

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:06:15 UTC

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


Tool: InvisiMole

Names	InvisiMole
Category	Malware
Type	Reconnaissance , Backdoor , Info stealer , Exfiltration
Description	(ESET) InvisiMole has a modular architecture, starting its journey with a wrapper DLL, and performing its activities using two other modules that are embedded in its resources. Both of the modules are feature-rich backdoors, which together give it the ability to gather as much information about the target as possible.
Information	< https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/ > < https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S0260/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.invisimole >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:invisimole >

Last change to this tool card: 23 June 2020

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

All groups using tool InvisiMole

Changed	Name	Country	Observed
APT groups			
	InvisiMole		2013-Mar 2022

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=ecc49b8a-8d7e-428f8813-4b4c7298b559>