Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:37:24 UTC

Tool: Bvp47

Names	Bvp47
Category	Malware
Type	Backdoor, Rootkit
Description	(Pangu Lab) In a certain month of 2013, during an in-depth forensic investigation of a host in a key domestic department, researchers from the Pangu Lab extracted a set of advanced backdoors on the Linux platform, which used advanced covert channel behavior based on TCP SYN packets, code obfuscation, system hiding, and self-destruction design. In case of failure to fully decrypt, It is further found that this backdoor needs the check code bound to the host to run normally. Then the researchers cracked the check code and successfully ran the backdoor. Judging from some behavioral functions, this is a top-tier APT backdoor, but further investigation requires the attacker's asymmetric encrypted private key to activate the remote control function. Based on the most common string 'Bvp' in the sample and the numerical value 0x47 used in the encryption algorithm, the team named the corresponding malicious code 'Bvp47' at the time.
Information	<https://www.pangulab.cn/en/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.bvp47>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool Bvp47

Changed	Name	Country	Observed	
APT groups				
	Equation Group		2001-Aug 2016	

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