Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:08:23 UTC

Tool: Leash

Names	Leash
Category	Malware
Type	Backdoor
Description	(Palo Alto) The Magic Hound campaign was also discovered deploying an IRC Bot, which we have named MagicHound.Leash. We discovered this connection when we observed a DropIt sample installing a backdoor Trojan that used IRC for its C2 communications. Leash obtains its commands via private messages (PRIVMSG) sent from the adversary who must also be connected to the IRC server. All of its available commands (see Appendix), except for the VER command seen in Figure 5, must be issued by individuals in the IRC channel with nicknames that start with “AS_” or “AF_”.
Information	<https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.leash>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Leash

Changed	Name	Country	Observed	
APT groups				
	Cutting Kitten, TG-2889		2012-Mar 2016	
	Magic Hound, APT 35, Cobalt Illusion, Charming Kitten		2012-Jun 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=cffb6ef7-2c27-43b6-87b8-a95d1b51fe75