New ZeuS binary | eternal-todo.com

Archived: 2026-04-05 22:04:40 UTC

- Botnet
- e-crime
- Malware
- ZeuS

The evolution continues. Some days ago a new ZeuS binary appeared with the version number 1.3.0.26. This new development is an attempt to improve the stealth techniques used to date, as stated in one of the TODO files found some time ago. After just a quick look, one can notice the following changes:

- When it's executed and the system isn't infected yet, it copies itself in the directory %SystemRoot%/system32, but with a different filename in each execution. Also it gets the basic file information from the %SystemRoot%/system32/ntdll.dll file (creation, last access and modification dates).
- If it finds a previous ZeuS version installed it deletes the binary, leaves and shows the hidden files in the next reboot. To give an idea of the situation, one of the latest samples with sdra64.exe as executable filename is the 1.2.12 one.
- Apparently the configuration and data files are not stored on disk anymore but they're exclusively stored in memory.

In addition to these important modifications, it’s worth mentioning the use of an IP instead of a domain name in the dropzone URL. Also, there doesn't seem to be a complete panel in the URL directory, but a small PHP file – probably a redirection. This is not something new, but maybe it's this version’s new way to hide and make difficult the analysis.

However, we've seen some samples with the version number 1.3.1.1 but featuring the usual behaviour (except deleting previous binaries): sdra64.exe as binary filename and storing configuration and data files on disk. Perhaps this is due to multiple options when creating the binary (builder) or to the existence of different authors.

As you can see, some of the techniques posted on this blog for detecting ZeuS have slightly changed in this case. Basically, all of them are still valid with the exception of the location of hidden configuration and data files function, which apparently don’t exist anymore.

This is only a preliminary analysis of this new binary, but we'll post more details as soon as we have them. Tune in again!

Submitted by jesparza on Fri, 2009/11/06 - 13:25
