WannaCry ransomware attack

The **WannaCry ransomware attack** was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[5] It propagated through EternalBlue, an exploit discovered by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers at least a year prior to the attack. While 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. 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 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. 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, United Kingdom and Australia formally asserted that North Korea was behind the attack.[6]

A new variant of WannaCry forced 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.[7]

Contents

- Description
- Attack
  - Defensive response
- Attribution
- Impact
  - Affected organizations
- Reactions
  - United Kingdom
- 2018 email scam
- See also
- References
- External links

WannaCry ransomware attack



Screenshot of the ransom note left on an infected system

Date	12 May 2017 – 15 May 2017 (initial outbreak)[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
Theme	Ransomware encrypting files with $300 – $600 USD demand (via bitcoin)
Cause	WannaCry worm
Outcome	200,000 victims 300,000+ computers infected[2][3][4]
Arrests	None
Suspects	Lazarus Group
Accused	Two North Koreans Indicted
Convictions	None

Description

WannaCry

Subtype	Ransomware
Point of origin	Pyongyang, North Korea
Author(s)	Lazarus Group

WannaCry is a ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The worm is also known as WannaCrypt,[8] Wana Decryptor 2.0,[9] WanaCryptor 2.0,[10] and Wanna Decryptor.[11] 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 exploit to gain access, and the DoublePulsar tool to install and execute a copy of itself.[12] WannaCry versions 0, 1, and 2 were created using Microsoft Visual C++ 6.0.[13]

EternalBlue is an exploit of Windows' Server Message Block (SMB) protocol released by The Shadow Brokers. Much of the attention and comment around the event was occasioned by the fact that the U.S. 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, rather than report it to Microsoft.[14][15] Microsoft eventually discovered the vulnerability, and on Tuesday, 14 March 2017, they issued security bulletin MS17-010, which detailed the flaw and announced that patches had been released for all Windows versions that were currently supported at that time, these being Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016.[16]

DoublePulsar is a backdoor tool, also released by 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.[17] By 25 April, reports estimated that the number of infected computers could be up to several hundred thousand, with numbers increasing every day.[18][19] The WannaCry code can take advantage of any existing DoublePulsar infection, or installs it itself.[12][20][21] On 9 May 2017, private cybersecurity company RiskSense released code on GitHub 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" domain name; if it is not found, then the ransomware encrypts the computer's data,[22][23][24] then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet,[25] and "laterally" to computers on the same network.[26] As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around US$300 in bitcoin within three days, or US$600 within seven days.[23][27] Three hardcoded 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 owners remain unknown.[28]

Several organizations released detailed technical writeups of the malware, including a senior security analyst at RiskSense,[29][30] Microsoft,[31] Cisco,[12] Malwarebytes,[25] Symantec and McAfee.[26]

Attack

The attack began on Friday, 12 May 2017,[32][33] with evidence pointing to an initial infection in Asia at 07:44 UTC.[32][34] The initial infection was likely through an exposed vulnerable SMB port,[35] rather than email phishing as initially assumed.[32] Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.[36][37]

Organizations that had not installed Microsoft's security update from April 2017 were affected by the attack.[38] Those still running unsupported versions of Microsoft Windows, such as Windows XP and Windows Server 2003[39][40] 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.[8] A 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.[8][41] 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.[42][43][44]

Defensive response

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.[45][46][47] 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.[48]

The day after the initial attack in May, Microsoft released out-of-band security updates for end of life products Windows XP, Windows Server 2003 and Windows 8; these patches had been created in February of that year following a tip off about the vulnerability in January of that year.[49][40] Organizations were advised to patch Windows and plug the vulnerability in order to protect themselves from the cyber attack.[50] 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]".[51][52]

Researcher Marcus Hutchins[53][54] discovered the kill switch domain hardcoded in the malware.[55][56][57] Registering a domain name for a 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.[58][59][60][61][62] On 14 May, a first variant of WannaCry appeared with a new and second[63] kill-switch registered by 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 threat intelligence analysts.[64][65] A few days later, a new version of WannaCry was detected that lacked the kill switch altogether.[66][67][68][69]

On 19 May, it was reported that hackers were trying to use a Mirai botnet variant to effect a distributed attack on WannaCry's kill-switch domain with the intention of knocking it offline.[70] 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.[71]

Separately, researchers from University College London and 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.[72][73]

It was discovered that Windows encryption APIs used by WannaCry may not completely clear the prime numbers 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.[74] This behaviour was used by a French researcher to develop a tool known as WannaKey, which automates this process on Windows XP systems.[75][76][77] 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.[78]

Within four days of the initial outbreak, new infections had slowed to a trickle due to these responses.[79]

Attribution

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.[80][81] According to an analysis by the FBI's Cyber Behavioral Analysis Center, the computer that created the ransomware language files had Hangul language fonts installed, as evidenced by the presence of the "\fcharset129" Rich Text Format tag.[13] Metadata in the language files also indicated that the computers that created the ransomware were set to UTC+09:00, used in Korea.[13]

A Google security researcher[82][83] initially posted a tweet[84] referencing code similarities between WannaCry and previous malware. The cybersecurity companies[85] Kaspersky Lab and Symantec have both said the code has some similarities with that previously used by the Lazarus Group[86] (believed to have carried out the cyberattack on Sony Pictures in 2014 and a Bangladesh bank heist in 2016—and linked to North Korea).[86] This could also be either simple re-use of code by another group[87] or an attempt to shift blame—as in a cyber false flag operation;[86] but a leaked internal NSA memo is alleged to have also linked the creation of the worm to North Korea.[88] Brad Smith, the president of Microsoft, said he believed North Korea was the originator of the WannaCry attack,[89] and the UK's National Cyber Security Centre reached the same conclusion.[90]

On 18 December 2017, the United States Government formally announced that it publicly considers North Korea to be the main culprit behind the WannaCry attack.[91] President Trump's Homeland Security Advisor, Tom Bossert, wrote an op-ed in *The Wall Street Journal* about this charge, saying "We do not make this allegation lightly. It is based on evidence."[92] In a press conference the following day, Bossert said that the evidence indicates that Kim Jong-un had given the order to launch the malware attack.[93] Bossert said that Canada, New Zealand and Japan agree with the United States' assessment of the evidence that links the attack to North Korea,[94] while the United Kingdom's Foreign and Commonwealth Office says it also stands behind the United States' assertion.[95]

North Korea, however, denied being responsible for the cyberattack.[96][97]

On 6 September 2018, the US Department of Justice (DoJ) announced formal charges against Park Jin-hyok for involvement in the 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. The Department of Justice asserted this team also had been involved in the WannaCry attack, among other activities.[98][99]

Impact

The ransomware campaign was unprecedented in scale according to Europol,[36] which estimates that around 200,000 computers were infected across 150 countries. According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India and Taiwan.[101]



Map of the countries initially affected[100]

One of the largest agencies struck by the attack was the National Health Service hospitals in England and Scotland,[102][103] and up to 70,000 devices – including computers, MRI scanners, blood-storage refrigerators and theatre equipment – may have been affected.[104] On 12 May, some NHS services had to turn away non-critical emergencies, and some ambulances were diverted.[105][106] In 2016, thousands of computers in 42 separate NHS trusts in England were reported to be still running Windows XP.[39] 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.[107][108] NHS hospitals in Wales and Northern Ireland were unaffected by the attack.[109][105]

Nissan Motor Manufacturing UK in Tyne and Wear, England, halted production after the ransomware infected some of their systems. Renault also stopped production at several sites in an attempt to stop the spread of the ransomware.[110][111] Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide.[112][113][114]

