Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:27:09 UTC

Tool: ShellClient

Names	ShellClient
Category	Malware
Type	Exfiltration
Description	(Cybereason) The investigation into Operation GhostShell also revealed that ShellClient dates back to at least 2018, and has been continuously evolving ever since while successfully evading most security tools and remaining completely unknown. By studying the ShellClient development cycles, the researchers were able to observe how ShellClient has morphed over time from a rather simple reverse shell to a sophisticated RAT used to facilitate cyber espionage operations while remaining undetected. The most recent ShellClient versions observed in Operation GhostShell follow the trend of abusing cloud-based storage services, in this case the popular Dropbox service. The ShellClient authors chose to abandon their previous C2 domain and replace the command and control mechanism of the malware with a more simple yet more stealthy C2 channel using Dropbox to exfiltrate the stolen data as well as to send commands to the malware. This trend has been increasingly adopted by many threat actors due to its simplicity and the ability to effectively blend in with legitimate network traffic.
Information	<https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms>

Last change to this tool card: 02 November 2021

Download this tool card in JSON format

All groups using tool ShellClient

Changed	Name	Country	Observed
APT groups			

	MalKamak		2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ee4d9bc0-74e7-4547-b189-5c25c86ee2ed