Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:24:45 UTC

Tool: ISMAgent

Names	ISMAgent
Category	Malware
Type	Backdoor
Description	(Palo Alto) On May 1, 2017, Arbor Networks published research on ISMDoor using DNS tunneling to communicate with its C2 server, which is nearly identical to the DNS tunneling the payload of this attack carries out. Due to considerable differences and evidence of potentially different authors between the previous ISMDoor samples and this newly discovered variant, we are tracking this new variant as ISMAgent. The ISMAgent tool comes with a default configuration that specifies the C2 domain and the number of minutes between further attempts to execute the tool. However, an actor can use command line arguments to create a new ISMAgent sample that is configured with a specified C2 domain and a specified number of minutes to automatically execute the Trojan.
Information	<https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/> <https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/> <http://www.clearskysec.com/ismagent/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ismagent>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ISMAgent>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool ISMAgent

Changed	Name	Country	Observed

APT groups

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=da73c338-cd73-48fb-be70-3498915cfad5