Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:50:31 UTC

Tool: DanBot

Names	DanBot
Category	Malware
Type	Backdoor
Description	(SecureWorks) A first-stage remote access trojan (RAT) that uses DNS and HTTP-based communication mechanisms and provides basic remote access capability, including the abilities to execute arbitrary commands via cmd.exe and to upload and download files. DanBot is written in C# using .NET Framework 2.0 and provides basic remote access capabilities. The DNS channel of DanBot's C2 protocol uses both IPv4 A records and IPv6 AAAA records for communication. The HTTP channel has evolved slightly since the early 2018 samples but retains common elements throughout.
Information	<https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign>
MITRE ATT&CK	<https://attack.mitre.org/software/S1014/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.danbot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DanBot>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool DanBot

Changed	Name	Country	Observed	
APT groups				
	Hexane		2017-Jun 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b730233d-5e3f-4046-af2d-9773b8258a50