Eliot Ivan Bernstein

From: Eliot Ivan Bernstein <iviewit@iviewit.tv>
Sent: Sunday, June 4, 2017 7:43 PM
To: 'Canaca-Com Inc. Support'; 'tourcandy@gmail.com'; [redacted]

[redacted]

Subject: RE: [HLE-25543]: IMPORTANT: Your Account is Sending Spam "iviewit.tv"

Also, as you may know from prior correspondences over the years, the site is linked into several ongoing federal and state, civil, criminal and ethical investigations with the site being used to host exhibits for these agencies. It is very important that you share what you can with me about the potential hackers who may be trying with intent to shut the site down. Please let me know of any information regarding the hacks over the last several weeks as the site and mail are central to courts and investigators involved in these matters. Thanks, Eliot

From: Canaca-Com Inc. Support [mailto:support@canaca.com]
Sent: Sunday, June 4, 2017 2:29 AM
To: iviewit@iviewit.tv; tourcandy@gmail.com; [redacted]ir-[redacted]
Subject: [HLE-25543]: IMPORTANT: Your Account is Sending Spam "iviewit.tv"

IMPORTANT: Your Account is Sending Spam "iviewit.tv"

Hello,

We just noticed that your account is being used for Spamming; to stop sending more emails (Spams) we changed the password for main cPanel account and all email accounts to: [redacted]
It was the first step and you might need to contact your webmaster and do the following steps if your account is abused for Spamming:

1. As mentioned he first thing you need to do is to change your passwords for all email accounts/FTP accounts, making sure that they have strong passwords. This may be enough to stop the Spam from being created.
2. The next thing to do is to stop all mail applications which send/receive email in your network (mail clients like Microsoft Outlook, Mac Mail, Smartphones Mail App etc).
3. Check the headers of the emails, usually you can find useful information like domains or IP addresses in the "from" field.
4. If there is no information in the "from" field then it is likely that you have malware, and you may have a spamming script installed on your account.
5. Check your scripts on any of the sites you own which contain forms (they may have been exploited by a Spamming script).
6. Check if your accounts have weak passwords. Spammers will typically connect to an account and try a few hundred common passwords before moving on. These may well include passwords that are the same as the username and domain name. They will also include common obfuscations of the word

password. Attackers will always make login attempts using either the full email address as the username or just common names. You should always have passwords with upper and lower case letter, numbers and symbols.

We hope you understand this is causing serious issues for all other hosted accounts on your server and also for our company which needs to be fixed as soon as possible.

- You have 24 hours to stop this issue and the account will be suspended temporarily if we notice the problem is persisting.
- Copy of a sample message including header and body information is attached to this ticket.

Best Regards,
Canaca-Com Inc.
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

---

Ticket ID:	HLE-25543
Tracking URL:	Click Here
Department:	Technical Support
Created On:	04 Jun 2017 02:29 AM
Last Update:	04 Jun 2017 02:29 AM
Status:	Open

Eliot Ivan Bernstein

From: Canaca-Com Inc (Morteza) <support@canaca.com>
Sent: Wednesday, May 31, 2017 10:46 AM
To: iviewit@gmail.com
Subject: [ZLP-38835]: mail down again

mail down again

Yes the emails you have received in return are because of the bulk mails sent out, not by you of course. I will keep you posted on this and would appreciate your patience.

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 10:28 AM
Status:	Closed

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:

[redacted]

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