

Re: Trojan/backdoor in fragroute 1.2 source distribution

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-05/0297.html>

From: Dug Song (dugsong@monkey.org)

Date: 05/31/02

Date: Fri, 31 May 2002 12:34:49 -0400

From: Dug Song <dugsong@monkey.org>

To: bugtraq@securityfocus.com

On Fri, May 31, 2002 at 09:55:21AM +0200, Anders Nordby wrote:

> *Although downloading it now seems safe, I think folks should know
> this. The changes done were similar to what happened to irssi, but
> with a different IP.*

monkey.org was compromised on May 14th, via an epic4-pre2.511 client-side hole which produced a shell to one of the local admin's accounts. this was later used to reattach to one of his screen sessions, which apparently had a root window open (su very bad!).

the dsniff-2.3, fragroute-1.2, and fragrouter-1.6 tarballs were all modified at 3 AM on May 17th to include the same configure backdoor as described in the irssi advisory. no other public web content was modified, and the system was restored a week later, from scratch. the correct checksums are:

MD5 (dsniff-2.3.tar.gz) = 183e336a45e38013f3af840bddec44b4

MD5 (fragroute-1.2.tar.gz) = 7e4de763fae35a50e871bdcd1ac8e23a

MD5 (fragrouter-1.6.tar.gz) = 73fdc73f8da0b41b995420ded00533cc

of the 1951 hosts that successfully downloaded one of the backdoored tarballs, 992 of them were Windows machines and 193 were automated ports downloads for the *BSD dsniff or fragrouter ports, leaving 746 Linux (and a few Solaris and MacOS) hosts potentially vulnerable, and 20 FreeBSD and OpenBSD hosts.

we have since migrated our system to OpenBSD-current, importing Niels Provos' excellent systrace subsystem:

<http://www.citi.umich.edu/u/provos/systrace>

which allows us to run all user sessions under a restricted syscall policy (e.g. so an IRC client cannot exec(), open() anything outside ~/.irc, etc.), similar in spirit to Goldberg and Wagner's Janus

SecurityFocus Bugtraq: Re: Trojan/backdoor in fragroute 1.2 source distribution

sandbox, or Cowen's SubDomain.

in the future, our software distributions may carry embedded signatures via gzsigs:

<http://www.monkey.org/~dugsong/gzsigs-0.1.tar.gz>

but for the time being, please be careful what you download, and carefully audit or sandbox any third-party scripts or software you run...

-d.

<http://www.monkey.org/~dugsong/>

- **Previous message:** [uid0@catastrophe.net: "Re: Trojan/backdoor in fragroute 1.2 source distribution"](#)
- **In reply to:** [Anders Nordby: "Trojan/backdoor in fragroute 1.2 source distribution"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)