

Forum: [Hack Forums](#)

Thread: [Did my website get hacked? How do I prevent it?](#)

Turf - December 4, 2018, 4:48 pm

I'm 100% certain I got hacked, because of the following:

- My index.html file got deleted randomly
- Random files uploaded in my File Manager..."moban.html" and "atomic" and "updatecorel" ring any bells? Can anybody explain what these do and how to prevent them?
- .htaccess file keeps getting modified to include the following rules:

```
RewriteRule ^.*[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1&{%QUERY_STRING} [L]
RewriteRule ^e(\d+)-.*$ updatecorel/index\.\php?id=$1&{%QUERY_STRING} [L]
RewriteRule ^g(\d+)[-/]e(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1-$2&{%QUERY_STRING} [L]
RewriteRule ^g(\d+)[-/]e(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1-$2&{%QUERY_STRING} [L]
RewriteRule ^e(\d+)[-/]g(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$2-$1&{%QUERY_STRING} [L]
RewriteRule ^e(\d+)[-/]g(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$2-$1&{%QUERY_STRING} [L]
RewriteRule ^.*[-/]e(\d+)[-/]g(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$2-$1&{%QUERY_STRING} [L]
RewriteRule ^.*[-/]g(\d+)[-/]e(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1-$2&{%QUERY_STRING} [L]
RewriteRule ^.*[-/]g(\d+)[-/]e(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1-$2&{%QUERY_STRING} [L]
```

Can anybody suggest what changes I should make to my site? It's just a normal HTML...if I go WP, are these less likely to happen?

sh4moon - December 4, 2018, 4:53 pm

(Dec 4, 2018 05:48 PM)Turf Wrote: [\[CITE\]](#) I'm 100% certain I got hacked, because of the following:

- My index.html file got deleted randomly
- Random files uploaded in my File Manager..."moban.html" and "atomic" and "updatecorel" ring any bells? Can anybody explain what these do and how to prevent them?
- .htaccess file keeps getting modified to include the following rules:

```
RewriteRule ^.*[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1&{%QUERY_STRING} [L]
RewriteRule ^e(\d+)-.*$ updatecorel/index\.\php?id=$1&{%QUERY_STRING} [L]
RewriteRule ^g(\d+)[-/]e(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1-$2&{%QUERY_STRING} [L]
RewriteRule ^g(\d+)[-/]e(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1-$2&{%QUERY_STRING} [L]
RewriteRule ^e(\d+)[-/]g(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$2-$1&{%QUERY_STRING} [L]
RewriteRule ^e(\d+)[-/]g(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$2-$1&{%QUERY_STRING} [L]
RewriteRule ^.*[-/]e(\d+)[-/]g(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$2-$1&{%QUERY_STRING} [L]
RewriteRule ^.*[-/]e(\d+)[-/]g(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$2-$1&{%QUERY_STRING} [L]
RewriteRule ^.*[-/]g(\d+)[-/]e(\d+)[-/]e(\d+)-.*$ updatecorel/index\.\php?id=$1-$2&{%QUERY_STRING} [L]
```

[L]

```
RewriteRule ^.*[-/]g(\d+)[-/]e(\d+)[-/].*$ updatecorel/index\..php?id=$1-$2&{%{QUERY_STRING}} [L]
```

Can anybody suggest what changes I should make to my site? It's just a normal HTML...if I go WP, are these less likely to happen?

it's likely some skid who doesn't know what he's doing I can help you out if you want.

realsunjester - December 4, 2018, 4:56 pm

i would first start by checking error and access logs for apache, or whatever web server software youre using for ip's and blacklist those changing the file..

access

Code tail /var/log/apache2/access.log

errors

Code tail /var/log/apache2/error.log

Turf - December 4, 2018, 6:39 pm

(Dec 4, 2018 05:56 PM)realsunjester Wrote: [\[CITE\]](#) i would first start by checking error and access logs for apache, or whatever web server software youre using for ip's and blacklist those changing the file..

access

Code tail /var/log/apache2/access.log

errors

Code tail /var/log/apache2/error.log

Where would I go to check these? I'm using cPanel.

VoIPv2 - December 4, 2018, 7:49 pm

(Dec 4, 2018 07:39 PM)Turf Wrote: [\[CITE\]](#) Where would I go to check these? I'm using cPanel.

You might be able to ftp into your server if you are using cpanel and depending on who hosts. You might have ssh access also. If running Windows you will need putty installed. Otherwise any Linux based OS can use Ssh

realsunjester - December 4, 2018, 8:26 pm

(Dec 4, 2018 07:39 PM)Turf Wrote: [\[CITE\]](#) Where would I go to check these? I'm using cPanel.

You can check the logs under the "visitor stats" block

or you can setup ssh access and go in that way, under the "Advanced" block