TrojanDownloader:Win32/Small.gen!AO

Article URL
malware.php?mal_id=15475254775e9d0b42386675.66465470

Author
SecurityHome.eu

Published: 20 April 2020

Aliases :

TrojanDownloader:Win32/Small.gen!AO

is also known as *Win32/TrojanDownloader.Banload.IE, W32/Downloader.TND*

.

Explanation :

TrojanDownloader:Win32/Small.gen!AO is a program that silently downloads and executes arbitrary files without the affected user's consent. Installation details and the files downloaded and executed may vary from instance to instance because of the generic nature of the detection.Â For example, one such file detected as TrojanDownloader:Win32/Small.gen!AO displayed the following characteristics:Â It was distributed asÂ a Win32Â packedÂ executable of 28,672 bytes in size. When executed this trojan performs the following actions: Attempts to download and execute aÂ file located at IP 70.147.30.110 (at the time of writing this remote file was not available). If successful the trojan stores the downloaded file locally as %windir%system svchots.exe. (Note the filename difference from the standard windows file svchost.exe). This file is then executed. DropsÂ the file %windir%sysreq2.txt. The trojan uses this fileÂ to store theÂ number of successful downloading attempts. The number is inÂ ASCII format (for instance numberÂ 1 is represented by hex value 31h). Attempts to terminateÂ the running process 'msconf.exe', which is normally associated with other malicious programs. Â Analysis by Oleg Petrovsky

Last update 20 April 2020