Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:12:10 UTC

Tool: Downdelph

Names	Downdelph Delphacy
Category	Malware
Type	Loader
Description	(ESET) Downdelph is a first-stage component deployed only in very rare cases by the Sednit operators. Over the past two years this low-profile approach has been combined with advanced persistence methods — a bootkit and a rootkit — probably in order to spy on special targets for long periods of time. Downdelph was used to deploy X-Agent and Sedreco on infected machines.
Information	<https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0134/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.downdelph>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DOWNDELPH>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Downdelph

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d262019e-e4a6-467a-9cb7-1c52e4bb426c