catchme 0.3

---

catchme is the rootkit/stealth malware scanner that scans for:

- hidden processes
- hidden registry keys
- hidden services
- hidden files

catchme can also delete, destroy and collect malicious files.

How to scan

- Download **catchme.exe** (137KB) to your desktop.
- Double click the **catchme.exe** to run it
- Click the "Scan" button to start scan
- Open **catchme.log** to see results

How to delete malware files

To delete malicious files on the "Script" tab paste the list after "Files to delete:" command and click the "Run" button. The selected files will be deleted and copy ZIPped to catchme.zip located on desktop. Restart machine to complete operation.

```
Files to delete:
c:\windows\system32\yruoykdhak.dat
c:\windows\system32\yruoykdhak.exe
c:\windows\system32\yruoykdhak_nav.dat
c:\windows\system32\yruoykdhak_navps.dat
```

content of catchme.log

```
Processing "Files to delete:"

file zipped: c:\windows\system32\yruoykdhak.dat -> catchme.zip -> yruoykdhak.dat ( 4761 bytes )
file "c:\windows\system32\yruoykdhak.dat" deleted successfully
file zipped: c:\windows\system32\yruoykdhak.exe -> catchme.zip -> yruoykdhak.exe ( 336384 bytes )
file "c:\windows\system32\yruoykdhak.exe" deleted successfully
file zipped: c:\windows\system32\yruoykdhak_nav.dat -> catchme.zip -> yruoykdhak_nav.dat ( 287805 bytes )
file "c:\windows\system32\yruoykdhak_nav.dat" deleted successfully
file zipped: c:\windows\system32\yruoykdhak_navps.dat -> catchme.zip -> yruoykdhak_navps.dat ( 331 bytes )
file "c:\windows\system32\yruoykdhak_navps.dat" deleted successfully
```

How to destroy malware files

To destroy malicious executable files on the "Script" tab paste the list after "Files to kill:" command and click the "Run" button. The selected files will be destroyed and copy ZIPped to catchme.zip located on desktop. Restart machine to complete operation.

```
Files to kill:
C:\WINDOWS\system32\drivers\symavc32.sys
C:\WINDOWS\system32\drivers\Deg39.sys
```

content of catchme.log

```
Processing "Files to kill:"

file zipped: C:\WINDOWS\system32\drivers\symavc32.sys -> catchme.zip -> symavc32.sys ( 178688 bytes )
PE file "C:\WINDOWS\system32\drivers\symavc32.sys" killed successfully
file zipped: C:\WINDOWS\system32\drivers\Deg39.sys -> catchme.zip -> Deg39.sys ( 178688 bytes )
PE file "C:\WINDOWS\system32\drivers\Deg39.sys" killed successfully
```

How to collect files

To collect files paste the list on the "Script" tab after "Files:" command and click the "Run" button. The selected files will be ZIPped

to catchme.zip located on desktop.

```
Files:
C:\WINDOWS\system32\drivers\symavc32.sys
C:\WINDOWS\system32\drivers\Deg39.sys
```

content of catchme.log

```
Processing "Files:"

file zipped: C:\WINDOWS\system32\drivers\symavc32.sys -> catchme.zip -> symavc32.sys ( 178688 bytes )
file zipped: C:\WINDOWS\system32\drivers\Deg39.sys -> catchme.zip -> Deg39.sys ( 178688 bytes )
```

