Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:37:34 UTC

APT group: Harvester

Names	Harvester *(Symantec)*
Country	[Unknown]
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2021
Description	(Symantec) A previously unseen actor, likely nation-state-backed, is targeting organizations in South Asia, with a focus on Afghanistan, in what appears to be an information-stealing campaign using a new toolset. The Harvester group uses both custom malware and publicly available tools in its attacks, which began in June 2021, with the most recent activity seen in October 2021. Sectors targeted include telecommunications, government, and information technology (IT). The capabilities of the tools, their custom development, and the victims targeted, all suggest that Harvester is a nation-state-backed actor.
Observed	Sectors: Government, IT, Telecommunications. Countries: Afghanistan and South Asia.
Tools used	Cobalt Strike, Graphon, Metasploit.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia>

Last change to this card: 03 November 2021

Download this actor card in PDF or JSON format