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 not discovered that a kill-switch had been built in by its creators[115][116] or if it had been specifically targeted on highly critical infrastructure, like nuclear power plants, dams or railway systems.[117][118]

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.[119]

Affected organizations

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

- Andhra Pradesh Police, India[120]
- Aristotle University of Thessaloniki, Greece[121][122]
- Automobile Dacia, Romania[123]
- Boeing Commercial Airplanes[124]
- Cambrian College, Canada[125]
- Chinese public security bureau[126]
- CJ CGV (a cinema chain)[127]
- Dalian Maritime University[128]
- Deutsche Bahn[129]
- Dharmais Hospital, Indonesia[130]
- Faculty Hospital, Nitra, Slovakia[131]
- FedEx[132]
- Garena Blade and Soul[133]
- Guilin University of Aerospace Technology[128]
- Guilin University of Electronic Technology[128]
- Harapan Kita Hospital, Indonesia[130]
- Hezhou University[128]
- Hitachi[134]
- Honda[135]
- Instituto Nacional de Salud, Colombia[136]
- Lakeridge Health[137]
- LAKS, Netherlands [138]
- LATAM Airlines Group[139]
- MegaFon[140]
- Ministry of Internal Affairs of the Russian Federation[141]
- National Health Service (England)[142][105][109]
- NHS Scotland[105][109]
- Nissan Motor Manufacturing UK[142]
- O2, Germany[143][144]
- Petrobrás[145]
- PetroChina[112][126]
- Portugal Telecom[146]
- Pulse FM[147]
- Q-Park[148]
- Renault[149]
- Russian Railways[150]
- Sandvik[130]
- Justice Court of São Paulo[145]
- Saudi Telecom Company[151]
- Sberbank[152]
- Shandong University[128]
- State Governments of India
  - Government of Gujarat[153]
  - Government of Kerala[153]
  - Government of Maharashtra[154]
  - Government of West Bengal[153]
- Suzhou Vehicle Administration[128]
- Sun Yat-sen University, China[130]
- Telefónica, Spain[155]
- Telenor Hungary, Hungary[156]
- Telkom (South Africa)[157]
- Timrå Municipality, Sweden[158]
- TSMC, Taiwan[159]
- Universitas Jember, Indonesia[160]
- University of Milano-Bicocca, Italy[161]
- University of Montreal, Canada[162]
- Vivo, Brazil[145]

Reactions

A number of experts highlighted the NSA's non-disclosure of the underlying vulnerability, and their loss of control over the EternalBlue attack tool that exploited it. Edward Snowden said that if the NSA had "privately disclosed the flaw used to attack hospitals when they found it, not when they lost it, the attack may not have happened".[163] British cybersecurity expert 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, they have a duty to protect their countries' citizens.[164] 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.[116] Microsoft president and chief legal officer Brad Smith 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 stolen."[165][166][167] Russian President Vladimir Putin placed the responsibility of the attack on U.S. intelligence services, for having created EternalBlue.[152]

On 17 May 2017, United States bipartisan lawmakers introduced the PATCH Act[168] 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".[169]

On 15 June 2017, the United States Congress was to hold a hearing on the attack.[170] 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.[170]

Marcus Hutchins, a cybersecurity researcher, working in loose collaboration with UK's National Cyber Security Centre,[171][172] researched the malware and discovered a "kill switch".[54] Later globally dispersed security researchers collaborated online to develop open source tools[173][174] that allow for decryption without payment under some circumstances.[175] Snowden states that when "NSA-enabled ransomware eats the Internet, help comes from researchers, not spy agencies" and asks why this is the case.[176][177][172]

Other experts also used the publicity around the attack as a chance to reiterate the value and importance of having good, regular and secure backups, good cybersecurity including isolating critical systems, using appropriate software, and having the latest security patches installed.[178] Adam Segal, director of the digital and cyberspace policy program at the Council on Foreign Relations, stated that "the patching and updating systems are broken, basically, in the private sector and in government agencies".[116] 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".[116] Arne Schönbohm, president of Germany's Federal Office for Information Security (BSI), stated that "the current attacks show how vulnerable our digital society is. It's a wake-up call for companies to finally take IT security [seriously]".[179]

United Kingdom

The effects of the attack also had political implications; in the United Kingdom, the impact on the 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.[180] Home Secretary Amber Rudd refused to say whether patient data had been backed up, and Shadow Health Secretary Jon Ashworth accused Health Secretary Jeremy Hunt of refusing to act on a critical note from Microsoft, the National Cyber Security Centre (NCSC) and the National Crime Agency that had been received two months previously.[181]

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.[182]

The NHS denied that it was still using XP, claiming only 4.7% of devices within the organization ran Windows XP.[183][42] The cost of the attack to the NHS was estimated as £92 million in disruption to services and IT upgrades.[184]

After the attack, NHS Digital refused to finance the estimated £1 billion to meet the Cyber Essentials Plus 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.[185]

2018 email scam

In late June, hundreds of computer users reported receiving an email claiming to be from the developers of WannaCry.[186] The email threatened to destroy the victims' data unless they sent 0.1 BTC to the Bitcoin address of the hackers. This also happened in 2019.

See also

- BlueKeep (security vulnerability)
- Computer security § Medical systems
- Comparison of computer viruses
- Conficker
- CryptoLocker
- Cyber self-defense
- Cyberweapon § Control and disarmament
- International Multilateral Partnership Against Cyber Threats
- Proactive cyber defence § Measures
- Security engineering
- Software versioning
- SQL Slammer
- Timeline of computer viruses and worms
- Vault 7
- Windows Update
- 2016 Dyn cyberattack
- 2017 Petya cyberattack

References

1. "The WannaCry ransomware attack was temporarily halted. But it's not over yet" (https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp). 15 May 2017.
2. "Ransomware attack still looms in Australia as Government warns WannaCry threat not over" (http://www.abc.net.au/news/2017-05-15/ransomware-attack-to-hit-victims-in-australia-government-says/8526346). Australian Broadcasting Corporation. 14 May 2017. Retrieved 15 May 2017.
3. Cameron, Dell (13 May 2017). "Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It" (https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/). *Gizmodo*. Retrieved 13 May 2017.
4. "Shadow Brokers threaten to release Windows 10 hacking tools" (https://tribune.com.pk/story/1423609/shadow-brokers-threaten-release-windows-10-hacking-tools/). *The Express Tribune*. 31 May 2017. Retrieved 31 May 2017.
5. "Two years after WannaCry, a million computers remain at risk" (https://social.techcrunch.com/2019/05/12/wannacry-two-years-on/). *TechCrunch*. Retrieved 16 January 2021.
6. Thomas P. Bossert (18 December 2017). "It's Official: North Korea Is Behind WannaCry" (https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537). *The Wall Street Journal*. Retrieved 19 December 2017.
7. "TSMC Chip Maker Blames WannaCry Malware for Production Halt" (https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html). *The Hacker News*. Retrieved 7 August 2018.
8. MSRC Team (13 May 2017). "Customer Guidance for WannaCrypt attacks" (https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/). Microsoft. Retrieved 13 May 2017.

