Eliot Ivan Bernstein

From: Canaca-Com Inc (Morteza) <support@canaca.com>
Sent: Wednesday, May 31, 2017 12:05 PM
To: iviewit@gmail.com
Subject: [ZLP-38835]: mail down again

mail down again

Hello again,

My colleagues have scanned your account to find the malicious codes used to send out the spam emails. We have found two PHP scripts injected:

css-gms.php
incv.php

The files are now moved to a folder named "hacked-2017-05-31" on your account. The files were uploaded via the WordPress installed at http://iviewit.tv/ShirleyBernstein/ which is not secured and out of date for a long time.

WordPress has several vulnerabilities and unfortunately is a popular target for hackers. Please install security plugins on this software to prevent intrusions. I went ahead and installed a WordPress plugin named "WordFence" which can be used to scan and detect malicious codes and restore the corrupt files if there are any injections. After installation I ran a full scan using this plugin and fixed the injected files. Please make sure to keep your WordPress and its plugins and themes updated -even if you aren't using them currently.

I noticed you have several WordPress installations on your website as well as this one. I would highly recommend doing the same (updating them and installing WordFence or other security plugins on them) to prevent such issues. More explanation can be found at:
http://wordpress.org/extend/plugins/wordfence/

After installation you can run a full scan using this plugin periodically and check the results found. You can also consult code providers and the forums to gather information on securing WP.

Options to increase WordFence security: Click "Options" from WordFence menu in WordPress control panel and mark the following options:

- Scan theme files against repository versions for changes
- Scan plugin files against repository versions for changes
- Scan files outside your WordPress installation

And enter your email address in its settings so that you can be alerted whenever something suspicious happens on WordPress.

The admin login information of your hosting account is reset to:

Username: iviewit
Password: Qr@kt!k@LLy

You will need to consult security experts for WordPress and monitor them constantly. Please make sure to keep backups of website contents on your computer.

I hope you understand that we are not responsible for the security of your content management systems and can't assist you any further than this.

Best Regards,
Technical Support Supervisor
Please mail us about the quality of your experience at feedback@canaca.com

- - - - - - - - - - -

We highly recommend backing up your data at least twice a month. For more information on backups please contact us at support@canaca.com

---

Rate this ticket: Helpful Not Helpful

Ticket ID:	ZLP-38835
Tracking URL:	Click Here
Department:	Technical Support
Created On:	31 May 2017 06:55 AM
Last Update:	31 May 2017 10:45 AM
Status:	Closed