Massive Phishing Attack Strikes Major Websites. Apple, Nasdaq, Amazon and Others at Risk of Password Thefts

WASHINGTON, DC, UNITED STATES, May 13, 2015 /EINPresswire.com/ -- Massive phishing attack strikes major websites. The attack uses the technique of proxy program relaying the requests to original servers, allowing to show users seemingly perfect copy of large number of affected sites.

Changes on sites are invisible to a common user but any information entered into forms, including usernames and passwords entered by users who didn't notice the replace, are sent to attacking server instead of the original one.

Modification of pages include adding the stat counter from http://statcounter.com/shopify/ (project 10183367) and changes necessary to keep visitors on the xzlyv.mobi site.

The attack also replaces robots.txt file with a different one allowing to scan a whole site. This results in making search engines index pages that are originally hidden to them.

Notes to Webmasters:

IP addresses:
94.242.57.216 (Russia)
104.194.16.230 (Las Vegas)

A partial list of affected sites:
http://apple.xzlyv.mobi/
http://nasdaq.xzlyv.mobi/
http://delta.xzlyv.mobi/
http://ba.xzlyv.mobi/
http://cnn.xzlyv.mobi/
http://rferl.xzlyv.mobi/
http://nbcnews.xzlyv.mobi/
http://huffingtonpost.xzlyv.mobi/
http://aol.xzlyv.mobi/
http://amazon.xzlyv.mobi/
http://comcast.xzlyv.mobi/
http://microsoft.xzlyv.mobi/
http://linkedin.xzlyv.mobi/
http://rackspace.xzlyv.mobi/

Media Contact:

David Rothstein
Internet Product Development Group
202-657-5158
email us here
