

Re: fun with posiden rootkit

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-03/0131.html>

From: Dave Dittrich (dittrich@cac.washington.edu)

Date: 03/26/02

Date: Mon, 25 Mar 2002 23:36:33 -0800 (PST)
From: Dave Dittrich <dittrich@cac.washington.edu>
To: Skip Carter <skip@tavgeta.com>

On Mon, 25 Mar 2002, Skip Carter wrote:

> > – *sometimes checking failed script–kiddies can be entertaining if time*
> > *permits to look around for any funny stuff*
>
> *I had one incident that I investigated for a client recently.*
>
> *It was the usual: gain entry, install rootkit, install password*
> *scanner, etc. Except he did it in the wrong order, so that his*
> *password scanner caught his own connection back to his rootkit*
> *archive; so when I started my investigation I was able to log in*
> *to his archive and pick up his entire stash of tools.*

I can't tell you how many times I've seen that over the years,
e.g.:

<http://staff.washington.edu/dittrich/talks/security/case1/hacksniff.txt>

This kind of thing is, according to an Assistant US Attorney, "a slam dunk" violation of the Wiretap statute. With a little correlation of events via timestamps on files and other logins in the sniffer file, you can show a direct link between an intruder, the sniffer, and the "fruits of crime" (the sniffed passwords). If you can get the owner of the site to save a copy for law enforcement (rather than popping in yourself and copying files), there is corroborating evidence from an independant source.

Then again, I've also seen the following:

```
/*  
* dontsniff2.c by XXXXXXXXX (today: 13 Nov 1998)  
* Regards to both XXXXXXX and XXXXXXX ;)  
* Paper:  
* T.Ptacek, T.Newsham "Insertion, Evasion, and Denial of Service: Eluding  
* Network Intrusion Detection," Secure Networks, Inc. January, 1998  
* Greetings to XXX@!#$
```

