

Re: Rogue PHP file

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-06/msg02674.html>

- *From:* "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@xxxxxxxxxxx>
 - *Date:* Sun, 29 Jun 2008 19:14:34 -0700
-

This is where the WOLF analysis comes in handy. Is there any other logs on the box that go back that far? Firewall logs? Anything?

Frank wrote:

Hi Susan,

The folder (xamplite) was created in C:\Documents and Settings on 3/17/2008 @ 10:43 AM. Nothing else was installed around that time. The Security Event logs only go back to April, 2008.

"Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@xxxxxxxxxxx> wrote in message <news:el8BSbi2IHA.4848@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Look at the date/time that the Apache folder was installed.
Look to see what else was installed at the same/or close time.
Look to the event security logs (if they go back that far) around the same time.

If the time that this folder got on the server doesn't make sense, they may not have installed anything themselves.

Frank wrote:

Thank you Cliff,

I have been on the phone with two other employees the owner wanted me to talk to directly. Of course none of them will admit to installing Apache server. And yes they have all sorts of DNS problems I saw right off the bat. They were very reluctant to answer any questions I asked them.

They also stated that they could not use RWW. I discovered the Default Company web was stopped. As soon as I disabled Apache I was able to restart RWW.

Thanks to everyone who posted on this topic.
"Cliff Galiher" <cgalihier@xxxxxxxxxxx> wrote in message <news:6986DDEF-53F7-436C-B3B6-0D5C0B4CF181@xxxxxxxxxxxxxxxxxxxx>

Re: Rogue PHP file

your SBS. It
is not
needed!

It appears to
have an
Apache
server
listening.
This is the
output after
quitting a
Telnet
session to
port 80:

```
<!DOCTYPE  
HTML  
PUBLIC  
"-//IETF//DTD  
HTML  
2.0//EN">  
<HTML><HEAD>
```

```
<TITLE>501  
Method Not  
Implemented</TITLE>
```

```
</HEAD><BODY>
```

```
<H1>  
Method Not  
Implemented</H1>  
?quit to  
/index.html  
not  
supported.<P>
```

```
Invalid  
method in  
request  
?quit<P>
```

```
<HR>
```

```
<ADDRESS>Apache/1  
.3.23 Server  
at localhost  
Port  
80</ADDRESS>  
</BODY></HTML>
```


Re: Rogue PHP file

<not@xxxxxxxxxxxx>

wrote

in

message

news:eXTwe2S2IHA.4912@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

G'day

Frank,

I

am

neither

the

'alarmist'

which

Susan

is

nor

the

'routers

are

evil'

that

you

will

get

from

Leythos.

I

have

the

benefit

of

having

seen

your

later

post

but,

so

far,

I'm

not

really

sure

whether

the

internet

name

for

Re: Rogue PHP file

your
SBS
is
actually
mail.xxxxxxxxxx.com.
There's
issues
about
bad/poisoned
DNS
that
would
need
to
be
investigated.
SBS
would
need
to
be
_pretty
thoroughly
'owned'_
before
'anything.php'
comes
into
play.

IF
the
server
has
been
compromised,
and
so
far
I'm
not
really
sure
it
has,
you
should
be
firstly
looking
to

Re: Rogue PHP file

PCSafety,
as
Susan
has
suggested,
and
then
considering
HOW
this
happened
and
the
cost
of
addressing
the
issue
(on
your
primary
DC,
which
you
should
now
trust
NOTHING
from),
vs
externally
hosting
your
public
(www)
domain.

Though
SBS
is
thoroughly
capable
of
hosting
websites
(I
do
it
myself)
it's
not

Re: Rogue PHP file

really
a
good
idea,
particularly
considering
the
_very
cheap_
alternatives
which
may
not
only
give
you
greater
facility
and
bandwidth
but
also
less
concern
about
'such
hacks'.

"Frank"

<ffarero@xxxxxxxxxxx>

wrote

in

message

[news:48658f04\\$0\\$5981\\$9a6e19ea@xxxxxxxxxxxxxxxx](mailto:news:48658f04$0$5981$9a6e19ea@xxxxxxxxxxxxxxxx)

Hi

all,

SBS

2003

server,

XP

pro

clients,

WRT54GS

router,

Static

IP

from

ISP

using

Re: Rogue PHP file

exchange
for
mail.

Not
sure
if
this
is
the
right
news
group.

I
got
a
call
today
from
a
new
client
stating
that
their
mail.xxxxxxxxxx.com
address

was
being
redirected
to

a
Banking
Phishing
website.

They
stated
that
they
got

a
call
from
a
security
firm
in
Calif.

stating
it
looked

Re: Rogue PHP file

Re: Rogue PHP file

to
them
like
a
rogue
PHP
file
was
accepting
requests.
Any
ideas
on
how
to
approach
this
to
find
fix
it?

Thanks