The Zeus Trojan How to Protect, Detect and Remove

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**The Zeus Trojan How to Protect, Detect and Remove**

1. **What is the Zeus Trojan :**

Zeus Trojan is a malware that uses encryption to keep its configuration secret. Zeus starts as a sensitive data theft tool specializing in the gathering of stored usernames and passwords as well as those that user type into the systems on which it resides. Zeus is designed to recognize high-security sites that require multiple factors to log on. Different versions will have different features such as plug-in architectures, anti-detection technologies, and multiple OS & platform attacks. It is claimed to be the first malware to use a randomly generated key rather than a static key (1).

1. **Protect:**

Do not download any files from unsuspecting websites, or social media. Do not open any emails with the zip file attached and then decrypt the zip file. These actions may download and decrypts the Zeus executable. Which mean limits on running executable file or scripts. At the enterprise level only recognized and authorized executables should be able to run (1).

Once Zeus is live, it then reaches out to command-and-control servers for an encrypted configuration file. Only download scripts and executable files from the official stores (Windows Stores, Apple Stores, Google Stores…)

1. **Detect:**

Zeus can be self-contained but process analyzing should reveal its identity. An occasional sweep with alternative anti-malware tools and rootkit detection tools may also be sensible though many of the vendors of what were just AV tools now include additional checks as well.

At the enterprise level, there should be additional checks on the network boundaries by using threat management tools. This should detect suspicious activity both coming into and going out of the network to block and report it (2).

1. **Remove**

One popular way to remove Zeus is to check Window Task Manager for suspicious processes that are not running by the Operating System (make sure we do not delete the wrong file by examining and researching the suspicious file), find their location, and remove them manually. This method should only apply when our antivirus is infected by Zeus. Another method is using good anti-malware with rapid updates to monitor and remove the virus at its early stage (2).

References

Chapple, M., & Seidl, D. (2023). Chapter 10: Cryptography and Cyberwar In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)

Stack Exchange (2014) *How to detect the so-called "undetectable" Gameover Zeus?* Retrieved from <https://security.stackexchange.com/questions/59418/how-to-detect-the-so-called-undetectable-gameover-zeus> (2)