



Dean Herbert <pe@ppy.sh>

[#25905943] ABUSE - 50.97.232.135 - MALWARE - IMMEDIATE ACTION REQUIRED

14 messages

abuse@midphase.com <abuse@midphase.com>

Tue, Feb 28, 2012 at 3:41 PM

Reply-To: abuse@midphase.com

To: Dean Herbert <pe@ppy.sh>

Hello Dean Herbert,

We have received the following abuse complaint regarding your host414753.mpdedicated.com server. Please investigate this issue, take the necessary action, and update us in this ticket to avoid any possible disruption to your service if we do not receive a response within 24 hours. Additionally, please let us know what steps will be taken to prevent this abuse from occurring in the future.

=====

Original Notice:

36351 | 50.97.232.135 | 2012-02-27 04:04:13 <http://puu.sh/hQP3.exe> MALWAREURL | SOFTLAYER - SoftLayer Technologies Inc.

=====

You may review our Acceptable Use Policy (AUP) at the following link:

<http://www.100tb.com/tos.php#acceptable>

Please reply to this email detailing the steps taken to resolve this issue. We thank you in advance for your quick action and cooperation.

—

Kind Regards,

—

Svitlana Khoroshylova
100TB.com

Dean Herbert <pe@ppy.sh>

Tue, Feb 28, 2012 at 3:47 PM

To: Jamie Taylor <jamie@dotneko.net>

Dean

Begin forwarded message:

差出人: abuse@midphase.com

日時: 28 February 2012 15:41:56 AWST

宛先: Dean Herbert <pe@ppy.sh>件名: [#25905943] ABUSE - 50.97.232.135 - MALWARE - IMMEDIATE ACTION REQUIREDReply-To: abuse@midphase.com

[Quoted text hidden]

Jamie Taylor <jamie@dotneko.net>**Tue, Feb 28, 2012 at 3:48 PM**

To: Dean Herbert <pe@ppy.sh>

This sure feels familiar.

Regards,
Jamie

[Quoted text hidden]

Dean Herbert <pe@ppy.sh>**Tue, Feb 28, 2012 at 6:11 PM**

To: abuse@midphase.com

Cc: puush@puush.me

Hi,

I will check the said file on a VM when I have access to one, but it looks clean as far as being a virus. Could you expand on what MALWAREURL means, and provide more details on where you are getting this report for?

For what it's worth, we provide a service to the public similar to dropbox/droplr where users can upload desktop screenshots and files, so are not directly responsible for uploading the said file.

Regards,
Dean

[Quoted text hidden]

abuse@midphase.com <abuse@midphase.com>**Tue, Feb 28, 2012 at 10:51 PM**

Reply-To: abuse@midphase.com

To: Dean Herbert <pe@ppy.sh>

Hello,

Typically it means that either the site or a file on it is being flagged as a malicious file. You may wish to have the file analyzed in <https://www.virustotal.com/> to see if and why some antivirus programs are flagging the file.

—
Kind Regards

—
Ilona Hlazunova

100TB.com

abuse@midphase.com <abuse@midphase.com>**Tue, Feb 28, 2012 at 11:42 PM**

Reply-To: abuse@midphase.com

To: Dean Herbert <pe@ppy.sh>

Hello Dean Herbert,

We still have not received a response to this complaint. Please let us know what actions have been taken within the next 16 hours to prevent suspension of service.

If you have any questions, please let us know.

—
Kind Regards

—
Nataliia Pryymak

CDN Support
100TB.com

Dean Herbert <pe@ppy.sh>**Tue, Feb 28, 2012 at 11:46 PM**

To: abuse@midphase.com

We already replied just earlier. We've checked the file and it doesn't seem to be of malicious intent.

<http://puu.sh/iJUJ>

Regards,
Dean

[Quoted text hidden]

abuse@midphase.com <abuse@midphase.com>**Wed, Feb 29, 2012 at 12:43 AM**

Reply-To: abuse@midphase.com

To: Dean Herbert <pe@ppy.sh>

Hello,

Have you reviewed why the file is being listed? Simply saying you do not think it's malicious is not a resolution.

[Quoted text hidden]

Dean Herbert <pe@ppy.sh>**Wed, Feb 29, 2012 at 12:52 AM**

To: abuse@midphase.com

Could you please explain in more detail where the file is being listed, and what you expect in a reply from us? Due to the nature of our service, this will likely come up again in the future so this is quite important to know.

Regards,
Dean

[Quoted text hidden]

abuse@midphase.com <abuse@midphase.com>**Wed, Feb 29, 2012 at 2:07 AM**

Reply-To: abuse@midphase.com

To: Dean Herbert <pe@ppy.sh>

Dean,

As explained before, you could have easily determined this here:

<https://www.virustotal.com/url/3fe9a53a134d81e08c636be66f3d8d860f1b001a650ef56ec72ab8504c441cb6/analysis/1330449636/>

Please take responsibility of the issue and ensure that you resolve it.

—

—

Kind Regards

—

Victoriya Ivanusa
100TB.com

Dean Herbert <pe@ppy.sh>**Wed, Feb 29, 2012 at 2:33 AM**

To: abuse@midphase.com

I have already examined the said site; the tests/parties listing the file as "malware" are detecting using generic heuristics, which regularly return false positives. This is one of those cases where the file has been (in my opinion, after testing it in a VM) falsely identified. I believe I have already taken responsibility and resolved the issue through this process, so please tell me if there are any further necessary steps in order to resolve it.

Regards,
Dean

[Quoted text hidden]

abuse@midphase.com <abuse@midphase.com>

Wed, Feb 29, 2012 at 3:41 AM

Reply-To: abuse@midphase.com

To: Dean Herbert <pe@ppy.sh>

Hello,

<https://www.virustotal.com/file/f99fceb476d77332f17c23ee7153cc057cd508773015a884d0ad83b0b35ea0e3/analysis/>

This file is malware, and as requested, we need it removed.

[Quoted text hidden]

abuse@midphase.com <abuse@midphase.com>

Wed, Feb 29, 2012 at 8:07 AM

Reply-To: abuse@midphase.com

To: Dean Herbert <pe@ppy.sh>

Hello,

we definitely need the .exe at <http://puu.sh/hQP3.exe> removed. It exhibits traits which flag it as malware, so it is best to remove it to be on the safe side. Softlayer will disconnect the server if this is not done.

—

Best regards,

Breanne "Cari" Carlson
Dedicated server engineer
Hosting Services INC.

Dean Herbert <pe@ppy.sh>

Wed, Feb 29, 2012 at 8:57 AM

To: abuse@midphase.com

Is there someone we can follow this up further with? I don't believe going forward we can remove our users' files like this and provide a justified response. This file is definitely a false detection, and there may be more in the future. Searching further, the generic heuristics it matches to seem to prove a common result for many legit commercial game executables and such as well.

Regards,
Dean

[Quoted text hidden]