

Re: Hacktool.Rootkit ??

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2007-06/msg00007.html>

- *From:* DBLWizard <ibflyfishin@xxxxxxxxxx>
 - *Date:* Fri, 01 Jun 2007 07:13:47 -0700
-

Thanks for pointing out things that I did forget to include in my initial post ...

Windows Server 2003 Service Pack 1
Norton AntiVirus Corp Edition 7.60.962
Virus Definition File: Version 5/31/2007 rev. 19

This server is connected to the internet behind a Linksys Wireless G Router with ports 21, 80 forwarded to it.

But you are still being obscure. What issues do seem to think that I have with the way that Norton operates? Are you telling me that these entries in the History are normal and to be expected?

Thanks

dbl

On Jun 1, 2:04 am, "Phil Weldon" <not.disclo...@xxxxxxxxxxxxx> wrote:

'DBLWizard' wrote, in part:
| Phil, Do you spend time on these groups just to try and insult people
| or is there a purpose to your ramblings.

Gee, what was not instructive in my post?
I thought it was pretty straightfoward.

I am glad you have decided to download and use the script and collection of antimalware scanners 'David H. Lipman' posted, but issues you have with the operating characteristics of Norton AntiVirus are best resolved with the publisher; I suggest you try 'Live Chat' available through http://www.symantec.com/home_homeoffice/support/selectproduct_ts.jsp.

You posted a request for help; the more work you do yourself before posting the easier it will be for a newsgroup participant to help.
An example of additional useful information you might have posted would be the VERSION of Norton Antivirus and the update state, and perhaps the Operating System used on the 'development server' and its interconnectivity.

Re: Hacktool.Rootkit ??

Phil Weldon

"DBLWizard" <ibflyfis...@xxxxxxxx> wrote in message

news:1180675534.783286.297370@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

| Phil, Do you spend time on these groups just to try and insult people
| or is there a purpose to your ramblings.

|
| I concluded that I "Might" have the Hacktool.Rootkit because that is
| what I got from Symantec's website when I did a search of their virus
| database.

|
| I posted the complete list because I thought it might be important ...
| figured that those that knew enough about these things could ignore
| what wasn't important.

|
| And as for reading the manual ... what manual ... I did look through
| the help files and could find no reason why I would have all these
| entries show up in my "Virus History" especially at the same time
| every night and none of the files that it says it "left alone" could
| be found anywhere on the system.

|
| If I'm ignorant then forgive me and educate me. If you have nothing
| instructive to say then shut up and sit down.

| dbl

|
| On May 31, 9:03 pm, "Phil Weldon" <not.disclo...@xxxxxxxx> wrote:

| > 'DBLWizard' wrote, in part:

| > | I am looking for a little help here. I think one of my Development
| > | servers is infected with Rootkit possibly called Hacktool.Rootkit.

| > | The reason I say this is I have Norton Antivirus Corp Edition
| > | installed and every night @ 12:03 for 2 minutes or if I do a "Scan
| > | Computer" I get the following entries in the log but no prompts or
| > | anything.

| > |
| > | Is there anyway to actually remove this or do I just need to rebuild
| > | this system?

| > |
| > | Here are the entries in the log:

| > .
| > .
| > 5/31/2007 14:59 regger.exe Hacktool File Left alone REVELATIONS SYSTEM
| > C:\WINDOWS\system32\ Infected C:\WINDOWS\system32\ Clean virus from
| > file Leave alone (log only) Manual scan

| > .
| > .
| > _____
| >

| > Was it really necessary to post ALL the duplicate Swen worm log entries?

Re: Hacktool.Rootkit ??

