Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:20:49 UTC

Tool: Gcat

Names	Gcat
Category	Tools
Type	Backdoor
Description	A PoC backdoor that uses Gmail as a C&C server (ESET) [During the Sandworm analysis] We expected to see the BlackEnergy malware as the final payload, but a different malware was used this time. The attackers used modified versions of an open-source gcat backdoor written in the Python programming language. The python script was converted into a stand-alone executable using PyInstaller program.
Information	<https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/> <https://github.com/byt3bl33d3r/gcat>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Gcat

Changed	Name	Country	Observed	
APT groups				
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	

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