Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:34:23 UTC

Tool: KasperAgent

Names	KasperAgent
Category	Malware
Type	Backdoor
Description	(Palo Alto) ASPERAGENT is developed in Microsoft Visual C++ and attempts to disguise itself as a product that does not exist: “Adobe Cinema Video Player”. The malware first establishes persistence using the classic method of adding a Run key, using the value “MediaSystem”. The malware connects to a C2 serverhosted on www.mailsinfo[.]net. The C2 server string in the binary is “obfuscated” in the most basic of senses, with the author adding ‘@’ characters between letters and splitting the starting “www.m” to another string.
Information	<https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/> <https://www.threatconnect.com/blog/kasperagent-malware-campaign/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kasperagent>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:KASPERAGENT>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool KasperAgent

Changed	Name	Country	Observed	
APT groups				
	Desert Falcons	[Gaza]	2011-Oct 2023	

	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0dd10463-768e-4b4e-b473-845cfe285f13