Bamboo Spider, TA544 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:58:16 UTC

Other threat group: Bamboo Spider, TA544

Names	Bamboo Spider *(CrowdStrike)* TA544 *(Proofpoint)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2016	
Description	Zeus Panda, Panda Banker, or Panda is a variant of the original Zeus under the banking Trojan category. Its discovery was in 2016 in Brazil around the time of the Olympic Games. The majority of the code is derived from the original Zeus trojan, and maintains the coding to carry out man-in-the-browser, keystroke logging, and form grabbing attacks. ZeuS Panda launches attack campaigns with a variety of exploit kits and loaders by way of drive-by downloads and phishing emails, and also hooking internet search results to infected pages. Stealth capabilities make not only detecting but analyzing the malware difficult. GozNym has been observed to be distributed via the Avalanche botnet. Zeus Panda has been observed to be distributed by Emotet (operated by Mummy Spider, TA542), Smoke Loader (operated by Smoky Spider), Cutwail (operated by Narwhal Spider) and Kelihos (operated by Zombie Spider).	
Observed	Sectors: Financial, Hospitality, IT, Manufacturing, Retail, Technology. Countries: Brazil, Canada, Germany, Italy, Japan, Netherlands, Poland, Spain, UK, USA and other.	
Tools used	Chthonic, Gozi ISFB, GozNym, Nymaim, Zeus OpenSSL, Zeus Panda, Smoke Loader, URLZone, ZLoader.	
Operations performed	Apr 2016	Attacks against more than 24 U.S. and Canadian banks <https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/>

Apr 2016	Attacks on banks in Poland <https://threatpost.com/attackers-behind-goznym-trojan-set-sights-on-europe/117647/>
Jun 2016	Attacks on banks in the USA <https://www.computerworld.com/article/3088102/goznym-trojan-targets-business-accounts-at-major-us-banks.html>
Jun 2016	LinkedIn information used to spread banking malware in the Netherlands <https://blog.fox-it.com/2016/06/07/linkedin-information-used-to-spread-banking-malware-in-the-netherlands/>
Jul 2016	Zeus Panda Delivered By Sundown - Targets UK Banks <https://www.forcepoint.com/tr/blog/x-labs/zeus-panda-delivered-sundown-targets-uk-banks>
Aug 2016	Banking Trojan Zeus Panda shambles into Brazil ahead of Olympics <https://techcrunch.com/2016/08/04/banking-trojan-zeus-panda-shambles-into-brazil-ahead-of-olympics/>
Aug 2016	Attacks on banks in Germany <https://threatpost.com/goznym-banking-trojan-targeting-german-banks/120075/>
Oct 2017	Poisoning the Well: Banking Trojan Targets Google Search Results <https://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html>
Dec 2017	Zeus Panda Banking Trojan Targets Online Holiday Shoppers <https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers> <https://blog.fox-it.com/2017/12/12/criminals-in-a-festive-mood/>
Mar 2018	Panda Banker Zeros in on Japanese Targets <https://www.netscout.com/blog/asert/panda-banker-zeros-japanese-targets>
Jun 2018	Zeus Panda Advanced Banking Trojan Gets Creative to Scam Affluent Victims in Italy <https://cofense.com/zeus-panda-advanced-banking-trojan-gets-creative-scam-affluent-victims-italy/>
Jul 2018	Emotet infection traffic with Zeus Panda Banker <https://www.malware-traffic-analysis.net/2018/07/19/index.html>

	Aug 2018	For the past weeks our Threat Intelligence team has been following an enxtesive campaign, possibly operated by the same group, targeting a large amount of financial institutions, cyptocurrency wallets and the occasional Google and Apple accounts. <https://reaqta.com/2018/09/global-malware-campaign-using-zeus-panda/>
	Mar 2020	Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy <https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/>
	May 2020	Zeus Sphinx Back in Business: Some Core Modifications Arise <https://securityintelligence.com/posts/zeus-sphinx-back-in-business-some-core-modifications-arise/>
	Sep 2021	TA544 Targets Italian Organizations with Ursnif Malware <https://www.proofpoint.com/us/blog/security-briefs/ta544-targets-italian-organizations-ursnif-malware>
Counter operations	May 2019	GozNym Malware: Cybercriminal Network Dismantled in International Operation <https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation>
	Apr 2022	Notorious cybercrime gang's botnet disrupted <https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/>

Last change to this card: 03 May 2022

Download this actor card in PDF or JSON format
