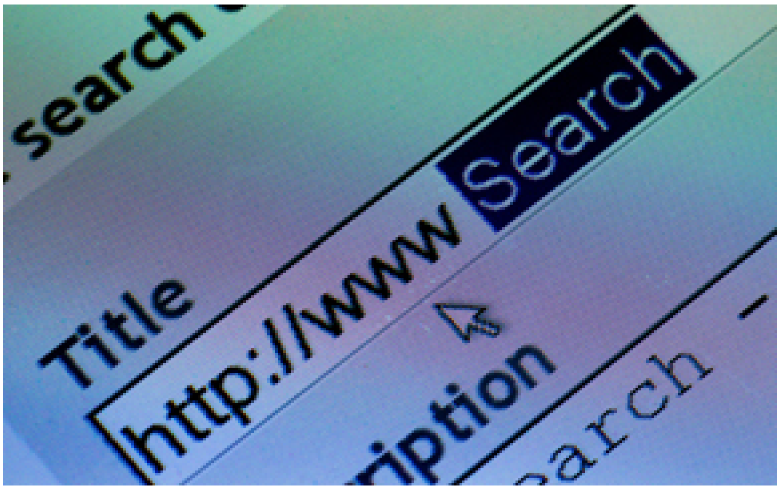
One Size Fits All

Written by DFM News
Thursday, 04 October 2012 11:14 -



Trusteer have discovered a new Man in the Browser (MitB) scam that does not target specific websites, but instead collects data submitted to all websites without the need for post-processing. This development, which we are calling Universal Man-in-the-Browser (uMitB), is significant.

First, let’s review how uMitB is different from traditional MitB configurations. Traditional MitB attacks typically collect data (login credentials, credit card numbers, etc.) entered by the victim in a specific web site. Additionally, MitB malware may collect all data entered by the victim into websites, but it requires post-processing by the fraudster to parse the logs and extract the valuable data. Parsers are easily available for purchase in underground markets, while some criminals simply sell off the logs in bulk.

According to Trusteer’s CTO Amit Klein. “In comparison, uMitB does not target a specific web site. Instead, it collects data entered in the browser at all websites and uses “generic” real time logic on the form submissions to perform the equivalent of post-processing. This attack can target victims of new infections as well as machines that were previously infected by updating the existing malware with a new configuration. The data stolen by uMitB malware is stored in a portal where it is organized and sold.

uMitB’s ability to steal sensitive data without targeting a specific website and perform real-time post-processing removes much of the friction associated with traditional MitB attacks. For example, it could be used to automate card fraud by integrating with and feeding freshly stolen information to card selling web sites. The impact of uMitB could be significant since information stolen in real-time is typically much more valuable than “stale” information, plus it eliminates the complexities associated with current post-processing approaches.

As always, the best protection against financial fraud attacks that use uMitB, MitB, Man-in-the-Middle, etc. is to secure the endpoint against the root cause of these problems – malware.