Rootkit.TmpHider | Wilders Security Forums

Thread Status:

Not open for further replies.

Page 1 of 16
1 ← 2 3 4 5 6 → 16 Next >

1. Modules of current malware were first time detected by "VirusBlokAda" (http://anti-virus.by/en/) company specialists on the 17th of June, 2010 and were added to the anti-virus bases as **Trojan-Spy.0485** and **Malware-Cryptor.Win32.Inject.gen.2**. During the analysis of malware there was revealed that it uses USB storage device for propagation.

   You should take into consideration that virus infects Operation System in unusual way through vulnerability in processing lnk-files (without usage of autorun.inf file).

   So you just have to open infected USB storage device using Microsoft Explorer or any other file manager which can display icons (for i.e. Total Commander) to infect your Operating System and allow execution of the malware.

   Malware installs two drivers: mrxnet.sys and mrxcls.sys. They are used to inject code into systems processes and hide malware itself. That's the reason why you can't see malware files on the infected USB storage device. We have added those drivers to anti-virus bases as **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2**. Note that both drivers are signed with digital signature of Realtek Semiconductor Corp. (www.realtek.com).

   Thus, current malware should be added to very dangerous category causes the risk of the virus epidemic at the current moment.

   After we have added a new recordes to the anti-virus bases we are admitting a lot of detections of **Rootkit.TmpHider** and **SScope.Rookit.TmpHider.2** all over the world.

   Source: http://anti-virus.by/en/tempo.shtml

2. **@sergey ulasen**

   Thanks for posting

   Fascinating, and potentially deadly to many out there, by the sound of it

   This would appear to circumvent USB autorun blockers. I expect that AntiExe etc programs like ProcessGuard etc, would block the .SYS etc from installing ? As not many people do not have such programs, i suppose unless their AV's etc have the Defs, they are vulnerable

   Please keep us updated on this

3. > **@sergey ulasen**
   >
   > Thanks for posting
   >
   > Fascinating, and potentially deadly to many out there, by the sound of it
   >
   > This would appear to circumvent USB autorun blockers. I expect that AntiExe etc programs like ProcessGuard etc, would block the .SYS etc from installing ? As not many people do not have such programs, i suppose unless their AV's etc have the Defs, they are vulnerable
   >
   > Please keep us updated on this

   I am sure Tight **SRP** or **AppLocker** policy will defeat the execution of this malware.

   Remember, if it cannot execute, it cannot infect.

4. Originally Posted by **AvinashR**

   > I am sure Tight SRP or AppLocker policy will defeat the execution of this malware.

   Quite possibly, **Sully** etc should know

   > Remember, if it cannot execute, it cannot infect.

   Yes and no *~Comments removed~*

Last edited by a moderator: Jul 12, 2010

5. Another disturbing feature is they are signed with digital signatures of the Realtek Semiconductor Corp

These must be either fake, or manipulated real ones ? Things like this were said to be Impossible, by so called "experts more than once in the last few years

> 6. You should take into consideration that virus infects Operation System in unusual way through vulnerability in processing lnk-files (without usage of autorun.inf file).

A shame there's so little information here. It doesn't sound like the average malware-du-jour. Isn't there any more information on the vulnerability in processing shortcut .LNK files?

> These must be either fake, or manipulated real ones ? Things like this were said to be Impossible, by so called "experts more than once in the last few years

I don't recall any expert saying "this" was impossible. It's always been possible to steal a legit certificate, if whoever owns that cert has lax enough security. It's possible to slap any cert on a file and at a glance it may look legit, but won't actually check out as valid *if* one bothers to check. There are possibilities like this - there's always even the option of fooling the certificate authority into issueing you a certificate that should belong to someone else (you're not Mozilla Corporation, but some CA might still give you a certificate with that name on it). In this particular case, there's not much information to go on to tell what's actually happened.

7.

> Originally Posted by **Windchild**
>
> I don't recall any expert saying "this" was impossible.

I was sure i did, so i went and searched. Here's several examples i found.

Even though this article is on PGP i think it's aplicable.

> Originally Posted by **dave**
>
> It is believed to be mathematically intractable for someone not in possession of (say) Microsoft's code-signing certificate to sign code and make it look like it came from Microsoft. So, if that's what you mean, fake certificates are as likely as magic pixie dust. http://www.broadbandreports.com/forum/remark,17299839

As i was searching for those conformation links, i also found an interesting article which explains the multiple weaknesses in 1st gen certs, and goes on to show how they can be improved

8.

> I was sure i did, so i went and searched. Here's several examples i found.

There seems to be some confusion here, due to the vagueness of some statements. None of those comments you quoted claims that it's impossible to have a (valid) digital signature on a malicious file. There's plenty of ways for that: for example, one could steal a cert from some innocent developer and then use it to sign malware. There's even more ways to get an invalid digital signature on a malware: for example, just copying it from some signed file. What those comments you quoted *are* saying is that it's not mathematically feasible to create a "fake" digital signature that also checks out as valid in someone else's name. When "so called experts" claim digital signatures can't be faked, they're referring to this mathematical difficulty of creating a fake signature that actually checks out as valid. They're not saying you can't steal a cert from someone, or fool a certificate authority into granting you someone else's cert, or such things.

