Threat Group Cards: A Threat Actor Encyclopedia

Tool: CreepySnail

Names	CreepySnail
Category	Malware
Type	Backdoor
Description	(ESET) CreepySnail is another PowerShell backdoor that sends HTTP requests to a C&C server and receives and executes PowerShell commands. We saw various versions of this backdoor in the wild, though the differences between them were minimal.
Information	<https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1024/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.creepysnail>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool CreepySnail

Changed	Name	Country	Observed	
APT groups				
	Polonium		2022-Sep 2022	

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