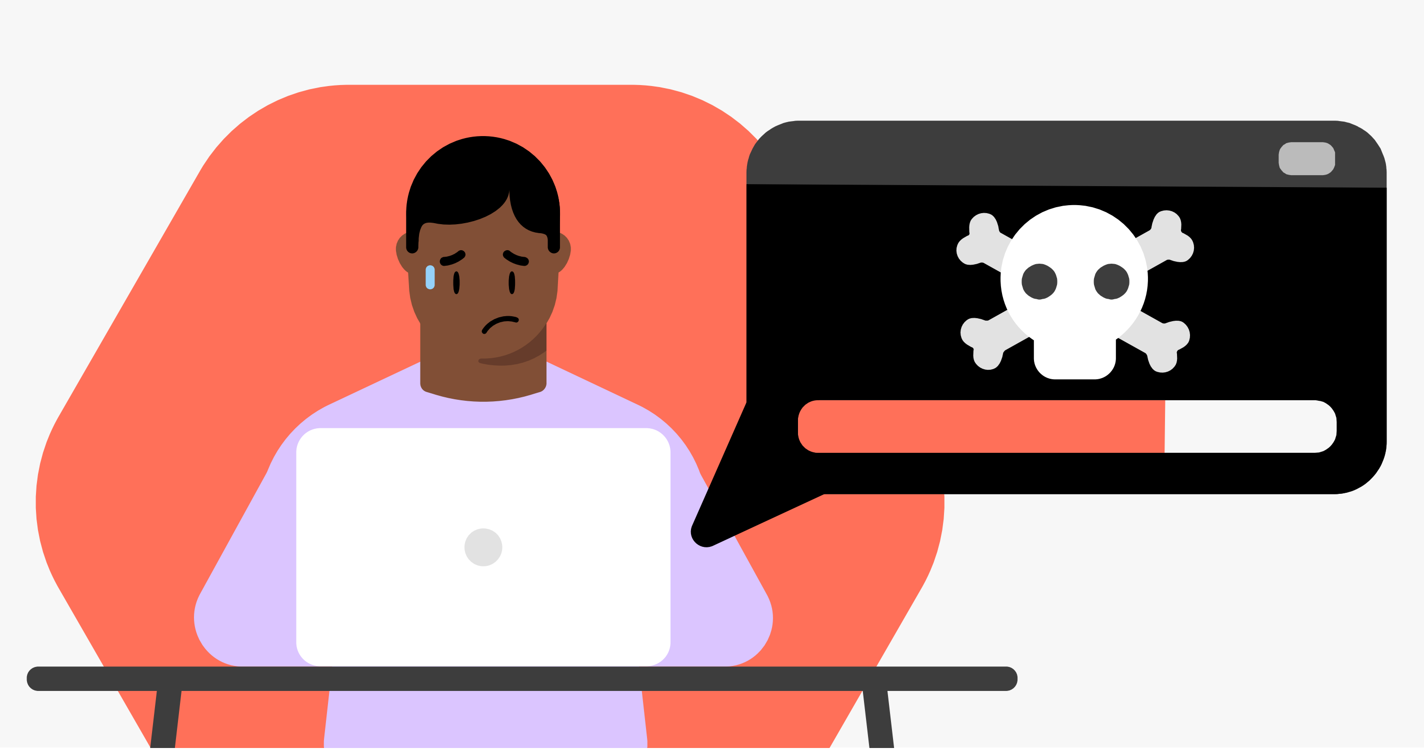
EternalBlue: What it is and how it works

Apr 28, 2023 4 min read

EternalBlue is a dangerous exploit that can be used to spread malware and put Windows users at risk. In this article, we explain what EternalBlue is and how to protect yourself against it.

Malcolm Higgins



What is EternalBlue?

EternalBlue is a Microsoft exploit which was used by the NSA in intelligence gathering operations. The exploit, officially named MS17-010 by Microsoft — gave the US National Security Agency (NSA) backend access to devices running Windows operating systems like Windows XP and Windows 7.

