Trojan-Spy.0485

And

Malware-Cryptor.Win32.Inject.gen.2

Review

Kupreev Oleg

Ulasen Sergey

VirusBlokAda

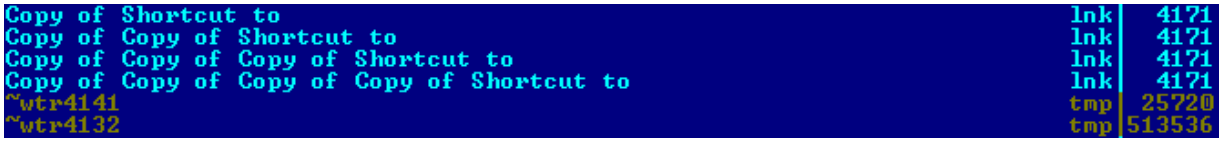
On the 17th of June, 2010 "VirusBlokAda" company specialists (www.anti-virus.by/en/) detected new malware modules. They have been added to the anti-virus bases as Trojan-Spy.0485 (http://www.virustotal.com/ru/analisis/9c891edb5da763398969b6aaa86a5d46971bd28a455b20c2067cb512c9f9a0f8-1278584177) and Malware-Cryptor.Win32.Inject.gen.2 (http://www.virustotal.com/ru/analisis/d58c95a68ae3debf9eedb3497b086c9d9289bc5692b72931f3a12c3041832628-1278584115). Files had names ~wtr4132.tmp (513536 bytes) and ~wtr4141.tmp (25720 bytes) accordingly. Functionality of this malware includes rootkit-technologies as well.

Propagation method

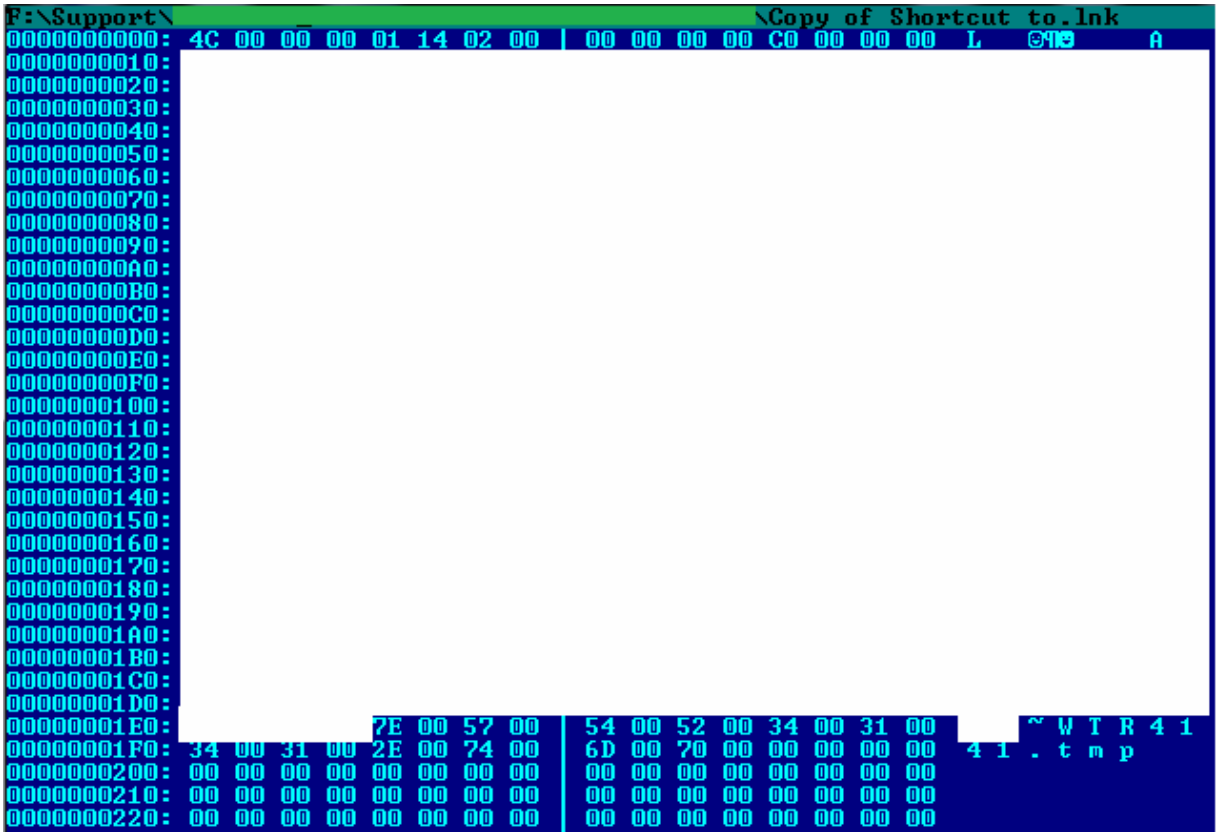
You should take into consideration that virus infects Operating System in unusual way (without usage of autorun.inf file) through vulnerability in processing lnk-files.

