

Re: FTP Tagging anyone?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-11/5966.html>

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

Date: 11/16/02

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

Date: Sat, 16 Nov 2002 09:58:07 -0500

"Alun Jones" <alun@taxis.com> wrote in message
news:0uhB9.1646\$Ni7.728720551@newssvr12.news.prodigy.com...

> *Not necessarily. There are many systems that run with firewalls in place,
> secured against various different kinds of vulnerabilities, and the one
thing
> they did wrong was think that they could allow anonymous FTP users to
upload
> and download.*

I think we're sort of in agreement... What I was saying is, all we know for sure at this point is that the FTP server had insufficient permissions to the FTP folders that permitted someone to drop static files there. This alone is hardly a hacking, since it normally does not allow the hacker to install and execute trojans or commands remotely or otherwise install back doors. If we could somehow prove that this was the only intrusion on this system, formatting the system is probably not necessary.

HOWEVER, I think it's possible but unlikely that a system would only have this one vulnerability. I think that this permissions issue may be mentioned in the Microsoft hardening IIS checklist, which would indicate that the administrator may not have followed that document and eliminated other more serious vulnerabilities. It's hard to prove for sure that this is the only hacking that went on. So you have to make an educated guess, or look for more clues, or format the system just in case. My choice was and is to try to describe the choices and issues in this dilemma, but to assume that the administrators in this situation probably don't have the experience to tell whether the machine was otherwise hacked, and to recommend that they format to eliminate uncertainties. No one needs security uncertainties around their web or ftp servers.

> *Each time I've observed this happen, the storage of extra files – in
> directories that are designed to be difficult for the administrator to
delete
> – has been the only attack on the system.*

I agree... but you can't be 100% sure. And if you could even be, say 95% sure, most of the administrators out there who don't have someone with your experience won't be able to do everything they need to do to be 95% secure.

> *In general, it should be possible to be reasonably certain, by a little analysis, and a little running of automated scanning tools, that your system*
> *is not infected with anything else. Investing in a little IDS tool may help*

I disagree that it's a little analysis. Most people don't know what a clean baseline server looks like, so they can't tell what is and isn't suspicious in an IDS log, Vision / Fport / PStools / Netstat results, Tripwire file change log, IIS log, etc. IDS and IIS logs nowadays are full of Code Red and Nimda, port scans, normal traffic, false alarms and other script kiddie stuff, making it hard for a novice to tell what is what.

Also, this depends on your security needs. For a home user, formatting might be excessive. But often you get a post from someone who says, "Help, our company relies on this web server for our well-being." AND, they don't have anyone on staff that can reliably tell whether or not other hacking went on. In that case, I would feel remiss if I didn't try to push them either to a good security consultant or to format and correctly harden the machine.

As you know, security isn't about making your system impenetrable. It's about weighing the financial and business impact of a security risk and of the associated safeguards, and choosing the least costly. The risk of leaving a compromised server on the network includes sniffed passwords and sensitive data and maybe hundreds of thousands of dollars of lost work and IT admin effort, which to me makes formatting the computer start to sound attractive. If nothing else, it lets you document and test the backup and disaster recovery process, which you can guess is also probably lacking here.

> *CompUSA. But this particular attack seems designed only to use your server as*
> *external storage.*

Yeah, that's sort of what I was trying to say too.