

Re: Spykids

Source: <http://www.derkeiler.com/Newsgroups/comp.security.unix/2005-07/0044.html>

From: The Doctor (doctor_at_doctor.nl2k.ab.ca)

Date: 07/28/05

Date: Thu, 28 Jul 2005 01:42:49 +0000 (UTC)

In article <MPG.1d52008b4f03a9a6989a7a@news-server.columbus.rr.com>,

Leythos <void@nowhere.lan> wrote:

>In article <dc8ti0\$nld\$2@gallifrey.nk.ca>, doctor@doctor.nl2k.ab.ca

>says...

>> *SPYkids is a known defacer of Web Site. How does one prevent them*

>> *from ever having access to Server or even a LAN?*

>>

>> *Customer complained:*

>>

>> *Spykids should not be able to get into our websites*

>> *regardless of whether they are*

>> *piggy-backing on a member or not. This has happened 2x so far.*

>

>*You need to learn how they are getting in, what measures you can do to*

>*block it and such.*

>

>*First, put the web server behind a dedicated firewall, not a NAT box, a*

>*firewall – only allow real HTTP or HTTPS sessions to it.*

>

>*Require users to have strong passwords, look it up if you don't know*

>*what that means.*

>

>*Block IP networks that don't need access to your web sites – as an*

>*example I block about 50 subnets in countries outside of our own and it*

>*cuts down on a lot of attempts.*

>

I am using pf via OpenBSD. What do I need to add?

--

Member - Liberal International

This is doctor@nl2k.ab.ca Ici doctor@nl2k.ab.ca

God Queen and country! Beware Anti-Christ rising!

Better to serve in Heaven than to Rule in Hell.