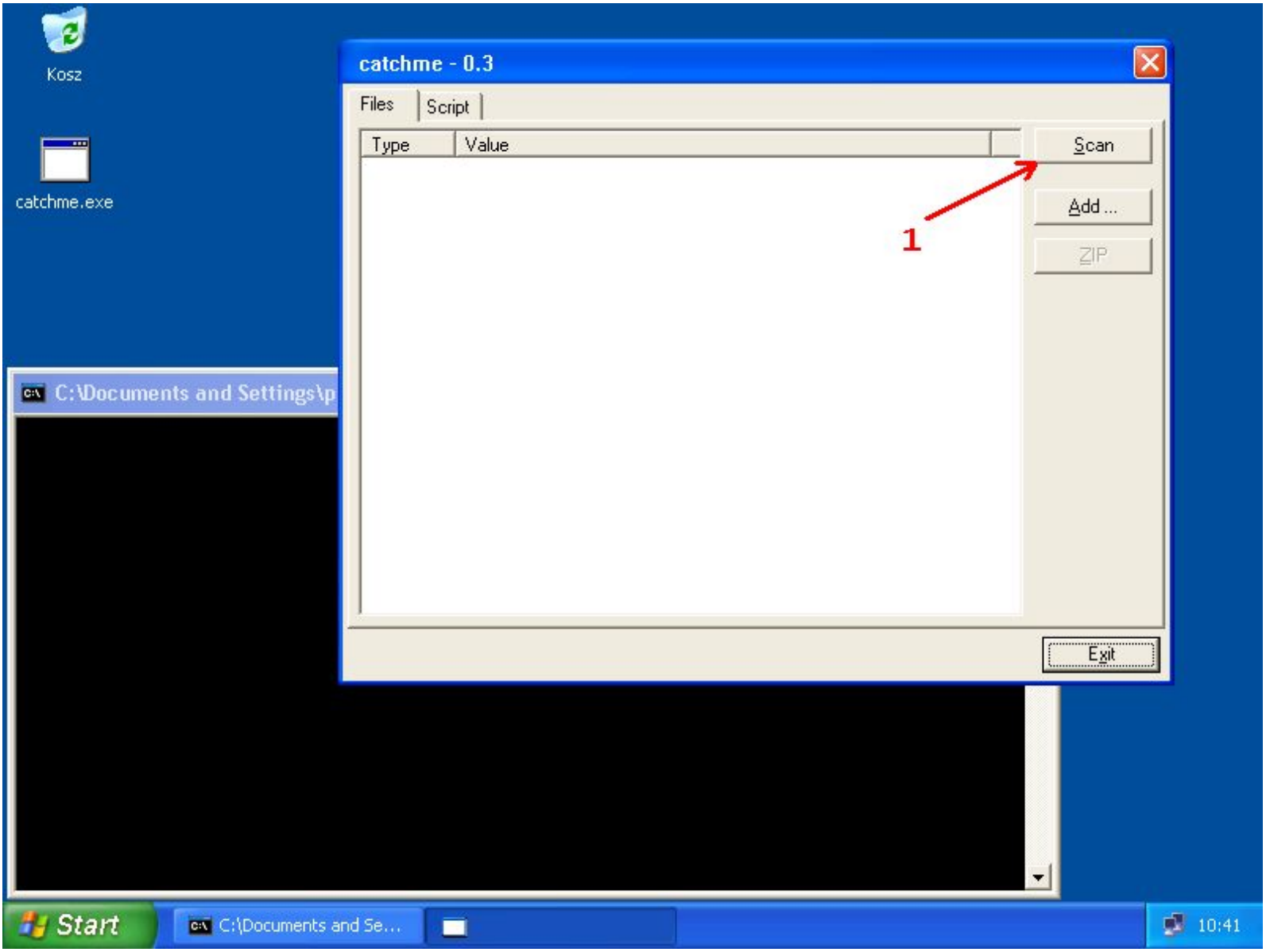
List of command line options recognized by catchme

