New and Improved Madi Spyware Campaign Continues

By Chris Brook

Published: 2012-07-25 · Archived: 2026-04-02 10:38:13 UTC

Madi, the religiously-titled spyware that was discovered last week and thought to be dead, appears to be making a comeback, complete with updates.

Madi, the religiously-titled spyware that was discovered last week and thought to be dead, appears to be making a comeback, complete with updates.

Kaspersky Lab researcher Nicolas Brulez reverse-engineered the new iteration of the malware, which surfaced on Wednesday. Unlike last week's original variant of Madi however, this version doesn't wait for instructions from the Command and Control (C&C) server and instead uploads all of the data it hijacks from users directly to the server, Brulez wrote in a blog post on Kaspersky Lab's Securelist.

This appears to be the largest difference between the new version and the version discovered last week as most of Madi's code has been copied from one variant to another.

New research has deduced the spyware, first unearthed by Kaspersky and Israeli security firm Seculert, "stays silent for two days before it starts its activities," according to Brulez.

The latest version of Madi also has the ability to monitor the Russian social network Vkontakte (VK) along with the Jabber messaging platform to look for users who visit websites that contain words like "USA," "Skype," and "gov." With each occurrence, Madi will capture screenshots of the incident and send them to the C&C server.

While Madi's C&C server was initially linked to Iran, recent variants of the spyware, including this one, can be traced to a C&C server in Montreal.

Madi was found capturing computer screens, recording audio and stealing screenshots, keystrokes, documents and e-mail correspondence from "Middle Eastern critical infrastructure engineering firms, government agencies, financial houses and academia." The spyware, which sometimes is referred to as Mahdi, takes its name from "Mahdi.txt," a malicious word document spread by the malware. The name also refers to a Shiite central religious idea that a foretold redeemer, the Mahdi, will appear before the Day of Judgment.
