

RBN - The Bank of India

Bank of India IT staff are mopping up the mess left by attackers who rigged the firm's website to feed malware to customers trying to access online services.

The bank managed to pry loose the rogue iframe responsible for the malware sometime early Friday morning California time. At time of writing, though, Bank of India's website was effectively cordoned off, bearing a terse notification saying: "This site is under temporary maintenance and will be available after 09:00 IST on 1.09.07."

The shuttering came a day after employees for security provider Sunbelt Software discovered someone had planted an iframe in the site that caused unpatched Windows machines to be infected with some of the most destructive pieces of malware currently in circulation. Sunbelt counted 31 separate pieces in all, including Pinch, a powerful and easy-to-use Trojan that siphons personal information from a user's PC. Other malware included Trojan.Netview, Trojan-Spy.Win32.Agent.ql, various rootkits and several spam bots.

Executives and IT administrators at US offices of Bank of India who were contacted Friday morning by IDG were initially unaware of the attack. A spokesman later told the news service that officials were aware of the problem and were working to correct it, but had no information concerning its severity or duration.

Some of the servers used to install the malware belonged to the notorious Russian Business Network, a group Spamhaus says is involved in child porn, phishing and other misdeeds. According to Verisign's iDefense unit, the RBN also played a hand in bringing us MPack, a powerful Trojan downloader that infected more than 10,000 websites in just three days.

In this case, the attackers appeared to use an exploit kit dubbed n404, according to this post by Dancho Danchev. It relies on a technique known as Fast Flux domain name service, which is proving to be resilient against bot hunters because there is no single point of weakness to take down.

Roger Thompson, a researcher with Exploit Prevention Labs, said he spotted one piece of code that exploited a vulnerability patched by last year's Microsoft Security Bulletin MS06-042. "It's pretty much a cut-and-paste of the original proof-of-concept that was put out on Metasploit last July," Thompson said of the code.