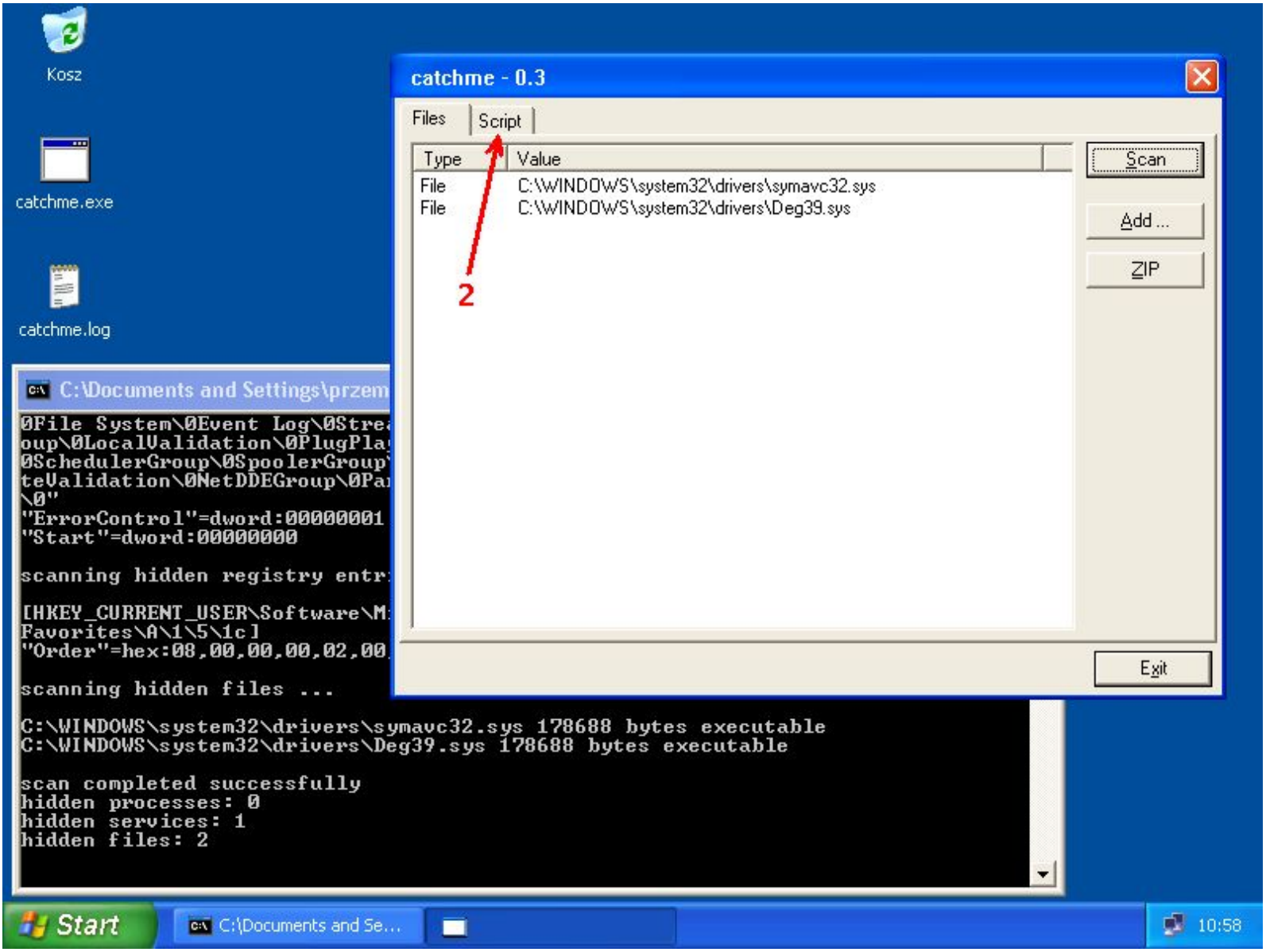
to display all available options type: **catchme -?**

