Zeus Virus

By Kaspersky

Published: 2017-09-28 · Archived: 2026-04-05 15:13:39 UTC

VIRUS DEFINITION

Also Called: Zbot, Zeus Gameover, Trojan-Spy.Win32.Zbot

Virus Type: Malware | Botnet

What is Zeus Virus?

Zeus Virus (or Zeus Trojan malware) is a form of malicious software that targets Microsoft Windows and is often used to steal financial data. First detected in 2007, the Zeus Trojan, which is often called Zbot, has become one of the most successful pieces of botnet software in the world, afflicting millions of machines and spawning a host of similar pieces of malware built off of its code. While the threat posed by Zeus dwindled when its creator purportedly retired in 2010, a number of variants showed up on the scene when the source code became public, making this particular malware relevant and dangerous once again.

What Zeus Virus Does to Computers

The Zeus Virus can do a number of nasty things once it infects a computer, but it really has two major pieces of functionality.

First, it creates a botnet, which is a network of corrupted machines that are covertly controlled by a command and control server under the control of the malware's owner. A botnet allows the owner to collect massive amounts of information or execute large-scale attacks.

Zeus also acts as a financial services Trojan designed to steal banking credentials from the machines it infects. It accomplishes this through website monitoring and keylogging, where the malware recognizes when the user is on a banking website and records the keystrokes used to log in. This means that the Trojan can get around the security in place on these websites, as the keystrokes required for logging in are recorded as the user enters them.

Some forms of this malware also affect mobile devices, attempting to get around two-factor authentication that is gaining popularity in the financial services world.

Originally, the Trojan only affected computers running versions of the Microsoft Windows operating system, but some newer versions of the malware have been found on Symbian, BlackBerry and Android mobile devices.

The creator of the malware released the Zeus source code to the public in 2011, opening the doors for the creation of a number of new, updated versions of the malware. These days, even though the original Zeus malware has

been largely neutralized, the Trojan lives on as its components are used (and built upon) in a large number of new and emerging malware.

How the Zeus Virus Infects Computers

The Zeus Virus has two main methods of infection:

- Spam messages
- Drive-by downloads

The spam messages often come in the form of email, but there have been social media campaigns designed to spread the malware through messages and postings on social media sites. Once users click on a link in the email or message, they are directed to a website that automatically installs the malware. Because the malware is adept at stealing login credentials, it can sometimes be configured to steal email and social media credentials, enabling the botnet to spam messages from trusted sources and greatly expand its range.

Drive-by downloads happen when the hackers are able to corrupt legitimate websites, inserting their malicious code into a website that the user trusts. The malware then installs itself when the user visits the website or when the user downloads and installs a benign program.

How to Protect Yourself

Prevention through safe Internet practices is always the first step in staying safe from the Zeus malware. This means avoiding potentially dangerous websites, like those offering illegal free software, adult material or illegal downloads, as the owners of these types of websites often have no problem allowing malware owners to host their software on the site. Being safe also means not clicking on links in email or social media messages unless you were expecting the message. Remember: Even if the message is from a trusted source, if that source is afflicted with Zeus, the message could still be corrupt.

Staying safe also means being safe when interacting with financial institutions while online. Two-factor authentication, where the website sends a confirmation code to a mobile device to confirm the login, is a must. Remember, though, that some offshoots from Zeus have also infected mobile devices, so using this kind of authentication shouldn't be seen as a cure-all.

A powerful, updated antivirus solution is a must. These kinds of solutions will not only help protect you from visiting unsafe websites where you might find the Trojan, but can detect the Trojan when it downloads, tries to install or tries to run. Additionally, these solutions can scan your system and remove the malware if it already exists on your machine.

While there are a number of antivirus solutions out there, including a number that offer a free trial period, it's important to choose one that's from a leader in the industry that updates their solutions constantly. The fact that the Zeus source code is public means that there will be no end to the damage that this malware can do, and every few years you can expect that new versions of the malware will arise. Only a security vendor that is constantly vigilant against new threats has what it takes to truly protect you from the Zeus Trojan in the future.

The Zeus Trojan has come a long way in just a few years, coming out of nowhere to infect millions of computers around the world in a relatively short amount of time. Even though the original creator may not be running the malware any longer, the fact that its code is online and constantly being talked about, updated and improved upon within hacker circles means that it will continue to be a threat for years to come. Understanding that it's out there and taking steps to keep yourself, your finances and your family safe is imperative for anyone who wants to avoid the headache and financial pain of identity theft.

Kaspersky Internet Security received two AV-TEST awards for the best performance & protection for an internet security product in 2021. In all tests Kaspersky Internet Security showed outstanding performance and protection against cyberthreats.

Other articles related to Zeus Trojan Malware

- Understanding SPAM and Phishing Scams
- Internet Threats and Computer Viruses
- What you Need to Know about Trojan Horse Virus
- Identity Theft and Personal Data Security
- What to Do if Your Identity is Stolen: A Step-By-Step Guide

Related Products:

- Kaspersky Premium Antivirus
- Download Kaspersky Premium Antivirus with 30-Day Free Trial
- Kaspersky Antivirus for Mac
- Kaspersky Antivirus for Android
