MOCHAHOST

Ticket #311435

Compromised account > pack1234

Status	Answered	Name	Arun Palaniswamy
Priority	Normal	Email	apalaniswamy@yahoo.com
Department	Abuse	Phone	
Create Date	04/09/2022 07:40:05 PM	Source	Email

04/09/2022 07:40:05 PM — Arun Palaniswamy

04/09/2022 07:40:05 PM — Barry B. @ MochaHost

Dear Client,

Our security monitor detected that your hosting space is compromised and is used for malicious activities, such as SPAM, port scanning, cryptocurrency mining, etc.

We will be happy to provide you all information possible in order for you to understand the reasons and prevent this from happening in future.

The most common reasons for a compromised account/server include:

- Outdated web application- Every popular web application (Joomla, WordPress, PhpBB etc.) has had security problems and that is why you have to use always the latest version.

- Outdated web application extension- If you have installed any third party extensions, you have to keep them up-to-date just as you keep your main web application. Very often users neglect this fact and outdated extensions become easily exploited by intruders.

- Weak user / administrator passwords- You must ensure that all users have strong passwords, especially the admin and the ones who can create content to your site.

- Infected local computer- Some computer viruses/worms are known to steal FTP logins and after that add malicious code to web files. For this reason make sure to have an updated antivirus software and scan your computer for viruses regularly.

Please investigate the issue and Reply us back as soon as possible, providing more information on the situation and actions taken in order to resolve the issue.

If you are using WordPress sites within your account you may find the below information helpful:

A WordPress infection is most likely result of:

1) Outdated WordPress version, outdated plugins, or outdated themes

2) Use of vulnerable themes or plugins. This is most likely the case if you have recently used themes or plugins with suspicious origin

3) Brute force attack towards your WordPress admin user/pass

At that point we have put under quarantine the infected content of the site in question, so you need to clear it out first.

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

structure 2900804 pack1234 cwd DIR 8,65 4096 38014238 /home3/pack1234/test1.empowerschool.com/wp-content

structure 2900804 pack1234 rtd DIR 8,161 4096 524289 /

structure 2900804 pack1234 txt REG 8,65 8607584 38011813 /home3/pack1234/test1.empowerschool.com/wp-content/structure4 (deleted)

structure 2900804 pack1234 mem REG 8,5 159312 184006 /lib64/ld-2.12.so

structure 2900804 pack1234 mem REG 8,5 143368 184088 /lib64/libpthread-2.12.so

structure 2900804 pack1234 mem REG 8,5 1924768 184016 /lib64/libc-2.12.so

structure 2900804 pack1234 0r CHR 1,3 0t0 529661 /dev/null

structure 2900804 pack1234 1w CHR 1,3 0t0 529661 /dev/null

structure 2900804 pack1234 2w CHR 1,3 0t0 529661 /dev/null

structure 2900804 pack1234 3r CHR 1,3 0t0 529661 /dev/null

structure 2900804 pack1234 4u REG 8,65 7 38011827 /home3/pack1234/test1.empowerschool.com/wp-content/.pid

structure 2900804 pack1234 5u CHR 1,3 0t0 529661 /dev/null

structure 2900804 pack1234 6u unix 0xffff880103748c00 0t0 3363703615 /var/run/mod_lsapi/lsapi_application-x-httpd-ea-php56___lsphp_2066_test1.empowerschool.com.sock

structure 2900804 pack1234 7u IPv4 3365191745 0t0 TCP mocha9001.mochahost.com:56778->orbit.bg:http (SYN_SENT)

structure 2900804 pack1234 8u 0000 0,9 0 6432 anon_inode

structure 2900804 pack1234 9u IPv4 3365179915 0t0 TCP mocha9001.mochahost.com:44090->sv90.ifastnet.com:http (SYN_SENT)

structure 2900804 pack1234 10u IPv4 3365194140 0t0 TCP mocha9001.mochahost.com:56406->ap9.cpanelhost.cl:https (SYN_SENT)

structure 2900804 pack1234 11u IPv4 3365184979 0t0 TCP mocha9001.mochahost.com:51708->hostingsrv4.dondominio.com:https (SYN_SENT)

structure 2900804 pack1234 12u IPv4 3365189720 0t0 TCP mocha9001.mochahost.com:56162->172.67.212.194:https (ESTABLISHED)

structure 2900804 pack1234 13u IPv4 3365184832 0t0 TCP mocha9001.mochahost.com:45364->172.67.194.80:https (ESTABLISHED)

structure 2900804 pack1234 14u IPv4 3365176832 0t0 TCP mocha9001.mochahost.com:46856->46.183.138.100:https (ESTABLISHED)

structure 2900804 pack1234 15u IPv4 3365191276 0t0 UDP mocha9001.mochahost.com:45956->ns1.rec.servercentral.net:domain

structure 2900804 pack1234 16u IPv4 3365193404 0t0 UDP mocha9001.mochahost.com:35445->ns1.rec.servercentral.net:domain

structure 2900804 pack1234 17u IPv4 3365186286 0t0 TCP mocha9001.mochahost.com:51138->dd47418.kasserver.com:https (SYN_SENT)

