Zeus OpenSSL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 03:25:34 UTC

This family describes the Zeus-variant that includes a version of OpenSSL and usually is downloaded by Zloader.

In June 2016, the version 1.5.4.0 (PE timestamp: 2016.05.11) appeared, downloaded by Zloader (known as DEloader at that time). OpenSSL 1.0.1p is statically linked to it, thus its size is roughly 1.2 MB. In subsequent months, that size increased up to 1.6 MB.
In January 2017, with version 1.14.8.0, OpenSSL 1.0.2j was linked to it, increasing the size to 1.8 MB. Soon after also in January 2017, with version v1.15.0.0 the code was obfuscated, blowing up the size of the binary to 2.2 MB.

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_openssl_auto (20251219 | Detects win.zeus_openssl.)