9. Jakub Kroustek (12 May 2017). "Avast reports on WanaCrypt0r 2.0 ransomware that infected NHS and Telefonica" (https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today). *Avast Security News*. Avast Software, Inc.
10. Fox-Brewster, Thomas. "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak" (https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/). *Forbes*. Retrieved 12 May 2017.
11. Woollaston, Victoria. "Wanna Decryptor: what is the 'atom bomb of ransomware' behind the NHS attack?" (https://www.wired.co.uk/article/wanna-decryptor-ransomware). *WIRED UK*. Retrieved 13 May 2017.
12. "Player 3 Has Entered the Game: Say Hello to 'WannaCry' " (http://blog.talosintelligence.com/2017/05/wannacry.html). *blog.talosintelligence.com*. Retrieved 16 May 2017.
13. Shields, Nathan P. (8 June 2018). "Criminal Complaint" (https://www.justice.gov/opa/press-release/file/1092091/download). United States Department of Justice.
14. "NHS cyber attack: Edward Snowden says NSA should have prevented cyber attack" (https://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-edward-snowden-accuses-nsa-not-preventing-ransomware-a7733941.html). *The Independent*. Retrieved 13 May 2017.
15. Graham, Chris (13 May 2017). "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history" (https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/). *The Daily Telegraph*. Retrieved 13 May 2017.
16. "NSA-leaking Shadow Brokers just dumped its most damaging release yet" (https://arstechnica.com/security/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/). *Ars Technica*. Retrieved 15 April 2017.
17. Goodin, Dan. "10,000 Windows computers may be infected by advanced NSA backdoor" (https://arstechnica.com/uwusecurity/2017/04/10000-windows-computers-may-be-infected-by-advanced-nsa-backdoor/). *Ars Technica*. Retrieved 14 May 2017.
18. Goodin, Dan. "NSA backdoor detected on >55,000 Windows boxes can now be remotely removed" (https://arstechnica.com/security/2017/04/nsa-backdoor-detected-on-55000-windows-boxes-can-now-be-remotely-removed/). *Ars Technica*. Retrieved 14 May 2017.
19. Broersma, Matthew. "NSA Malware 'Infects Nearly 200,000 Systems' " (http://www.silicon.co.uk/security/nsa-malware-security-210253). *Silicon*. Retrieved 14 May 2017.
20. Cameron, Dell (13 May 2017). "Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It" (https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/). *Gizmodo*. Retrieved 15 May 2017.
21. "How One Simple Trick Just Put Out That Huge Ransomware Fire" (https://www.forbes.com/sites/thomasbrewster/2017/05/13/wannacry-ransomware-outbreak-stopped-by-researcher/). *Forbes*. 24 April 2017. Retrieved 15 May 2017.
22. "Russian-linked cyber gang blamed for NHS computer hack using bug stolen from US spy agency" (https://www.telegraph.co.uk/news/2017/05/12/russian-linked-cyber-gang-shadow-brokers-blamed-nhs-computer/). *The Telegraph*. Retrieved 12 May 2017.
23. "What you need to know about the WannaCry Ransomware" (https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware). Symantec Security Response. Retrieved 14 May 2017.
24. Bilefsky, Dan; Perlroth, Nicole (12 May 2017). "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool" (https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 12 May 2017.
25. Clark, Zammis (13 May 2017). "The worm that spreads WanaCrypt0r" (https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/). *Malwarebytes Labs*. malwarebytes.com. Retrieved 13 May 2017.
26. Samani, Raj. "An Analysis of the WANNACRY Ransomware outbreak" (https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/). McAfee. Retrieved 13 May 2017.
27. Thomas, Andrea; Grove, Thomas; Gross, Jenny (13 May 2017). "More Cyberattack Victims Emerge as Agencies Search for Clues" (https://www.wsj.com/articles/more-cyberattack-victims-emerge-as-agencies-search-for-clues-1494671938). *The Wall Street Journal*. ISSN 0099-9660 (https://www.worldcat.org/issn/0099-9660). Retrieved 14 May 2017.

28. Collins, Keith. "Watch as these bitcoin wallets receive ransomware payments from the global cyberattack" (https://qz.com/982993/watch-as-these-bitcoin-wallets-receive-ransomware-payments-from-the-ongoing-cyberattack/). *Quartz*. Retrieved 14 May 2017.
29. "MS17-010 (SMB RCE) Metasploit Scanner Detection Module" (https://zerosum0x0.blogspot.com/2017/04/ms17-010-smb-rce-metasploit-scanner.html). *@zerosum0x0*. @zerosum0x0. 18 April 2017. Retrieved 18 April 2017.
30. "DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis" (https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html). *@zerosum0x0*. @zerosum0x0. 21 April 2017. Retrieved 21 April 2017.
31. "WannaCrypt ransomware worm targets out-of-date systems" (https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/). *TechNet*. Microsoft. 13 May 2017. Retrieved 20 May 2017.
32. Brenner, Bill (16 May 2017). "WannaCry: the ransomware worm that didn't arrive on a phishing hook" (https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/). *Naked Security*. Sophos. Retrieved 18 May 2017.
33. Newman, Lily Hay (12 May 2017). "The Ransomware Meltdown Experts Warned About Is Here" (https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/). *Wired*. Retrieved 13 May 2017.
34. Yuzifovich, Yuriy. "WannaCry: views from the DNS frontline" (https://www.nominum.com/tech-blog/wannacry-views-dns-frontline/). *Security and Data Science*. nominum. Retrieved 18 May 2017.
35. Goodin, Dan. "An NSA-derived ransomware worm is shutting down computers worldwide" (https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/). *Ars Technica*. Retrieved 14 May 2017.
36. "Cyber-attack: Europol says it was unprecedented in scale" (https://www.bbc.com/news/world-europe-39907965). *BBC News*. 13 May 2017. Retrieved 13 May 2017.
37. " 'Unprecedented' cyberattack hits 200,000 in at least 150 countries, and the threat is escalating" (https://www.cnbc.com/2017/05/14/cyber-attack-hits-200000-in-at-least-150-countries-europol.html). CNBC. 14 May 2017. Retrieved 16 May 2017.
38. "WannaCry Ransomware Attack Hits Victims With Microsoft SMB Exploit" (http://www.eweek.com/security/wannacry-ransomware-attack-hits-victims-with-microsoft-smb-exploit). *eWeek*. Retrieved 13 May 2017.
39. "NHS Hospitals Are Running Thousands of Computers on Unsupported Windows XP" (https://motherboard.vice.com/en_us/article/nhs-hospitals-are-running-thousands-of-computers-on-unsupported-windows-xp). *Motherboard*. Retrieved 13 May 2017.
40. "Microsoft issues 'highly unusual' Windows XP patch to prevent massive ransomware attack" (https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack). *The Verge*. Vox Media. 13 May 2017. Retrieved 13 May 2017.
41. Brandom, Russell (19 May 2017). "Almost all WannaCry victims were running Windows 7" (https://www.theverge.com/2017/5/19/15665488/wannacry-windows-7-version-xp-patched-victim-statistics). *The Verge*. Vox Media. Retrieved 10 December 2020.
42. Brandom, Russell (30 May 2017). "Windows XP computers were mostly immune to WannaCry" (https://www.theverge.com/2017/5/30/15712542/windows-xp-wannacry-protect-ransomware-blue-screen). *The Verge*. Vox Media. Retrieved 10 December 2020.
43. "WannaCry: Two Weeks and 16 Million Averted Ransoms Later" (https://blog.kryptoslogic.com/malware/2017/05/29/two-weeks-later.html). Kryptos Logic. Retrieved 30 May 2017.
44. "Παγκόσμιος τρόμος: Πάνω από 100 χώρες "χτύπησε" ο WannaCry που ζητάει λύτρα!" (https://www.newsit.gr/kosmos/pagkosmios-tromos-pano-apo-100-xores-xtypisan-oi-xakers-poy-zitoyn-lytra/1023246/). *newsit.gr*. 13 May 2017.
45. Reynolds, Matt (17 May 2017). "Ransomware attack hits 200,000 computers across the globe" (https://www.newscientist.com/article/mg23431263-500-ransomware-attack-hits-200000-computers-across-the-globe/). *New Scientist*. Retrieved 10 December 2020.
46. Baraniuk, Chris (15 May 2017). "Should you pay the WannaCry ransom?" (https://www.bbc.com/news/technology-39920269). *BBC News*. Retrieved 10 December 2020.
47. Palmer, Danny (22 May 2017). "Ransomware: WannaCry was basic, next time could be much worse" (https://www.zdnet.com/article/ransomware-wannacry-was-basic-next-time-could-be-much-worse/). *ZDNet*. Retrieved 10 December 2020.

