Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:20:10 UTC

APT group: InvisiMole

Names	InvisiMole *(ESET)* UAC-0035 *(CERT-UA)*	
Country	Russia	
Motivation	Information theft and espionage	
First seen	2013	
Description	(ESET) This is the modus operandi of the two malicious components of InvisiMole. They turn the affected computer into a video camera, letting the attackers see and hear what's going on in the victim's office or wherever their device may be. Uninvited, InvisiMole's operators access the system, closely monitoring the victim's activities and stealing the victim's secrets. Our telemetry indicates that the malicious actors behind this malware have been active at least since 2013, yet the cyber-espionage tool was never analyzed nor detected until discovered by ESET products on compromised computers in Ukraine and Russia. The campaign is highly targeted – no wonder the malware has a low infection ratio, with only a few dozen computers being affected. ESET also found that InvisiMole targeted computers already compromised by Gamaredon Group.	
Observed	Sectors: Defense, Government. Countries: Russia, Ukraine and Eastern Europe.	
Tools used	InvisiMole.	
Operations performed	Late 2019	ESET researchers reveal the modus operandi of the elusive InvisiMole group, including newly discovered ties with the Gamaredon group <https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/>

	Mar 2022	Ukraine warns of InvisiMole attacks tied to state-sponsored Russian hackers <https://www.zdnet.com/article/ukraine-warns-of-invisimole-attacks-tied-to-state-sponsored-russian-hackers/>
Information	<https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/>	

Last change to this card: 08 April 2022

Download this actor card in PDF or JSON format