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

Below you can see screenshot of infected USB storage device in the file manager FAR (it doesn't infect Operating System):



From the screenshot you can see that in the USB-device root there are 2 files with tmp extension (they are executable) and 4 files with lnk extension. The following screenshot presents one of the lnk-files content:



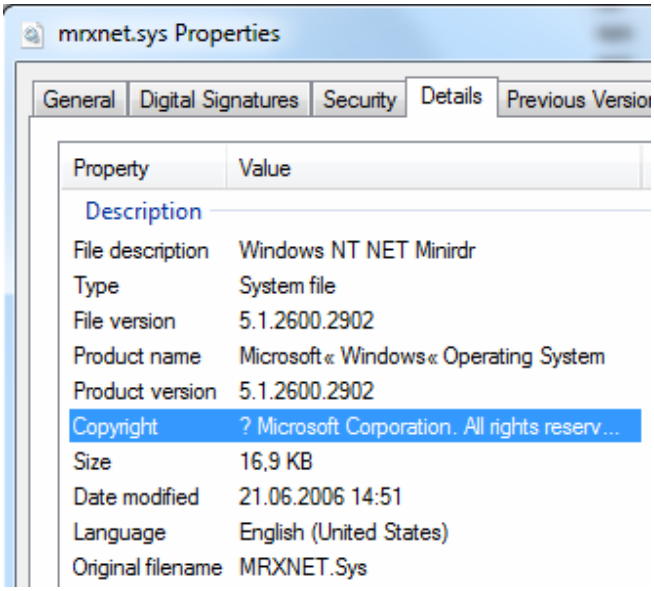
Operating System Windows 7 Enterprise Edition x86 with all latest updates is vulnerable, that means malware uses vulnerability that still exists and hasn't been closed in OS Windows.