As far as the malware mentioned by the original poster is concerned, there is no information given that would tell us how the Realtek digital signature got on the malicious files. Was a legit Realtek cert stolen? Or is it just a case of copying the cert onto a malware binary, in which case the signature would check out as invalid? Or is it really a case where someone has successfully created a fake cert that checks out as valid, in spite of the mathematical difficulty of this? With the scarce information given here, it's impossible to tell, but the latter is very unlikely. Sure, there's the option of exploiting MD5 collisions, but even though that's theoretically possible, it's not exactly easy, and it's not like you have to use MD5 anyway. What I'm saying here is that the information given in this thread gives us no reason to suspect those "experts" were wrong about the mathematical infeasibility of creating fake digital signatures.

There's a good reason for wanting more information on this case. When so little info is given, it's very difficult to say anything useful about the case. It would be nice to know more details on the .LNK file vulnerability, for example, and details on the digital signature on the malicious files, and many other factors. When one leaves such information out, it feels kind of like a movie teaser trailer - all the good stuff is missing.

9.

> Originally Posted by **Windchild**
>
> Was a legit Realtek cert stolen? Or is it just a case of copying the cert onto a malware binary, in which case the signature would check out as invalid? Or is it really a case where someone has successfully created a fake cert that checks out as valid, in spite of the mathematical difficulty of this?

I've asked **sergey ulasen** to keep us updated, so hopefully he will include this aspect too

10. Why create when it can be bought.....people in position(s) have been known to sell out.....

11. I haven't received any kind of information from other vendors too, Hope **Sergey Ulasen** keep us updatedon this topic**...**

12.

> I haven't received any kind of information from other vendors too, Hope **Sergey Ulasen** keep us updatedon this topic**...**

Additional information about malware is in document:

View attachment new_rootkit_en.pdf

13. Thanks for additional document...

14. Thanks for that There's still some questions about the .LNK file vulnerability worth asking, though. Such as: Has the vulnerability been reported to Microsoft? And most importantly the nature of the vulnerability. I assume it leads to arbitrary code execution with the privileges of explorer.exe (the privileges of currently logged-in user, that is to say)? If that is so, then the malware wouldn't be able to infect a system unless the user was logged in as an administrator. It would be nice for such details to be mentioned, seeing how it has a great effect on how dangerous the vulnerability is, especially considering that new Windows versions come with UAC enabled by default.

> Why create when it can be bought.....people in position(s) have been known to sell out.....

Indeed. Most everyone has a price, and in larger companies it isn't even all that unusual to have a rogue-ish employee. Of course, the problem is in the risk of getting caught.

15. Good work **Ulasen Sergey** and **Kupreev Oleg**

Quotes from the PDF

> Operating System Windows 7 Enterprise Edition x86 with all latest updates is vulnerable, that means malware uses vulnerability that still exists and hasn’t been closed in OS Windows

Amazing, there's always something for the bad guys to keep them busy and find, and they sure do, and make use of them.

Unbelievable you havn't heard back from Realtek

> Drivers that have digital signature are used for hiding. That is the reason why it is difficult to identify them independently since antirootkits are misled. Also detection of these drivers by antivirus companies is absent for a long time, probably because of screening these examples out on the primary stage of processing binary files in incoming flow.

Vendors have known for several years that numerous fake etc certs have accompanied malware. So they havn't had any excuse for ignoring this vector

Nice to see Gmer still on the ball

Re - **oem6c.pnf** and **oem7a.pnf**

> The **PNF** file type is primarily associated with 'Portable Network Graphics Frame'.
>
> Detailed information for file extension PNF:
>
> Primary association: Portable Network Graphics Frame
> Other applications associated with file type PNF:
>
> * Precompiled Setup Information(Temporary file seen during installs)
>
> * Windows (Precompiled Setup Information) by Microsoft Corporation
>
> A precompiled INF file. Windows creates a PNF file for each INF file to facilitate efficient processing. If a PNF file does not exist, Setup generates one for the INF file. The identifying characters used for this association are - Hex: 01 01
>
> http://filext.com/file-extension/PNF

Could this be partially a new Graphics vulnerabilty exploit ? similar in "some" way/s to the MetaFiles exploits https://www.wilderssecurity.com/showthread.php?t=113044

16. No, I don't see how it could. According to Sergey's PDF, the malware infects the system by exploiting an unpatched vulnerability in processing LNK files. There is no mention of any other vulnerability being exploited. Those .pnf files are not graphic files - as stated in the PDF, they're encrypted. They probably contain things like the malware's configuration data.

17. The questions I have are:

    1. what is the Windows vulnerability?
    2. How do the files get from the usb stick to the directories, especially in a standard account?
    3. how do the malicious files execute?
    4. would a whitelist or other anti-executable measure stop this?

