Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:45:41 UTC

APT group: Madi

Names	Madi *(Kaspersky)* Mahdi *(Kaspersky)*	
Country	Iran	
Motivation	Information theft and espionage	
First seen	2011	
Description	(Kaspersky) Kaspersky Lab and Seculert worked together to sinkhole the Madi Command & Control (C&C) servers to monitor the campaign. Kaspersky Lab and Seculert identified more than 800 victims located in Iran, Israel and select countries across the globe connecting to the C&Cs over the past eight months. Statistics from the sinkhole revealed that the victims were primarily business people working on Iranian and Israeli critical infrastructure projects, Israeli financial institutions, Middle Eastern engineering students, and various government agencies communicating in the Middle East. Common applications and websites that were spied on include accounts on Gmail, Hotmail, Yahoo! Mail, ICQ, Skype, Google+, and Facebook. Surveillance is also performed over integrated ERP/CRM systems, business contracts, and financial management systems.	
Observed	Sectors: Education, Engineering, Financial, Government, Oil and gas, Think Tanks. Countries: Australia, Ecuador, Greece, Iran, Iraq, Israel, Mozambique, New Zealand, Pakistan, Saudi Arabia, Switzerland, USA, Vietnam.	
Tools used	Madi.	
Operations performed	Jul 2012	New and Improved Madi Spyware Campaign Continues Madi, the religiously-titled spyware that was discovered last week and thought to be dead, appears to be making a comeback, complete with updates. <https://threatpost.com/new-and-improved-madi-spyware-campaign-continues-072512/76849/>
Counter operations		The C&C servers have been sinkholed by Kaspersky and Seculert.

Information	<https://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns> <https://securelist.com/the-madi-campaign-part-i-5/33693/> <https://securelist.com/the-madi-campaign-part-ii-53/33701/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=2afc9634-8895-4535-bb80-8843d4830e04