Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:22:45 UTC

Tool: DDG

Names	DDG
Category	Malware
Type	Miner
Description	(Qihoo 360) DDG uses a C2 and HUB layout to communicate with its clients. The HUB is a set of IPs and domain names that are used to provide Miner program for the compromised clients to download.
Information	<https://blog.netlab.360.com/ddg-a-mining-botnet-aiming-at-database-server-en/> <https://blog.netlab.360.com/ddg-mining-botnet-jin-qi-huo-dong-fen-xi/> <https://blog.netlab.360.com/threat-alert-ddg-3013-is-out/> <https://blog.netlab.360.com/ddg-botnet-round-x-is-there-an-ending/> <https://blog.netlab.360.com/old-botnets-never-die-and-ddg-refuse-to-fade-away/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.ddg>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DDG>

Last change to this tool card: 28 December 2021

Download this tool card in JSON format

All groups using tool DDG

Changed	Name	Country	Observed	
Other groups				
	Pacha Group		2018-May 2019	

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

↑
