

Re: help:site hacked

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2004-07/0003.html>

From: Hernán Castelo (hcastelo_at_cedi.frba.utn.edu.ar)

Date: 06/30/04

Date: Wed, 30 Jun 2004 14:42:20 -0300

it could have been the Download.Ject trojan reported in MS04-011?

```
--
atte,
Hernán Castelo
SGA - UTN - FRBA
"Jonathan Maltz [MS-MVP]" <jmaltz@mvp.org> escribió en el mensaje
news:eBtM2UiXEHA.3516@TK2MSFTNGP09.phx.gbl...
> Hi,
>
> Was OpenBSD kept up to date with all of the latest kernel patches, etc?
> Were the servers behind the BSD box?
>
> Do you still have an image or something of the server when it was hacked?
>
> You mentioned IWAM...Could you have meant IWAP_WWW?
>
> --
> --Jonathan Maltz [Microsoft MVP - Windows Server, Virtual PC]
> http://www.visualwin.com - A Windows Server 2003 visual, step-by-step
> tutorial site :-)
> http://vpc.visualwin.com - Does <insert OS name> work on VPC 2004? Find
out
> here
> Only reply by newsgroup. I do not do technical support via email. Any
> emails I have not authorized are deleted before I see them.
>
>
> "Hernán Castelo" <hcastelo@cedi.frba.utn.edu.ar> wrote in message
> news:uDStO2dXEHA.3716@TK2MSFTNGP11.phx.gbl...
> > i have a firewall openbsd,
> > ( do you mean an app firewall?
> > like ie. norton personal fw )
> >
> > the server was updated
> > with mbsa, had iislockdown, etc
> >
> > IS THERE any way to determine
> > what kind of attack i received ???
> >
> > thanks
> >
> > --
> > atte,
> > Hernán Castelo
```

microsoft.public.windows.server.security: Re: help:site hacked

> > SGA - UTN - FRBA
> >
> > "Jonathan Maltz [MS-MVP]" <jmaltz@mvp.org> escribió en el mensaje
> > news:%23wFoh%23UXEHA.2844@TK2MSFTNGP11.phx.gbl...
> > > Hi,
> > >
> > > Stay up to date on security and other hotfixes
> > > Get some sort of firewall
> > >
> > > That's a good start
> > >
> > > --
> > > --Jonathan Maltz [Microsoft MVP - Windows Server, Virtual PC]
> > > <http://www.visualwin.com> - A Windows Server 2003 visual, step-by-step
> > > tutorial site :-)
> > > <http://vpc.visualwin.com> - Does <insert OS name> work on VPC 2004?
Find
> > out
> > > here
> > > Only reply by newsgroup. I do not do technical support via email.
Any
> > > emails I have not authorized are deleted before I see them.
> > >
> > >
> > > "Hernán Castelo" <hcastelo@cedi.frba.utn.edu.ar>wrote in message
> > > news:%23ERCwhRXEHA.2520@TK2MSFTNGP12.phx.gbl...
> > > hi
> > > someone was hacked my site
> > > i have 2 servers :
> > > web--> IIS 5 / w2k adv Srv IIS lockdown
> > > sql--> SQL2k / w2k adv Srv
> > >
> > > i found the web srv doing "beeps"
> > > soon i found it serves html pages
> > > but don't serves asp with an error like
> > > "Error in the server application"
> > >
> > > sql srv lost sa password
> > > and don't recognize the local admin
> > > then i can't access to sql applications
> > >
> > > except of that,
> > > servers appears to work normal
> > >
> > > the web srv log is saying
> > > that attacked the iwam_
> > > and many "login misses" under DCOMSCM
> > > and then, "login hits"
> > >
> > > i go now to restore
> > > my backup and images
> > > but
> > > what can i do to prevent the next attack ?
> > > how can i protect better the site ?
> > >
> > > thanks
> > >
> > >
> > >
> > > --
> > > atte,

Re: help:site hacked

microsoft.public.windows.server.security: Re: help:site hacked

> > > Hernán
> > >
> > >
> >
> >
> >
>
>