After being aware of a weakness in Microsoft's SMBv1 (Server Message Block version 1) file-sharing protocol for five years, the NSA finally informed Microsoft of its existence. However, by the time they did, it had been leaked by a notorious hacking collective known as Shadow Brokers.

The leak put millions of users at risk and the entire incident underlined the threats posed by the NSA's development and maintenance of software backdoors.

How was EternalBlue developed?

EternalBlue was developed by the NSA, which had spent years searching for potential vulnerabilities in Microsoft software. When it finally found a weakness in the SMBv1 protocol, the NSA developed its exploit as a way to take advantage of that vulnerability.

Instead of alerting Microsoft to the risks its users faced, the NSA used EternalBlue to aid in antiterrorism and counterintelligence operations for half a decade. EternalBlue is just one example of the NSA's use of exploits and software backdoors.

When the NSA finally decided to alert Microsoft, steps were taken to fix the vulnerability. Microsoft released patches for the exploit, but by then, for many, it was too late. Let's now take a closer look at how this exploit actually works.

How does EternalBlue work?

The EternalBlue exploit worked by taking advantage of the unsecure SMBv1 protocol. This protocol allowed Microsoft devices to communicate with other Microsoft systems — carrying out file and print services, for example — but was vulnerable to manipulation.

To carry out the EternalBlue exploit, attackers just needed to send a malicious SMBv1 data packet to a Windows server that had the vulnerability. The packet would contain a payload of malware, which could then be rapidly disseminated to other devices installed with the vulnerable Microsoft software.

Once the Shadow Brokers leaked the exploit in 2017, hackers took advantage of the vulnerability to carry out devastating attacks and spread massive amounts of malware. Two notable incidents exemplify the effects of the vulnerability.

WannaCry

On May 12, 2017, the WannaCry ransomware began to spread rapidly through the EternalBlue vulnerability, infecting 10,000 devices an hour. Within 24 hours, 230,000 Microsoft Windows machines had been infected in 150 different countries. The ransomware, which encrypts data on the infected device, ended up impacting major organizations like FedEx, Deutsche Bahn, and the UK's NHS.

NotPetya

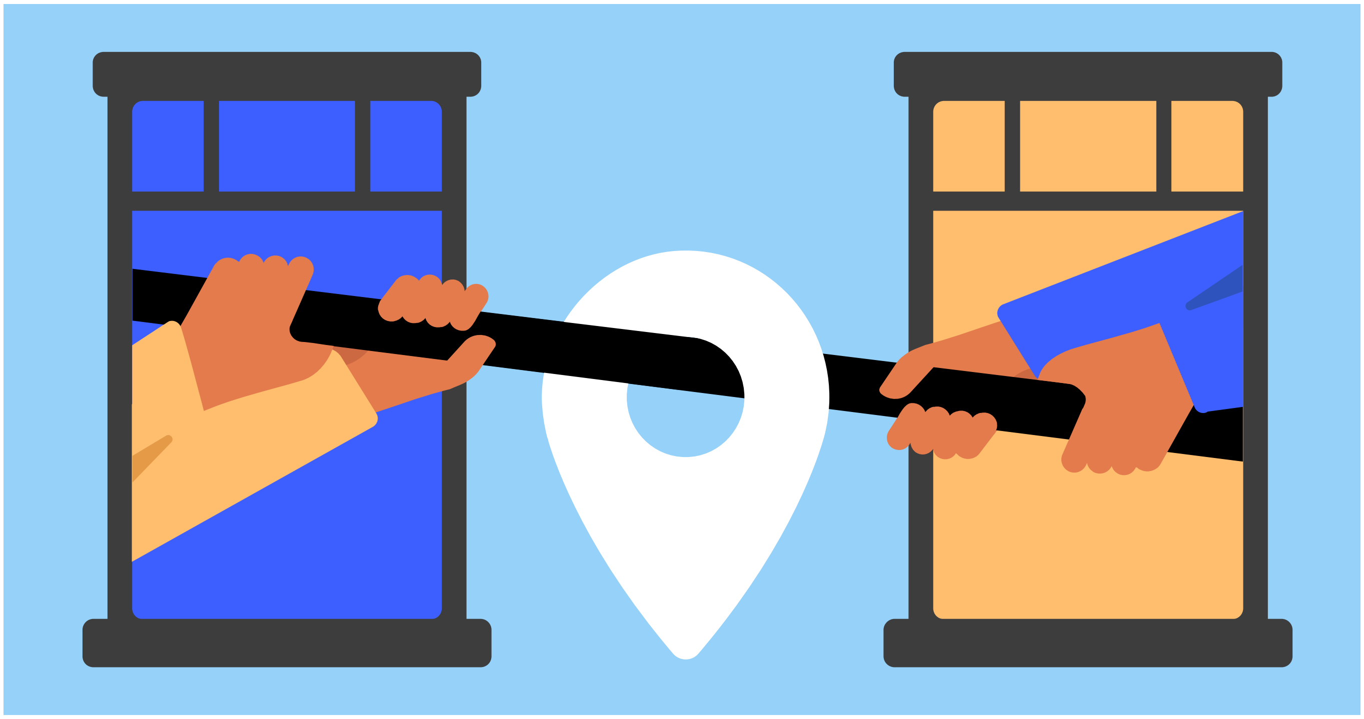
The Petya ransomware attack used the EternalBlue exploit to spread quickly across Microsoft devices in 2017. The malware would install itself, encrypt data on the host device, and then demand a ransom of $300 dollars in return for a decryption key.