|> That worm hasn't been active for four years. As for your concern about
|> 'Hacktool.Rootkit', the log you posted does not include that finding;
what
|> Symantec identifies as 'Hacktool' is NOT the same as 'Hacktool.Rootkit',
and
|> is not viral. Symantec identifies 'Hacktool' as generic for tools that
can
|> be used to attack OTHER systems.
|>
|> You now have the 'sourmilk' problem. Since the question has been raised
of
|> possible infection, by all means follow the suggestions posted by 'David
H.
|> Lipman'. And you might want to contact Symnatec also (and possibly read
the
|> manual.)
|>
|> Phil Weldon
|>
|> "DBLWizard" <ibflyfis...@xxxxxxxx> wrote in message
|>
|> news:1180646048.620294.106330@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
|> | Howdy,
|> |
|> | I am looking for a little help here. I think one of my Development
|> | servers is infected with Rootkit possibly called Hacktool.Rootkit.
|> | The reason I say this is I have Norton Antivirus Corp Edition
|> | installed and every night @ 12:03 for 2 minutes or if I do a "Scan
|> | Computer" I get the following entries in the log but no prompts or
|> | anything.
|> |
|> | Is there anyway to actually remove this or do I just need to rebuild
|> | this system?
|> |
|> | Here are the entries in the log:
|> |
|> | Date Filename Virus Name Virus Type Action Taken Computer User
|> | Original Location Status Current Location Primary Action Secondary
|> | Action Scan Type
|> | 5/31/2007 14:59 tmp.edb IRC.Family.Gen File Left alone REVELATIONS
|> | SYSTEM C:\WINDOWS\SoftwareDistribution\DataStore\Logs\ Infected C:
|> | \WINDOWS\SoftwareDistribution\DataStore\Logs\ Clean virus from file
|> | Leave alone (log only) Manual scan
|> | 5/31/2007 14:59 pack1771.exe W32.Swen.A@mm File Left alone REVELATIONS
|> | SYSTEM C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Infected C:
|> | \DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Clean virus from file
|> | Leave alone (log only) Manual scan
|>
|> <additional W32.Swen.A@mm snipped as redundant>
|>
|> 5/31/2007 14:59 regger.exe Hacktool File Left alone REVELATIONS SYSTEM

Re: Hacktool.Rootkit ??

|> C:\WINDOWS\system32\ Infected C:\WINDOWS\system32\ Clean virus from
|> file Leave alone (log only) Manual scan
|> 5/31/2007 14:59 pack1771.exe W32.Swen.A@mm File Left alone REVELATIONS
|> SYSTEM C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Infected C:
|> \DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Clean virus from file
|> Leave alone (log only) Manual scan
|> 5/31/2007 14:59 pack1771.exe W32.Swen.A@mm File Left alone REVELATIONS
|> SYSTEM C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Infected C:
|> \DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Clean virus from file
|> Leave alone (log only) Manual scan
|> 5/31/2007 14:59 mspool.exe Backdoor.Usirf File Left alone REVELATIONS
|> SYSTEM C:\WINDOWS\system32\ Infected C:\WINDOWS\system32\ Clean virus
|> from file Leave alone (log only) Manual scan
|>
|> <additional W32.Swen.A@mm snipped as redundant>
|>
|> | 5/31/2007 14:58 MSOffExport[1].exe Trojan Horse File Left alone
|> | REVELATIONS SYSTEM P:\CDrive\Documents and Settings\Default User\Local
|> | Settings\Temporary Internet Files\Content.IE5\O9AVGDQZ\ Infected P:
|> | \CDrive\Documents and Settings\Default User\Local Settings\Temporary
|> | Internet Files\Content.IE5\O9AVGDQZ\ Clean virus from file Leave alone
|> | (log only) Manual scan
|> | 5/31/2007 14:58 MSOffExport[1].exe Trojan Horse File Left alone
|> | REVELATIONS SYSTEM P:\CDrive\Documents and Settings\ASPNET\Local
|> | Settings\Temporary Internet Files\Content.IE5\O9AVGDQZ\ Infected P:
|> | \CDrive\Documents and Settings\ASPNET\Local Settings\Temporary
|> | Internet Files\Content.IE5\O9AVGDQZ\ Clean virus from file Leave alone
|> | (log only) Manual scan
|> | 5/31/2007 14:58 MSOffExport[1].exe Trojan Horse File Left alone
|> | REVELATIONS SYSTEM P:\CDrive\Documents and Settings\sshadmin\Local
|> | Settings\Temporary Internet Files\Content.IE5\O9AVGDQZ\ Infected P:
|> | \CDrive\Documents and Settings\sshadmin\Local Settings\Temporary
|> | Internet Files\Content.IE5\O9AVGDQZ\ Clean virus from file Leave alone
|> | (log only) Manual scan
|> | 5/31/2007 14:58 pack1771.exe W32.Swen.A@mm File Left alone REVELATIONS
|> | SYSTEM C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Infected C:
|> | \DOCUME~1\ADMINI~1\LOCALS~1\Temp\ActiveSync\ Clean virus from file
|> | Leave alone (log only) Manual scan
|>
|> <additional W32.SWEN.A@mm entries snipped as redundant>
|
|