

Trojan-Spy.0485
And
Malware-Cryptor.Win32.Inject.gen.2
Review

Kupreev Oleg

Ulasen Sergey



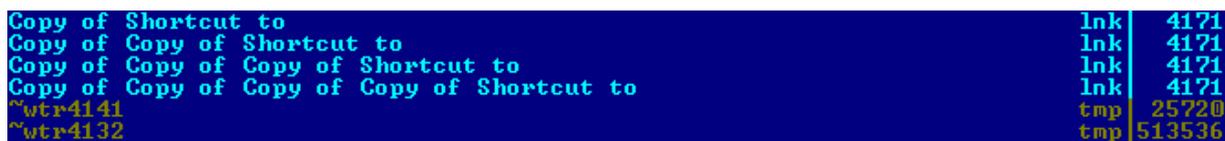
On the 17th of June, 2010 "VirusBlokAda" company specialists (www.anti-virus.by/en/) detected new malware modules. They have been added to the anti-virus bases as Trojan-Spy.0485 (<http://www.virustotal.com/ru/analisis/9c891edb5da763398969b6aaa86a5d46971bd28a455b20c2067cb512c9f9a0f8-1278584177>) and 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):



Copy of Shortcut to	lnk	4171
Copy of Copy of Shortcut to	lnk	4171
Copy of Copy of Copy of Shortcut to	lnk	4171
Copy of Copy of Copy of Copy of Shortcut to	lnk	4171
~wtr4141	tmp	25720
~wtr4132	tmp	513536

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:

```

F:\Support\          \Copy of Shortcut to .lnk
00000000: 4C 00 00 00 01 14 02 00 | 00 00 00 00 C0 00 00 00 L 04E A
00000001:
00000002:
00000003:
00000004:
00000005:
00000006:
00000007:
00000008:
00000009:
0000000A:
0000000B:
0000000C:
0000000D:
0000000E:
0000000F:
00000010:
00000011:
00000012:
00000013:
00000014:
00000015:
00000016:
00000017:
00000018:
00000019:
0000001A:
0000001B:
0000001C:
0000001D:
0000001E: 7E 00 57 00 | 54 00 52 00 34 00 31 00 ~ W T R 4 1
0000001F: 34 00 31 00 2E 00 74 00 | 6D 00 70 00 00 00 00 00 4 1 . t m p
00000020: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
00000021: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
00000022: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00

```

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:

