Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:23:35 UTC

Tool: PyMICROPSIA

Names	PyMICROPSIA
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Keylogger, Credential stealer, Downloader
Description	(Palo Alto) PyMICROPSIA has a rich set of information-stealing and control capabilities, including: • File uploading. • Payload downloading and execution. • Browser credential stealing. Clearing browsing history and profiles. • Taking screenshots. • Keylogging. • Compressing RAR files for stolen information. • Collecting process information and killing processes. • Collecting file listing information. • Deleting files. • Rebooting machine. • Collecting Outlook .ost file. Killing and disabling Outlook process. • Deleting, creating, compressing and exfiltrating files and folders. • Collecting information from USB drives, including file exfiltration. • Audio recording. • Executing commands.
Information	<https://unit42.paloaltonetworks.com/pymicropsia/>

Last change to this tool card: 06 January 2021

Download this tool card in JSON format

All groups using tool PyMICROPSIA

Changed	Name	Country	Observed

APT groups

	Desert Falcons	[Gaza]	2011-Oct 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=baa168d6-593b-486f-b52e-cc12182de231