

14 March 2008



"This page is temporarily shut down for emergency maintenance" Trend Micro via Sophos

By: Marius Oiaga, Technology News Editor

[Anti-Virus Maker Trend Micro Infects Users with Malware via Hacked Website](#)

Both Japanese and English users put at risk

Japanese anti-virus developer Trend Micro managed to diverge from its default strategy of offering protection from malicious code, switching a full 180 degrees by serving malware to users, although through no real fault of its own. On March 12, 2008, Trend Micro announced that a portion of its official website had been hacked three days earlier, on March 9, and that it was set up to deliver malware to visitors. Trend Micro warned the users that landed on the malformed webpages of a strong possibility that their systems might have been compromised by a Trojan Horse labeled JS_DLOADER.TZE. The malicious pages were up for no less than three days before Trend Micro identified the problem and shut them down. The Shibuya Ward Tokyo-based outfit considered it necessary to inform only the [Japanese customers of the issue](#). However, security company Sophos revealed that both the English and Japanese sections of the official Trend Micro website had been hacked. "A number of webpages on the firm's Japanese and English-language website were altered by hackers on Sunday 9 March, who used a malicious iFrame exploit to deliver a Trojan horse onto surfers' computers. Trend Micro is believed to have uncovered the problem on Wednesday 12 March and replaced affected pages with a message saying 'This page is temporarily shut down for emergency maintenance' as the following image from the [www.trendmicro.co.jp](#)," explained [Graham Cluley](#), senior technology consultant at Sophos. Cluley opined that a software vulnerability was the most probable cause of the hack. Trend Micro failed to confirm whether an exploit of a security flaw was the open door for the hack, or to pin point another cause. According to Sophos, the visitors on the malformed pages of Trend Micro's website have been exposed to the malware not only by accessing the infected content, but also by clicking URL links embedded in the malware's name. "In a nutshell - what has happened here is a criminal act, and our friends at Trend Micro (and people visiting the hacked pages) are victims of the crime. Sadly it's not an uncommon crime these days - and all kinds of businesses have suffered. This isn't the time or place to make cheap shots against a competitor. All other companies with a web presence should take this unfortunate incident as an opportunity to check that their own websites are properly secured," Cluley advised.