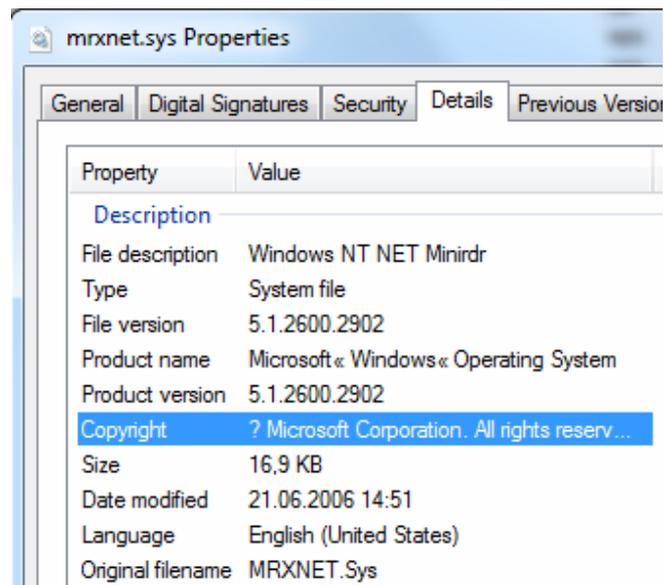
- Both files (mrxnet.sys and mrxccls.sys, one of them works as driver-filter of file system and the second one is injector of malicious code) are placed in the %SystemRoot%\System32\drivers directory. It is seen as follows in gmer anti-rootkit:

```

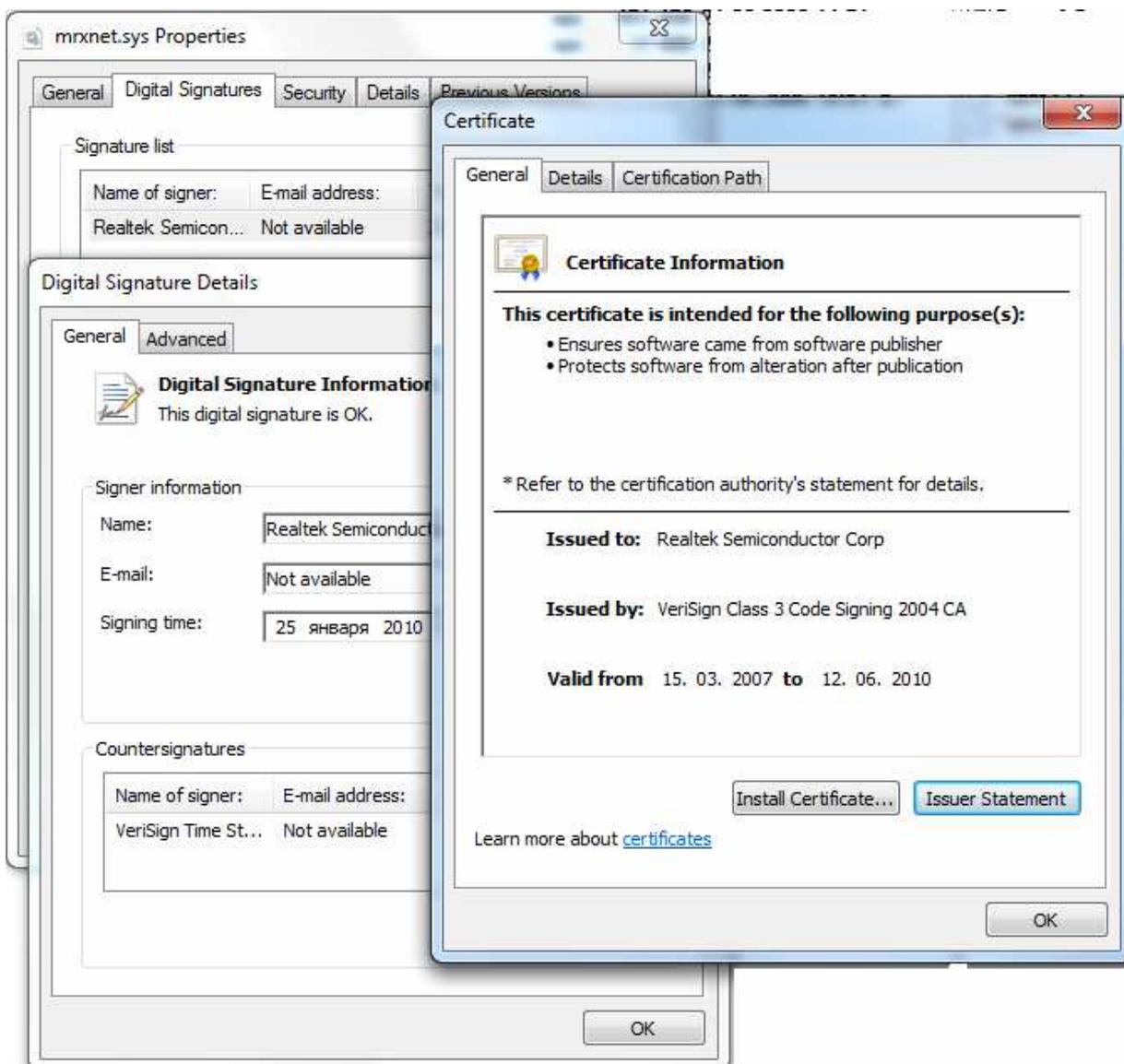
AttachedDevice \FileSystem\Ntfs\Ntfs mrxnet.sys
Device \Driver\ACPI_HAL\Device\00000004 ntiaacpi.sys (Hardware Abstraction Layer DLL/Microsoft Corpora
AttachedDevice \Driver\volmgr\Device\HarddiskVolume1 fvevol.sys (BitLocker Drive Encryption Driver/Microsoft Corpora
AttachedDevice \Driver\volmgr\Device\HarddiskVolume2 fvevol.sys (BitLocker Drive Encryption Driver/Microsoft Corpora
AttachedDevice \Driver\volmgr\Device\HarddiskVolume3 fvevol.sys (BitLocker Drive Encryption Driver/Microsoft Corpora
AttachedDevice \FileSystem\Fastfat\Fat fltmgr.sys (Microsoft Filesystem Filter Manager/Microsoft Corpora
AttachedDevice \FileSystem\Fastfat\Fat mrxnet.sys

