Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:40:57 UTC

APT group: MalKamak

Names	MalKamak *(Cybereason)* Operation GhostShell *(Cybereason)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2018
Description	(Cybereason) In July 2021, the Cybereason Nocturnus and Incident Response Teams responded to Operation GhostShell, a highly-targeted cyber espionage campaign targeting the Aerospace and Telecommunications industries mainly in the Middle East, with additional victims in the U.S., Russia and Europe. The Operation GhostShell campaign aims to steal sensitive information about critical assets, organizations' infrastructure and technology. During the investigation, the Nocturnus Team uncovered a previously undocumented and stealthy RAT (Remote Access Trojan) dubbed ShellClient which was employed as the primary espionage tool. The Nocturnus Team found evidence that the ShellClient RAT has been under ongoing development since at least 2018, with several iterations that introduced new functionalities, while it evaded antivirus tools and managed to remain undetected and publicly unknown. Assessments as to the identity of the operators and authors of ShellClient resulted in the identification of a new Iranian threat actor dubbed MalKamak that has operated since at least 2018 and remained publicly unknown thus far. In addition, our research points out possible connections to other Iranian state-sponsored APT threat actors such as Chafer, APT 39 and Agrius APT. However, we assess that MalKamak has distinct features that separate it from the other Iranian groups.
Observed	Sectors: Aerospace, Telecommunications. Countries: Russia, USA and Europe and Middle East.
Tools used	PAExec, SafetyKatz, ShellClient, WinRAR.
Information	<https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms>

Last change to this card: 02 November 2021

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=1ef36ba9-41f8-42a4-94e6-56678a7b8268