48. Collins, Keith (13 May 2017). "Watch as these bitcoin wallets receive ransomware payments from the ongoing global cyberattack" (https://qz.com/982993/watch-as-these-bitcoin-wallets-receive-ransomware-payments-from-the-ongoing-cyberattack/). *Quartz*. Retrieved 10 December 2020.
49. Thompson, Iain (16 May 2017). "While Microsoft griped about NSA exploit stockpiles, it stockpiled patches: Friday's WinXP fix was built in February" (https://www.theregister.co.uk/2017/05/16/microsoft_stockpiling_flaws_too/). *The Register*. Retrieved 19 December 2017.
50. "Global Reports of WannaCry Ransomware Attacks – Defensorum" (https://www.defensorum.com/global-reports-wannacry-ransomware-attacks/). *Defensorum*. 18 August 2017. Retrieved 16 October 2017.
51. Hern, Alex (14 June 2017). "WannaCry attacks prompt Microsoft to release Windows updates for older versions" (https://www.theguardian.com/technology/2017/jun/14/wannacry-attacks-prompt-microsoft-to-release-updates-for-older-windows-versions). *The Guardian*. ISSN 0261-3077 (https://www.worldcat.org/issn/0261-3077). Retrieved 14 June 2017.
52. "Microsoft rushes out patch for Windows XP to prevent another WannaCry attack via a Shadow Brokers release" (https://www.computing.co.uk/ctg/news/3011916/microsoft-rushes-out-patch-for-windows-xp-to-prevent-another-wannacry-attack-via-a-shadow-brokers-release). *Computing.com*. 14 June 2017. ISSN 0261-3077 (https://www.worldcat.org/issn/0261-3077). Retrieved 14 June 2017.
53. " 'Just doing my bit': The 22yo who blocked the WannaCry cyberattack" (http://www.abc.net.au/news/2017-05-16/ransomware-cyberattack-marcus-hutchins-gives-interview/8530574). *ABC News*. 16 May 2017. Retrieved 17 May 2017.
54. MalwareTech (13 May 2017). "How to Accidentally Stop a Global Cyber Attacks" (https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html).
55. Bodkin, Henry; Henderson, Barney; Donnelly, Laura; Mendick, Robert; Farmer, Ben; Graham, Chris (12 May 2017). "Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms" (https://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/). *The Telegraph*.
56. Thomson, Iain (13 May 2017). "74 countries hit by NSA-powered WannaCrypt ransomware backdoor: Emergency fixes emitted by Microsoft for WinXP+" (https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/). *The Register*.
57. Khomami, Nadia; Solon, Olivia (13 May 2017). " 'Accidental hero' halts ransomware attack and warns: this is not over" (https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack). *The Guardian*.
58. Newman, Lily Hay. "How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack" (https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/). *Wired Security*. Retrieved 14 May 2017.
59. Solon, Olivia (13 May 2017). " 'Accidental hero' finds kill switch to stop spread of ransomware cyber-attack" (https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack). *The Guardian*. London. Retrieved 13 May 2017.
60. Foxx, Chris (13 May 2017). "Global cyber-attack: Security blogger halts ransomware 'by accident' " (https://www.bbc.co.uk/news/technology-39907049). BBC. Retrieved 13 May 2017.
61. Kan, Micael (12 May 2017). "A 'kill switch' is slowing the spread of WannaCry ransomware" (http://www.pcworld.com/article/3196515/security/a-kill-switch-is-slowing-the-spread-of-wannacry-ransomware.html). *PC World*. Retrieved 13 May 2017.
62. "How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack" (https://www.computerworld.com/article/3196686/security/kill-switch-helps-slow-the-spread-of-wannacry-ransomware.html/). 12 May 2017. Retrieved 19 December 2017.
63. Wong, Joon Ian; Wong, Joon Ian. "Just two domain names now stand between the world and global ransomware chaos" (https://qz.com/983569/a-second-wave-of-wannacry-infections-has-been-halted-with-a-new-killswitch/). *Quartz*.
64. "The Hours of WannaCry" (https://umbrella.cisco.com/blog/2017/05/16/the-hours-of-wannacry/). 17 May 2017.
65. "WannaCry – New Kill-Switch, New Sinkhole" (https://blog.checkpoint.com/2017/05/15/wannacry-new-kill-switch-new-sinkhole/). *Check Point Software Blog*. 15 May 2017.
66. Khandelwal, Swati. "It's Not Over, WannaCry 2.0 Ransomware Just Arrived With No 'Kill-Switch' " (http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html). *The Hacker News*. Retrieved 14 May 2017.

