Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:30:26 UTC

Tool: StoneDrill

Names	StoneDrill DROPSHOT
Category	Malware
Type	Wiper
Description	StoneDrill is wiper malware discovered in destructive campaigns against both Middle Eastern and European targets in association with APT33.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf> <https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html> <https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-1/> <https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-2/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0380/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.stonedrill> <https://malpedia.caad.fkie.fraunhofer.de/details/win.dropshot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:stonedrill>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool StoneDrill

Changed	Name	Country	Observed	
APT groups				
	APT 33, Elfin, Magnallium		2013-Apr 2024	

	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3fbd9978-1421-4d34-9a4e-507fd1880629