Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:38:29 UTC

Tool: Micropsia

Names	Micropsia
Category	Malware
Type	Info stealer, Keylogger, Exfiltration
Description	(Palo Alto) The MICROPSIA malware family is written in Delphi and is an information stealing malware family with a wide range of data theft functionality built in. The main capabilities of the malware are as follows: • Logging of keystrokes to a hardcoded text file and exfiltration to a remote server • Capturing screenshots of the infected machines • Searching for files with extensions matching Microsoft Office documents and using WinRAR to archive these prior to exfiltration.
Information	<https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/> <http://blog.talosintelligence.com/2017/06/palestine-delphi.html> <https://research.checkpoint.com/apt-attack-middle-east-big-bang/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0339/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.micropsia>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Micropsia>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Micropsia

Changed	Name	Country	Observed
APT groups			

	The Big Bang	[Unknown]	2017	
	Desert Falcons	[Gaza]	2011-Oct 2023	
	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	

3 groups listed (3 APT, 0 other, 0 unknown)
