

Re: non-paged memory inside a kernel driver

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2008-04/msg00142.h>

- *From:* "Alexander Grigoriev" <alegr@xxxxxxxxxxxxx>
 - *Date:* Thu, 3 Apr 2008 07:20:56 -0700
-

I've seen kernel memory leaks up to full memory exhaustion when Symantec AV was present on the system.

"Don Burn" <burn@xxxxxxxxxxxxxxxxxxxxx> wrote in message news:uNvmlNYIIHA.1212@xxxxxxxxxxxxxxxxxxxxxxxxx

My complaints with Symantec are:

1. Hooking of system calls and in some cases modifying the actions in ways against the spec. Sorry do no harm is the first rule of software.
2. Inserting themselves in the storage stack, then selectively skipping drivers below them (and in some versions with hooking drivers above them). Gee no one elses filter works, because Symantec owns the machine.
3. Disabling their code on detection of a kernel debugger, so that you cannot easily prove #1 and #2 above.
4. Having multiple times opened security holes with their product, and not informed the customers when they did.

As someone who has had to debug file system filters in the presence of SymanCRAP I urge everyone I know to avoid them like the plague. Their protests to the EU about Microsoft blocking hooking (and therefore the Symantec product) was to me proof they care more about profit than a product that works.

--
Don Burn (MVP, Windows DDK)
Windows 2k/XP/2k3 Filesystem and Driver Consulting
Website: <http://www.windrvr.com>
Blog: <http://msmvps.com/blogs/WinDrvr>

"David Craig" <drivers@xxxxxxxxx> wrote in message news:ucPIhaSIIHA.5160@xxxxxxxxxxxxxxxxxxxxxxxxx

Re: non-paged memory inside a kernel driver

I like Symantec. I get it at work and it is not that bad of a load on the system. Some versions have been a little excessive, but newer versions are better. Every one of them will make mistakes or design decisions that have a direct impact on some of us. You have to decide which impact you can live with or are you bold and don't want any antivirus or other protection. None are light in weight on the system and can't really be and get the job done with all the attacks being developed. There are much better programmers working on the virus, trojan, etc. software than ever before since a lot of money can be made without any criminal liability. Many are in countries where there is no civil liability either and that means they can write the 'toolkits' for the crooks to use.

I do not work for Symantec and have no current relationship with them other than as a customer. I usually buy any Norton stuff at Fry's when it is on sale with rebates equal to the purchase price. For the cost of sales tax and a couple of stamps, I get new versions without having to pay their renewal rates. I like them, but I won't give my money away if I don't have to do so.

"Don Burn" <burn@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:%23G6xG%23QIHA.4536@xxxxxxxxxxxxxxxxxxxxxx

Yes that is why a number of consider it MALWARE instead of anti-MALWARE.

It is ironic that the big names McAfee, Symantec and Trend Micro all produce products that do more harm than good.

--

Don Burn (MVP, Windows DDK)
Windows 2k/XP/2k3 Filesystem and Driver Consulting
Website: <http://www.windrvr.com>
Blog: <http://msmvps.com/blogs/WinDrvr>
Remove StopSpam to reply

"usfinecats" <usfinecats@xxxxxxxxxxxx> wrote in message
news:295661B1-20D3-4C46-BDB7-0A4DF047ED5A@xxxxxxxxxxxxxxxxxx

If you look at Trend Micro's PC-cillan product, and run poolmon you'll discover they suck up ~80MBs and never release it (on XP) that's enough to hose my application.

With their stuff running I cannot allocate 10 MB 's on a XP system. I don't

Re: non-paged memory inside a kernel driver

crash, but then again I cannot perform my tasks.

--

Gak -
Finecats

"krish" wrote:

Hi Doron, There is just one instance of the driver and it will be loaded during the windows startup. I have two devices one rotating disk and one flash. In my driver I keep a table map which tells me what data is in the flash and what is in the disk, using which I direct the request to either flash or disk. The size of this table is big, around 100MB. I do not want this table to ever page out to disk./ flash, so I need 100MB of non-paged memory inside my driver. Do you have any suggestions?

On Mar 31, 2:22 pm,
"Doron Holan [MSFT]"
<dor...@xxxxxxxxxxxxxxxxxxxxxx>
wrote:

you will not get such a number. let's say 20 instance of such a driver was loaded and the number was 10%. then at least half of them would not

Re: non-paged memory inside a kernel driver

be able
to load.
moreover, it
depends on
the state of
system
memory
when
you try to
allocate
memory,
the virtual
address
space has to
have a big
enough
gap
(e.g. it is
not
fragmented)
to fit your
allocation.

what are
you going
to do with
the memory
once you
have
allocated it?

d
--
Please do
not send
e-mail
directly to
this alias.
this alias is
for
newsgroup
purposes
only.
This posting
is provided
"AS IS"
with no
warranties,
and confers
no
rights.

Re: non-paged memory inside a kernel driver

"krish"
<pradeep_bi...@xxxxxxxx>
wrote in
message

news:551587ae-46e4-49bb-bb70-06900bca6125@xxxxxxxxxxxxxxxx

Hi
Don,
large
is
kind
of
relative
term
:-).
Would
you
suggest
any
number
in
terms
of
percentage
of
the
available
memory
like
10%,
20%
etc
which
you
think
is
safe
enough?
Or
from
your
experience,
what
is
the
largest
amount
that

Re: non-paged memory inside a kernel driver

Re: non-paged memory inside a kernel driver

you
have
seen
in
a
well
performing
kernel
mode
driver?
Thanks.

On
Mar
31,
2:01
pm,
"Don
Burn"
<b...@xxxxxxxxxxxxxxxxxxxxxx>
wrote:

Pre-Vista
it
is
128MB,
but
even
in
Vista
doing
a
large
allocate
is
a
really
bad
idea,
since
then
the
rest
of
the
system
will
be
starved,

Re: non-paged memory inside a kernel driver

and
likely
to
crash.

--
Don
Burn
(MVP,
Windows
DDK)
Windows
2k/XP/2k3
Filesystem
and
Driver
Consulting
Website:<http://www.windrvr.com>
Blog:<http://msmvps.com/blogs/WinDrvR>
Remove
StopSpam
to
reply

"krish"
<pradeep_bi...@xxxxxxxx>
wrote
in
message

news:a4bc5006-05a9-4340-8e3c-b7a2ca72cf76@x

Hi,
what
is
the
maximum
size
of
non-paged
memory
that
I

Re: non-paged memory inside a kernel driver

can
allocate
inside
inside
my
kernel
driver
in
XP
and
Vista?
I
took
the
diskperf
from
WDK,
modified
it
and
on
Vista,
32-bit,
2GB
RAM,
I
tried
allocating
4/8/100/512
MB
and
I
was
able
to
do
it
successfully
while
allocating
1GB
and
above
failed.
Is
there
any
hard
restriction
on
the

Re: non-paged memory inside a kernel driver

amount
of
non-paged
memory
I
can
allocate
inside
my
driver?

Thanks
in
anticipation.