

Re: Rogue PHP file

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-06/msg02618.html>

- *From:* "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@xxxxxxxxxxxx>
 - *Date:* Sat, 28 Jun 2008 16:27:17 –0700
-

Chances are there is a phishing site on the server. Calling support on Monday morning is a free call and they have forensic investigation tools to let you know what (if anything else) is on that box.

If someone has rights to install stuff on a system from inside the lan (say from a phishing email they got) no amount of a firewall will help unless you have rules monitoring what's going on.

If there is stupid user interaction behind this, firewalls won't help gang.

Frank wrote:

Hi Leythos,SuperGumby

Unfortunately for me I have installed 10 SBS 2003 systems and always insisted that a WatchGuard or equivalent security appliance be purchased so I have never run across a situation like this before. The FQDN is ASI01.ASI.local The domain name is www.attachmentsales.com. Please let me know what other info you need. Thanks for the kick in my behind I needed a wakeup call!

"Leythos" <void@xxxxxxxxxxxx> wrote in message
news:1214689991_158065@xxxxxxxxxxxxxxxxxxxxxx

In article <eXTwe2S2IHA.4912@xxxxxxxxxxxxxxxxxxxxxxxxxx>,
not@xxxxxxxxxxxx
says...

I am neither the 'alarmist' which Susan is nor the 'routers are evil' that you will get from Leythos.

In most cases, a SBS setup is installed and not-maintained by anyone technical, it's sold as a simple solution and installed by noobs in almost every case I've come across.

The same is true for network security, it's an after thought or a cheap device that claims to be a firewall on the packaging is used because they wanted to save money...

Re: Rogue PHP file

Routers are simple devices, they can not be evil.

NAT Routers used to be called ROUTER in the days of honesty, then marketing types got the idea that NAT was a firewall method, except NAT could pass everything inbound without blocking anything if it was 1:1 NAT, or if the unknowing person put the server in the DMZ IP address since those devices don't really have a DMZ network.

So, it comes down to badly installed SBS installations protected by Routers that are not even in the firewall class, managed by people that don't have much of a clue, and then they wonder when something happens....

Yes, it's a soapbox but if you've got any real experience around the country you will see exactly what I'm saying in just about any location.

The information we're provided in this problem is very vague, and I've checked out the DNS records, DNS Servers, website, etc...

Since we don't know much, all I can say is that the DNS resolves to a an address in Florida, a Domain Name company up north, and that the IP of mail... is not on any black list....

Without more details we can't really help here.

- Igitur qui desiderat pacem, praeparet bellum.
 - Calling an illegal alien an "undocumented worker" is like calling a drug dealer an "unlicensed pharmacist"
- spam999free@xxxxxxxxxxx (remove 999 for proper email address)