

Re: ?hack cause?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2002-03/0028.html>

From: Gordon Ewasiuk (gewasiuk@unixfanatic.com)

Date: 03/26/02

Date: Tue, 26 Mar 2002 14:32:20 -0500 (EST)
From: Gordon Ewasiuk <gewasiuk@unixfanatic.com>
To: Andy Gabor <ajgabor@ucdavis.edu>

On Mon, 25 Mar 2002, Andy Gabor wrote:

> *Hi, I think I got hacked but not sure how.*
>
> *Env: Sol8 (all security patches installed – I think), Ultra 10*
>
> *Log:*

<snip restart of inetd>

usual behavior when a bad guy has modified inetd.conf. they restart it.
some even launch a second version...

> *Effect:*
> *1. lost /usr/dt/bin/rpc.cmsd*
> *2. new files /usr/bin/login /usr/bin/.login.*

assume it's been compromised and replace from read-only media. better
yet, dissect it and post it here. =)

> *Checked sunsolve for cmsd alerts – none.*

some older rpc.cmsd notes:

http://www.cert.org/incident_notes/IN-99-04.html

also, heed the other fella's advice. www.chkrootkit.org is good stuff.

finally, do an md5 hash on /usr/bin/login and compare it to:

<http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl>

Sun hit a home run with it's "Fingerprints Database"

<http://www.sun.com/blueprints/0501/Fingerprint.pdf>

Good luck. Rootkits, if it's a rootkit, suck.

Re: ?hack cause?

-gordo

- *Previous message:* Rex Monty di Bona: "Re: ?hack cause?"
- *In reply to:* Andy Gabor: "?hack cause?"
- *Next in thread:* b. nyec: "RE: ?hack cause?"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]