Process of system infection and hiding

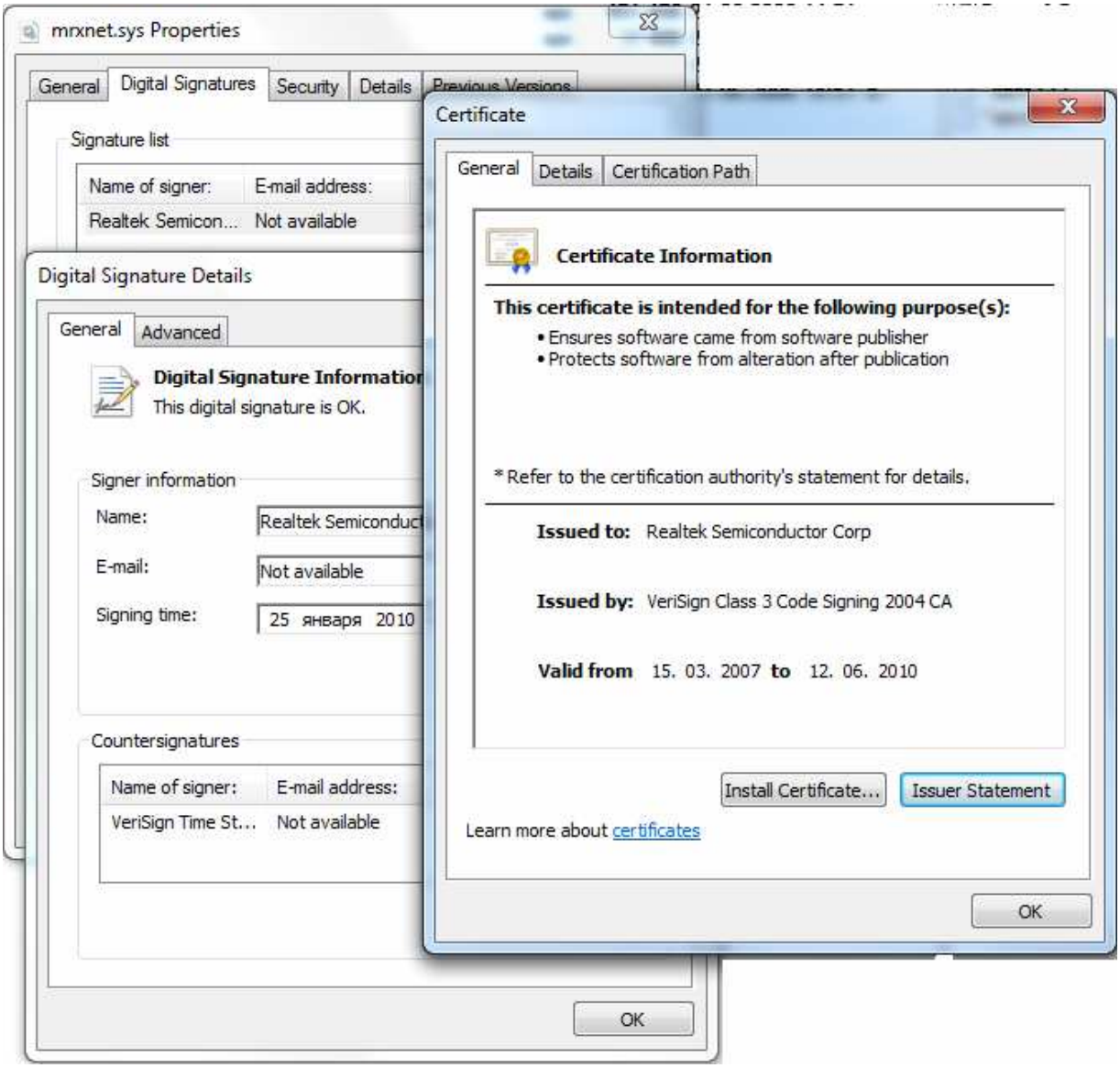
Process of system infection proceeds in the following way:

1. Both files (mrxnet.sys and mrxcls.sys, one of them works as driver-filter of file system and the second one is injector of malicious code) are placed in the %SystemRoot%\System32\drivers directory. It is seen as follows in gmer anti-rootkit:

Analysis of current drivers showed that files have resources section where the following information is presented:



Note that drivers are signed with digital signature of Realtek Semiconductor Corp. On the 24th of June, 2010 we sent a letter to Realtek Company containing the warning and description of current problem. However, the reply from Relatek Company still hasn't been received.

