What is Zeus Trojan Malware?

crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware

The Zeus Trojan Malware — Definition and Prevention

March 14, 2023

Since it was introduced to the internet in 2007, the Zeus malware attack (also called Zbot) has become a hugely successful trojan horse virus. Even today, the Zeus trojan and its variants are a major cybersecurity threat, and many computers that run Microsoft Windows are still at risk. As some variants of the Zeus virus are fileless malware, it can also be difficult for antivirus software to detect.

Zeus malware can give attackers full access to infected machines. While the original Zeus variant primarily utilized man-in-the-browser keyloggers to gain access to an infected computer's banking credentials and other financial information, many forms of the Zeus virus can also be used to add CryptoLocker ransomware to an operating system or add infected computers to a botnet to perform distributed denial-of-service (DDoS) attacks.

What Is Zeus Malware?

The Zeus trojan virus was first created in 2007, when hackers in Eastern Europe used it to target the United States Department of Transportation. While it's hard to say for certain who created it, the attack really took off when its malicious code became public in 2011. Since then, it has spawned dozens of variants that have kept internet security experts and law enforcement busy.

There are two common attack vectors that open Windows computers to Zeus trojan malware attacks. Drive-by downloads require a user to visit a website that has the backdoor trojan code on it. They then download files into the user's computer without the user's knowledge. Modern browsers such as Google Chrome usually block these downloads and the sites they are found on, but hackers are constantly implementing new workarounds for this. Meanwhile, older web browsers like Internet Explorer may not block drive-by downloads at all. Zeus's other main mode of infection is through phishing attacks where users think they are downloading benign software from links in a phishing email or a post on social media.

The two primary goals of the Zeus trojan horse virus are stealing people's financial information and adding machines to a botnet. Unlike many types of malware, most Zeus variants try to avoid doing long-term damage to the devices they infect. Their aim is to avoid detection from antivirus software. The longer they last, the more likely the hacker is to pick up valuable information from your financial institution.

Any number of computers can become part of a Zeus botnet: the FBI and the United States Department of Justice estimated in 2014 that up to one million computers around the world were infected with the Gameover variant of Zeus.

Types and Use Cases of Zeus Malware

The Zeus virus is both versatile and insidious, and its public source code makes it easy for bad actors to customize it for their needs. Some of the most common Zeus variants are:

- **Gameover Zeus:** The most dangerous Zeus variant, Gameover Zeus malware allows the people who deploy it to launch a potentially devastating ransomware attack on a computer running Microsoft Windows.
- **SpyEye:** This banking malware works similarly to Zeus malware, and in fact the programs are closely related to each other.
- **Ice IX:** After the Zeus virus was leaked, the Ice IX system was the first botnet based on its source code. It uses rogue forms to steal financial information such as your banking credentials.
- **Carberp:** This banking trojan impacts older versions of Windows, such as Windows XP and Windows 7. Someone combined this financial trojan with Zeus's code base to create a malware called "Zberp."
- **Shylock:** This malware infection uses man-in-the-browser attacks to steal bank account information as well.

Implementing strong endpoint security and keeping your antivirus software up to date are two of the best ways to protect against Zeus and its many variants.

A few signs that a computer is infected with a Zeus trojan include:

- A sudden slowdown in your device's operating speed
- Unusual transactions on your online banking portal
- Unknown programs running on your operating system
- Your computer begins to overheat suddenly

Risks of Zeus Virus

Just because a risk is well established doesn't mean that it's no longer a threat. Buffer overflow exploits, for instance, have been around for nearly 40 years, and they can still devastate servers and systems that refuse to make their cybersecurity a priority.

As technology evolves, so do the techniques that bad actors use to gain access to that technology. Moreover, the infrastructure of our society is growing increasingly digital. This only raises the stakes even further.

When the FBI cracked down on Gameover Zeus in 2014, they estimated that the malware had already infected up to a million computers, 25% of which were in the United States. In turn, this resulted in more than $100 million in financial damages. The most immediate risk of a Zeus infection is the financial loss that results from having your banking credentials compromised. If the attacker can find a corporate target who has deep pockets, so much the better for them.

The other primary risk of the Zeus trojan is more subtle. The virus and its variants can sit undetected on a computer for months or even longer, only activating when the botnet requires the machine. Unlike many other types of botnet, there is no centralized command computer that law enforcement can shut down; any computer can send commands at any time.

Much like the Sidoh exfiltration tool, the longer Zeus is allowed to run undetected on a system, the more damage it can do. An infected computer may simply log a user's keystrokes and send them to the attacker, or it may actively generate fake login pages to common social media networks to harvest and sell login credentials. It may organize a DDoS attack against a person, company or government; it may simply lie in wait until the botnet is needed.

In all cases, it's better for companies large and small to be proactive about their cybersecurity. Sites that allow users to log in, for instance, can implement security measures such as two-factor authentication and endpoint security measures.

Preventing Zeus Malware Attacks

As is the case with many threats on the internet, the best way to prevent a Zeus malware attack is to take a multipronged approach. Don't simply assume that an antimalware tool will be enough. Keep that software updated on every machine your company monitors and

make sure that it is running properly.

Another critical element of protecting against any form of malware, ransomware or other exploit is the human factor. Train all your employees to spot phishing attacks and spam and have a reporting system in place if they suspect any form of malicious action. Likewise, you should set up a robust acceptable use policy and unified endpoint management for your company's devices.

The good news is that the source code for the Zeus trojan has been public since 2011. This means that good actors in addition to malicious ones have a lot of lessons they can learn from it. Especially after the FBI's 2014 crackdown on Gameover Zeus, security professionals have been hard at work applying these lessons.

While Zeus primarily targets financial information and login credentials, botnets like the one run by Gameover Zeus generally aren't picky about their targets. Anyone can fall lax and become the victim of a drive-by download. A few best practices that you can implement to prevent Zeus from causing problems in the future include:

- Good cyber hygiene practices are key to preventing any breach. Keep your security software, browser and firewalls updated.
- Avoid clicking links in suspected phishing emails.
- Use an antivirus program from a trusted source and update its virus definitions at least once per month.
- Keep abreast of new developments in security news and be proactively aware of the new threats that are based on old code.
- Train your entire team — and not only your IT staff — in these best practices.

As with most forms of malware, the key to preventing a Zeus attack (or any other banker trojan) is a combination of advanced technology and human effort. Everyone has a role to play in cybersecurity, so bringing on an expert partner is one of the best things you can do.

How to Prevent Zeus Malware with CrowdStrike

There is an eternal push and pull between the people who create malicious software and the people who protect computers, servers and networks against it. At its heart, information security is never only a job for one person. True security practices require research and knowledge from the whole world. That's where CrowdStrike's team of experts comes in.

The CrowdStrike Falcon® platform delivers cloud-native, next-generation endpoint protection via a single lightweight agent and offers an array of complementary prevention and detection methods. To learn more, contact our organization to schedule a demo or enroll in a trial.