HACKING

What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?

Known as the most enduring and damaging exploit of all time, EternalBlue is the cyberattack nightmare that won't go away. Learn what EternalBlue is, how the hacking tool got leaked, and why the US National Security Agency developed it in the first place. Then, find out how to protect yourself against exploits with an award-winning cybersecurity app.

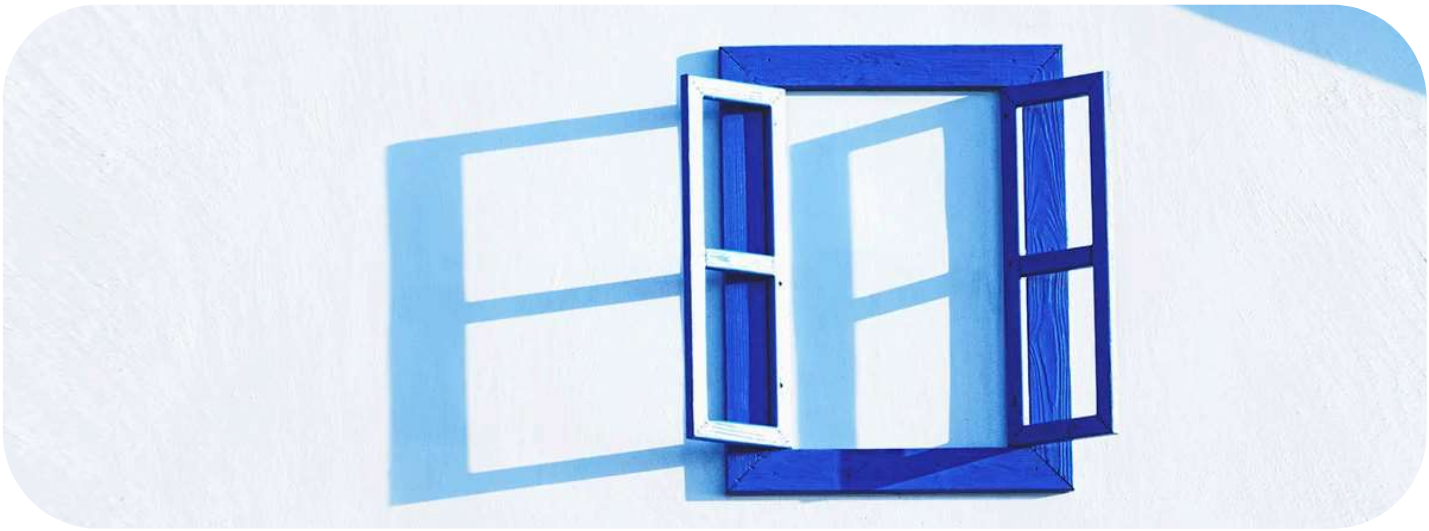
Download free Avast One

Get it for **Android**, **iOS**, **Mac**

2023
Editors' choice

Great
16,505 reviews on
Trustpilot

2022
Top Rated Product



Written by **Carly Burdova**
Published on June 18, 2020

What is EternalBlue?

EternalBlue is both the given name to a series of **Microsoft software vulnerabilities and the exploit created by the NSA as a cyberattack tool.** Although the EternalBlue exploit — officially named MS17-010 by Microsoft — affects only Windows operating systems, anything that uses the SMBv1 (Server Message Block version 1) file-sharing protocol is technically at risk of being targeted for ransomware and other cyberattacks.

How was EternalBlue developed?

You may be wondering **who created EternalBlue in the first place?** The origins of the SMB vulnerability are what spy stories are made of — dangerous NSA hacking tools leaked, a notorious group called Shadow Brokers on the hunt for common vulnerabilities and exposures, and a massively popular operating system used by individuals, governments, and corporations worldwide

According to condemning statements made by Microsoft, **EternalBlue was developed by the United State's National Security Agency** as part of their controversial program of stockpiling and weaponizing cybersecurity vulnerabilities, rather than flagging them to the appropriate vendor

---

Before it leaked, EternalBlue was one of the most useful exploits in the NSA's cyber arsenal ... used in countless

intelligence-gathering and counterterrorism missions.

