

I used next software:

OS: Windows XP Home Edition SP2 (RUS)

Virtual machine: Vmware Player 2.0.2 build-59824

Guest OS: Windows XP Professional SP2 (RUS)

For analysing: IDA Pro 5.2, QUnpack 2.2, DiE (Detect it Easy) 0.63, Total Commander's Lister.

For removal instructions automation: AutoIT v3.

Results of analysing:

This program gives full access to computer. Infected computer can be remote managed thru internet using IRC. So it can be classified as backdoor.

It's windows executable file (PE EXE). Size: 75264 bytes. Packed with UPX 3.03 modification.

Unpacked with the help of Qunpack 2.2, OEP — 0x004109CC.

Behavior

Backdoor checks it's name and if it isn't:

`%SystemRoot%\Winsec32.exe`

copies it's own executable to windows directory:

`%SystemRoot%\Winsec32.exe`

Gets adress of «RegisterServiceProcess» and runs it. It makes backdoor's process invisible for «Task Manager», but this function exists only in kernel32.dll of Windows 9x family

Reads file times «created» and «changed» of explorer.exe and sets them for it's copy.

Also backdoor sets attributes «read only» and «system» for copy.

Than backdoor runs it's copy and ends own process.

If backdoor's executable name is:

`%SystemRoot%\Winsec32.exe`

it makes next:

- gets adress of «RegisterServiceProcess» and runs it. It makes backdoor's process invisible for «Task Manager», but this function exists only in kernel32.dll of Windows 9x family.
- creates next autorun keys:

`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]`
`"Microsoft Svchost local services"="Winsec32.exe"`

`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]`
`"Microsoft Svchost local services"="Winsec32.exe"`

`[HKEY_CURRENT_USER\Software\Microsoft\OLE]`

```
"Microsoft Svchost local services"="Winsec32.exe"
```

- tries to connect to testirc1.sh1xy2bg.NET every 2 seconds.
- logons to this server with nickname "%localization of windows%[%window's family%] %tick count%". For example: RUS[XP]495789, USA[2k]547284
- connects to chanell <happy12>.

Backdoor can receive huge count of commands and provide different action. For example it can: send files with the help of ftp.exe, kill processes, delete files, send content of clipboard, reboot system, log key downs, share files etc.

Also there is a function which creates and runs file:

```
C:\a.bat (5 804 bytes)
```

This file creates and runs file <%Temp%\1.reg> (3 807 bytes, %Temp% -- temporary folder of current user). This reg file makes next changes in system registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters]
"TransportBindName"=""
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess]
"Start"=dword:00000004
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauerv]
"Start"=dword:00000004
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wscsvc]
"Start"=dword:00000004
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole]
"EnableDCOM"="N"
"EnableRemoteConnect"="N"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"restrictanonymous"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
s\PCT1.0\Server]
"Enabled"=hex:00
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
"AutoShareWks"=dword:00000000
"AutoShareServer"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"NameServer"=""
"ForwardBroadcasts"=dword:00000000
"IPEnableRouter"=dword:00000000
"Domain"=""
"SearchList"=""
"UseDomainNameDevolution"=dword:00000001
"EnableICMPRedirect"=dword:00000000
"DeadGWDetectDefault"=dword:00000001
"DontAddDefaultGatewayDefault"=dword:00000000
"EnableSecurityFilters"=dword:00000001
"AllowUnqualifiedQuery"=dword:00000000
"PrioritizeRecordData"=dword:00000001
"TCP1320Opts"=dword:00000003
"KeepAliveTime"=dword:00023280
```

"BcastQueryTimeout"=dword:000002ee
"BcastNameQueryCount"=dword:00000001
"CacheTimeout"=dword:0000ea60
"Size/Small/Medium/Large"=dword:00000003
"LargeBufferSize"=dword:00001000
"SynAckProtect"=dword:00000002
"PerformRouterDiscovery"=dword:00000000
"EnablePMTUBHDetect"=dword:00000000
"FastSendDatagramThreshold " =dword:00000400
"StandardAddressLength " =dword:00000018
"DefaultReceiveWindow " =dword:00004000
"DefaultSendWindow"=dword:00004000
"BufferMultiplier"=dword:00000200
"PriorityBoost"=dword:00000002
"IrpStackSize"=dword:00000004
"IgnorePushBitOnReceives"=dword:00000000
"DisableAddressSharing"=dword:00000000
"AllowUserRawAccess"=dword:00000000
"DisableRawSecurity"=dword:00000000
"DynamicBacklogGrowthDelta"=dword:00000032
"FastCopyReceiveThreshold"=dword:00000400
"LargeBufferListDepth"=dword:0000000a
"MaxActiveTransmitFileCount"=dword:00000002
"MaxFastTransmit"=dword:00000040
"OverheadChargeGranularity"=dword:00000001
"SmallBufferListDepth"=dword:00000020
"SmallerBufferSize"=dword:00000080
"TransmitWorker"=dword:00000020
"DNSQueryTimeouts" =hex(7):
31,00,00,00,32,00,00,00,32,00,00,00,34,00,00,00,38,00,00,00,30,00,00,00,00,00
"DefaultRegistrationTTL"=dword:00000014
"DisableReplaceAddressesInConflicts"=dword:00000000
"DisableReverseAddressRegistrations"=dword:00000001
"UpdateSecurityLevel " =dword:00000000
"DisjointNameSpace"=dword:00000001
"QueryIpMatching"=dword:00000000
"NoNameReleaseOnDemand"=dword:00000001
"EnableDeadGWDetect"=dword:00000000
"EnableFastRouteLookup"=dword:00000001
"MaxFreeTcbs"=dword:000007d0
"MaxHashTableSize"=dword:00000800
"SackOpts"=dword:00000001
"Tcp1323Opts"=dword:00000003
"TcpMaxDupAcks"=dword:00000001
"TcpRecvSegmentSize"=dword:00000585
"TcpSendSegmentSize"=dword:00000585
"TcpWindowSize"=dword:0007d200
"DefaultTTL"=dword:00000030
"TcpMaxHalfOpen"=dword:0000004b
"TcpMaxHalfOpenRetried"=dword:00000050
"TcpTimedWaitDelay"=dword:00000000
"MaxNormLookupMemory"=dword:00030d40
"FFPControlFlags"=dword:00000001
"FFPFastForwardingCacheSize"=dword:00030d40
"MaxForwardBufferMemory"=dword:00019df7
"MaxFreeTWTcbs"=dword:000007d0
"GlobalMaxTcpWindowSize"=dword:0007d200
"EnablePMTUDiscovery"=dword:00000001
"ForwardBufferMemory"=dword:00019df7

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]

"MaxConnectionsPerI_0Server"=dword:00000050

"MaxConnectionsPerServer"=dword:00000050

After it «C:\a.bat» deletes «%Temp%\1.reg» and itself.

But looks like this function will never work....

Removal instructions

1. Kill process with name: «Winsec32.exe»
2. Delete file %Systemroot%\Winsec32.exe
3. Delete registry keys:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Microsoft Svchost local services"="Winsec32.exe"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]
"Microsoft Svchost local services"="Winsec32.exe"
```

```
[HKEY_CURRENT_USER\Software\Microsoft\OLE]
"Microsoft Svchost local services"="Winsec32.exe"
```

4. Install anti virus or use online antivirus scan to find original file of backdoor.