Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:26:19 UTC

Tool: ISMDoor

Names	ISMDoor
Category	Tools
Type	Backdoor, Tunneling
Description	(Arbor) Ismdoor has an encrypted configuration that contains a primary and secondary C2 domain, various identifiers, timeouts, and flags. These values can be updated by later C2 commands. A substitution cipher is used to decrypt the configuration when it is needed. The character mapping has been consistent across samples and we have made available a Python snippet of it on Github.
Information	<https://www.netscout.com/blog/asert/greenbugs-dns-isms>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ismdoor>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ismdoor>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool ISMDoor

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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