

## Re: Exploit or trojan

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2003-12/0007.html>

---

**From:** dav ([dav\\_at\\_r00tworld.com](mailto:dav_at_r00tworld.com))

**Date:** 12/19/03

Date: Fri, 19 Dec 2003 15:36:57 +0100

To: Felipe Franciosi <[ozzybugt@terra.com.br](mailto:ozzybugt@terra.com.br)>

Felipe Franciosi [[ozzybugt@terra.com.br](mailto:ozzybugt@terra.com.br)] a écrit:

> > *Oops.*  
> >  
> > *Such kind of kernel backdoors (e.g. loadable kernel modules) are also*  
> > *present for Solaris, \*BSD and Windows systems. If you are unsure whether*  
> > *someone has compromised your system, don't trust the system's kernel!*  
>  
> *Yeah you are right! I was just reading about coding solaris kernel*  
> *modules. It is pretty easy, actually. Anyone can find a lot of*  
> *documents on google.*  
>  
> *A little addition here: Some Linux backdoors (Suckit, for example)*  
> *doesn't work as a kernel module. It just opens /dev/kmem and patch*  
> *it on the fly. It is still detectable, though, through some imple-*  
> *mentation flaws or checking mechanisms that verify the kernel*  
> *syscall table integrity.*

For solaris systems, you can look at papillon kernel module. This module try to make same than gr-security for linux kernel...

I'm using it on production servers, and I've no trouble to report after one year.

<http://www.roqe.org/papillon/>

dav.

--

PGP: <http://www.r00tworld.com/~dav/dav.gpg>