Zeus OpenSSL - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:43:40 UTC

Tool: Zeus OpenSSL

Names	Zeus OpenSSL Zeus Sphinx XSphinx
Category	Malware
Type	Banking trojan, Credential stealer, Botnet, Downloader
Description	(Malpedia) 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)
Information	<https://threatvector.cylance.com/en_us/home/threat-spotlight-terdot-a-zloader-malicious-downloader.html> <https://asert.arbornetworks.com/great-dga-sphinx/>

	<https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/> <https://blog.malwarebytes.com/cybercrime/2017/01/zbot-with-legitimate-applications-on-board/> <https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/> <https://securityintelligence.com/posts/zeus-sphinx-back-in-business-some-core-modifications-arise/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_openssl> <https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_sphinx>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool Zeus OpenSSL

Changed	Name	Country	Observed	
Other groups				
	Bamboo Spider, TA544	[Unknown]	2016-Apr 2022	

1 group listed (0 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0e1c08c2-3e35-4ad7-bb51-3c135b5065d8