PAWS - Threat Group Cards: A Threat Actor Encyclopedia

Tool: SUBTLE-PAWS

Names	SUBTLE-PAWS
Category	Malware
Type	Backdoor
Description	(Securonix) An interesting campaign leveraging a new SUBTLE-PAWS PowerShell-based backdoor has been identified targeting Ukraine which follows stealthy tactics to evade detection and spreads by infecting USB drives.
Information	<https://www.securonix.com/blog/security-advisory-steadyursa-attack-campaign-targets-ukraine-military/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.subtle_paws>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool SUBTLE-PAWS

Changed	Name	Country	Observed	
APT groups				
	Gamaredon Group		2013-Feb 2025	

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