

Re: VX2 – My Victory!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-08/0438.html>

From: boaz (nospam_at_yahoo.com)

Date: 08/31/05

Date: Tue, 30 Aug 2005 17:35:01 -0700

I think you can use CACLS.EXE to set the Access Control List in XP Home. Never try it though.

You can also move the users in XP Home to the Power Users group instead of the default Admin group.

"Michael Herchel bbi-cm.com" <mike@[at]> wrote in message news:%23PL8nKWrfHA.3792@TK2MSFTNGP10.phx.gbl...
> I always found out that a really good way to get rid of crap like that is
> to remove all NTFS file permissions to that file (even for yourself and
> system account). Then just reboot, and the program will not have permission
> to run.

>
> Of course, you need to be running XP pro to do this

>
>
>
> "bz" <nospam@yahoo.com> wrote in message
> news:OgHQX3SrFHA.2540@TK2MSFTNGP09.phx.gbl...

>> Hi,

>>

>> Couple posts below, I was having problem with an unknown VX2 spyware. I
>> have tried everything but nothing works.

>> After couple hours of intense fighting, I finally got rid of this stupid
>> crap!

>>

>> First of all, nothing will work. So, don't waste your time running any
>> of the spyware in Safe Mode or whatsoever.

>>

>> This is how this VX2 crap works:

>>

>> 1)

>> It adds an registry entry in this key:

>> ...Mircrosft\Windows NT\Current Version\Winlogon\Notify\CSCSettings

>>

>> By looking at this key, it seems to me that everytime you logon or
>> logoff, it will call a DLL. And you can't delete that file with any of
>> the scanners becasue it is IN-USED. (Thanks XP!!!)

>>
>> *Of course, by my Volcan logic, this DLL must be the source of the*
>> *spyware. It must be the one doing the recreation of the same file.*
>>
>> *Since everytime you delete this file, it somehow recreates another one in*
>> *the System32 folder. Logic dictates that the running DLL must be copying*
>> *a hidden file hiding somewhere. Since it is hidden, there is no point to*
>> *hunt it down. Even you hunt it down, the running process will probably*
>> *recreate another one somewhere.*
>>
>> 2)
>> *Now this is another interesting Volcan logic. If it copies another file*
>> *to a new file, the file size of both files must be the same.*
>>
>> *Doing a DIR /S (and ATTRIB) will show you that there are a whole bunch of*
>> *the hidden files with different file names but with the exact same file*
>> *size. The file size is 417792.*
>>
>> *By looking at these files for couple hours, there is a patent. The file*
>> *names are not random. It looks at the files before and after it, and*
>> *then it creates the file name from the two files.*
>>
>> *For example if you have these two files:*
>> *Expand.DLL*
>> *Explorer.DLL*
>> *It will add a file: Expbnf.DLL right in between these two files. This*
>> *make the file look legit. The most interesting thing is that all the*
>> *file are DLL except one. There is one file called GUARD.TMP. This must*
>> *be the initial infestation!!!!*
>>
>> 3)
>> *I have tried but after couple hours, I finally realize that there is no*
>> *way to delete all these files by hand. There are hundred of these*
>> *depending how many times you login and logout over the past... huh...*
>> *since you got this spyware! SO DON'T BOTHER TO DELETE THE FILES.*
>>
>> 4)
>> *So, I fire Norton Antivirus to see what happens. Lucky Me! Norton*
>> *reports that there are TWO files among these hundreds of files that it is*
>> *not able to scan because these two files are IN-USED. Ah-HAAA!!!!*
>> *Bullseye!*
>>
>> 5)
>> *War is almost over!!!*
>> *I search the registry for these two files. Deleted couple of registry*
>> *keys. I DID NOT RESTART THE COMPUTER. DO NOT RESTART THE COMPUTER.*
>> *Remember there is something hooked to the login/logout thing. I PULL THE*
>> *POWER CORD instead.*
>>
>> 6)
>> *I restart my computer with the XP CD. Get into the Recovery Console.*

>> *And then deleted the two specific files.*
>>
>> 7)
>> *After I reboot, somehow the registry comes back. BUT Adaware does not
>> find any VX2. YES!!! There must be something else that is writing the
>> registry back. Now this is another Volcan logic. If the two active
>> files have already been removed, there must be another 3rd file
>> responsible to written the registry back.*
>>
>> 8)
>> *War is over!*
>> *I run the Task Manager to see if there is any strange looking running
>> process. Ah HAA! There is one called POLETMGR.EXE. Everytime I try to
>> end this process, it pops right back in. I figure out that I can safely
>> remove this file because when I end this process, it restarts itself
>> with the same POLETMGR name; not something random. Interestingly, I
>> don't find any reference in the registry. I guess this guy is just a one
>> time thing.*
>>
>> 9)
>> *I reboot from the XP CD and to the Recover Console. Deleted this POLE
>> something file.*
>>
>> 10)
>> *Victory!!!*
>> *Run Adaware and M\$ Antispyware to clean out whatever that is left.*
>>
>> 11)
>> *Yes! Done!!! Nada spyware!!! No strange process running!!!*
>>
>>
>> *Hope this helps!!!*
>>
>> *P.S. I still have hundred of those DLL sitting in my hard disk. Not one
>> single Antivirus or spyware scanner can recognize them. So, if you want
>> some, drop me a mail. ;)*
>>
>>
>>
>>
>
>