

SecurityFocus Incidents: Closed thread– Anyone seen this before?

Closed thread– Anyone seen this before?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-07/0015.html>

From: Michael B. Morell (MMorell@vdat.com)

Date: 07/03/02

From: "Michael B. Morell" <MMorell@vdat.com>
To: "'dbrain@lewisellis.com'" <dbrain@lewisellis.com>
Date: Wed, 3 Jul 2002 14:39:26 -0400

I would like to thank David Brain for his insight on this one.

It turns out that it was **not** an exploit at all. Let's just say **user error**.

The confusion was in the fact that the address bar that can be called up on the toolbar was **HIDDEN** underneath/behind the regular toolbar. Making it so that I could not see it.

I moved the normal tool bar at the bottom of the screen and lo and behold, there was the address window.

So it was technically on the desktop, which is why it showed up as an app and why it was linked to explorer.exe and also why it had a desktop handle.

My apologies to the community for the wild goose chase. I do appreciate everyone's suggestions.

Now the question is, who was at the server while I was on my hiatus! But that is for me to find out.

Thanx again,

Mike

Now back to more important things like harassing users and playing UT. And not in that order.

-----Original Message-----

From: David Brain [<mailto:dbrain@lewisellis.com>]

Sent: Wednesday, July 03, 2002 1:16 PM

To: 'Michael B. Morell'

Subject: RE: Anyone seen this before?

Closed thread– Anyone seen this before?

SecurityFocus Incidents: Closed thread– Anyone seen this before?

Hi,

I make it go away by closing the window – I get a little window that just has the word 'Address' a text entry box and a little IE style 'Go' icon.

However on moving it around further it seems like it is possible to make the window 'hide' behind the task bar and or 'dock' to the top/left/right of the screen and still show the 'Address' app in task manager.

Killing it in Task Manager kills explorer, which at least on my machine then restarts itself with much flickering of icons.

This is all on a Win2k Pro SP2 box.

David.

> -----Original Message-----
> From: Michael B. Morell [mailto:MMorell@vdat.com]
> Sent: Wednesday, July 03, 2002 12:00 PM
> To: 'dbrain@lewisellis.com'
> Subject: RE: Anyone seen this before?
>
>
> Could be.....
>
> It sounds right.....
>
> Can you get it to go away? What happens if you kill the
> address app in tsk
> mgr? Does it come back?
>
> -----Original Message-----
> From: David Brain [mailto:dbrain@lewisellis.com]
> Sent: Wednesday, July 03, 2002 12:30 PM
> To: 'Michael B. Morell'
> Subject: RE: Anyone seen this before?
>
>
> Hi,
>
> I can reproduce this by adding an Address bar to my toolbar, and the
> 'tearing' it
> off. I get a generic looking app called address in
> Taskmanager, the process
> is
> explorer.exe.
>
> Not sure if this is any use to you, but thought it might help.

Closed thread– Anyone seen this before?

SecurityFocus Incidents: Closed thread– Anyone seen this before?

>
> David.
>
>> -----Original Message-----
>> From: Michael B. Morell [mailto:MMorell@vdat.com]
>> Sent: Wednesday, July 03, 2002 9:15 AM
>> To: 'Sergey Latkin'
>> Cc: incidents@securityfocus.com
>> Subject: RE: Anyone seen this before?
>>
>>
>> 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
>> 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?
>>
>>

Closed thread– Anyone seen this before?

SecurityFocus Incidents: Closed thread– 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 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*

Closed thread– Anyone seen this before?

SecurityFocus Incidents: Closed thread– Anyone seen this before?

> > > *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>*

> >

> >

>

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:** [Sergey Latkin: "Re: Additional– Anyone seen this before?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)