Kaspersky Lab and Seculert Announce ‘Madi,’ a Newly Discovered Cyber-Espionage Campaign in the Middle East

kaspersky.com/about/press-releases/2012_kaspersky-lab-and-seculert-announce--madi--a-newly-discovered-cyber-espionage-campaign-in-the-middle-east

May 26, 2021

Today, Kaspersky Lab researchers announced the results of a joint-investigation with Seculert, an Advanced Threat Detection company, regarding “Madi,” an active cyber-espionage campaign targeting victims in the Middle East. Originally discovered by Seculert, Madi is a computer network infiltration campaign that involves a malicious Trojan which is delivered via social engineering schemes to carefully selected targets.

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.

In addition, examination of the malware identified an unusual amount of religious and political ‘distraction’ documents and images that were dropped when the initial infection occurred.

“While the malware and infrastructure is very basic compared to other similar projects, the Madi attackers have been able to conduct a sustained surveillance operation against high-profile victims,” said Nicolas Brulez, Senior Malware Researcher, Kaspersky Lab. “Perhaps the amateurish and rudimentary approach helped the operation fly under the radar and evade detection.”

“Interestingly, our joint analysis uncovered a lot of Persian strings littered throughout the malware and the C&C tools, which is unusual to see in malicious code. The attackers were no doubt fluent in this language,” said Aviv Raff, Chief Technology Officer, Seculert.

The Madi info-stealing Trojan enables remote attackers to steal sensitive files from infected Windows computers, monitor sensitive communications such as email and instant messages, record audio, log keystrokes, and take screenshots of victims’ activities. Data analysis suggests that multiple gigabytes of data have been uploaded from victims’ computers.

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.

Kaspersky Lab’s Anti-Virus system detects the Madi malware variants along with its associated droppers and modules, classified as Trojan.Win32.Madi.

To read the full research post by Kaspersky Lab’s experts please visit Securelist.

To read Seculert’s research about the Madi campaign please visit the Seculert Blog.

Kaspersky
Today, Kaspersky Lab researchers announced the results of a joint-investigation with Seculert, an Advanced Threat Detection company, regarding “Madi,” an active cyber-espionage campaign targeting victims in the Middle East

kaspersky

Related Articles Virus News

- **Russian-speaking APTs Turla and Sofacy share malware delivery scheme, and overlap some targets in Asia**

  Kaspersky Lab researchers monitoring the various clusters of the long standing, Russian-speaking threat actor, Turla (also known as Snake or Uroburos) have discovered that the most recent evolution of its KopiLuwak malware is delivered to victims using code nearly identical to that used just a month earlier by the Zebrocy operation

  Read More >

- **New variant of SynAck ransomware uses sophisticated Doppelgänging technique to evade security**

  Kaspersky Lab researchers have discovered a new variant of the SynAck ransomware Trojan using the Doppelgänging technique to bypass anti-virus security by hiding in legitimate processes.

  Read More >