Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:05:52 UTC

Tool: Industroyer2

Names	Industroyer2
Category	Malware
Type	ICS malware, Backdoor
Description	(ESET) ESET researchers responded to a cyber-incident affecting an energy provider in Ukraine. We worked closely with CERT-UA in order to remediate and protect this critical infrastructure network. The collaboration resulted in the discovery of a new variant of Industroyer malware, which we together with CERT-UA named Industroyer2 – see CERT-UA publication here. Industroyer is an infamous piece of malware that was used in 2016 by the Sandworm APT group to cut power in Ukraine.
Information	<https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/> <https://cert.gov.ua/article/39518> <https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1072>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer2>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool Industroyer2

Changed	Name	Country	Observed
APT groups			

	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=008fade3-cb57-4c9e-b74a-bdcadffca9f1