**WannaCry Ransomware attack**

The WannaCry [ransomware](https://www.cloudflare.com/learning/security/ransomware/what-is-ransomware/)\* attack was a major security incident that impacted organizations all over the world. On May 12, 2017, the WannaCry ransomware worm spread to more than 200,000 computers in over 150 countries. Notable victims included FedEx, Honda, Nissan, and the UK's National Health Service (NHS), the latter of which was forced to divert some of its ambulances to alternate hospitals.

Within hours of the attack, WannaCry was temporarily neutralized. A security researcher discovered a "kill switch" that essentially turned off the [malware](https://www.cloudflare.com/learning/ddos/glossary/malware/). However, many affected computers remained encrypted and unusable until the victims paid the ransom or were able to reverse the encryption.

WannaCry spread by using a vulnerability exploit called "EternalBlue." The US National Security Agency (NSA) had developed this exploit, presumably for their own use, but it was stolen and released to the public by a group called the Shadow Brokers after the NSA was itself compromised. EternalBlue only worked on older, unpatched versions of Microsoft Windows, but there were more than enough machines running such versions to enable WannaCry's rapid spread.

\**Ransomware is malicious software that locks up files and data via*[*encryption*](https://www.cloudflare.com/learning/ssl/what-is-encryption/)*and holds them for ransom.*

**What is a worm?**

In the security field, a worm is a malicious software program that automatically spreads itself to multiple computers in a network. A worm uses operating system vulnerabilities to jump from computer to computer, installing copies of itself on each computer.

Think of a worm as being like a thief who walks around an office park checking for unlocked doors. Once the thief finds one, imagine that he can create a duplicate of himself that remains inside the unlocked office, and both versions continue their search for unlocked doors.

Most worms do not contain ransomware. Ransomware typically spreads through malicious emails, credential compromise, botnets, or highly targeted vulnerability exploits ([Ryuk](https://www.cloudflare.com/learning/security/ransomware/ryuk-ransomware/) is one example of the latter). WannaCry was unique in that it not only combined ransomware with a worm, but also used a particularly powerful worm-enabling vulnerability that had been created by the NSA.

**Who are the Shadow Brokers?**

The Shadow Brokers are a group of attackers who began leaking malware tools and [zero-day exploits](https://www.cloudflare.com/learning/security/threats/zero-day-exploit/) to the public in 2016. They are suspected of having acquired a number of exploits developed by the NSA, possibly due to an [insider attack](https://www.cloudflare.com/learning/access-management/what-is-an-insider-threat/) at the agency. On April 14, 2017, the Shadow Brokers leaked the EternalBlue exploit that WannaCry would eventually use.

Microsoft issued a patch for EternalBlue on March 14, one month before the Shadow Brokers leaked it, but many computers remained unpatched at the time of the WannaCry attack.

**Who was responsible for the WannaCry ransomware attack?**

In late 2017, the US and the UK [announced](https://www.bbc.com/news/world-us-canada-42407488) that the government of North Korea was behind WannaCry. However, some security researchers [dispute](https://www.darkreading.com/attacks-breaches/three-years-after-wannacry-ransomware-accelerating-while-patching-still-problematic) this attribution. WannaCry may have been the work of the North Korea-based Lazarus Group, some argue, without coming directly from the government of North Korea. Others suggest that the authorship clues in the malware may have been planted there to cast blame on North Korea-based attackers, and that WannaCry may be from another region altogether.

**How was the WannaCry attack stopped?**

On the day of the attack, a security blogger and researcher named Marcus Hutchins began reverse-engineering the WannaCry source code. He discovered that WannaCry included an unusual function: before executing, it would query the [domain](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. This website did not exist.

So, he registered the domain. (It cost [$10.69](https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/).)

After Hutchins did so, copies of WannaCry continued to spread, but they stopped executing. Essentially, WannaCry turned itself off once it began getting a response from iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.

**Why did this stop the attack?**

While the WannaCry authors' motivations cannot be known for certain, it is theorized that this domain query function was included in WannaCry so that the ransomware could check if it was inside a sandbox.

