Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:55:24 UTC

Tool: LEMONSTICK

Names	LEMONSTICK
Category	Malware
Type	Backdoor, Tunneling
Description	(FireEye) LEMONSTICK is a Linux executable command line utility with backdoor capabilities. The backdoor can execute files, transfer files, and tunnel connections. LEMONSTICK can be started in two different ways: passing the `-c` command line argument (with an optional file) and setting the 'OCB' environment variable. When started with the `-c` command line argument, LEMONSTICK spawns an interactive shell. When started in OCB mode, LEMONSTICK expects to read from STDIN. The STDIN data is expected to be encrypted with the blowfish algorithm. After decrypting, it dispatches commands based on the name—for example: 'executes terminal command', 'connect to remote system', 'send & retrieve file', 'create socket connection'.
Information	<https://www.mandiant.com/resources/live-off-the-land-an-overview-of-unc1945>

Last change to this tool card: 03 April 2022

Download this tool card in JSON format

All groups using tool LEMONSTICK

Changed	Name	Country	Observed	
APT groups				
	LightBasin		2016	

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