]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Cina-126)
* [Deutsche Bahn](https://en.wikipedia.org/wiki/Deutsche_Bahn)[[127]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-127)
* [Dharmais Hospital](https://en.wikipedia.org/wiki/Dharmais_Hospital), Indonesia[[128]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-misc-128)
* [Faculty Hospital, Nitra](https://en.wikipedia.org/wiki/Faculty_Hospital,_Nitra), Slovakia[[129]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-nitra-129)
* [FedEx](https://en.wikipedia.org/wiki/FedEx)[[130]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-130)
* Garena Blade and Soul[[131]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-131)
* [Guilin University of Aerospace Technology](https://en.wikipedia.org/wiki/Guilin_University_of_Aerospace_Technology)[[126]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Cina-126)
* [Guilin University of Electronic Technology](https://en.wikipedia.org/wiki/Guilin_University_of_Electronic_Technology)[[126]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Cina-126)
* [Harapan Kita Hospital](https://en.wikipedia.org/w/index.php?title=Pusat_Jantung_Nasional_Harapan_Kita&action=edit&redlink=1), Indonesia[[128]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-misc-128)
* Hezhou University[[126]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Cina-126)
* [Hitachi](https://en.wikipedia.org/wiki/Hitachi)[[132]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-132)
* [Honda](https://en.wikipedia.org/wiki/Honda)[[133]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-133)
* Instituto Nacional de Salud, [Colombia](https://en.wikipedia.org/wiki/Colombia)[[134]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-134)
* [Lakeridge Health](https://en.wikipedia.org/wiki/Lakeridge_Health)[[135]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-135)
* LAKS, Netherlands [[136]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-136)
* [LATAM Airlines Group](https://en.wikipedia.org/wiki/LATAM_Airlines_Group)[[137]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-137)
* [MegaFon](https://en.wikipedia.org/wiki/MegaFon)[[138]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-138)
* [Ministry of Internal Affairs of the Russian Federation](https://en.wikipedia.org/wiki/Ministry_of_Internal_Affairs_(Russia))[[139]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-139)
* [Ministry of Foreign Affairs (Romania)](https://en.wikipedia.org/wiki/Ministry_of_Foreign_Affairs_(Romania))[[140]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-140)
* [National Health Service (England)](https://en.wikipedia.org/wiki/National_Health_Service_(England))[[141]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-uk-141)[[104]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-BBC_news-104)[[108]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-guardian-nhs-108)
* [NHS Scotland](https://en.wikipedia.org/wiki/NHS_Scotland)[[104]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-BBC_news-104)[[108]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-guardian-nhs-108)
* [Nissan Motor Manufacturing UK](https://en.wikipedia.org/wiki/Nissan_Motor_Manufacturing_UK)[[141]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-uk-141)
* [O2](https://en.wikipedia.org/wiki/Telef%C3%B3nica_Europe), Germany[[142]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-142)[[143]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-143)
* [Petrobrás](https://en.wikipedia.org/wiki/Petrobr%C3%A1s)[[144]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-auto1-144)
* [PetroChina](https://en.wikipedia.org/wiki/PetroChina)[[111]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-cnn99countries-111)[[124]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-scmp-124)
* [Portugal Telecom](https://en.wikipedia.org/wiki/Portugal_Telecom)[[145]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-145)
* [Pulse FM](https://en.wikipedia.org/wiki/Pulse_FM)[[146]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-146)
* [Q-Park](https://en.wikipedia.org/wiki/Q-Park)[[147]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-147)
* [Renault](https://en.wikipedia.org/wiki/Renault)[[148]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-148)
* [Russian Railways](https://en.wikipedia.org/wiki/Russian_Railways)[[149]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-149)
* [Sandvik](https://en.wikipedia.org/wiki/Sandvik)[[128]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-misc-128)
* [Justice Court of São Paulo](https://en.wikipedia.org/wiki/Justice_Court_of_S%C3%A3o_Paulo)[[144]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-auto1-144)
* [Saudi Telecom Company](https://en.wikipedia.org/wiki/Saudi_Telecom_Company)[[150]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-150)
* [Sberbank](https://en.wikipedia.org/wiki/Sberbank_of_Russia)[[151]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-vidal-151)
* [Shandong University](https://en.wikipedia.org/wiki/Shandong_University)[[126]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Cina-126)
* State Governments of India
  + [Government of Gujarat](https://en.wikipedia.org/wiki/Government_of_Gujarat)[[152]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-auto2-152)
  + [Government of Kerala](https://en.wikipedia.org/wiki/Government_of_Kerala)[[152]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-auto2-152)
  + [Government of Maharashtra](https://en.wikipedia.org/wiki/Government_of_Maharashtra)[[153]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-153)
  + [Government of West Bengal](https://en.wikipedia.org/wiki/Government_of_West_Bengal)[[152]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-auto2-152)
* Suzhou Vehicle Administration[[126]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-Cina-126)
* [Sun Yat-sen University](https://en.wikipedia.org/wiki/Sun_Yat-sen_University), China[[128]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-misc-128)
* [Telefónica](https://en.wikipedia.org/wiki/Telef%C3%B3nica), Spain[[154]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-spain-154)
* [Telenor Hungary](https://en.wikipedia.org/wiki/Telenor_Hungary), Hungary[[155]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-155)
* [Telkom (South Africa)](https://en.wikipedia.org/wiki/Telkom_(South_Africa))[[156]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-156)
* [Timrå Municipality](https://en.wikipedia.org/wiki/Timr%C3%A5_Municipality), Sweden[[157]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-157)
* [TSMC](https://en.wikipedia.org/wiki/TSMC), Taiwan[[158]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-158)
* [Universitas Jember](https://en.wikipedia.org/wiki/Universitas_Jember), Indonesia[[159]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-159)
* [University of Milano-Bicocca](https://en.wikipedia.org/wiki/University_of_Milano-Bicocca), Italy[[160]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-160)
* [University of Montreal](https://en.wikipedia.org/wiki/Universit%C3%A9_de_Montr%C3%A9al), Canada[[161]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-161)
* [Vivo](https://en.wikipedia.org/wiki/Vivo_(telecommunications)), Brazil[[144]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-auto1-144)