A sandbox is an anti-malware tool. It is a [virtual machine](https://www.cloudflare.com/learning/cloud/what-is-a-virtual-machine/) running separately from all other systems and networks. It provides a safe environment to execute untrusted files and see what they do.

A sandbox is not actually connected to the Internet. But sandboxes aim to imitate a real computer as closely as possible, so they may generate a fake response to a query directed at a given domain by the malware. As a result, one way that malware could check if it is inside a sandbox is by sending a query to a fake domain. If it gets a "real" response (generated by the sandbox), it can assume it is in a sandbox and shut itself down so that the sandbox does not detect it as malicious.

However, if the malware sends its test query to a hard-coded domain, then it can be tricked into thinking it is always in a sandbox if someone registers the domain. This could be what happened with WannaCry: copies of WannaCry across the world were tricked into thinking they were inside a sandbox and shut themselves down. (A better design from the perspective of the malware author would be to query a randomized domain that was different every time — that way, the odds of getting a response from the domain outside of a sandbox would be close to zero.)

Another possible explanation is that the copy of WannaCry that spread across the world was unfinished. The authors of WannaCry may have hard-coded that domain as a placeholder, intending to replace it with the address of their command-and-control (C&C) server before releasing the worm. Or they may have meant to register iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com themselves. ([DNS filtering](https://www.cloudflare.com/learning/access-management/what-is-dns-filtering/) or [URL filtering](https://www.cloudflare.com/learning/access-management/what-is-url-filtering/) perhaps could have stopped queries to that domain, but most organizations would not have been able to deploy this safety measure in time.)

Regardless of the reason, it was a stroke of luck that such a simple action could save computers and networks around the world from further infection.

**What happened to Marcus Hutchins?**

It turned out that before Hutchins began working and blogging as a security researcher, he had spent years frequenting malware forums on the dark web, [building and selling his own malware](https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/). A few months after the WannaCry incident, the FBI arrested Hutchins in Las Vegas, Nevada, for authoring Kronos, a strain of banking malware.

**Is WannaCry a threat today?**

The version of WannaCry that was released into the world in 2017 no longer functions, thanks to Hutchins' kill switch domain. Additionally, a patch has been available for the EternalBlue vulnerability that WannaCry exploited since March 2017.

However, WannaCry attacks continue to occur. As of March 2021, WannaCry was [still using](https://www.netsec.news/wannacry-ransomware-attacks-up-53-since-january-2021/) the EternalBlue vulnerability, meaning only extremely old, out-of-date Windows systems were at risk. Newer versions of WannaCry have removed the kill switch feature present in the original version. Updating operating systems and installing security updates immediately is highly recommended.

While the original version of WannaCry is no longer active, several key lessons can be learned from the May 2017 attack:

1. **Networks around the world are highly interconnected.** In the Internet age, this may go without saying, but many organizations still assume that their networks cannot be penetrated from the outside (like a [castle with a moat](https://www.cloudflare.com/learning/access-management/castle-and-moat-network-security/)). WannaCry showed that unless a network is air-gapped — meaning it is completely separate from all outside connections — external threats can likely still get in.
2. **Even patched vulnerabilities can be dangerous.** A vulnerability patch is only as effective as the number of systems that apply it. The EternalBlue patch was available for almost two months prior to the WannaCry attack, but it seems that few organizations had installed the patch. (Even by 2021, some had not yet installed it.)
3. **Many crucial organizations are vulnerable to cyber attack.** This continues to be the case; ransomware attacks have impacted hospitals, schools, fuel pipelines, and governments in recent years. In fact, ransomware groups such as Ryuk seem to target these organizations. In some instances, organizations may not have the funding, resources, or commitment to technological updates that they need to face attacks. The NHS in particular faced scrutiny for continuing to use Windows XP, a highly vulnerable operating system that Microsoft no longer supported, in the wake of the attack.
4. **Ransomware is a major threat.** [Cloudflare One](https://www.cloudflare.com/cloudflare-one/) is a Zero Trust platform that can help organizations combat this threat. A [Zero Trust security](https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/) approach assumes that all users and devices present threats. It regularly re-authenticates users and assesses device security, ensuring that any unsafe or unauthorized devices have their application and network access revoked immediately. This helps prevent the spread of ransomware.