67. Shieber, Jonathan. "Companies, governments brace for a second round of cyberattacks in WannaCry's wake" (https://techcrunch.com/2017/05/14/companies-governments-brace-for-a-second-round-of-cyberattacks-in-wannacrys-wake/). *TechCrunch*. Retrieved 14 May 2017.
68. Chan, Sewell; Scott, Mark (14 May 2017). "Cyberattack's Impact Could Worsen in 'Second Wave' of Ransomware" (https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html). *The New York Times*. Retrieved 14 May 2017.
69. "Warning: Blockbuster 'WannaCry' malware could just be getting started" (https://www.nbcnews.com/news/us-news/blockbuster-wannacry-malware-could-just-be-getting-started-experts-n759356). NBC News. Retrieved 14 May 2017.
70. Greenberg, Andy (19 May 2017). "Botnets Are Trying to Reignite the Ransomware Outbreak" (https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack/). *WIRED*. Retrieved 22 May 2017.
71. Gibbs, Samuel (22 May 2017). "WannaCry hackers still trying to revive attack says accidental hero" (https://www.theguardian.com/technology/2017/may/22/wannacry-hackers-ransomware-attack-kill-switch-windows-xp-7-nhs-accidental-hero-marcus-hutchins). *The Guardian*. Retrieved 22 May 2017.
72. "Protection from Ransomware like WannaCry" (https://www.bu.edu/eng/2017/05/18/protection-from-ransomware-like-wannacry/). College of Engineering. Boston University. Retrieved 19 May 2017.
73. Kolodenker, Eugene (16 May 2017). "PayBreak able to defeat WannaCry/WannaCryptor ransomware" (https://www.benthamsgaze.org/2017/05/16/paybreak-able-to-defeat-wannacrywannacryptor-ransomware/). Information Security Research & Education. *Bentham's Gaze*. University College London. Retrieved 19 May 2017.
74. Suiche, Matt (19 May 2017). "WannaCry — Decrypting files with WanaKiwi + Demos" (https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d). *Comae Technologies*.
75. "Windows XP hit by WannaCry ransomware? This tool could decrypt your infected files" (https://www.zdnet.com/article/windows-xp-hit-by-wannacry-ransomware-this-tool-could-decrypt-your-infected-files/). *ZDNet*. Retrieved 30 May 2017.
76. "Windows XP PCs infected by WannaCry can be decrypted without paying ransom" (https://arstechnica.co.uk/security/2017/05/windows-xp-wannacry-decryption/). *Ars Technica*. 18 May 2017. Retrieved 30 May 2017.
77. Greenberg, Andy (18 May 2017). "A WannaCry flaw could help some windows XP users get files back" (https://www.wired.com/2017/05/wannacry-flaw-help-windows-xp-victims-get-files-back/). *Wired*.
78. "More people infected by recent WCry worm can unlock PCs without paying ransom" (https://arstechnica.com/security/2017/05/more-people-infected-by-recent-wcry-worm-can-unlock-pcs-without-paying-ransom/). *Ars Technica*. 19 May 2017. Retrieved 30 May 2017.
79. Volz, Dustin (17 May 2017). "Cyber attack eases, hacking group threatens to sell code" (https://www.reuters.com/article/us-cyber-attack-idUSKCN18B0AC). *Reuters*. https://www.reuters.com. Retrieved 21 May 2017.
80. Leyden, John (26 May 2017). "WannaCrypt ransomware note likely written by Google Translate-using Chinese speakers" (https://www.theregister.co.uk/2017/05/26/wannacrypt_ransom_note_linguistics/). *The Register*. Retrieved 26 May 2017.
81. Condra, Jon; Costello, John; Chu, Sherman (25 May 2017). "Linguistic Analysis of WannaCry Ransomware Messages Suggests Chinese-Speaking Authors" (https://web.archive.org/web/20170527181100/https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/). Flashpoint. Archived from the original (https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/) on 27 May 2017. "Flashpoint assesses with high confidence that the author(s) of WannaCry's ransomware notes are fluent in Chinese, as the language used is consistent with that of Southern China, Hong Kong, Taiwan, or Singapore. Flashpoint also assesses with high confidence that the author(s) are familiar with the English language, though not native. [...] Flashpoint assesses with moderate confidence that the Chinese ransom note served as the original source for the English version, which then generated machine translated versions of the other notes. The Chinese version contains content not in any of the others, though no other notes contain content not in the Chinese. The relative familiarity found in the Chinese text compared to the others suggests the authors were fluent in the language—perhaps comfortable enough to use the language to write the initial note."
82. Greenberg, Andy (15 May 2017). "The Ransomware Outbreak Has a Possible Link to North Korea" (https://www.wired.com/2017/05/wannacry-ransomware-link-suspected-north-korean-hackers/). *Wired*.
83. "Google Researcher Finds Link Between WannaCry Attacks and North Korea" (https://thehackernews.com/2017/05/wannacry-lazarus-north-korea.html). *The Hacker News — Cyber Security and Hacking News Website*.

84. Mehta, Neel [@neelmehta] (15 May 2017). "9c7c7149387a1c79679a87dd1ba755bc @ 0x402560, 0x40F598 ac21c8ad899727137c4b94458d7aa8d8 @ 0x10004ba0, 0x10012AA4 #WannaCryptAttribution" (https://twitter.com/neelmehta/status/864164081116225536) (Tweet) – via Twitter.
85. McMillan, Robert (16 May 2017). "Researchers Identify Clue Connecting Ransomware Assault to Group Tied to North Korea" (https://www.wsj.com/articles/researchers-identify-clue-connecting-ransomware-assault-to-group-tied-to-north-korea-1494898740). *The Wall Street Journal*.
86. Solong, Olivia (15 May 2017). "WannaCry ransomware has links to North Korea, cybersecurity experts say" (https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group). *The Guardian*.
87. Talmadge, Eric (19 May 2017). "Experts question North Korea role in WannaCry cyberattack" (https://www.independent.ie/world-news/experts-question-north-korea-role-in-wannacry-cyber-attack-35732827.html). *independent.ie*. AP. Retrieved 22 May 2017.
88. Nakashima, Ellen. "The NSA has linked the WannaCry computer worm to North Korea" (https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html). *The Washington Post*. The Washington Post. Retrieved 15 June 2017.
89. Harley, Nicola (14 October 2017). "North Korea behind WannaCry attack which crippled the NHS after stealing US cyber weapons, Microsoft chief claims" (https://www.telegraph.co.uk/news/2017/10/14/north-korea-behind-wannacry-attack-crippled-nhs-stealing-us/). *The Telegraph*. ISSN 0307-1235 (https://www.worldcat.org/issn/0307-1235). Retrieved 14 October 2017.
90. Hern, Alex (26 October 2017). "NHS could have avoided WannaCry hack with basic IT security' says report" (https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office). *The Guardian*. Retrieved 26 October 2017.
91. Nakashima, Ellen (18 December 2017). "U.S. declares North Korea carried out massive WannaCry cyberattack" (https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html). *The Washington Post*. Retrieved 18 December 2017.
92. Bossert, Thomas P. (18 December 2017). "It's Official: North Korea Is Behind WannaCry" (https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537). *The Wall Street Journal*. Retrieved 18 December 2017.
93. Uchill, Joe (19 December 2017). "WH: Kim Jong Un behind massive WannaCry malware attack" (http://thehill.com/policy/cybersecurity/365580-wh-kim-jong-un-ordered-release-of-disastrous-wannacry-malware). *The Hill*. Retrieved 19 December 2017.
94. "White House says WannaCry attack was carried out by North Korea" (https://www.cbsnews.com/news/white-house-says-wannacry-attack-was-carried-out-by-north-korea/). *CBS News*. 19 December 2017. Retrieved 19 December 2017.
95. Hern, Alex; McCurry, Justin (19 December 2017). "UK and US blame WannaCry cyber-attack on North Korea" (https://www.theguardian.com/technology/2017/dec/19/wannacry-cyberattack-us-says-it-has-evidence-north-korea-was-directly-responsible). *The Guardian*. Retrieved 19 December 2017.
96. "North Korea says linking cyber attacks to Pyongyang is 'ridiculous' " (https://www.reuters.com/article/us-cyber-attack-northkorea-idUSKCN18F1X3). *Reuters*. 19 May 2017. Retrieved 21 May 2017.
97. "Experts Question North Korea Role in WannaCry Cyberattack" (https://www.nytimes.com/aponline/2017/05/19/world/asia/ap-as-nkorea-wannacry-cyberattack-.html). *The New York Times*. 19 May 2017. Retrieved 21 May 2017.
98. Sanger, David; Benner, Katie; Goldman, Adam (6 September 2018). "North Korean Spy to Be Charged in Sony Pictures Hacking" (https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html). *The New York Times*. Retrieved 6 September 2018.
99. Talley, Ian; Volz, Dustin (16 September 2019). "U.S. Targets North Korean Hacking as National-Security Threat" (https://www.msn.com/en-us/news/world/us-targets-north-korean-hacking-as-national-security-threat/ar-AAHkAGU). *msn*. Retrieved 16 September 2019.
00. "Cyber-attack: Europol says it was unprecedented in scale" (https://www.bbc.com/news/world-europe-39907965). BBC. 13 May 2017.
01. Jones, Sam (14 May 2017). "Global alert to prepare for fresh cyber attacks". *Financial Times*.

