Ticket 2339371 for account congregation-of-non-contradiction.org

Posted: 16 Jul, 2017 14:49 CDT **Status:** Resolved
Ticket Subject: Illegal activity through your website detected

Ticket Messages:

You
Posted On 16 Jul, 2017 14:49 CDT

Dear Douglas,

SiteGround has received a complaint that some illegal activity has been performed through your website.

The infringing material is located at:

http://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=update&/IDMSWebAuth/update.html?appIdKey=0ac5cea9921ac5ade78a2e1105ea22e6&id=abuse@icloud.com *(http://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=update&/IDMSWebAuth/update.html?appIdKey=0ac5cea9921ac5ade78a2e1105ea22e6&id=abuse@icloud.com)*

You can find the complaint we have received at the bottom of this message.

Due to the fact that this activity severely violates SiteGround's Terms of Use and Acceptable Use Policy, we were forced to suspend your account in order to prevent any further issues caused by the illegal activity.

We are very much aware of the inconvenience this issue may cause you, so we would like to take a moment and explain the reasons for our actions: as you know, your account is hosted on a shared hosting server and thus sharing the resources of the server with other customers' accounts. When some illegal activity performed through a shared hosting account is detected, we must take immediate actions to stop that activity, otherwise we risk having the whole server unplugged. And we cannot allow the entire hosting server with hundreds of accounts on it to be unplugged because of one single account.

This is why the above explained precaution was absolutely necessary.

We believe the illegal activity through your account is a result of a hacked script. For more information about such problems please check this link:

http://kb.siteground.com/hacked_website/

We have scanned your account. The list with the suspicious files is stored in your account's home folder. Its name is suspicious_files.txt and it can be downloaded either through cPanel->File Manager *(https://www.siteground.com/tutorials/cpanel/file_manager.htm)* or using your local FTP client *(https://www.siteground.com/tutorials/ftp/)*.

In order to continue using your account with us you have 3 options:

- Delete all of your web content and lose all of your web files. This is an option in case you can recreate easily your website from scratch. Thus you will ensure that no malicious code and backdoors are left by the attacker.

- Have a professional security audit. We recommend the website security company Sucuri for malware detection, malware cleanup and malware prevention. Their 2-in-1 Website AntiVirus + Website Firewall (WAF) solution supports and protects all websites built on any platform.

https://siteground.com/sucuri

- Clean and secure your site by yourself. This option requires advanced technical skills and your responsibility is huge. Furthermore, in future you will have to take extra care making sure your site remains secured. This includes applying regular updates and security patches.

Thank you for your understanding and cooperation.

Regards,

Valcho Valchev
System Administrator
SiteGround.com

--- EMAIL COMPLAINT COPY STARTS HERE ---

Hello,

My name is Jitesh Khanna and I work for PhishLabs. We investigate computer crime incidents on behalf of other organizations.

During an investigation of fraud, we have identified a phishing site which is hosted on your network and attempting to defraud the customers of Apple.

The following URLs are some components of this phishing attack:

hXXps://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=update&/IDMSWebAuth/update.html?appIdKey=0ac5cea9921ac5ade78a2e1105ea22e6&id=abuse@icloud.com
hXXps://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=login&Key=ba6a832f74efec77463da9e4acc64c3b&login&path=/signin/?referrer
hXXps://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/
hXXps://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=update&/IDMSWebAuth/update.html
hXXps://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=verifica&/IDMSWebAuth/update.html

First detection of malicious activity: 07-16-2017 19:32:06 UTC
Most recent observation of malicious activity: 07-16-2017 19:34:10 UTC
Associated IP Address: 37.60.247.123
Hostname of Server: congregation-of-non-contradiction.org

If you agree that this is malicious, we kindly request that you take steps to have the content removed as soon as possible. It is likely that the intruder who set up this phishing site has also left additional fraudulent material on this server.

If we have contacted you in error, or if there is a better way for us to report this incident, please let us know so that we may continue our investigation.

We are extremely grateful for your assistance.

Kind Regards,

Jitesh Khanna
PhishLabs Security Operations
soc@phishlabs.com

+1.202.386.6001
hXXp://www.phishlabs.com

--- EMAIL COMPLAINT COPY ENDS HERE ---

You
Posted On 24 Jul, 2017 11:48 CDT

Nikolay Arabadzhiev
Support Guru Posts: 86700 Posted On 24 Jul, 2017 12:01 CDT

You
Posted On 24 Jul, 2017 13:25 CDT

Nikolay Arabadzhiev
Support Guru Posts: 86700 Posted On 24 Jul, 2017 14:02 CDT

You
Posted On 29 Jul, 2017 13:27 CDT

Good morning.
This whole thing is looking like a scam. My site is held hostage. None of the offending urls or the "shell script" can be found.

Georgi Tsenov
Support Guru Posts: 28204 Posted On 29 Jul, 2017 14:14 CDT

Hello Douglas,

I verified that the phishing URL has been removed:
http://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=update&/IDMSWebAuth/update.html?appIdKey=0ac5cea9921ac5ade78a2e1105ea22e6&id=abuse@icloud.com *(http://congregation-of-non-contradiction.org/wordpress/wp-content/themes/twentyseventeen/up/ro/?ID=update&/IDMSWebAuth/update.html?appIdKey=0ac5cea9921ac5ade78a2e1105ea22e6&id=abuse@icloud.com)*

I scanned your website:
Code:

```
Scanning [/home/congreg8/public_html] ... Please wait...
----------------------------------------
Scanned Files : 6782
Scanner Hits : 0
Time Taken : 17 (sec)
```

The limit has been lifted and the Abuse case - closed.

Best Regards,
Georgi Tsenov
Senior Technical Support