Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:20:13 UTC

Tool: SPINNER

Names	SPINNER
Category	Malware
Type	Reconnaissance, Backdoor, Exfiltration
Description	(Check Point) Many of the functions inside the final payload share similar logic with the SPINNER variant described above, but the payload lacks the compiler-level obfuscations observed in the newer campaign making it easier to analyze. Furthermore, the previous version of the backdoor contains additional features. This is another indication that the initial SPINNER backdoor version we observed is only a part of the bigger payload. It's likely the actors eventually split the payload and only equipped the first stage of the main backdoor with essential functions: enumeration of the victim's machine and execution of the next stage payloads received from the C&C server. The full version of the SPINNER backdoor contains the following capabilities: • Collects information about the infected machine (enumerate disks, files). • Exfiltrates files from the infected machine and manipulates the local files. • Runs OS commands and executes downloaded payload, as part of typical backdoor capabilities.
Information	<https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/>

Last change to this tool card: 19 July 2022

Download this tool card in JSON format

All groups using tool SPINNER

Changed	Name	Country	Observed
APT groups			

	Twisted Panda		2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=783d3b2e-0298-469d-84b5-e10fa395d6e3