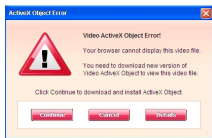


15 May 2008

By: Traian Teglet, Technology News Editor



An error window asking you to download a piece of malware
Trend Micro Blog

[Trend Micro Warns of Attack of Over Half a Million Web Pages](#)

Another SQL injection has been found in half a million web pages worldwide

Not long after we [informed](#) you of the SQL injection threat that has been found last week loose on the web, a new similar massive attack compromises more than half a million websites. As reported on the TrendLabs Malware blog, the threat comes in the form of a standard SQL injection, which some of you might already have heard plenty of. The malicious script, dubbed JS_SMALL.QT, has been found by Ivan Macalintal, Advanced Threats Research Program Manager, in various websites. These sites are believed to use poor implementations of phpBB or are using older versions, which have known exploits. These infections are said to have been noticed since early February this year. Website owners are encouraged to verify their phpBB implementations or to upgrade the specified application to a more "bug-free" version. It appears that the working method for this Trojan horse is similar to what the experts at TrendLabs have previously seen evolving on the web. Compromised websites redirect the users to a series of other sites, which ultimately ends with them downloading the malware. At the end of the trace is the TROJ_ZLOB.CCW Trojan horse, which poses as a video codec installer. The false codec advertises itself as the only means of viewing a free adult movie. The malware is reported to be hosted on servers from Columbus (OH), Concord (CA) and Moscow. This is virtually making this attack the potential work of a Russian/Ukrainian criminal gang known for initiating previous ZBLOB attacks. After downloading the codecs, users are left with a number of detected Trojan horses that are known for changing the victims' local DNS and Internet browser settings, thus making the system vulnerable to even more potential threats. Users of Trend Micro Web Threat Protection application are said to be protected by the malicious URLs.