Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:41:05 UTC

Tool: DEPLOYLOG

Names	DEPLOYLOG
Category	Malware
Type	Loader
Description	(Cybereason) DEPLOYLOG (dbghelp.dll) is a 64 bit DLL, with two purposes: • The first one is responsible for extracting and executing the attackers' rootkit, dubbed WINNKIT, from the CLFS log file. • After a successful deployment of the WINNKIT rootkit, DEPLOYLOG switches to its second task, which is communicating both with the remote C2 and the kernel-level rootkit. It's noteworthy to mention that to evade detection, the attackers deployed DEPLOYLOG as dbghelp.dll, a generic, widely used name leveraged to masquerade as a legitimate file at the same location as PRIVATELOG (C:\Windows\System32\WindowsPowerShell\v1.0).
Information	<https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive>

Last change to this tool card: 19 July 2022

Download this tool card in JSON format

All groups using tool DEPLOYLOG

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c8cfd354-2ba8-4668-bd5b-73cf20816f26