Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:42:39 UTC

Tool: BigpipeLoader

Names	BigpipeLoader
Category	Malware
Type	Loader
Description	(Trend Micro) Since this loader will read/write encrypted payload through a named pipe, we named this shellcode loader BigpipeLoader. In one of our threat hunting sessions, we found two variants of this loader with different execution procedures. The first variant of BigpipeLoader just drops the decoy file and loads the Cobalt Strike payload into the memory, then proceeds to execute it. In the second variant, however, the attacker creates a dropper, which drops the malicious WTSAPI32.dll designed to be sideloaded by a legitimate application with the file name “wusa.exe”. This launches the encrypted BigpipeLoader (chrome.inf). Both variants of BigpipeLoader use the AES-128-CFB algorithm to decrypt the payload.
Information	<https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html>

Last change to this tool card: 19 November 2022

Download this tool card in JSON format

All groups using tool BigpipeLoader

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Earth Longzhi		2020-Apr 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bf77aa3f-d900-4311-91f0-47f5d8c9a6e1