

Re: hacktool.rootkit

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-10/0284.html>

From: Scherbina Vladimir ([vladimir.scherbina\[anti-spam\]gmail.com](mailto:vladimir.scherbina[anti-spam]gmail.com))

Date: 10/22/05

Date: Sat, 22 Oct 2005 10:45:00 +0300

In addition to "what is a rootkit".

There is an interesting article where author explains how to create rootkits and how to detect them,

http://www.security.org.sg/code/SIG2_DefeatingNativeAPIHookers.pdf

The problem is that rootkit usually implemented as a driver, that hooks windows api in kernel mode.

You may think that you've deleted some "bad" file, or registry value, but actually not – driver just hooked CreateFile(A,W), RegCreateKey(Ex), RegOpenKey(Ex) and returns invalid values for a "needed" file, registry value.

Another problem is that removing rootkit is unsafe operation. One may write a driver that should restore Service Dispatch Table, or perform restoring in user mode using \device\physicalmemory.

There are no guranties that all will be removed successfully, so you need cross you fingers and hope everything will be ok, and OS would not fall into bluse screen of death.

--

Scherbina Vladimir.

"Shawn E. Hale" <SEHale@NOSPAMcomcast.net> wrote in message news:uNEZEmk1FHA.3180@TK2MSFTNGP14.phx.gbl...

> Thanks to you guys who replied with a wealth of advice and information. I
> appreciate that and the patience you have taken.

>

> There is a lot to work through but so far, in addition to what I already
> listed, I did the things that were suggested in the Symantec site (re:
> safe

> mode virus scanning, registry entry purging, etc.). I also ran the Panda
> and Micro Trend online scans, safe mode virus scanning, system restore
> purging and turning back on, deleting temp files, and checking the
> downloaded applications folder. I also checked the running services and
> if

> I could not identify something, I googled it to see what it was.

> Everything

> was clean with no infected files and no bad services. I am leaning
> towards

> believing that I had initially wiped it out and the latest Symantec
> definitions caught an orphan. I was able to find a list of what was in
> the

microsoft.public.security.virus: Re: hacktool.rootkit

```
> Symantec definitions that were downloaded on 10/19 and there was a piece
> that looked for the SVKP.sys file. Since I am not having any other slow
> downs and issues, I think I have it beat. I will get to Mr. Lipman's
> advice
> this weekend.
>
> Thanks again.
>
>
> "David H. Lipman" <DLipman-nospam~@Verizon.Net> wrote in message
> news:uDFBPBc1FHA.2792@tk2msftngp13.phx.gbl...
>> From: "Shawn E. Hale" <SEHale@NOSPAMcomcast.net>
>>
>> | I am trying to be as detailed about this as I can. Sorry if it is too
> long
>> | but I figure more info is better than less. Using a new Dell laptop
> with XP
>> | Home, SP2 and all updates. Norton Antivirus 2005 installed and set for
>> | automatic updates. It is also set for real time (constant) scanning.
>> |
>> | 2 weeks ago (10/3/05) my daughter was using AOL IM when someone
>> | inadvertently sent her a link which she followed and ran. Immediately
> all
>> | of her other buddies on IM got the same link from her even though she
> didn't
>> | manually forward it. Sensing something was wrong, she disconnected
>> from
> the
>> | IM. Norton Antivirus reported the following:
>> |
>> | Auto-Protect, Hacktool.rootkit, Access Denied. Source:
>> | c:\windows\system32\msdirectx.sys
>> | Auto-Protect, Hacktool.rootkit, Repair failed. Source:
>> | c:\windows\system32\msdirectx.sys
>> |
>> | I did some research and deleted all references in the registry, and all
>> | files relative to, lock1.exe, xz.bat, and msdirectx.sys (although that
>> | particular file was not found). I found a lock1 exception added to my
>> | Windows firewall so I removed that. I rebooted several times, ran
> various
>> | online virus scanners and Norton antivirus numerous times and all
>> seemed
> to
>> | be fine. No error messages, no computer slowdowns, no vulnerabilities
>> | according to Shields Up!. Nothing odd looking in the MSCONFIG startup.
>> |
>> | Yesterday, 10/19/05, Norton Antivirus downloaded the latest definitions
> and
>> | I came home to find this pop-up warning from Norton (no one had been on
> the
>> | computer all day and it was fine when I left in the morning):
>> |
>> | Virus scanner, Hacktool.rootkit, Quarantined file, Virus Source:
>> | C:\windows\system32\svkp.sys. (A related registry key was also
> removed).
>> | The virus definitions date that found this problem was 10/19/05.
>> |
>> | I did some more research and found that SVKP.sys may be a legitimate
> file,
>> | or it may not (depending on the source). There were registry entries
> for
>> | Legacy_SVKP which I deleted. Rebooted several times, ran Norton full
```