— New York Times

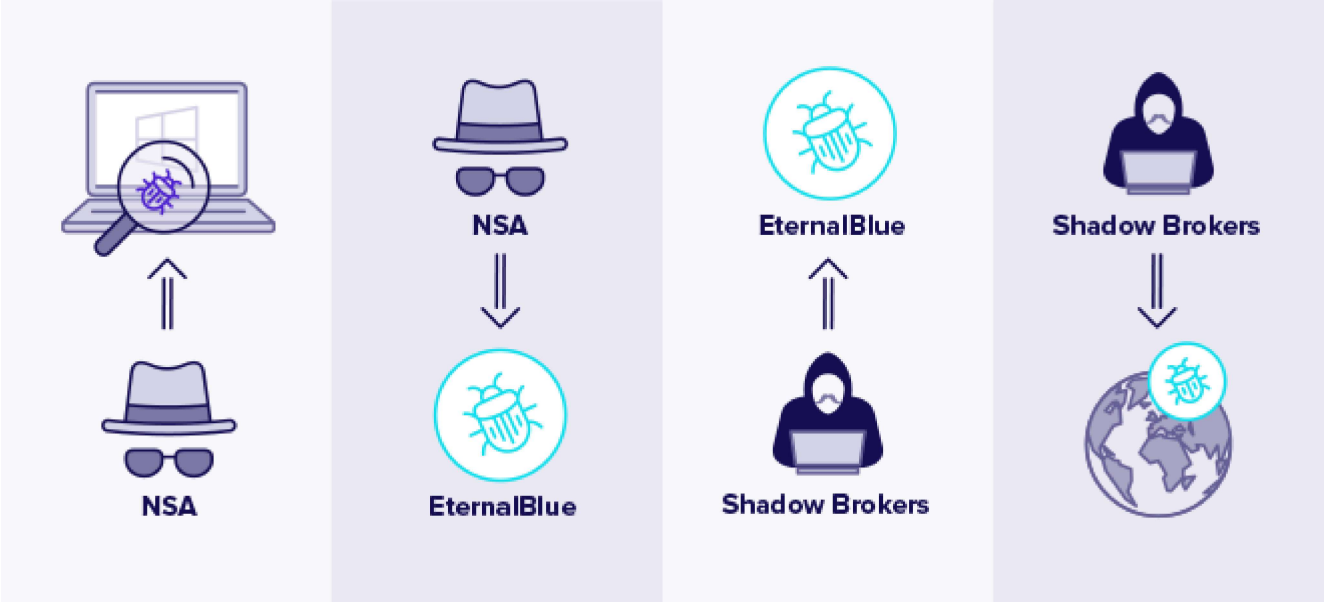
The NSA allegedly spent almost a year hunting for a bug in Microsoft's software. Once they found it, the NSA developed EternalBlue to exploit the vulnerability. **The NSA used EternalBlue for five years before alerting Microsoft of its existence**.

Microsoft has since called upon the NSA and other government bodies to support a Digital Geneva Convention, which calls for an end to nation-state stockpiling of software vulnerabilities.

Initial leak and fallout

Here's where things get interesting — the NSA gets hacked and unwittingly unleashes EternalBlue's eternal threat out into the world. Little is officially known about how the NSA got hacked, but here's what we know about how EternalBlue was leaked.

Shadow Brokers, the now notorious hacking group, gained access to EternalBlue and **leaked the NSA hacking tool on April 14, 2017** via a link on their Twitter account. This was not the first time Shadow Brokers hackers struck, but rather the fifth time they leaked sensitive exploits and vulnerabilities online. This particular release, titled "Lost in Translation," included the EternalBlue exploit targeting Windows operating systems.



The NSA discovered a Windows security vulnerability and created the EternalBlue exploit, which was then stolen and leaked by the hacker group Shadow Brokers.

