Zeus Panda - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:39:56 UTC

Tool: Zeus Panda

Names	Zeus Panda ZeusPanda PandaBanker
Category	Malware
Type	Banking trojan, Info stealer, Credential stealer, Downloader, Botnet
Description	(Proofpoint) Banking Trojans work by injecting code into web pages as they are viewed on infected machines, allowing the malware to harvest banking credentials and credit card information as victims interact with legitimate sites. Most often, the injects -- the code that actually performs the man-in-the-browser attacks -- are configured for region-specific banking sites. More recently, we have seen injects for online payment sites, casinos, retailers, and more appearing in banking Trojan campaigns. Since November -- a period of time that includes Thanksgiving, Black Friday, Cyber Monday and now leading up to Christmas -- we have observed Zeus Panda banking Trojan campaigns that have an increasing focus on non-banking targets with an extensive list of injects clearly designed to capitalize on holiday shopping and activities.
Information	<https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers> <https://github.com/JR0driguezB/malware_configs/tree/master/PandaBanker> <https://cyber.wtf/2017/02/03/zeus-panda-webinjects-a-case-study/> <https://cyber.wtf/2017/03/13/zeus-panda-webinjects-dont-trust-your-eyes/> <https://www.arbornetworks.com/blog/asert/panda-bankers-future-dga/> <https://f5.com/labs/articles/threat-intelligence/malware/panda-malware-broadens-targets-to-cryptocurrency-exchanges-and-social-media> <https://www.proofpoint.com/tw/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market> <https://www.spamhaus.org/news/article/771/> <https://www.vkremez.com/2018/08/lets-learn-dissecting-panda-banker.html> <http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html> <https://blogs.forcepoint.com/security-labs/zeus-panda-delivered-sundown-targets-uk-

	banks> <https://www.arbornetworks.com/blog/asert/panda-banker-zeros-in-on-japanese-targets/> <https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf> <https://www.arbornetworks.com/blog/asert/let-pandas-zeus-zeus-zeus-zeus/> <http://www.vkremez.com/2018/01/lets-learn-dissect-panda-banking.html> <https://en.wikipedia.org/wiki/ZeuS_Panda>
MITRE ATT&CK	<https://attack.mitre.org/software/S0330/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pandabanker>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:zeus%20panda>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool Zeus Panda

Changed	Name	Country	Observed	
Other groups				
	Bamboo Spider, TA544	[Unknown]	2016-Apr 2022	
	TA516	[Unknown]	2016-Feb 2020	

2 groups listed (0 APT, 2 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=863ac646-bf1b-4f62-8a85-7b4569a88808