

RE: strange windows behaviour.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-10/0040.html>

From: J Mike Rollins (*rollins_at_wfu.edu*)

Date: 10/09/03

Date: Thu, 9 Oct 2003 11:12:55 -0400 (EDT)

To: "Schmehl, Paul L" <pauls@utdallas.edu>

I have just tested the ideas expressed here and have to report that streams can still be a threat.

When I try to make a copy of the dll stored within the stream, the virus scanning software does find it.

However, when I run the contents of the dll stream by using rundll32 the program is not caught by the virus scanning software. And the trojan continues to execute undetected.

So, I believe this to be a serious threat.

On Wed, 8 Oct 2003, Schmehl, Paul L wrote:

> > -----Original Message-----
> > From: J Mike Rollins [*mailto:rollins@wfu.edu*]
> > Sent: Wednesday, October 08, 2003 12:46 PM
> > To: *incidents@securityfocus.com*
> > Subject: *Re: strange windows behaviour.*
> >
> >
> >
> > *One trick that hackers are exploiting is to store executable*
> > *files as NTFS Streams. You should check you registry for*
> > *programs set to run at startup with the following format*
> >
> > *rundll32.exe C:\Some\Directory:trojan.dll*
> >
> > *The : in front of the trojan signifies that the file is*
> > *really an NTFS Stream. Trojans stored in this format may not*
> > *be detected by many virus scanners.*
> >
> > *There's been a lot of discussion about this amongst av professionals.*
> > *There's really no advantage to scanning streams because they are*
> > *"inert". In order for the trojan to do anything, it has to "come out of*
> > *hiding" as it were, and when it does, av on access scanning will detect*

SecurityFocus Incidents: RE: strange windows behaviour.

- > *it **if it's a known trojan**. While it's in the stream it's merely in*
- > *storage, not being used.*
- >
- > *Paul Schmehl (pauls@utdallas.edu)*
- > *Adjunct Information Security Officer*