Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:45:43 UTC

Tool: Dorshel

Names	Dorshel
Category	Malware
Type	Backdoor
Description	(Symantec) In 2014, Symantec observed the Dragonfly group compromise legitimate software in order to deliver malware to victims, a practice also employed in the earlier 2011 campaigns. In the 2016 and 2017 campaigns the group is using the evasion framework Shellter in order to develop Trojanized applications. In particular, Backdoor.Dorshel was delivered as a trojanized version of standard Windows applications.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dorshel>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Dorshel

Changed	Name	Country	Observed	
APT groups				
	Energetic Bear, Dragonfly		2010-Mar 2022	

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