Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:22:13 UTC

Tool: BrittleBush

Names	BrittleBush
Category	Malware
Type	Backdoor
Description	(Proofpoint) Later versions of the RAR files that deliver NimbleMamba also included a small trojan application Proofpoint dubbed BrittleBush (2E4671C517040CBD66A1BE0F04FB8F2AF7064FEF2B5EE5E33D1F9D347E4C419F). This trojan communicated with easyuploadservice[.]com and received commands as base64 encoded JSON structure.
Information	<https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.brittle_bush>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool BrittleBush

Changed	Name	Country	Observed	
APT groups				
	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	

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