18. **oem6c.pnf** and **oem7a.pnf** listed in here -

http://www.threatexpert.com/report.aspx?md5=74ddc49a7c121a61b8d06c03f92d0c13

Malware-Cryptor.Win32.Inject.gen.2 - **Inject.gen.2** "might" be connected with the Bifrost Trojan ? - http://www.threatexpert.com/reports.aspx?find=Inject.gen.2&x=7&y=8

MRXCLS - MRXNET - mrxcls.sys - http://www.sophos.com/security/analyses/viruses-and-spyware/trojstuxneta.html

Those same 3 files in this ComboFix log Files Created on 2010-07-04 - http://pastebin.com/r5QvBHRt

Also here - http://forum.drweb.com/index.php?showtopic=293997

*

@Windchild

Re - **oem6c.pnf** and **oem7a.pnf**

OK, the .PNF extension must just be a coincidence then !

19. Thanks Sergey for analysis.

Files put in root of vm, detection by arks

Last edited: Jul 14, 2010

20. We wrote an e-mail to Microsoft, but they haven't answered us.
I think most of the antivirus vendors have paid attention to this virus and I hope that they report Microsoft and Realtek about problem too.

21. thanks EP

Attached Files:

-

Last edited: Jul 14, 2010

22. hi guys,

has anyone already taken a deeper look at the malware?

i found stuff like this after some decryption/unpacking stages of MD5 sample 016169ebebf1cec2aad6c7f0d0ee9026

```
SOFTWARE\Microsoft\MSSQLServer
pdl
GracS\
2WSXcder
WinCCConnect
master
.\WinCC
sqloledb
GracS\cc_tlg7.sav
Step7\Example
use [%s]
declare @t varchar(4000), @e int, @f int if exists (select text from db
declare @t varchar(4000), @e int, @f int if exists (select * from dbo.s
use master
select name from master..sysdatabases where filename like N'%s'
exec master..sp_attach_db 'wincc_svr',N'%s',N'%s'
exec master..sp_detach_db 'wincc_svr'
use wincc_svr


or

SOFTWARE\SIEMENS\WinCC\Setup
STEP7_Version
SOFTWARE\SIEMENS\STEP7
SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation
NTVDM TRACE
.MCP
.zip
~DT
%s\WINCC
 DECLARE @vr varchar(256) SET @vr = CONVERT(varchar(256), (SELECT serve
EXEC sp_configure 'show advanced options', 1  RECONFIGURE WITH OVERRIDE
EXEC sp_configure 'Ole Automation Procedures', 1
RECONFIGURE WITH OVERRIDE END
 DECLARE @ashl int,         @aind varchar(260),         @ainf varchar(2
       @adss int,
       @aip int,
       @abf varbinary(4096) EXEC @hr = sp_OACreate 'ADODB.Stream', @aod
  EXEC sp_dropextendedproc sp_dumpdbilog
 DECLARE @ashl int,         @aind varchar(260),         @ainf varchar(2
 DECLARE @ashl int,         @aind varchar(260),         @ainf varchar(2
 DROP TABLE sysbinlog
0123456789ABCDEF
 CREATE TABLE sysbinlog ( abin image ) INSERT INTO sysbinlog VALUES(0x
%SystemRoot%\system32\netapi32.dll
%SystemRoot%\system32\kernel32.dll
.xp_cmdshell ''''extrac32 /y "''+@t+''" "''+@t+''x"'''''';exec(@s);set
 view MCPVREADVARPERCON as select MCPTVARIABLEDESC.VARIABLEID,MCPTVARIA
 ((SELECT top 1 1 FROM MCPVREADVARPERCON)='1') --CC-SP
 0;set IMPLICIT_TRANSACTIONS off;declare @z nvarchar(999);set @z=''use
```

this points me to the Siemens WinCC SCADA system.

looks like this malware was made for espionage.

23.

WawaSeb *Registered Member*

Joined:
May 26, 2008
Posts:
2

Hello everybody,

***** Thank both Ulasen Sergey and Kupreev Oleg for this work ! *****

ComboFix (by sUBs) and **MBAM** are already able to remove the infection.

I'm looking forward to test it with KIS 2011.

==> *Edit : KIS 2011 successfully prvent the infection*
http://www.lutile.be/images/erf/tmphider.JPG

Best regards,

Last edited: Jul 15, 2010

24.

> hi guys,
>
> has anyone already taken a deeper look at the malware?..looks like this malware was made for espionage.

Mm, what other reason for targeting WinCC Scada system.

Last edited: Jul 15, 2010

25.

> Human machine interface (HMI) software enables operators to manage industrial and process control machinery via a computer-based graphical user interface (GUI). The computer on which HMI software is installed

is called a human machine interface or HMI. There are two basic types of HMI: supervisory level and machine level. Supervisory level HMI is designed for control room environments and used for system control and data acquisition (SCADA), a process control application which collects data from sensors on the shop floor and sends the information to a central computer for processing. Machine level HMI uses embedded, machine-level devices within the production facility itself. Most human machine interface (HMI) software is designed for either supervisory level HMI or machine level HMI

Industrial_Engineering_Software

Page 1 of 16
1 ← 2 3 4 5 6 → 16 Next >

Thread Status:
Not open for further replies.

WILDERS SECURITY FORUMS