Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:41:56 UTC

APT group: Sima

Names	Sima *(Amnesty International)*
Country	Iran
Motivation	Information theft and espionage
First seen	2016
Description	In February 2016, Iranfocused individuals received messages purporting to be from Human RightsWatch's (HRW) Emergencies Director, requesting that they read an article about Iran pressing Afghan refugees to fight in Syria. While referencing a real report published by HRW, the links provided for the Director's biography and article directed the recipient to malware hosted elsewhere. These spear-phishing attempts represent an evolution of Iranian actors based on their social engineering tactics and narrow targeting. Although the messages still had minor grammatical and stylistic errors that would be obvious to a native speaker, the actors demonstrated stronger Englishlanguage proficiency than past intrusion sets and a deeper investment in background research prior to the attempt. The actors appropriated a real identity that would be expected to professionally interact with the subject, then offered validation through links to their biography and social media, the former of which itself was malware as well. The bait documents contained a real article relevant to their interests and topic referenced, and the message attempted to address to how it aligned with their professional research or field of employment. The referenced documents sent were malware binaries posing as legitimate files using the common righttoleft filenames tactic in order to conceal the actual file extension. All of these techniques, while common pretexting mechanisms, are a refinement compared to a tendency amongst other groups to simply continually send different forms of generic malware or phishing, in the hopes that one would eventually be successful.
Observed	Countries: This group targets Iranians in diaspora.
Tools used	Luminosity RAT, Sima.
Information	<https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format