ZeuS Panda

By Contributors to Wikimedia projects

Published: 2018-04-08 · Archived: 2026-04-05 20:14:00 UTC

From Wikipedia, the free encyclopedia

ZeuS Panda, Panda Banker, or Panda is a variant of the original Zeus (Trojan horse) 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.

ZeuS Panda utilizes the capabilities from numerous loaders such as Emotet, Smoke Loader,[1] Godzilla,[2] and Hancitor.[3] The methods of the loaders vary but the same end state goal of installing ZeuS Panda into a system is the same. Many of the loaders were originally trojans before were retooled as a delivery system for ZeuS Panda. The delivery mechanisms do not stop necessarily with the aforementioned loaders as Exploit kits such as Angler, Nuclear, Neutrino, Sundown[4] are also utilized. Coders of the ZeuS Panda banking trojan, as well as other trojan coders, lean toward employing loaders over exploit kits due to the higher potential yield in monetary gain.[5] The loaders also add the persistent capability of ZeuS Panda across reboot and also if it is deleted.[6][7] If ZeuS Panda no longer detected on a system and if the loader is still present, it will re-download the nefarious code and start running all over again.

One of the key distinctions of ZeuS Panda over other banking trojans is the ability to target systems in specific regions of the world. It does this by a rudimentary process by which it detects the Human Interface Device code the attached keyboard. If a keyboard code from Russia (0x419), Belarus (0x423), Kazakhstan (0x43f) or Ukraine (0x422) is detected Zeus Panda will self delete. This falls in line with the ethics of Russian cyber criminals abide to avoid detainment: “Russians must not hack Russians…”, second “If a Russian Intelligence service asks for help, you provide it”, and last “Watch where you vacation”.[8]

ZeuS Panda employs many methods of infection, namely drive by downloads, poisoned email, word document macro.[9] The drive by downloads are “Downloads which a person has authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically.” Including “Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.” Poisoned email occurs when a mailing list is injected with a number of invalid e-mail addresses, the resources required to send a message to this list has increased, even though the number of valid recipients has not. Command and control servers are how ZeuS Panda is able to spread across the vastness of the world but also remain under control by a handful of operators.[10]

First discovered in 2016 prior to the Olympics in Brazil, ZeuS Panda has spread to all parts of the globe in similar fashion to the original Zeus banking trojan. This is similar to the map of Zeus infections across the global, especially in regional concentrations of infection. Locations of the infected domains by region and concentration are similar to the original Zeus infection locations. Though there are still locations within Russia which are listed as infections, it is likely to be a standalone server distributing the banking trojan. Countries which are targeted more than others are likely based on the GDP.

There are regions which do not have as many reported infections. Some of the reasons are likely lack of sufficient GDP to be a target, one of the protected areas which Russian cybercriminals do not attack, or simply lack of reporting by personnel and antivirus in the region.[10]

Stealth capabilities

[edit]

ZeuS Panda is able to detect and counter many forensic analytic tools and sandbox environments. Currently there is at least 23 known tools it can detect and if any of them are found on the system, ZeuS Panda stops installation and removes itself from the system. Adding the “-f” command line parameter at the start of the malware will do away with this security feature in effort to raise infection rate at the risk of detection. Aside from the anti-detection capabilities, it also has anti-analysis protocols should the “-f” function be used or a program not on the trojans watchlist detect it. It does so by inspecting the file, mutex, running process, and registry key.[11]

After the anti-detection and analysis parameters are met, ZeuS Panda will deeply embed itself into the system registry. It will looks for empty folders with a long subfolder chain without the names Microsoft or Firefox in the tree.[10] Encrypting its data adds to the difficulty of detection by cyber forensics. The configuration settings are encrypted with RC4 and AES encryption, but is also known to use cryptographic hash functions employing SHA256 and SHA1 algorithms.[11]

Certain anti-virus companies have been able to overcome ZeuS Panda's stealth capabilities and remove it from the infected system. Some of them go off of a list of Indicators of Compromise (IoC), and can also determine which campaign the version of ZeuS Panda originated. The IoCs are signatures left behind by the malware as well as IP addresses, hashes, or URLs linked to command and control servers. Once the anti-virus determines it is ZeuS Panda infecting the system, it goes through an automatic algorithm to completely remove it and its loader if possible. There are also ways to remove it manually.[12][13]

1. ^ *"Smoke Loader"*.
2. ^ *"New "Panda Banker" Trojan Borrows Code From Zeus - SecurityWeek.Com"*. *www.securityweek.com*.
3. ^ *"Malware-Traffic-Analysis.net - 2018-04-04 - Hancitor malspam - Fake DHL notifications"*. *www.malware-traffic-analysis.net*.
4. ^ *"Zeus Panda Delivered By Sundown - Targets UK Banks - Forcepoint"*. *blogs.forcepoint.com. 26 July 2016. Archived from the original on 10 August 2017. Retrieved 8 April 2018.*
5. ^ *"Major decline in exploit kits - less financially viable than ransomware"*. [*permanent dead link*]
6. ^ *"Smoke Loader - downloader with a smokescreen still alive - Malwarebytes Labs - Malwarebytes Labs"*. *blog.malwarebytes.com*.

7. ^ *"Panda Banker: New Banking Trojan Hits the Market"*. *www.proofpoint.com. 20 April 2016.*
8. ^ *"Russian Cybercrime Rule No. 1: Don't Hack Russians"*. *www.bankinfosecurity.com.*
9. ^ *"Zeus Panda Targeting - Northwest Bank"*. *www.bank-northwest.com.*
10. ^ Jump up to: ***a*** ***b*** ***c*** *Berghoff, Tim (11 August 2017). "Analysis: ZeuS Panda". www.gdatasoftware.com.*
11. ^ Jump up to: ***a*** ***b*** *"Analysis Results of Zeus.Variant.Panda" (PDF).*
12. ^ *"Panda Banker - IBM X-Force Collection"*. *exchange.xforce.ibmcloud.com.*
13. ^ *K., Maria (13 December 2017). "Zeus Panda Malware Removal (March 2018 Update)".*
