Twisted Panda - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:04:31 UTC

APT group: Twisted Panda

Names	Twisted Panda *(Check Point)*
Country	China
Motivation	Information theft and espionage
First seen	2021
Description	(Check Point) Check Point Research (CPR) unveils a targeted campaign against at least two research institutes in Russia, which are part of the Rostec corporation, a state-owned defense conglomerate. This campaign is a continuation of what is believed to be a long-running espionage operation against Russian-related entities that has persisted since at least July 2021. The operation may still be ongoing, as the most recent activity was observed in April 2022. This activity was attributed to a Chinese threat actor, with possible connections to Stone Panda, APT 10, menuPass, a sophisticated and experienced nation-state-backed actor, and Mustang Panda, another proficient China-based cyber espionage group. The campaign has been dubbed Twisted Panda to reflect the sophistication of the tools observed and the attribution to China. The hackers use new tools, which have not previously been described: a sophisticated multi-layered loader and a backdoor dubbed SPINNER. These tools use advanced evasion and anti-analysis techniques such as multi-layer in-memory loaders and compiler-level obfuscations.
Observed	Sectors: Defense. Countries: Belarus, Russia.
Tools used	SPINNER.
Information	<https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/>

Last change to this card: 19 July 2022

Download this actor card in PDF or JSON format