Reactions[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=7)]

A number of experts highlighted the [NSA](https://en.wikipedia.org/wiki/National_Security_Agency)'s non-disclosure of the underlying vulnerability, and their loss of control over the EternalBlue attack tool that exploited it. [Edward Snowden](https://en.wikipedia.org/wiki/Edward_Snowden) said that if the NSA had "[privately disclosed](https://en.wikipedia.org/wiki/Responsible_disclosure) the flaw used to attack hospitals when they found it, not when they lost it, the attack may not have happened".[[162]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-162) British cybersecurity expert [Graham Cluley](https://en.wikipedia.org/wiki/Graham_Cluley) also sees "some culpability on the part of the U.S. intelligence services". According to him and others "they could have done something ages ago to get this problem fixed, and they didn't do it". He also said that despite obvious uses for such tools [to spy on people of interest](https://en.wikipedia.org/wiki/Targeted_surveillance), they have a duty to protect their countries' citizens.[[163]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-163) Others have also commented that this attack shows that the practice of intelligence agencies to stockpile exploits for offensive purposes rather than disclosing them for defensive purposes may be problematic.[[115]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-guard1-115) Microsoft president and chief legal officer [Brad Smith](https://en.wikipedia.org/wiki/Brad_Smith_(American_lawyer)) wrote, "Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its [Tomahawk missiles](https://en.wikipedia.org/wiki/Tomahawk_(missile)) stolen."[[164]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-164)[[165]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-165)[[166]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-166) Russian President [Vladimir Putin](https://en.wikipedia.org/wiki/Vladimir_Putin) placed the responsibility of the attack on U.S. intelligence services, for having created EternalBlue.[[151]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-vidal-151)

On 17 May 2017, United States bipartisan lawmakers introduced the [PATCH Act](https://en.wikipedia.org/w/index.php?title=PATCH_Act&action=edit&redlink=1)[[167]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-167) that aims to have exploits reviewed by an independent board to "balance the need to disclose vulnerabilities with other national security interests while increasing transparency and accountability to maintain public trust in the process".[[168]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-168)

On 15 June 2017, the United States Congress was to hold a hearing on the attack.[[169]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-thehill.com-169) Two subpanels of the House Science Committee were to hear the testimonies from various individuals working in the government and non-governmental sector about how the US can improve its protection mechanisms for its systems against similar attacks in the future.[[169]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-thehill.com-169)

[Marcus Hutchins](https://en.wikipedia.org/wiki/Marcus_Hutchins), a cybersecurity researcher, working in loose collaboration with UK's [National Cyber Security Centre](https://en.wikipedia.org/wiki/National_Cyber_Security_Centre_(United_Kingdom)),[[170]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-170)[[171]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-sky1-171) researched the malware and discovered a "kill switch".[[53]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-MalwareTech-53) Later globally dispersed security researchers [collaborated online](https://en.wikipedia.org/wiki/Collaboration#Technology) to [develop](https://en.wikipedia.org/wiki/Civic_hacking) [open source](https://en.wikipedia.org/wiki/Open-source_software) tools[[172]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-wanakiwi-172)[[173]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-173) that allow for decryption without payment under some circumstances.[[174]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-reuters1-174) Snowden states that when "[NSA](https://en.wikipedia.org/wiki/NSA)-enabled ransomware eats the Internet, help comes from researchers, not spy agencies" and asks why this is the case.[[175]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-175)[[176]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-176)[[171]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-sky1-171)

