Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:43:27 UTC

Tool: Powerkatz

Names	Powerkatz
Category	Malware
Type	Loader
Description	(Yoroi) As intended by its name, it is able to start a new asynchronous task on the victim's machine, executing the task object passed as _app parameter. Once the task is started, the function waits its completion using repeated 1-sec sleeps cycle, and then it returns a valid code status to the function caller. Probably this module can be used in conjunction with some other functions, belonging to other pieces of the implant, to perform malicious actions in background, making all more stealth. Note: not the same software as an open source project on GitHub.
Information	<https://yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.powerkatz>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Powerkatz

Changed	Name	Country	Observed	
APT groups				
	Iridium		2018-Dec 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bff71209-edc8-43d5-9351-3ce94114171e