

27 June 2009

By: Lucian Constantin, Web News Editor



FTP accounts belonging to high-profile websites have been stolen openDesktop

FTP Credentials for Major Websites Compromised

Found on a Chinese server used by cyber-criminals

Security researchers from antivirus vendor Prevx have uncovered a major security breach that affects more than 68,000 websites, including some high-profile ones. FTP credentials belonging to the likes of Amazon, Cisco, BBC, Symantec, McAfee, Monster, or even Bank of America have been found on a Zbot dumping site hosted in China.

Jacques Erasmus, director of research at Prevx, made the discovery while investigating a new strain of Zbot. "The data is harvested from users' machines, when they get infected. A typical scenario might be that a web designer for one of the organisations gets infected, his stored ftp login details gets compromised, and so the attacker in this case is able to log in to the ftp site and compromise the website pages," the researcher explained, according to [The Register](#).

Investigations have revealed that the capture is "fresh," the credentials being stolen during the last two weeks. Compromised FTP accounts are very valuable to attackers, and this has been particularly well reflected in recent mass injection attacks such as [Gumblar](#), [Beladen](#) and [Nine-Ball](#), which affected hundred of thousands of websites and relied on stolen FTP logins.

By having FTP access to a website, malicious hackers can insert malicious code into its pages. Such rogue code can then be used to load exploits that target vulnerabilities in various applications installed on visitors' computers and infect them with malware.

Mr. Erasmus also pointed out that the data was stored in plain text, making it very easy for other hackers to find it and abuse it too. It's no secret that many cyber-criminals have no problem with stealing from their competition.

Prevx has started alerting the affected organizations about the security breaches, probably based on the severity of the impact they could have on users. Financial companies or those running large websites are likely to have priority, but, given the massive number of compromised accounts, it might take a while until everyone is notified. The security vendor has also submitted an abuse complaint with the company hosting the dump site.