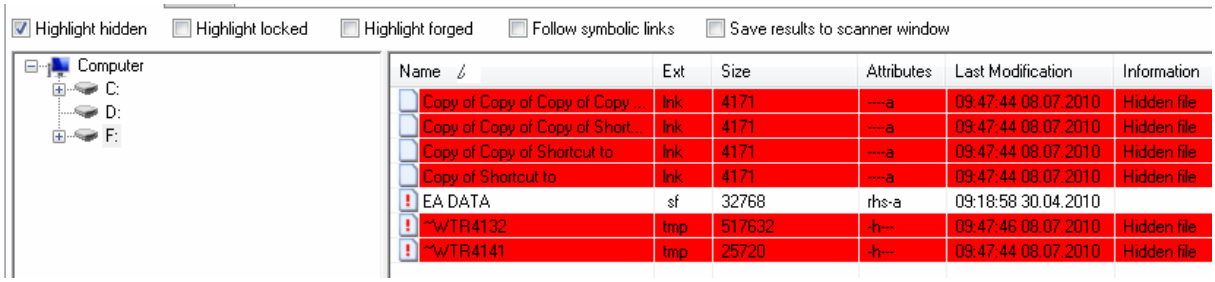


Files mrxnet.sys and mrxcls.sys were also added to virus databases of VirusBlokAda as Rootkit.TmpHider (http://www.virustotal.com/ru/analisis/0d8c2bcb575378f6a88d17b5f6ce70e794a264cdc8556c8e812f0b5f9c709198-1278584497) and SScope.Rookit.TmpHider.2 (http://www.virustotal.com/ru/analisis/1635ec04f069ccc8331d01fdf31132a4bc8f6fd3830ac94739df95ee093c555c-1278661251) accordingly.

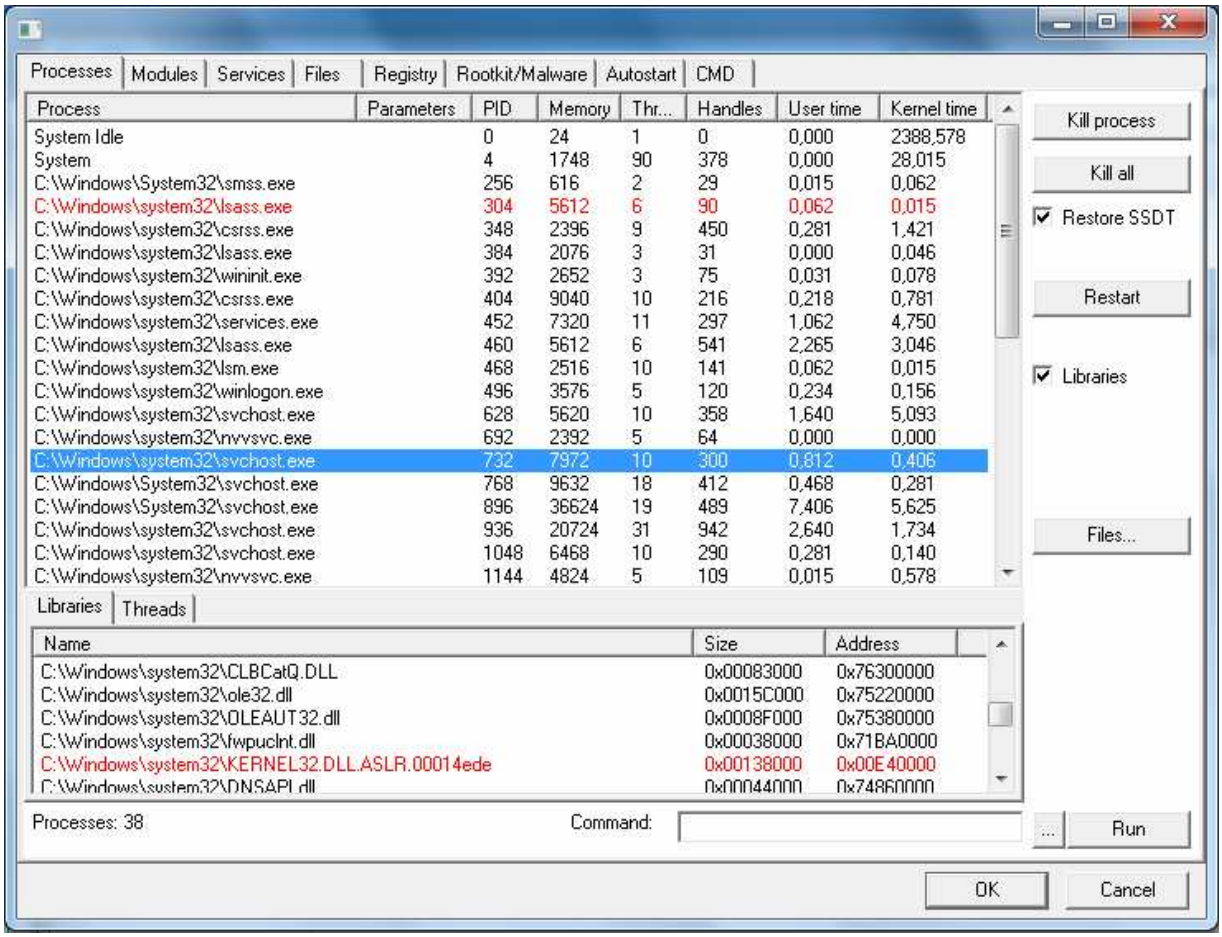
2. Two files (oem6c.pnf and oem7a.pnf, content of which is encrypted) are placed in the %SystemRoot%\inf directory.

