Threat Group Cards: A Threat Actor Encyclopedia

Tool: DNSMessenger

Names	DNSMessenger TEXTMATE
Category	Malware
Type	Tunneling
Description	DNSMessenger makes use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker.
Information	<https://blog.talosintelligence.com/2017/03/dnsmessenger.html> <https://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html> <http://wraithhacker.com/2017/10/11/more-info-on-evolved-dnsmessenger/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0146/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dnsmessenger>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DNSmessenger>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool DNSMessenger

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	FIN7		2013-Jul 2024	

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