structure 2900804 pack1234 18u IPv4 3365200944 0t0 TCP mocha9001.mochahost.com:45372->viserion.aserv.co.za:https (ESTABLISHED)

structure 2900804 pack1234 19u IPv4 3365194041 0t0 TCP mocha9001.mochahost.com:55204->cpanel21.mywebserver.co.za:http (ESTABLISHED)

structure 2900804 pack1234 20w REG 8,3 12320124 65701 /var/log/apache2/sulsphp_log

structure 2900804 pack1234 21u IPv4 3365190796 0t0 TCP mocha9001.mochahost.com:58252->hostingweb54-202.netsons.net:https (SYN_SENT)

structure 2900804 pack1234 22u IPv4 3365197873 0t0 TCP mocha9001.mochahost.com:34012->hubble.servers.prgn.misp.co.uk:https (ESTABLISHED)

structure 2900804 pack1234 23u IPv4 3365196372 0t0 TCP mocha9001.mochahost.com:42874->host8.gophermedia.com:https (SYN_SENT)

structure 2900804 pack1234 24u IPv4 3365197945 0t0 TCP

mocha9001.mochahost.com:42466->ip70.ip-144-217-120.net:https (ESTABLISHED)

structure 2900804 pack1234 25u IPv4 3365200054 0t0 TCP
mocha9001.mochahost.com:55660->web2213.webbedrijf.nl:https (ESTABLISHED)

structure 2900804 pack1234 26u IPv4 3365197383 0t0 TCP
mocha9001.mochahost.com:54746->fereshteh.dnswebhost.com:https (ESTABLISHED)

structure 2900804 pack1234 27u IPv4 3365195100 0t0 TCP
mocha9001.mochahost.com:36970->server.aheadoftheweb.biz:https (ESTABLISHED)

structure 2900804 pack1234 28u IPv4 3365194120 0t0 TCP
mocha9001.mochahost.com:52458->dd27438.kasserver.com:https (SYN_SENT)

structure 2900804 pack1234 29u IPv4 3365198041 0t0 UDP
mocha9001.mochahost.com:35215->ns1.rec.servercentral.net:domain

structure 2900804 pack1234 30u IPv4 3365200409 0t0 TCP
mocha9001.mochahost.com:39304->sl1454.web.hostpoint.ch:https (SYN_SENT)

structure 2900804 pack1234 31u IPv4 3365197921 0t0 TCP
mocha9001.mochahost.com:47148->cluster023.hosting.ovh.net:https (ESTABLISHED)

structure 2900804 pack1234 32u IPv4 3365172865 0t0 TCP
mocha9001.mochahost.com:47194->103.62.52.188:https (ESTABLISHED)

structure 2900804 pack1234 33u IPv4 3365197793 0t0 TCP
mocha9001.mochahost.com:51372->167.71.143.195:https (ESTABLISHED)

structure 2900804 pack1234 34u IPv4 3365185138 0t0 TCP
mocha9001.mochahost.com:35060->static.251.242.9.176.clients.your-server.de:http (SYN_SENT)

structure 2900804 pack1234 35u IPv4 3365189553 0t0 UDP
mocha9001.mochahost.com:55007->ns1.rec.servercentral.net:domain

In order to rectify this issue and prevent any similar from happening in the future we recommended that you take immediately the following steps:

1) Update all of your site applications by installing all new security updates – check the following articles:
http://blog.mochahost.com/important-tips-on-wordpress-security/
http://codex.wordpress.org/FAQ_My_site_was_hacked

2) Review our Brute-Force Attack blog post and take necessary measures to avoid this form happening in

the future.

http://blog.mochahost.com/brute-force-attack-what-is-this-attack-about

3) Change all of your account passwords /control panel, ftp, email ... etc/. Please, review the following IMPORTANT article on how to select a good password:

http://blog.mochahost.com/selecting-good-password/

4) *Change your Secret Key (Salt) – * If you have installed WordPress 2.5 or later, then you will have the SECRET_KEY defined in the wp-config.php already. You will want to change the value in it because hackers will know what it is. If you have upgraded to WordPress 2.5 or later version from a version before WordPress 2.5, then you should add the constant to your wp-config.php file.

Please check the following articled for more information on WP Salt:

http://blog.mochahost.com/change-of-wordpress-security-keys/

http://codex.wordpress.org/Function_Reference/wp_salt

http://wordpress.org/support/topic/wp-security-keys

For more details regarding this problem, please visit following articles.

http://www.mochasupport.com/kayako/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=582&nav=0,46

If you need additional information regarding how to secure your account, please review following article:

http://blog.mochahost.com/10-tips-on-wordpress-security/

Other 3rd party WordPress security solutions which we strongly recommend are available at:

1) WordFence - available through: https://www.wordfence.com/ (Offering Free + Premium version)

2) Sucuri - available through: https://sucuri.net/wordpress-security/wordpress-security-monitoring

Please, review the ENTIRE information above and get back to us within 24 when you are ready to take actions.

Please, note that in order to protect other customers and 3rd parties, failure to take action regarding this notice may result in site or account suspension.