Other experts also used the publicity around the attack as a chance to reiterate the value and importance of having good, regular and [secure](https://en.wikipedia.org/wiki/Storage_security) [backups](https://en.wikipedia.org/wiki/Backup), good [cybersecurity](https://en.wikipedia.org/wiki/Cybersecurity) including isolating critical systems, using appropriate software, and having the latest security patches installed.[[177]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-177) [Adam Segal](https://en.wikipedia.org/wiki/Adam_Segal), director of the digital and cyberspace policy program at the [Council on Foreign Relations](https://en.wikipedia.org/wiki/Council_on_Foreign_Relations), stated that "the patching and updating systems are broken, basically, in the private sector and in government agencies".[[115]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-guard1-115) In addition, Segal said that governments' apparent inability to secure vulnerabilities "opens a lot of questions about backdoors and access to encryption that the government argues it needs from the private sector for security".[[115]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-guard1-115) [Arne Schönbohm](https://en.wikipedia.org/wiki/Arne_Sch%C3%B6nbohm), president of Germany's [Federal Office for Information Security](https://en.wikipedia.org/wiki/Federal_Office_for_Information_Security) (BSI), stated that "the current attacks show how vulnerable our [digital society](https://en.wikipedia.org/wiki/Information_society) is. It's a wake-up call for companies to finally take IT security [seriously]".[[178]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-hei-178)

**United Kingdom**[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=8)]

The effects of the attack also had political implications; in the [United Kingdom](https://en.wikipedia.org/wiki/United_Kingdom), the impact on the [National Health Service](https://en.wikipedia.org/wiki/National_Health_Service) quickly became political, with claims that the effects were exacerbated by Government underfunding of the NHS; in particular, the NHS ceased its paid Custom Support arrangement to continue receiving support for unsupported Microsoft software used within the organization, including Windows XP.[[179]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-179) [Home Secretary](https://en.wikipedia.org/wiki/Home_Secretary) [Amber Rudd](https://en.wikipedia.org/wiki/Amber_Rudd) refused to say whether patient data had been [backed up](https://en.wikipedia.org/wiki/Backup), and [Shadow Health Secretary](https://en.wikipedia.org/wiki/Shadow_Secretary_of_State_for_Health) [Jon Ashworth](https://en.wikipedia.org/wiki/Jon_Ashworth) accused [Health Secretary](https://en.wikipedia.org/wiki/Secretary_of_State_for_Health) [Jeremy Hunt](https://en.wikipedia.org/wiki/Jeremy_Hunt) of refusing to act on a critical note from Microsoft, the [National Cyber Security Centre](https://en.wikipedia.org/wiki/National_Cyber_Security_Centre_(United_Kingdom)) (NCSC) and the [National Crime Agency](https://en.wikipedia.org/wiki/National_Crime_Agency) that had been received two months previously.[[180]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-180)

Others argued that hardware and software vendors often fail to account for future security flaws, selling systems that − due to their technical design and market incentives − eventually won't be able to properly receive and apply patches.[[181]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-181)

The NHS denied that it was still using XP, claiming only 4.7% of devices within the organization ran Windows XP.[[182]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-nhs-noxp-182)[[41]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-verge-xpimpact-41) The cost of the attack to the NHS was estimated as £92 million in disruption to services and IT upgrades.[[183]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-183)

After the attack, [NHS Digital](https://en.wikipedia.org/wiki/NHS_Digital) refused to finance the estimated £1 billion to meet the [Cyber Essentials Plus](https://en.wikipedia.org/wiki/Cyber_Essentials#Assurance_framework) standard, an information security certification organized by the UK NCSC, saying this would not constitute "value for money", and that it had invested over £60 million and planned "to spend a further £150 [million] over the next two years" to address key cyber security weaknesses.[[184]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-184)

2018 email scam[[edit](https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&action=edit&section=9)]

In late June, hundreds of computer users reported being sent an email from someone (or multiple people), claiming to be the developers of WannaCry.[[185]](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#cite_note-185) The email threatened to destroy the victims' data unless they sent 0.1 [BTC](https://en.wikipedia.org/wiki/Bitcoin) to the Bitcoin address of the hackers. This has also happened in 2019.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]