

Re: Anyone seen this before?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-07/0011.html>

From: Sergey Latkin (slatkin@phg.com)

Date: 07/03/02

From: Sergey Latkin <slatkin@phg.com>
To: "Michael B. Morell" <MMorell@vdat.com>
Date: Wed, 3 Jul 2002 11:33:35 -0400

Michael

- > > *It is facing the public*
- > > *so the standard extra precautions have been taken.*
- [and]
- > *This machine is generally locked down both physically and electronically.*
- > *You just can't walk up to the machine and log in. So where ever it came*
- > *from was not installed interactively and is hidden somewhere.*

What did you mean by "it is facing the public"? Showcase display? Public network service? Or it is just connected to Internet as a client w/o firewall?

now, let's go in a different direction. Is the active desktop enabled there? Try to locate shell extensions in the registry. Application name shown in a task mgr is actually a window title/caption and may have no connection with the executable file name. It may be helpful if you can run some debugging/development tool such as MS Spy++ to show all the windows and their processes.

Sergey

On 3 July 2002 10:14, Michael B. Morell wrote:

- > *Thx.... But there is no folder located on that system named 'address', I*
- > *know where you are going with this but it's not the correct path.*
- >
- > *The icon is a generic program icon.*
- >
- > *HC asked – What do you mean by "linked"? What does this mean,*
- > *and what did you do (or what tool did you use) to*
- > *verify or discover this?*
- >
- > *The answer to this is, in task manager, you can right click on any app*
- > *running in the applications window, and choose "go to process".*
- > *The process that I was brought to was explorer.exe.*
- >
- > *If i kill explorer.exe (which get's rid of my desktop as expected) the*

SecurityFocus Incidents: Re: Anyone seen this before?

> address app is also killed. If I start explorer.exe up again, the app
> reappears.
>
> I was unable to find any shell= reference in the registry. No programs
> that even remotely resemble what I am seeing exist on this machine.
>
> This machine is generally locked down both physically and electronically.
> You just can't walk up to the machine and log in. So where ever it came
> from was not installed interactively and is hidden somewhere.
>
>
> -----Original Message-----
> From: Sergey Latkin [mailto:slatkin@phg.com]
> Sent: Tuesday, July 02, 2002 7:15 PM
> To: Michael B. Morell
> Cc: incidents@securityfocus.com
> Subject: Re: Anyone seen this before?
>
>
> Michael
>
> If you open folder named 'address' in explorer, the task mgr will show
> exactly what you described. BTW, what icon was shown next to the app?
>
> Sergey
>
> On 2 July 2002 18:04, Michael B. Morell wrote:
> > I found a odd application running on a 2k server box that I have not seen
> > before, or is at least not
> > obvious to me.
> >
> > In task mgr, The application 'address' (w/o quotes) is running and is
> > linked to the explorer.exe proc.
> >
> > <!--begin the obvious-->
>
> [snip the obvious :]]
>
> > <!--end the obvious-->
> >
> > If anyone has seen this before please let me know. A search on google
> > did not provide
> > any solid leads. I did follow thru on checking for known code
> > red/nimda/things that were
> > close but not really leads.
> >
> > I appreciate any insight from the list.
> >
> > Oh, and please don't bother to tell me to blow away the OS and start from
> > scratch.
> > While I appreciate the suggestion, i'm looking for leads, not the

Re: Anyone seen this before?

SecurityFocus Incidents: Re: Anyone seen this before?

> > *obvious.*

> >

> > *Thanks,*

> >

> > *Mike*

> >

> > -----

> > *\Your mission is to destroy users will to use bandwidth/*

> > -----

>

>

>

> > - *This list is provided by the SecurityFocus ARIS analyzer service.*

> > *For more information on this free incident handling, management*

> > *and tracking system please see: <http://aris.securityfocus.com>*

--

Sergey Latkin
Chief Technology Officer
Pinnacle Health Group
1-(800)-492-7771
slatkin@phg.com
<http://www.phg.com>

This list is provided by the SecurityFocus ARIS analyzer service. For more information on this free incident handling, management and tracking system please see: <http://aris.securityfocus.com>

- **Previous message:** [Michael B. Morell: "RE: Anyone seen this before?"](#)
- **In reply to:** [Michael B. Morell: "RE: Anyone seen this before?"](#)
- **Next in thread:** [george.wasgatt@insurity.com: "RE: Anyone seen this before?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)