02. Millar, Sheila A.; Marshall, Tracy P.; Cardon, Nathan A. (22 May 2017). "WannaCry: Are Your Security Tools Up to Date?" (https://www.natlawreview.com/article/wannacry-are-your-security-tools-to-date). *The National Law Review*. Keller and Heckman LLP. Retrieved 9 July 2017.
03. "Global cyberattack strikes dozens of countries, cripples U.K. hospitals" (https://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/). CBS News. Retrieved 13 May 2017.
04. Ungoed-Thomas, Jon; Henry, Robin; Gadher, Dipesh (14 May 2017). "Cyber-attack guides promoted on YouTube" (https://www.thetimes.co.uk/article/cyber-attack-guides-promoted-on-youtube-972s0hh2c). *The Sunday Times*. Retrieved 14 May 2017.
05. "NHS cyber-attack: GPs and hospitals hit by ransomware" (https://www.bbc.co.uk/news/health-39899646). *BBC News*. 12 May 2017. Retrieved 12 May 2017.
06. Wong, Julia Carrie; Solon, Olivia (12 May 2017). "Massive ransomware cyber-attack hits 74 countries around the world" (https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs). *The Guardian*. London. Retrieved 12 May 2017.
07. Health Editor, Chris Smyth (18 April 2018). "Every hospital tested for cybersecurity has failed" (https://www.thetimes.co.uk/article/every-hospital-tested-for-cybersecurity-has-failed-97vc6rqkq). *The Times*. ISSN 0140-0460 (https://www.worldcat.org/issn/0140-0460). Retrieved 18 April 2018.
08. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf
09. Marsh, Sarah (12 May 2017). "The NHS trusts hit by malware – full list" (https://www.theguardian.com/society/2017/may/12/global-cyber-attack-nhs-trusts-malware). *The Guardian*. London. Retrieved 12 May 2017.
10. Sharman, Jon (13 May 2017). "Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France" (https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html). *The Independent*. Retrieved 13 May 2017.
11. Rosemain, Mathieu; Le Guernigou, Yann; Davey, James (13 May 2017). "Renault stops production at several plants after ransomware cyber attack as Nissan also hacked" (https://www.mirror.co.uk/news/world-news/renault-stops-production-several-plants-10413994). *Daily Mirror*. Retrieved 13 May 2017.
12. Larson, Selena (12 May 2017). "Massive ransomware attack hits 99 countries" (https://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/). CNN. Retrieved 12 May 2017.
13. "The WannaCry ransomware attack has spread to 150 countries" (https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries). *The Verge*. 14 May 2017. Retrieved 16 May 2017.
14. Hern, Alex; Gibbs, Samuel (12 May 2017). "What is 'WanaCrypt0r 2.0' ransomware and why is it attacking the NHS?" (https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20). *The Guardian*. London. ISSN 0261-3077 (https://www.worldcat.org/issn/0261-3077). Retrieved 12 May 2017.
15. "Lucky break slows global cyberattack; what's coming could be worse" (https://www.chicagotribune.com/news/nationworld/ct-nsa-cyberattacks-20170513-story.html). *Chicago Tribune*. Retrieved 14 May 2017.
16. Helmore, Edward (13 May 2017). "Ransomware attack reveals breakdown in US intelligence protocols, expert says" (https://www.theguardian.com/technology/2017/may/13/ransomware-cyber-attack-us-intelligence). *The Guardian*. Retrieved 14 May 2017.
17. "The Latest: Researcher who helped halt cyberattack applauded" (https://web.archive.org/web/20170516182233/http://www.startribune.com/the-latest-turkey-among-countries-hit-in-cyberattack/422161813/). *Star Tribune*. Archived from the original (http://www.startribune.com/the-latest-turkey-among-countries-hit-in-cyberattack/422161813/) on 16 May 2017. Retrieved 14 May 2017.
18. "Global 'WannaCry' ransomware cyberattack seeks cash for data" (https://www.washingtonpost.com/world/europe/uk-working-to-restore-hospital-systems-after-cyberattack/2017/05/13/472ef544-37c1-11e7-ab03-aa29f656f13e_story.html). *Washington Post*. Retrieved 16 May 2017.
19. " "WannaCry" ransomware attack losses could reach $4 billion" (https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/). Retrieved 14 June 2017.
20. "Andhra police computers hit by cyberattack" (http://timesofindia.indiatimes.com/india/andhra-police-computers-hit-by-cyberattack/articleshow/58658853.cms). *The Times of India*. 13 May 2017. Retrieved 13 May 2017.
21. " "Χάκαραν" και το ΑΠΘ στην παγκόσμια κυβερνοεπίθεση!" (http://www.protothema.gr/greece/article/679082/hakaran-kai-to-apth-stin-pagosmia-kuvernoepithesi/). *Proto Thema* (in Greek). 13 May 2017. Retrieved 18 May 2017.

