

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:54:58 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool sip_telephone

Tool: sip_telephone

Names	sip_telephone
Category	Malware
Type	Reconnaissance
Description	(Trend Micro) sip_telephone, also named in the PDB path as such, uses Windows Management Instrumentation (WMI) to get the AV installed in the machine, its computer name, and processor ID, among others. It performs tasks in an endless loop, with 100 seconds of sleep time.
Information	< https://documents.trendmicro.com/assets/research-deciphering-confucius-cyberespionage-operations.pdf >

Last change to this tool card: 20 April 2020

Download this tool card in [JSON](#) format

All groups using tool sip_telephone

Changed	Name	Country	Observed
APT groups			
	Confucius		2013-Aug 2021

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2024b85f-ceda-41afb11a-85d77d136e85>