Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:00:14 UTC

Tool: Gemcutter

Names	Gemcutter
Category	Malware
Type	Downloader
Description	(FireEye) GEMCUTTER is used in a similar capacity as BackBend, but maintains persistence by creating a Windows registry run key.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/05/20081935/rpt-apt30.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gemcutter>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:GEMCUTTER>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Gemcutter

Changed	Name	Country	Observed	
APT groups				
	APT 30, Override Panda		2005	
	Naikon, Lotus Panda		2010-Apr 2022	

2 groups listed (2 APT, 0 other, 0 unknown)