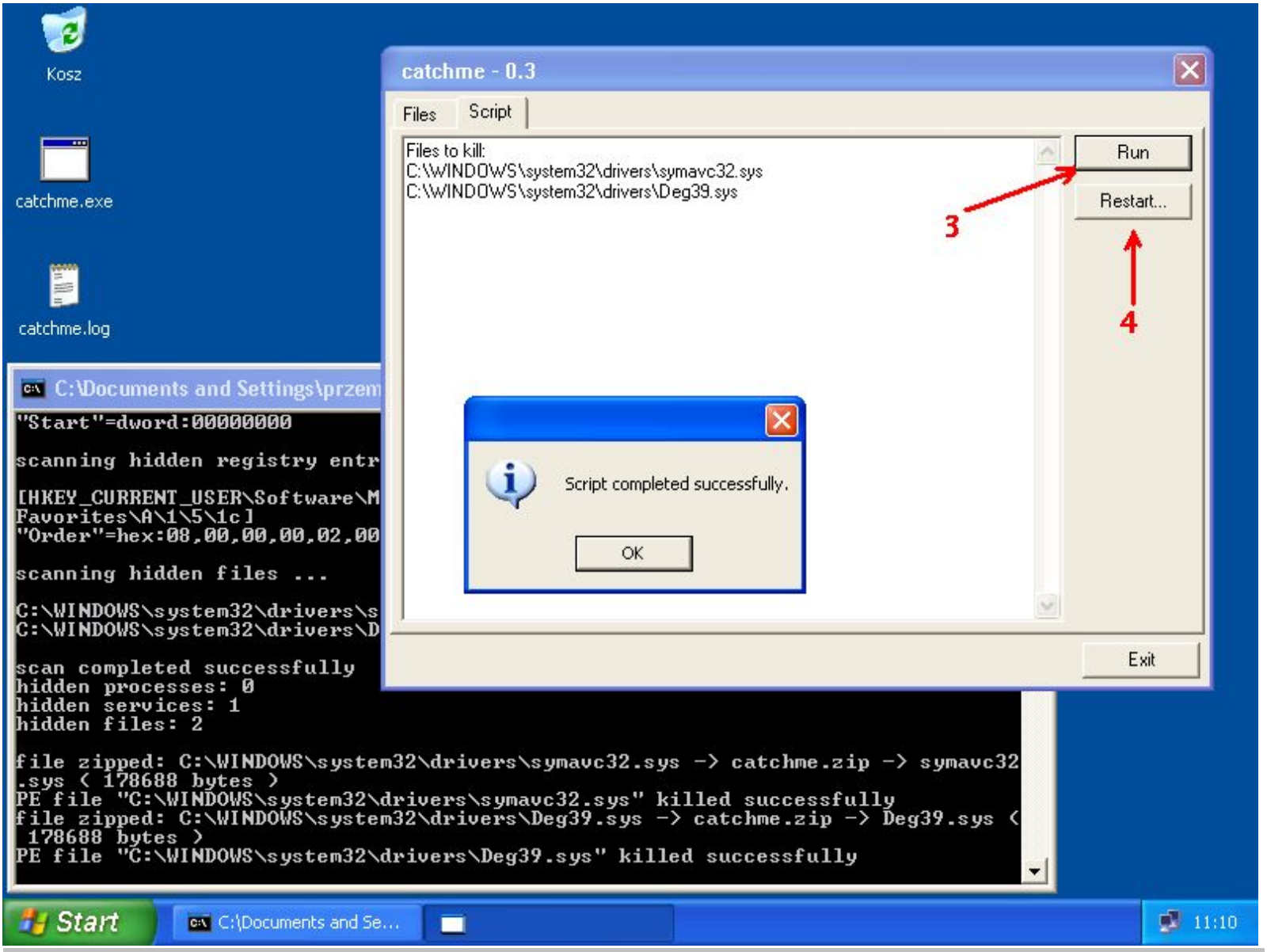
```
Usage: catchme.exe [options]

    -p                        processes scan
    -s                        servicess scan
    -r                        autostart entries scan
    -f [folder]               files scan
    -c source destination     copy file
    -e filename               delete file
    -E filename               delete file without making a copy
    -k filename               kill file
    -K filename               kill file without making a copy
    -o filename dummy         overwrite/replace file with dummy
    -O filename dummy         overwrite/replace file with dummy without making a copy
    -w filename str1 str2     replace unicode str1 with str2 in the file
    -W filename str1 str2     replace unicode str1 with str2 in the file without making a copy
    -m filename str1 str2     replace ascii str1 with str2 in the file
    -M filename str1 str2     replace ascii str1 with str2 in the file without making a copy

    -u                        do not display GUI
    -a                        display all information
    -t                        show all Alternate Data Streams
    -g                        grab hidden files to %DESKTOP%\catchme.zip
    -n                        use NTAPI
    -d                        scan subfolders ( use with options -f and -a )
    -l                        log file name
    -I                        detect hidden items via catchme process
    -q                        do not pause at end of scan
    -h                        display this help

samples of usage:

    catchme.exe -a -p
    catchme.exe -a -s
    catchme.exe -a -f C:\WINDOWS
    catchme.exe -a -d -f C:\WINDOWS
    catchme.exe -k C:\WINDOWS\system32:pe386.sys
    catchme.exe -c C:\WINDOWS\system32:pe386.sys C:\pe386.sys

please note that you need administrator rights to perform deep scan
```

Example of using catchme - Trojan.Srizbi:

- Run catchme.exe
- Click the "Scan" button to start scan
- When the scan finishes go to the "Script" tab
- Paste list of "Files to kill:"
- Restart machine to complete operation


Kosz
catchme.exe
catchme - 0.3
Files
Script
Type
Value
Scan
Add ...
ZIP
1
Exit
C:\Documents and Settings\p
Start
C:\Documents and Se...
10:41


