Zeus Sphinx (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:29:02 UTC

This family describes the vanilla Zeus-variant that includes TOR (and Polipo proxy). It has an almost 90% overlap with Zeus v2.0.8.9.
Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

Zeus Sphinx on the one hand has the following versioning ("slow increase")
- 2015/09 v1.0.1.0 (Zeus Sphinx size: 1.5 MB)
- 2016/02 v1.0.1.2 (Zeus Sphinx size: 1.5 MB)
- 2016/04 v1.0.2.0 (Zeus Sphinx size: 1.5 MB)

Zeus OpenSSL on the other hand has the following versioning ("fast increase")
- 2016/05 v1.5.4.0 (Zeus OpenSSL size: 1.2 MB)
- 2017/01 v1.14.8.0 (Zeus OpenSSL size: 1.8 MB)
- 2017/01 v1.15.0.0 (Zeus OpenSSL size: 2.2 MB)

▶ [TLP:WHITE] win_zeus_sphinx_auto (20251219 | Detects win.zeus_sphinx.)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_sphinx