

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:22:21 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Zeus

Tool: Zeus

Names	Zeus Zeus Zbot Trojan.Zbot Wsnpoem Gorhax Kneber
Category	Malware
Type	Banking trojan , Info stealer , Credential stealer , Downloader , Botnet
Description	<p>(Talos) One of the most high-profile pieces of malware in the current threat landscape is Zeus/Zbot, a nasty little trojan that has been employed by botnet operators around the world to steal banking credentials and other personal data, participate in click-fraud schemes, and likely numerous other criminal enterprises. It is the engine behind notorious botnets such as Kneber, which has recently made headlines worldwide. The following is an analysis of the network traffic generated by machines that Talos intentionally infected with known Zeus samples, in order to study post-infection behavior. The machines were all base installations of Windows XP, Service Pack 2, with no patches - i.e., designed to be as vulnerable as possible.</p>
Information	<p><https://talosintelligence.com/zeus_trojan></p> <p><https://usa.kaspersky.com/resource-center/threats/zeus-virus></p> <p><http://malwareint.blogspot.com/2010/02/facebook-phishing-campaign-proposed-by.html></p> <p><http://malwareint.blogspot.com/2010/02/zeus-on-irs-scam-remains-actively.html></p> <p><http://eternal-todo.com/blog/new-zeus-binary></p> <p><https://nakedsecurity.sophos.com/2010/07/24/sample-run/></p> <p><https://www.mnin.org/write/ZeusMalware.pdf></p> <p><http://malwareint.blogspot.com/2010/01/leveraging-zeus-to-send-spam-through.html></p> <p><http://eternal-todo.com/blog/zeus-spreading-facebook></p> <p><http://malwareint.blogspot.com/2010/03/new-phishing-campaign-against-facebook.html></p> <p><http://eternal-todo.com/blog/detecting-zeus></p> <p><https://www.secureworks.com/research/zeus?threat=zeus></p> <p><http://malwareint.blogspot.com/2009/07/special-zeus-botnet-for-dummies.html></p>

	< https://en.wikipedia.org/wiki/Zeus_(malware) > < https://blog.malwarebytes.com/101/2021/07/the-life-and-death-of-the-zeus-trojan/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus >

Last change to this tool card: 09 August 2021

Download this tool card in [JSON](#) format

All groups using tool Zeus

Changed	Name	Country	Observed	
APT groups				
	TA505 , Graceful Spider , Gold Evergreen		2006-Nov 2022	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f186f5ea-0a67-47ff-affc-41f34e62725e>