Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:57:56 UTC

Tool: BELLHOP

Names	BELLHOP
Category	Malware
Type	Backdoor, Downloader
Description	BELLHOP is a JavaScript backdoor interpreted using the native Windows Scripting Host (WSH). After performing some basic host information gathering, the BELLHOP dropper downloads a base64-encoded blob of JavaScript to disk and sets up persistence in three ways: • Creating a Run key in the Registry • Creating a RunOnce key in the Registry • Creating a persistent named scheduled task • BELLHOP communicates using HTTP and HTTPS with primarily benign sites such as Google Docs and PasteBin.
Information	<https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.bellhop>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool BELLHOP

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d4b98d7f-6fe7-4cee-9e84-dc702c41bab5