

Re: strange telnet behavior

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-02/0173.html>

From: Paul Gear (paulgear@bigfoot.com)

Date: 02/22/02

Date: Sat, 23 Feb 2002 07:09:01 +1000
From: Paul Gear <paulgear@bigfoot.com>
To: incidents@securityfocus.com

Gideon Lenkey wrote:

- > *On Tue, 19 Feb 2002, Bryan Andersen wrote:*
- >
- > */* Make a backup. wipe and reload. Then restore your data only.*
- > */* It has been rooted. Telnet should not be doing that at all.*
- >
- > *You really don't have to wipe and reload to recover from this root kit.*
- > *It really doesn't change much. See the instructions in the archive:*
- >
- > <http://online.securityfocus.com/archive/75/249597>

Those instructions may be sufficient for cleaning up the residue of the *attack*, but because it's a root kit, they could have done anything to the system. Unless you know exactly what they've done (which is highly unlikely unless you're running full auditing), standard practice after any root compromise should be to reinstall and restore from backup.

Paul

<http://paulgear.webhop.net>

This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: <http://aris.securityfocus.com>

- **Previous message:** [Robert Graham: "Re: UDP Scan port 53\(dns\) -> dst port <1024"](#)
- **In reply to:** [Gideon Lenkey: "Re: strange telnet behavior"](#)
- **Next in thread:** [tfm@tfm.org: "Re: strange telnet behavior"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)