Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:53:29 UTC

Tool: PowerDuke

Names	PowerDuke
Category	Malware
Type	Backdoor
Description	(Volexity) The PowerDuke backdoor boasts a pretty extensive list of features that allow the Dukes to examine and control a system. Volexity suspects the feature set that has been built into PowerDuke is an extension of their anti-VM capabilities in the initial dropper files. Several commands supported by PowerDuke facilitate getting information about the system.
Information	<https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0139/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.powerduke>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:powerduke>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool PowerDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7859036b-5f71-44e0-ad91-b85726302fd4