

Re: windows 2000 professional hacked with Serv-U FTP Server

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-11/12276.html>

From: Karl Levinson [x y] mvp (jamescagney90210@excite.com)

Date: 11/24/02

From: "Karl Levinson [x y] mvp" <jamescagney90210@excite.com>

Date: Sun, 24 Nov 2002 11:04:46 -0500

"Tony" <tony.wong@sbcglobal.net> wrote in message
news:KiZD9.3089\$Wq7.231812136@newssvr21.news.prodigy.com...
> *Someone hacked into my windows 2000 machine running sp2 and installed
Serv-U
> FTP server and was uploading movies files to this box. This box was
running
> sp2. Looking in the local users, a bunch of users were created and belong
to
> the local administrator group. File and print sharing, was enabled on this
> box.
>
> How did hacked get into the machine and installed Serv-U ftp server?*

Start by checking your IIS web logs. Look for anything that says .EXE or %
and that also has a 200 or 502 in it. Frequently, an unpatched
vulnerability in the IIS web service on your machine will let a hacker
remotely send commands to your computer by sending URLs to your IIS web
server service.

More information:

<http://securityadmin.info/faq.htm#hacked>

<http://securityadmin.info/faq.htm#iislogs2>

<http://securityadmin.info/faq.htm#iislogs>

> *How do I prevent this from happening?*

Secure your machine properly. [But first, determine how the hack occurred
and whether other machines are infected, using the instructions above.
Then, consider formatting and reinstalling Windows and all other software
from scratch. The reason for this is that it's hard to tell what other back
doors might have been added to your machine or passwords or credit card
numbers gotten from your machine.]

microsoft.public.win2000.security: Re: windows 2000 professional hacked with Serv-U FTP Server

It sounds like you're not running a firewall or antivirus, for one, are missing Microsoft patches, and haven't used one or more hardening checklist documents to remove the vulnerabilities in the default install of Windows.

More info:

<http://securityadmin.info/faq.htm#re-secure>

<http://securityadmin.info/faq.htm#harden>

<http://securityadmin.info/faq.htm#firewall>

<http://securityadmin.info/faq.htm#virus>