



Advisory for cPanel-based site owners – cPanel/FTP phishing campaign

2009© All Rights Reserved.

Trusteer makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of Trusteer. No patent liability is assumed with respect to the use of the information contained herein. While every precaution has been taken in the preparation of this publication, Trusteer assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

cPanel/FTP Phishing

cPanel is a very popular CMS (Content Management System), used by many leading hosting providers, including Yahoo. cPanel manages all sorts of site operations, including FTP account control and setup (though cPanel does not engage in the actual FTP sessions). FTP can be used to upload content to the cPanel-managed web site.

Over the last few days, Trusteer has seen phishing email campaign targeting owners of cPanel-based sites in various hosting providers, trying to phish the FTP credentials of those site owners using cPanel-oriented messaging.

A typical phishing email looks like this (in this case, a Yahoo webhosting user is targeted):

From: support@yahoo.com
To: [REMOVED]
Sent: Fri Dec 04 11:05:39 2009
Subject: for yahoo.com webhosting user

Dear user of the yahoo.com,

Due to the system maintenance, we kindly ask you to take a few minutes to confirm your FTP details.

Please confirm your FTP details by using the link below:

[http://cpanel.yahoo.com/scripts/cpanel-ftp-confirmation.php?session=\[REMOVED\]&email=\[REMOVED\]&service=yahoo.com](http://cpanel.yahoo.com/scripts/cpanel-ftp-confirmation.php?session=[REMOVED]&email=[REMOVED]&service=yahoo.com)

yahoo.com webhosting service.

The actual URL is of course not the one visible in the email, but rather a URL served from the tyghggi.org.uk domain, which is not associated with Yahoo at all...:

[http://cpanel.yahoo.com.tygrhggi.org.uk/scripts/cpanel-ftp-confirmation.php?session=\[REMOVED\]&email=\[REMOVED\]&service=yahoo.com](http://cpanel.yahoo.com.tygrhggi.org.uk/scripts/cpanel-ftp-confirmation.php?session=[REMOVED]&email=[REMOVED]&service=yahoo.com)

When clicking the link, the following page is displayed in the browser:



The spam campaign contains many variants – both in terms of hosting targeted, and in terms of the domain used for phishing.

But where's the money?

The ability to upload arbitrary content into relatively small and less popular sites may seem un-interesting fraud-wise. However, evidence collected by Trusteer over the last few months connects cPanel-driven sites to phishing attacks. Earlier this year, Trusteer investigated several phishing incidents involving fraudsters who specialize in cPanel-driven sites and use solely such sites as a basis for their phishing sites. Trusteer also observed that these fraudsters did not use typical hacking tools (such as their own rogue control panel) to upload content to the site, but rather used standard cPanel functionality to do so. This may indicate that in those cases, the phishers had access to the cPanel credentials.

The current campaign takes a similar approach by requesting the FTP credentials, which, while weaker than the cPanel login credentials, still suffice for data upload.

Concluded attack flow

1. Send spam emails for FTP credentials – target site owners whose sites are hosted by major hosting providers.

2. Collect FTP credentials from cPanel-based site owners.
3. Connect via FTP to the compromised cPanel accounts and upload bank phishing pages to them.
4. Send spam emails for bank credentials (regular bank phishing).

Impact on site owners

Having one's site used for phishing incurs several types of damages:

- Possible downtime due to aggressive take-down actions taken by the bank
- Downtime/work/expenses needed to restore the site and remove the phishing content
- Possible legal repercussions – theoretically a subpoena can be issued for the server
- Inclusion in black-lists of various phishing filters (difficult to track and remove)
- Damage to reputation by having phishing content served (demonstrates lack of security)

On top of this, even if the uploaded content is not phishing-related, it may still be a serious issue, legal and otherwise (e.g. porn and other questionable materials), and may damage the site's reputation (e.g. defacement).

Recommendations

- Never click on links provided in emails.
- Be cautious with sensitive information and credentials, especially those enabling web site manipulation. FTP credentials that can be used to upload content into sections of the site are therefore sensitive and should be well guarded
 - Make sure such credentials are only used with their designated sites, e.g. copy and paste the login/site URL from a safe location.
- Be aware of phishing emails against site management applications and FTP credentials.
- Use security products to secure sensitive credentials.

Appendix – ownership data for cpanel.yahoo.com.tygrhggi.org.uk

Domain ownership (tygkrggi.org.uk): the domain was registered in the UK (on December 4th, 2009) for an individual listing her address in Belgium. The following is the relevant excerpt from the WHOIS database:

Registrant:

Sherry Ajemian

Registrant type:

Non-UK Individual

Registrant's address:

5105 Otis Ave
Koningshooikt
5244
Belgium

The host cpanel.yahoo.com.tygrhggi.org.uk currently resolves into the IP address 119.95.219.171, which belongs to the Philippine Long Distance Telephone Company.