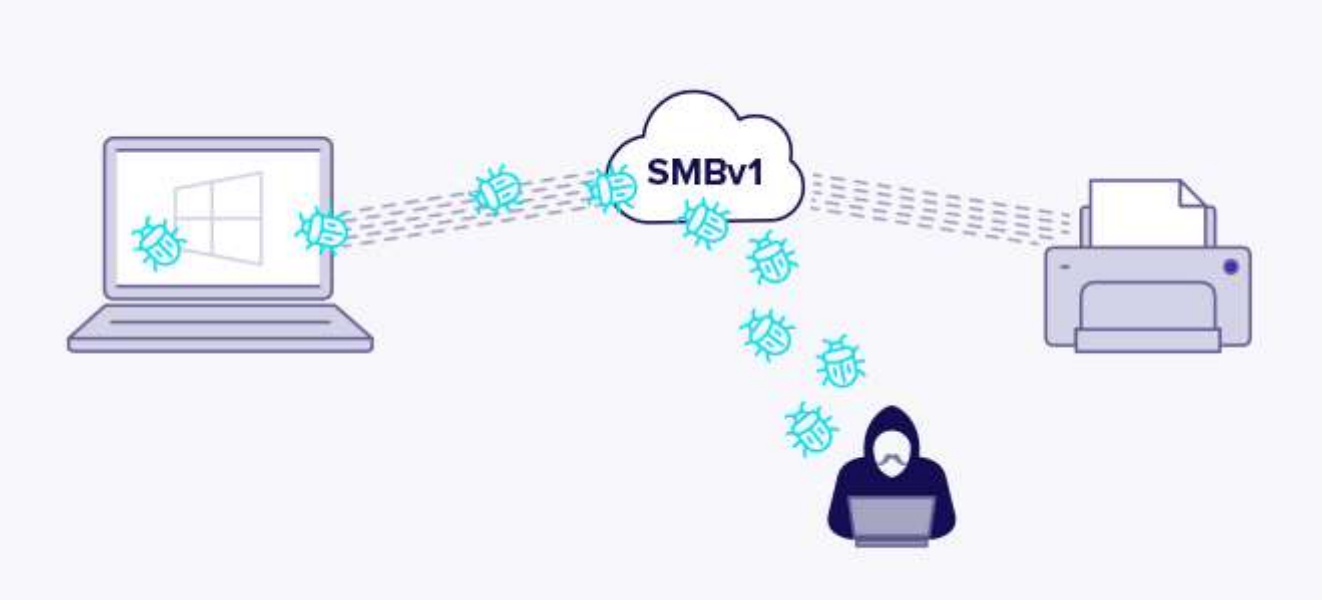
On March 14, 2017, exactly one month before the Shadow Brokers leak, Microsoft released Security Bulletin MS17-010. The timeline suggests that Microsoft was tipped off about the NSA breach and rushed to do all they could to protect the millions of vulnerable Windows systems.

The MS17-010 patch was designed to fix the SMBv1 software flaws for all supported Windows operating systems, including **Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016**. Microsoft also automatically disabled SMBv1 in the latest versions of Windows 10 and Windows Servers 2012 and 2016 by default.

Additionally, in an unprecedented move to demonstrate the severity of the EternalBlue exploit, Microsoft released a second emergency patch for *unsupported* operating systems once the leak was made public. This second release supported **Windows XP, Windows 8, and Windows Server 2003**.

How does EternalBlue work?

The EternalBlue exploit works by **taking advantage of SMBv1 vulnerabilities** present in older versions of Microsoft operating systems. SMBv1 was first developed in early 1983 as a network communication protocol to enable shared access to files, printers, and ports. It was essentially a way for Windows machines to talk to one another and other devices for remote services.



EternalBlue exploits SMBv1 vulnerabilities to insert malicious data packets and spread malware over the network.

The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers. All the attacker needs to do is **send a maliciously-crafted packet to the target server**, and, boom, the malware propagates and a cyberattack ensues.

EternalBlue's Common Vulnerabilities and Exposures number is logged in the National Vulnerability Database as CVE-2017-0144.

