Threat Group Cards: A Threat Actor Encyclopedia

Tool: DropPhone

Names	DropPhone
Category	Malware
Type	Reconnaissance, Info stealer
Description	(Kaspersky) DropPhone launches sdclt.exe, then collects environment information from the victim machine and sends it to Dropbox. The last thing this implant does is delete data.dat without ever accessing its contents. We speculate that they are consumed by sdclt.exe, and that this is another way to lock together the execution of two components, frustrating the efforts of the reverse-engineers who are missing pieces of the puzzle – as is our case here.
Information	<https://securelist.com/the-leap-of-a-cycldek-related-threat-actor/101243/>

Last change to this tool card: 15 May 2021

Download this tool card in JSON format

All groups using tool DropPhone

Changed	Name	Country	Observed	
APT groups				
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	

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