Malware gets execution right after system has been infected, additional system reboot isn't needed.

Driver-filter hides ~wtr4132.tmp and ~wtr4141.tmp files and appropriate lnk-files. That's why users may even not notice that there are extra files on their USB-devices. Vba32 AntiRootkit (http://anti-virus.by/en/beta.shtml) detects hidden modules in the following way:



3. Also rootkit runs additional threads in the system processes, at the same time it hides modules which started the threads. AntiRootkit gmer detects these anomalies in the following way:



4. Rootkit installs interceptions in system processes:

.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtClose + 6	76DD4936 4 Bytes [50, 00, D9, 76]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtClose + B	76DD493B 1 Byte [D2]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtCreateSection + 6	76DD4B56 4 Bytes [48, 00, D9, 76]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtCreateSection + B	76DD4B5B 1 Byte [D2]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtMapViewOfSection + 6	76DD5096 4 Bytes [44, 00, D9, 76]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtMapViewOfSection + B	76DD509B 1 Byte [D2]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtOpenFile + 6	76DD5146 4 Bytes [4C, 00, D9, 76]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtOpenFile + B	76DD514B 1 Byte [D2]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtQueryAttributesFile + 6	76DD53A6 4 Bytes [54, 00, D9, 76]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtQueryAttributesFile + B	76DD53AB 1 Byte [D2]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtQuerySection + 6	76DD55F6 4 Bytes [58, 00, D9, 76]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtQuerySection + B	76DD55FB 1 Byte [D2]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtClose + 6	76DD4936 4 Bytes [50, 00, D9, 76]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtClose + B	76DD493B 1 Byte [D2]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtCreateSection + 6	76DD4B56 4 Bytes [48, 00, D9, 76]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtCreateSection + B	76DD4B5B 1 Byte [D2]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtMapViewOfSection + 6	76DD5096 4 Bytes [44, 00, D9, 76]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtMapViewOfSection + B	76DD509B 1 Byte [D2]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtOpenFile + 6	76DD5146 4 Bytes [4C, 00, D9, 76]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtOpenFile + B	76DD514B 1 Byte [D2]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtQueryAttributesFile + 6	76DD53A6 4 Bytes [54, 00, D9, 76]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtQueryAttributesFile + B	76DD53AB 1 Byte [D2]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtQuerySection + 6	76DD55F6 4 Bytes [58, 00, D9, 76]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtQuerySection + B	76DD55FB 1 Byte [D2]

Thus, current malware should be added to very dangerous category cause there is a risk of virus epidemic at the current moment. The reasons are:

1. Vulnarability of the operation system that hasn't been still closed is used for propagation. Malware starts to hide itself right after system has been infected;

2. 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.

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