Related articles

HOW-TO

How to turn on and troubleshoot Windows Defender

May 20, 2020 · 4 min read



HOW-TO

Windows has detected an IP address conflict

Dec 21, 2023 · 6 min read

Is EternalBlue still out there?

The vulnerability exploited by EternalBlue was resolved with a security patch from Microsoft in 2017, after the NSA let Microsoft know it existed. As a result, Windows devices with up-to-date software are safe from this specific threat.

Although the vulnerability was patched back in 2017, EternalBlue attacks still take place regularly. The security company Avast estimates that every month it blocks around 20 million EternalBlue exploit attempts. With this in mind, you might be wondering if you should still be afraid of EternalBlue today.

Should I be afraid of EternalBlue?

If you use older Windows versions or have not updated devices since 2017, you are almost certainly still at risk from EternalBlue. If you are using an up-to-date version of Windows and install new updates regularly, you don't need to worry about the EternalBlue exploit.

However, that doesn't mean you are immune to malware and ransomware attacks, like WannaCry and Petya. These malicious programs can spread in other ways, so it's important to stay vigilant, even if the EternalBlue exploit doesn't pose a specific threat to you.

The good news is that you can take steps to protect yourself from malware and other online threats right now.

How to protect yourself

To protect yourself from online risks like ransomware, follow these simple steps:

Keep software up to date. If you learn one lesson from the EternalBlue situation, it is the importance of updating your software. As soon as updates become available for applications and operating systems, install them so you can benefit from the latest security patches.

Use anti-malware software. Make sure your device is protected with strong anti-malware software. These systems can protect your device from malicious software and other online threats, though — like all cybersecurity tools — none make you completely safe.

Be wary of links. Even if you're not at risk from EternalBlue anymore, you could still download malware by clicking on a dangerous link. Phishing emails often try to trick you into visiting pages that will infect your device. To protect yourself, never click on a link in an online message unless you are absolutely certain that the sender is genuine.

Get NordVPN's additional Threat Protection feature. Threat Protection is a powerful suite of tools to keep you safe online. As well as blocking ads and online trackers, Threat Protection scans downloads for malware and prevents you from visiting sites known to install malicious software.

Malcolm Higgins

Malcolm is a content writer specializing in cybersecurity and tech news. With a background in journalism and a passion for digital privacy, he hopes his work will empower people to control their own data.