Microsoft's patch closes the security vulnerability completely, thus preventing attempts at deploying ransomware, malware, cryptojacking, or any other worm-like attempts at digital infiltration using the EternalBlue exploit. But a key problem remains — for many versions of Windows, **the software update must be installed in order to provide protection**

It is this key problem that gives EternalBlue such a long shelf life — many people and even businesses fail to update their software regularly, leaving their operating systems unpatched and thus vulnerable to EternalBlue and other attacks. To this day, the number of **unpatched vulnerable Windows systems remains in the millions**.

How is EternalBlue used in cyberattacks?

EternalBlue has been famously used to spread WannaCry and Petya ransomware. But the exploit can be used to deploy any type of cyberattack, including cryptojacking and worm-like malware. The NSA hack opened the door for any attacker to send a malicious packet to a vulnerable server that has not applied the patch to fix CVE-2017-0144.

WannaCry

The name says it all. WannaCry is the name of **a worldwide ransomware attack made possible by the EternalBlue exploit**. See, even hackers have a comedic side

The WannaCry cyberattack began on May 12, 2017 and immediately had a global impact. The ransomware spread at a rate of 10,000 devices per hour, **infecting over 230,000 Windows PCs across 150 countries in a single day**

Although no specific targets were apparent, some big names and entities were hit, including FedEx, the University of Montreal, LATAM Airlines, Deutsche Bahn, and notably, the UK's National Health Service (NHS). The NHS reported that thousands of appointments and operations were cancelled and that patients had to travel farther to accident and emergency departments due to the security breach.

Petya

Petya is another ransomware cyberattack that used the EternalBlue exploit to wreak havoc

Petya technically launched in early 2016, before WannaCry, but to little fanfare and damage. The first version of Petya was spread via a malicious email attachment and was a fairly straightforward form of ransomware — your computer gets infected and your files become encrypted (or held ransom) until you pay $300 worth of Bitcoin to purchase a decryption key

By the way, we recommend you never, ever, ever, (ever) pay the ransom.

Petya ransomware encrypts files and demands a ransom in Bitcoin to release them.

Thanks to EternalBlue and the unfortunate success of WannaCry, Petya ransomware was given a second chance at destruction. In June 2017, NotPetya was deployed using the EternalBlue exploit, and this time, people noticed

The key difference between the first and second versions of Petya was that NotPetya (Petya V2) was aimed at completely disabling a system. **Ransom paid or not, there was no cure**. The cyberattack permanently encrypted a computer's master file table (MFT) and the master boot record (MBR).

How much financial damage did EternalBlue cause?

So what's the bill for EternalBlue and who's footing it? The answer starts with a B, as in billions, and the people paying for it range from individuals like you, both directly and through taxes, to multinational corporations

Estimates put the cost of NotPetya at over $10 billion in damages and WannaCry at around $4 billion in damages

Some big names were hit quite hard. The world's largest shipping firm, Maersk, lost $300 million; the delivery company FedEx lost $400 million; and Merck Pharmaceuticals (known as MSD outside North America) lost $870 million after 15,000 of their Windows machines succumbed to NotPetya in just 90 seconds.

A deeper loss, one not as quantifiable in USD, was the loss of data and access for hospitals and health care institutions

When a network crashes at a hospital, doctors can't see information on potentially life saving surgeries that are meant to take place. Nor can they record or access changes to medication. Hospitals may even lose GPS signals for locating ambulances, as happened in Ukraine during the NotPetya cyberattack.

It's these types of non-monetary losses that make cyberattacks so dangerous for society at large.

Is EternalBlue still out there?

The short answer is, **yes, EternalBlue is alive** and well. Although WannaCry and NotPetya did most of their damage in early 2017, other attacks exploiting EternalBlue are unfortunately still going strong. As of May 2019, there were **hundreds of thousands of EternalBlue attack attempts daily**.

In fact, as of June 2020, **Avast is still blocking around 20 million EternalBlue attack attempts every month**.

