

Re: Detecting compromised systems?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-01/0336.html>

From: Mike (michael.owen@hushmail.com)

Date: 01/17/03

From: michael.owen@hushmail.com (Mike)

Date: 17 Jan 2003 04:01:53 -0800

mycorner6@yahoo.com (Michele) wrote in message
news:<3ea7c5a8.0301161150.3c82cf36@posting.google.com>...
> *I am trying to help a company that currently has all their servers and
> desktops directly connected to the Internet. They are unwilling to
> rebuild their machines to move them behind a firewall, but instead
> want to know how to detect which systems may have been compromised,
> and attempt to correct those. If there is a system showing a sign of
> unrecoverable compromise, they are willing to rebuild it.*
>
> *Are there any suggestions for how to detect Windows desktops and
> servers that may have been compromised?*
>
> *Thanks in advance, for the advice and the flames. :-)*
>
> *-Michele*

Do you work for this company or contract? Either way, you'd best explain to them the perils of ignoring corporate best practices with information systems. Not having a firewall is a real liability, not only in security terms, but in legal terms if a court case were ever to arise which questioned the company's IT Security stance.

In terms of finding compromised systems, it can be extremely difficult to guarantee that a system hasn't been compromised. It's rather like being a weapon's inspector – damn difficult to find it when you aren't sure where to look, don't know entirely what you're looking for, and are relying on information being provided by the very system you're suspicious of. File fingerprints and datestamp comparisons against a clean machine brought to the same patch level with the exact same software base sounds like a good start to me.

have fun,
Mike