```

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/analysis/0d8c2bcb575378f6a88d17b5f6ce70e794a264cdc8556c8e812f0b5f9c709198-1278584497>) and SScope.Rootkit.TmpHider.2 (<http://www.virustotal.com/ru/analysis/1635ec04f069ccc8331d01df31132a4bc8f6fd3830ac94739df95ee093c555c-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:

Name	Ext	Size	Attributes	Last Modification	Information
Copy of Copy of Copy of Copy ...	Ink	4171	----	09:47:44 08.07.2010	Hidden file
Copy of Copy of Copy of Short...	Ink	4171	----	09:47:44 08.07.2010	Hidden file
Copy of Copy of Shortcut to	Ink	4171	----	09:47:44 08.07.2010	Hidden file
Copy of Shortcut to	Ink	4171	----	09:47:44 08.07.2010	Hidden file
EA DATA	sf	32768	rhs-a	09:18:58 30.04.2010	
~\WTR4132	tmp	517632	-h---	09:47:46 08.07.2010	Hidden file
~\WTR4141	tmp	25720	-h---	09:47:44 08.07.2010	Hidden file

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:

Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
System Idle		0	24	1	0	0,000	2388,578
System		4	1748	90	378	0,000	28,015
C:\Windows\System32\smss.exe		256	616	2	29	0,015	0,062
C:\Windows\system32\sass.exe		304	5612	6	90	0,062	0,015
C:\Windows\system32\csrss.exe		348	2396	9	450	0,281	1,421
C:\Windows\system32\sass.exe		384	2076	3	31	0,000	0,046
C:\Windows\system32\wininit.exe		392	2652	3	75	0,031	0,078
C:\Windows\system32\csrss.exe		404	9040	10	216	0,218	0,781
C:\Windows\system32\services.exe		452	7320	11	297	1,062	4,750
C:\Windows\system32\sass.exe		460	5612	6	541	2,265	3,046
C:\Windows\system32\sm.exe		468	2516	10	141	0,062	0,015
C:\Windows\system32\winlogon.exe		496	3576	5	120	0,234	0,156
C:\Windows\system32\svchost.exe		628	5620	10	358	1,640	5,093
C:\Windows\system32\invsvcs.exe		692	2392	5	64	0,000	0,000
C:\Windows\system32\svchost.exe		732	7972	10	300	0,812	0,406
C:\Windows\System32\svchost.exe		768	9632	18	412	0,468	0,281
C:\Windows\System32\svchost.exe		896	36624	19	489	7,406	5,625
C:\Windows\system32\svchost.exe		936	20724	31	942	2,640	1,734
C:\Windows\system32\svchost.exe		1048	6468	10	290	0,281	0,140
C:\Windows\system32\invsvcs.exe		1144	4824	5	109	0,015	0,578

Name	Size	Address
C:\Windows\system32\CLBCatQ.DLL	0x00083000	0x76300000
C:\Windows\system32\ole32.dll	0x0015C000	0x75220000
C:\Windows\system32\OLEAUT32.dll	0x0008F000	0x75380000
C:\Windows\system32\fwpuclnt.dll	0x00038000	0x71BA0000
C:\Windows\system32\KERNEL32.DLL.ASLR.00014ede	0x00138000	0x00E40000
C:\Windows\system32\DNSAPI.dll	0x00044000	0x74860000

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	76DD4856 4 Bytes [48, 00, D9, 76]
.text	C:\Windows\system32\lsass.exe[304] ntdll.dll!NtCreateSection + B	76DD485B 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	76DD4856 4 Bytes [48, 00, D9, 76]
.text	C:\Windows\system32\svchost.exe[732] ntdll.dll!NtCreateSection + B	76DD485B 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. Vulnerability 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.Rootkit.TmpHider.2 all over the world.