22. " "Θεσσαλονίκη: Στόχος της παγκόσμιας κυβερνοεπίθεσης το Αριστοτέλειο – Συναγερμός για τον ισχυρό ιό!" (https://www.newsit.gr/topikes-eidhseis/thessaloniki-stoxos-tis-pagkosmias-kyvernoepithesis-to-aristoteleio-synagermos-gia-ton-isxyro-io/1027391/). *NewsIT* (in Greek). 13 May 2017.
23. "Atacul cibernetic global a afectat și Uzina Dacia de la Mioveni. Renault a anunțat că a oprit producția și în Franța" (http://stirileprotv.ro/stiri/actualitate/atacul-informatic-global-ar-fi-afectat-si-uzina-dacia-de-la-mioveni-reactia-ministrului-comunicatiilor-augustin-jianu.html). *Pro TV* (in Romanian). 13 May 2017.
24. "Boeing production plant hit with WannaCry ransomware attack" (https://www.theverge.com/2018/3/28/17174540/boeing-wannacry-ransomware-attack-production-plant-charleston-south-carolina). *theverge.com*. 28 March 2018. Retrieved 29 March 2018.
25. "Hackers demand $54K in Cambrian College ransomware attack" (http://www.cbc.ca/news/canada/sudbury/cambrian-college-ransomware-hack-1.4093634). *CBC.ca*. Retrieved 16 May 2017.
26. Mimi Lau (14 May 2017). "Chinese police and petrol stations hit by ransomware attack" (http://www.scmp.com/news/china/society/article/2094291/chinese-police-and-petrol-stations-hit-ransomware-attack). *South China Morning Post*. Retrieved 15 May 2017.
27. "Korean gov't computers safe from WannaCry attack" (http://www.koreaherald.com/view.php?ud=20170515000574). *The Korea Herald*. Retrieved 15 May 2017.
28. "一夜之间 勒索病毒"永恒之蓝"席卷 国内近3万机构被攻陷 全球 超十万台电脑"中毒"江苏等十省市受害最严重" (http://news.163.com/17/0514/08/CKCOOATU000187VI.html).
29. "Weltweite Cyberattacke trifft Computer der Deutschen Bahn" (https://www.faz.net/aktuell/wirtschaft/unternehmen/hacker-angriff-weltweite-cyberattacke-trifft-computer-der-deutschen-bahn-15013583.html). *Frankfurter Allgemeine Zeitung* (in German). 13 May 2017. Retrieved 13 May 2017.
30. "Global cyber attack: A look at some prominent victims" (http://www.straitstimes.com/world/organisations-hit-by-global-cyberattack) (in Spanish). elperiodico.com. 13 May 2017. Retrieved 14 May 2017.
31. "Hackerský útok zasiahol aj Fakultnú nemocnicu v Nitre" (https://www.etrend.sk/ekonomika/hackersky-utok-zasiahol-aj-fakultnu-nemocnicu-v-nitre.html). *etrend.sk* (in Slovak). 15 May 2017. Retrieved 15 May 2017.
32. "What is Wannacry and how can it be stopped?" (https://www.ft.com/content/af74e3f4-373d-11e7-99bd-13beb0903fa3). *Financial Times*. 12 May 2017. Retrieved 13 May 2017.
33. "เซิร์ฟเวอร์เกม Blade & Soul ของ Garena ประเทศไทยถูก WannaCrypt โจมตี" (https://www.blognone.com/node/92406) (in Thai). blognone.com. 13 May 2017. Retrieved 14 May 2017.
34. "日立、社内システムの一部に障害 サイバー攻撃の影響か" (http://www.nikkei.com/article/DGXLASFL15HC6_V10C17A5000000). 日本経済新聞 (in Japanese). 15 May 2017. Retrieved 21 June 2017.
35. "Honda halts Japan car plant after WannaCry virus hits computer network" (https://www.reuters.com/article/us-honda-cyberattack-idUSKBN19C0EI). *Reuters*. 21 June 2017. Retrieved 21 June 2017.
36. "Instituto Nacional de Salud, entre víctimas de ciberataque mundial" (http://www.eltiempo.com/tecnosfera/novedades-tecnologia/alerta-por-cibertaque-que-golpeo-a-74-paises-87602). *El Tiempo* (in Spanish). 13 May 2017.
37. "Ontario health ministry on high alert amid global cyberattack" (https://www.thestar.com/news/canada/2017/05/13/ontario-health-ministry-on-high-alert-amid-global-cyberattack.html). *Toronto Star*. 13 May 2017.
38. "Laks second Dutch victim of WannaCry" (http://www.nu.nl/internet/4706262/laks-tweede-nederlandse-slachtoffer-ransomware-wannacry.html). *Nu.nl*. 19 May 2017.
39. "LATAM Airlines también está alerta por ataque informático" (https://www.fayerwayer.com/2017/05/latam-airlines-tambien-estaria-comprometida-en-ataque-ransomware/). Fayerwayer. Retrieved 13 May 2017.
40. "Massive cyber attack creates chaos around the world" (http://www.news.com.au/technology/online/hacking/massive-cyber-attack-creates-chaos-around-the-world/news-story/b248da44b753489a3f207dfee2ce78a9). news.com.au. 12 May 2017. Retrieved 13 May 2017.
41. "Researcher 'accidentally' stops spread of unprecedented global cyberattack" (https://abcnews.go.com/International/researcher-accidentally-stops-spread-unprecedented-global-cyberattack/story?id=47390745). ABC News. Retrieved 13 May 2017.
42. "Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France" (https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html). *The Independent*. 13 May 2017. Retrieved 13 May 2017.
43. "Nach Attacke mit Trojaner WannaCry: Kundensystem bei O2 ausgefallen" (http://www.focus.de/digital/es-ist-ein-technischer-fehler-aufgetreten-nutzer-koennen-twitter-nicht-aufrufen_id_7156840.html) (in German). FOCUS Online. Retrieved 20 May 2017.

44. "Erhebliche Störungen – WannaCry: Kundendienst von O2 ausgefallen – HAZ – Hannoversche Allgemeine" (http://www.haz.de/Nachrichten/Wirtschaft/Deutschland-Welt/WannaCry-Kundendienst-von-O2-ausgefallen) (in German). Hannoversche Allgemeine Zeitung. Retrieved 20 May 2017.
45. "WannaCry no Brasil e no mundo" (http://www.opovo.com.br/jornal/economia/2017/05/wannacry-no-brasil-e-no-mundo.html). *O Povo* (in Portuguese). 13 May 2017. Retrieved 13 May 2017.
46. "PT Portugal alvo de ataque informático internacional" (http://observador.pt/2017/05/12/portugal-telecom-alvo-de-ataque-informatico-internacional/). *Observador* (in Portuguese). 12 May 2017. Retrieved 13 May 2017.
47. "Ransomware infects narrowcast radio station" (https://www.radioinfo.com.au/news/ransomware-infects-narrowcast-radio-station/). *RadioInfo*. 15 May 2017. Retrieved 30 September 2017.
48. "Parkeerbedrijf Q-Park getroffen door ransomware-aanval" (http://www.nu.nl/internet/4691349/parkeerbedrijf-q-park-getroffen-ransomware-aanval.html). *Nu.nl* (in Dutch). 13 May 2017. Retrieved 14 May 2017.
49. "France's Renault hit in worldwide 'ransomware' cyber attack" (http://www.france24.com/en/20170512-cyberattack-ransomware-renault-worldwide-british-hospitals) (in Spanish). France 24. 13 May 2017. Retrieved 13 May 2017.
50. "Компьютеры РЖД подверглись хакерской атаке и заражены вирусом" (https://www.svoboda.org/a/28483898.html). Radio Free Europe/Radio Liberty. Retrieved 13 May 2017.
51. Amjad Shacker [@AmjadShacker] (14 May 2017). "-" (https://twitter.com/AmjadShacker/status/863749329017868293) [screenshot of message] (Tweet) (in Arabic) – via Twitter.
52. Vidal Liy, Macarena (15 May 2017). "Putin culpa a los servicios secretos de EE UU por el virus 'WannaCry' que desencadenó el ciberataque mundial" (http://internacional.elpais.com/internacional/2017/05/15/actualidad/1494855826_022843.html). *El País* (in Spanish). Retrieved 16 May 2017.
53. "Ransomware WannaCry Surfaces In Kerala, Bengal: 10 Facts" (http://www.ndtv.com/india-news/ransomware-wannacry-surfaces-in-kerala-bengal-10-facts-1693806). *New Delhi Television Limited (NDTV)*. Retrieved 15 May 2017.
54. Sanjana Nambiar (16 May 2017). "Hit by WannaCry ransomware, civic body in Mumbai suburb to take 3 more days to fix computers" (http://www.hindustantimes.com/mumbai-news/hit-by-wannacry-ransomware-civic-body-in-mumbai-suburb-to-take-3-more-days-to-fix-computers/story-eSIMZQ2NFT217erJAFkS0J.html). *Hindustan Times*. Retrieved 17 May 2017.
55. "Un ataque informático masivo con 'ransomware' afecta a medio mundo" (http://www.elperiodico.com/es/noticias/sociedad/ataque-informatico-masivo-infecta-las-grandes-empresas-espana-6033534) (in Spanish). elperiodico.com. 12 May 2017. Retrieved 13 May 2017.
56. Balogh, Csaba (12 May 2017). "Ideért a baj: Magyarországra is elért az óriási kibertámadás" (http://hvg.hu/tudomany/20170512_wannacry_zsarolovirus_aldozatok_magyar_ceg). *HVG* (in Hungarian). Retrieved 13 May 2017.
57. "Telkom systems crippled by WannaCry ransomware" (https://mybroadband.co.za/news/security/211576-telkom-systems-crippled-by-wannacry-ransomware.html). *MyBroadband*. 21 May 2017. Retrieved 21 May 2017.
58. "Timrå kommun drabbat av utpressningsattack" (https://www.svt.se/nyheter/inrikes/timra-kommun-drabbat-av-utpressningsattack) (in Swedish). Sveriges Television. 13 May 2017. Retrieved 15 May 2017.
59. Kirk, Jeremy. "WannaCry Outbreak Hits Chipmaker, Could Cost $170 Million" (https://www.bankinfosecurity.com/chipmaker-tsmc-wannacry-attack-could-cost-us170-million-a-11285). Information Security Media Group, Corp. "Taiwan Semiconductor Manufacturing Co., the world's largest chip manufacturer, says a WannaCry infection hit unpatched Windows 7 systems in its fabrication facilities, leaving multiple factories crippled."
60. "Virus Ransomware Wannacry Serang Perpustakaan Universitas Jember" (https://m.tempo.co/read/news/2017/05/16/058875604/virus-ransomware-wannacry-serang-perpustakaan-universitas-jember). *Tempo* (in Indonesian). 16 May 2017. Retrieved 17 May 2017.
61. "Il virus Wannacry arrivato a Milano: colpiti computer dell'università Bicocca" (http://milano.repubblica.it/cronaca/2017/05/12/news/milano_virus_ransomware_universita_bicocca-165302056/). *la Repubblica* (in Italian). 12 May 2017. Retrieved 13 May 2017.
62. "Some University of Montreal computers hit with WannaCry virus" (https://www.theglobeandmail.com/news/national/universite-de-montreal-computers-hit-with-wannacry-virus/article35004991/). *The Globe and Mail*. 16 May 2017. Retrieved 16 May 2017.
63. Wong, Julia Carrie; Solon, Olivia (12 May 2017). "Massive ransomware cyber-attack hits 74 countries around the world" (https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs). *The Guardian*. Retrieved 12 May 2017.