Almost a **million machines still use the vulnerable SMBv1 protocol** and remain online. This fact alone ensures the persistence of EternalBlue. As long as computers remain unpatched and online, they remain unprotected

The deeper threat, however, may be in untapped exploits that were also released during the NSA hack by Shadow Brokers. EternalBlue was just one of many.

The most dangerous threat looming on the horizon has been dubbed EternalRocks, and it's on the cusp of being developed. Unlike WannaCry, which made use of two of the exploits exposed in the NSA hack, **EternalRocks is said to use seven exploits**, including EternalBlue, EternalRomance, EternalSynergy, EternalChampion, ArchiTouch, and SMBTouch. Potential threats include shellcode that executes right after Eternal exploits, such as DoublePulsar.

Is my system under threat?

Maybe.

But the good news is **there are strong tools to help you protect yourself**. While the EternalBlue threat remains, you can fight back by using security patches like MS17-

010 and free antivirus software.

We recommend **all Windows users deploy the security patch** available from Microsoft in MS17-010. All you need to do is update your software to the latest version of Windows. Without doing this, you'd be trying to fight problems of the present with tools from the past. The SMBv1 protocol needs to be made obsolete, so all Windows users need to apply the patch.

Do your part by **updating your computer with the latest available software updates** and follow these five tips for ultimate online security and privacy.

Want to see if your PC is vulnerable to an EternalBlue cyberattack? Our Wi-Fi Inspector can check for you right now.

Defend yourself against future exploits

Cyber attackers mean business, but so do we. That's why Avast has created powerful antivirus software to block harmful ransomware attacks like WannaCry and Petya. We use cloud-based artificial intelligence to provide six layers of protection against malware and other threats, including those which make use of the SMBv1 vulnerability. Plus, our firewall will check all incoming and outgoing traffic to your network to ensure your stay safe.

Avast One automatically detects and prevents malware attacks while also scanning your computer for outdated software that may contain vulnerabilities like EternalBlue. Stay safe from exploits and other current and future online threats with a world-class cybersecurity solution.

This Article Contains :

- **What is EternalBlue?**
- How was EternalBlue developed?
- Initial leak and fallout
- How does EternalBlue work?
- How is EternalBlue used in cyberattacks?
- Is EternalBlue still out there?

> Is my system under threat?
>
> Defend yourself against future exploits

You Might Also Like...

What Is Spyware, Who Can Be Attacked, and How to Prevent It

What Is Malware and How to Protect Against Malware Attacks?

What Is Scareware? Detection, Prevention, and Removal

What Is Pegasus Spyware and Is Your Phone Infected with Pegasus?

How to Detect and Remove Spyware From an iPhone

Latest Security Articles

You Might Also Like...

What Is Spyware, Who Can Be Attacked, and How to Prevent It

What Is Malware and How to Protect Against Malware Attacks?

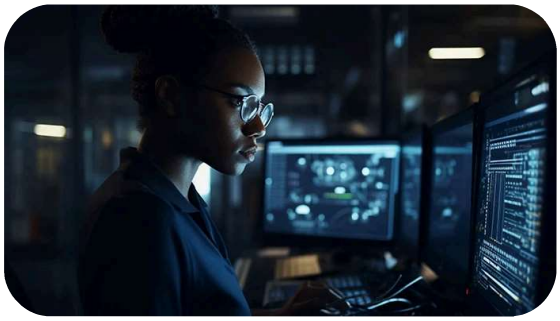
What Is Scareware? Detection, Prevention, and Removal

What Is Pegasus Spyware and Is Your Phone Infected with Pegasus?

How to Detect and Remove Spyware From an iPhone

Has My Amazon Account Been Hacked?

Can Someone Hack Your Phone by Calling or Texting You?



Packet Sniffing Explained: Definition, Types, and Protection

Support

Security

Privacy

Performance

Blog

Forum

For Business

Business support

Business products

Business partners

Business blog

Affiliates

For Partners

Mobile Carriers

Company

Contact Us

Investors

Careers

Press Center

Responsibility

Technology

Research Participation

Cookie Preferences