microsoft.public.security.virus: Re: hacktool.rootkit

```
> virus
>> | scan a few times, no problems or error messages.
>> |
>> | Here are my questions/concerns:
>> |
>> | In the original Norton message about msdirectx, what does it actually
> mean
>> | "repair failed" and "access denied." Is that a good thing that Norton
>> | stopped it or is it a bad thing that Norton didn't catch it in time?
>> |
>> | Would I be correct in assuming that the new virus definitions
>> downloaded
> on
>> | 10/19 simply found a remnant of the original hacktool.rootkit and
> scrubbed
>> | it out OR is this thing still in my system and somehow regenerating
> itself?
>> |
>> | If it is regenerating itself, should I really be too concerned or is it
> more
>> | of an annoyance? We have the XP firewall running and WEP encryption on
> our
>> | home wifi network.
>> |
>> | I don't want to go thru the process of re-formatting and re-installing
> if I
>> | don't have to. I guess I am looking for confirmation of my suspicion
> that
>> | the new anti-virus definitions took out a remnant/orphan of the
>> original
>> | problem and that since I am having no other problems (before or now
> after),
>> | I am OK. Am I just wishful thinking?
>> |
>> | Thanks for any advice.
>> |
>>
>> Shawn:
>>
>> Please excute; %SystemRoot%\system32\services.msc
>>
>> Then examine *all* services. Look for NON Microsoft services with
>> oddball
> names.
>> Lsets say that you find a service called; meaoi
>>
>> Use the Resource Kit utility, DELSRV.EXE, and execute; delsrv meaoi
>> Reboot and then scan the system using the following Multi AV scanning
> tool.
>>
>> I posted the DELSERV.EXE utility in a ZIP file...
>>
>> Post Subject: DELSRV for Hacktool.Rootkit
>> Posted in: alt.binaries.comp.virus
>>
>>
>> Download MULTI_AV.EXE from the URL --
>> http://www.ik-cs.com/programs/virtools/Multi\_AV.exe
>>
>> It is a self-extracting ZIP file that contains the Kixtart Script
> Interpreter {
>> http://kixtart.org Kixtart is CareWare } 4 batch files, 6 Kixtart
```

microsoft.public.security.virus: Re: hacktool.rootkit

```
>> scripts,
> one Link
>> (.LNK) file, a PDF instruction file and two utilities; UNZIP.EXE and
> WGET.EXE. It will
>> simplify the process of using; Sophos, Trend, Kasperski and McAfee Anti
> Virus Command
>> Line Scanners to remove viruses, Trojans and various other malware.
>>
>> C:\AV-CLS\StartMenu.BAT -- { or Double-click on 'Start Menu' in
>> C:\AV-CLS}
>> This will bring up the initial menu of choices and should be executed in
> Normal Mode.
>> This way all the components can be downloaded from each AV vendor's web
> site.
>> The choices are; Sophos, Trend, McAfee, Kaspersky, Exit this menu and
> Reboot the PC.
>>
>> You can choose to go to each menu item and just download the needed files
> or you can
>> download the files and perform a scan in Normal Mode. Once you have
> downloaded the files
>> needed for each scanner you want to use, you should reboot the PC into
> Safe Mode [F8 key
>> during boot] and re-run the menu again and choose which scanner you want
> to run in Safe
>> Mode. It is suggested to run the scanners in both Safe Mode and Normal
> Mode.
>>
>> When the menu is displayed hitting 'H' or 'h' will bring up a more
> comprehensive PDF help
>> file.
>>
>> To use this utility, perform the following...
>> Execute; Multi_AV.exe { Note: You must use the default folder C:\AV-CLS }
>> Choose; Unzip
>> Choose; Close
>>
>> Execute; C:\AV-CLS\StartMenu.BAT
>> { or Double-click on 'Start Menu' in C:\AV-CLS }
>>
>> NOTE: You may have to disable your software FireWall or allow WGET.EXE to
> go through your
>> FireWall to allow it to download the needed AV vendor related files.
>>
>> * * * Please report back your results * * *
>>
>>
>> --
>> Dave
>> http://www.claymania.com/removal-trojan-adware.html
>> http://www.ik-cs.com/got-a-virus.htm
>>
>>
>
>
```