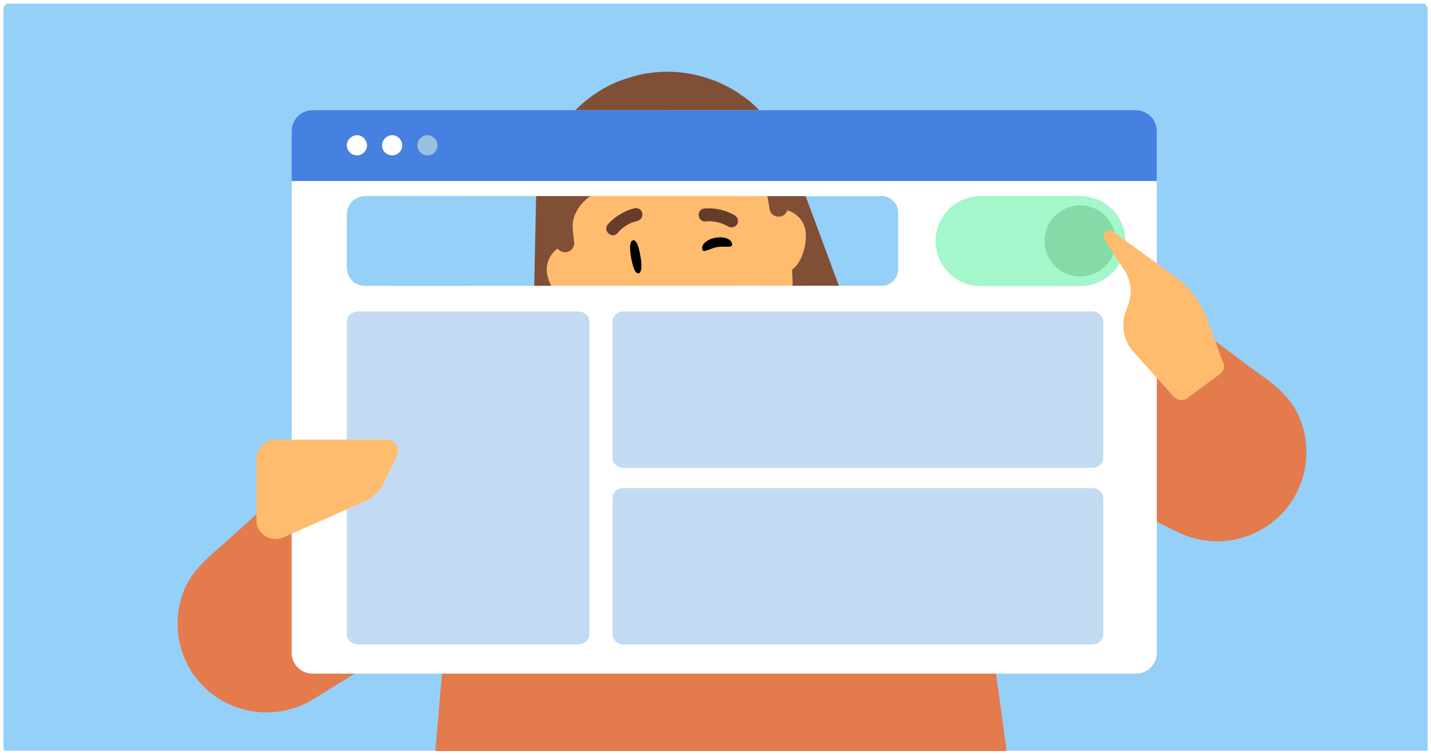
Trending articles

APP UPDATES

May 27, 2024 9 min read

NordVPN for Windows: Release notes

Veronica Kaptur

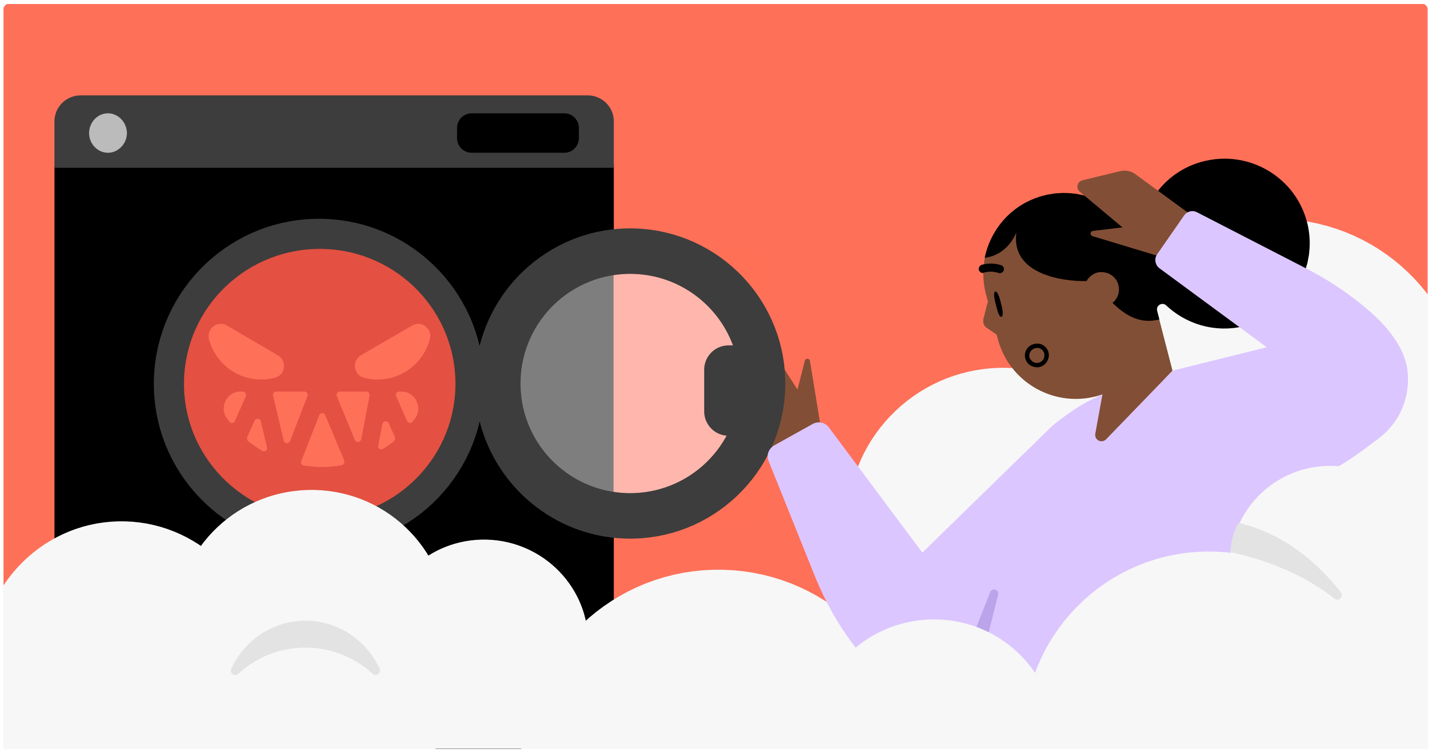


ANONYMITY

May 11, 2024 📖 11 min read

Using Google Chrome incognito mode: On or off?

Violeta Lyskoit



ONLINE THREATS

Jun 07, 2024 📖 5 min read

Devices that spy on you: How to tell they’re doing it, and what steps to take

Aurelija Einorytė

- Careers
- Money-Back Guarantee
- VPN Routers
- Reviews
- Student & Employee Discount
- Refer a Friend
- Research Lab

- macOS
- Linux
- Android
- iOS: iPhone / iPad
- Chrome
- Firefox
- Edge

ENGAGE

- What Is a VPN?
- IP Lookup
- What Is My IP?
- Cybersecurity Glossary
- Social Responsibility
- Cybersecurity Hub
- Press Area
- Become a Partner

HELP

- Support Center
- Tutorials
- FAQ
- Privacy Policy
- Cookie Preferences
- Terms of Service
- Contact Us

FOLLOW US

- Facebook
- Twitter
- LinkedIn
- YouTube

DISCOVER

- Nord Security
- NordLayer
- NordPass
- NordLocker

Instagram

English