Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:11:21 UTC

Tool: BUBBLEWRAP

Names	BUBBLEWRAP Backdoor.APT.FakeWinHTTPHelper
Category	Malware
Type	Reconnaissance, Backdoor
Description	(FireEye) BUBBLEWRAP is a full-featured backdoor that is set to run when the system boots, and can communicate using HTTP, HTTPS, or a SOCKS proxy. This backdoor collects system information, including the operating system version and hostname, and includes functionality to check, upload, and register plugins that can further enhance its capabilities.
Information	<https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0043/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bubblewrap>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool BUBBLEWRAP

Changed	Name	Country	Observed	
APT groups				
	Temper Panda, admin@338		2014	

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