Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:48:43 UTC

Tool: SPARKLOG

Names	SPARKLOG
Category	Malware
Type	Loader
Description	(Cybereason) SPARKLOG (spark.exe) is a 32 bit executable written in C++, employed in this attack to extract a DLL from the CLFS file, decrypt it and then launch it for side-loading by Windows services running as SYSTEM. Executing this phase of the attack successfully enables the attackers to gain Privilege Escalation and also Persistence in a specific case.
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 SPARKLOG

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

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