The Madi Attacks: Series of Social Engineering Campaigns

Jul 17, 2012 06:40 PM

A L Johnson

Symantec Security Response is aware of recent reports of Madi, a Trojan used in targeted campaigns and observed in the wild since December 2011.

The following is an email example, discovered in the Madi campaign, which included a malicious PowerPoint attachment:

Figure 1. *Targeted email containing malicious PowerPoint*

In one example, opening the PowerPoint attachment displays a series of video stills showing a missile destroying a jet plane. During the final PowerPoint slide, a dialog window is displayed to the user requesting permission to run an executable file:

Figure 2. *Final PowerPoint slide prompts user to run a .scr file*

Symantec detects this malicious executable as Trojan.Madi using the latest LiveUpdate definitions. It is capable of stealing information—including keylogging functionality. The Trojan can also update itself. We have observed Trojan.Madi communicating with command-and-control servers hosted in Iran and, more recently, Azerbaijan.

Targets of the Madi campaign appear to be all over the spectrum but include oil companies, US-based think tanks, a foreign consulate, as well as various governmental agencies, including some in the energy sector.

Figure 3. *Heat map distribution of global Madi infections*

Although Madi has been seen targeting various Middle Eastern countries, it has also been found across the globe from the United States to New Zealand.

Figure 4. *Infection percentages of Madi from December 2011 to July 2012*

Where high profile attacks such as Flamer, Duqu, and Stuxnet utilize different techniques to exploit systems—including leveraging zero-day attacks—the Madi attack relies on social engineering techniques to get onto targeted computers.

Targets like Iran, Israel, and Saudi Arabia might suggest involvement of a nation state, however our research has not found evidence that this is the case. Instead, the current research indicates these attacks are being conducted by an unknown Farsi-speaking hacker with a broad agenda.

Update [July 18, 2012] - Distribution map (Figure 3) and pie chart (Figure 4) updated to reflect telemetry data.

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.