64. Heintz, Sylvia Hui, Allen G. Breed and Jim. "Lucky break slows global cyberattack; what's coming could be worse" (https://www.chicagotribune.com/news/nationworld/ct-nsa-cyberattacks-20170513-story.html). *Chicago Tribune*. Retrieved 14 May 2017.
65. "Ransomware attack 'like having a Tomahawk missile stolen', says Microsoft boss" (https://www.theguardian.com/technology/2017/may/15/ransomware-attack-like-having-a-tomahawk-missile-stolen-says-microsoft-boss). *The Guardian*. 14 May 2017. Retrieved 15 May 2017.
66. Storm, Darlene (15 May 2017). "WikiLeaks posts user guides for CIA malware implants Assassin and AfterMidnight" (http://www.computerworld.com/article/3196987/security/wikileaks-posts-user-guides-for-cia-malware-implants-assassin-and-aftermidnight.html). *Computerworld*. Retrieved 17 May 2017.
67. Smith, Brad (14 May 2017). "The need for urgent collective action to keep people safe online" (https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/). Microsoft. Retrieved 14 May 2017.
68. "Patch Act bill before Congress" (https://www.documentcloud.org/documents/3725905-Patch-Act-bill-before-Congress.html). Retrieved 23 May 2017.
69. Whittaker, Zack. "Congress introduces bill to stop US from stockpiling cyber-weapons" (https://www.zdnet.com/article/congress-introduces-bill-to-prevent-us-from-stockpiling-cyber-weapons/). *ZDNet*. Retrieved 23 May 2017.
70. Chalfant, Morgan (12 June 2017). "Lawmakers to hold hearing on 'Wanna Cry' ransomware attack" (http://thehill.com/business-a-lobbying/337440-lawmakers-to-hold-hearing-on-wanna-cry-ransomware-attack). *TheHill*. Retrieved 14 June 2017.
71. "Finding the kill switch to stop the spread of ransomware – NCSC Site" (https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0+). *www.ncsc.gov.uk*. Retrieved 21 May 2017.
72. "Sky Views: Stop the cyberattack blame game" (http://news.sky.com/story/sky-views-stop-the-cyberattack-blame-game-10880726). Sky News. Retrieved 21 May 2017.
73. "gentilkiwi/wanakiwi" (https://github.com/gentilkiwi/wanakiwi). *GitHub*. Retrieved 20 May 2017.
74. "aguinet/wannakey" (https://github.com/aguinet/wannakey). *GitHub*. Retrieved 20 May 2017.
75. Auchard, Eric (19 May 2017). "French researchers find way to unlock WannaCry without ransom" (https://www.reuters.com/article/us-cyber-attack-cure-idUSKCN18F1CA). *Reuters*. Retrieved 19 May 2017.
76. Snowden, Edward [@Snowden] (13 May 2017). "When @NSAGov-enabled ransomware eats the internet, help comes from researchers, not spy agencies. Amazing story" (https://twitter.com/Snowden/status/863422022994481152) (Tweet). Retrieved 20 May 2017 – via Twitter.
77. Snowden, Edward [@Snowden] (13 May 2017). "Pause a moment to consider why we're left with researchers, not governments, trying to counter the @NSAGov-enabled ransomware mess. Hint:" (https://twitter.com/Snowden/status/863425539616284673) (Tweet). Retrieved 20 May 2017 – via Twitter.
78. Coughlin, Tom. "WannaCry Ransomware Demonstrations The Value of Better Security and Backups" (https://www.forbes.com/sites/tomcoughlin/2017/05/14/wannacry-ransomware-demonstrations-the-value-of-better-security-and-backups/). *Forbes*. Retrieved 14 May 2017.
79. "WannaCry: BSI ruft Betroffene auf, Infektionen zu melden" (https://www.heise.de/newsticker/meldung/WannaCry-BSI-ruft-Betroffene-auf-Infektionen-zu-melden-3713442.html) (in German). heise online. Retrieved 14 May 2017.
80. "The ransomware attack is all about the insufficient funding of the NHS" (https://www.theguardian.com/commentisfree/2017/may/13/nhs-computer-systems-insufficient-funding). *The Guardian*. 13 May 2017. Retrieved 14 May 2017.
81. "Jeremy Hunt 'ignored warning signs' before cyber-attack hit NHS" (https://www.theguardian.com/society/2017/may/13/jeremy-hunt-ignored-warning-signs-before-cyber-attack-hit-nhs). *The Guardian*. 13 May 2017. Retrieved 14 May 2017.
82. Larson, Selena (17 May 2017). "Why WannaCry ransomware took down so many businesses" (https://money.cnn.com/2017/05/17/technology/wannacry-ransomware-business-security/index.html). *CNN Money*. CNN. Retrieved 22 May 2017.
83. "UPDATED Statement on reported NHS cyber-attack (13 May)" (https://digital.nhs.uk/article/1493/UPDATED-Statement-on-reported-NHS-cyber-attack-13-May-). National Health Service. Retrieved 30 May 2017.
84. "Cyber-attack cost NHS £92m – DHSC" (https://www.hsj.co.uk/technology-and-innovation/cyber-attack-cost-nhs-92m--dhsc/7023560.article). Health Service Journal. 11 October 2018. Retrieved 13 November 2018.

85. "Health chiefs refuse to foot £1bn bill to improve NHS cyber security" (https://www.buildingbetterhealthcare.co.uk/news/article_page/Health_chiefs_refuse_to_foot_1bn_bill_to_improve_NHS_cyber_security/147855/cn164706). Building Better Healthcare. 15 October 2018. Retrieved 27 November 2018.
86. "Wannacry is back!" (https://www.theregister.co.uk/2018/06/21/wannacry_is_back_except_its_not). heise online. Retrieved 21 June 2018.

External links

- Ransom:Win32/WannaCrypt (https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt) at Microsoft Malware Protection Center
- @actual_ransom (https://twitter.com/actual_ransom) on Twitter, a Twitterbot tracking the ransom payments

Retrieved from "https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&oldid=1005823187"

This page was last edited on 9 February 2021, at 16:06 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.