Kosz
catchme.exe
catchme.log
catchme - 0.3
Files
Script
Type
Value
File
C:\WINDOWS\system32\drivers\symavc32.sys
File
C:\WINDOWS\system32\drivers\Deg39.sys
Scan
Add ...
ZIP
Exit
2
C:\Documents and Settings\przem
0File System\0Event Log\0Stre
oup\0LocalValidation\0PlugPla
0SchedulerGroup\0SpoolerGroup
teValidation\0NetDDEGroup\0Pa
\0"
"ErrorControl"=dword:00000001
"Start"=dword:00000000
scanning hidden registry entr
[HKEY_CURRENT_USER\Software\M
Favorites\A\1\5\1c]
"Order"=hex:08,00,00,00,02,00
scanning hidden files ...
C:\WINDOWS\system32\drivers\symavc32.sys 178688 bytes executable
C:\WINDOWS\system32\drivers\Deg39.sys 178688 bytes executable
scan completed successfully
hidden processes: 0
hidden services: 1
hidden files: 2
Start
C:\Documents and Se...
10:58




```
catchme 0.3.1262 W2K/XP/Vista - rootkit/stealth malware detector by Gmer, http://www.gmer.net
Rootkit scan 2007-10-16 11:02:47
Windows 5.1.2600 Dodatek Service Pack 2 NTFS

scanning hidden processes ...

scanning hidden services & system hive ...

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Deg39]
"Type"=dword:00000001
"Tag"=dword:00000001
"Group"="System Reserved\0Boot Bus Extender\0System Bus Extender\0SCSI miniport\0Port\0
Primary Disk\0SCSI Class\0SCSI CDROM Class\0FSFilter Infrastructure\0FSFilter System\0
FSFilter Bottom\0FSFilter Copy Protection\0FSFilter Security Enhancer\0FSFilter Open File\0
FSFilter Physical Quota Management\0FSFilter Encryption\0FSFilter Compression\0FSFilter HSM\0
FSFilter Cluster File System\0FSFilter System Recovery\0FSFilter Quota Management\0
FSFilter Content Screener\0FSFilter Continuous Backup\0FSFilter Replication\0
FSFilter Anti-Virus\0FSFilter Undelete\0FSFilter Activity Monitor\0FSFilter Top\0
Filter\0Boot File System\0Base\0Pointer Port\0Keyboard Port\0Pointer Class\0Keyboard Class\0
Video Init\0Video\0Video Save\0File System\0Event Log\0Streams Drivers\0NDIS Wrapper\0
COM Infrastructure\0UIGroup\0LocalValidation\0PlugPlay\0PNP_TDI\0NDIS\0TDI\0NetBIOSGroup\0
ShellSvcGroup\0SchedulerGroup\0SpoolerGroup\0AudioGroup\0SmartCardGroup\0NetworkProvider\0
RemoteValidation\0NetDDEGroup\0Parallel arbitrator\0Extended Base\0PCI Configuration\0"
"ErrorControl"=dword:00000001
"Start"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\Deg39]
"Type"=dword:00000001
"Tag"=dword:00000001
"Group"="System Reserved\0Boot Bus Extender\0System Bus Extender\0SCSI miniport\0Port\0
```

```
Primary Disk\0SCSI Class\0SCSI CDROM Class\0FSFilter Infrastructure\0FSFilter System\0
FSFilter Bottom\0FSFilter Copy Protection\0FSFilter Security Enhancer\0FSFilter Open File\0
FSFilter Physical Quota Management\0FSFilter Encryption\0FSFilter Compression\0FSFilter HSM\0
FSFilter Cluster File System\0FSFilter System Recovery\0FSFilter Quota Management\0
FSFilter Content Screener\0FSFilter Continuous Backup\0FSFilter Replication\0
FSFilter Anti-Virus\0FSFilter Undelete\0FSFilter Activity Monitor\0FSFilter Top\0Filter\0
Boot File System\0Base\0Pointer Port\0Keyboard Port\0Pointer Class\0Keyboard Class\0
Video Init\0Video\0Video Save\0File System\0Event Log\0Streams Drivers\0NDIS Wrapper\0
COM Infrastructure\0UIGroup\0LocalValidation\0PlugPlay\0PNP_TDI\0NDIS\0TDI\0NetBIOSGroup\0
ShellSvcGroup\0SchedulerGroup\0SpoolerGroup\0AudioGroup\0SmartCardGroup\0NetworkProvider\0
RemoteValidation\0NetDDEGroup\0Parallel arbitrator\0Extended Base\0PCI Configuration\0"
"ErrorControl"=dword:00000001
"Start"=dword:00000000

scanning hidden registry entries ...

scanning hidden files ...

C:\WINDOWS\system32\drivers\symavc32.sys 178688 bytes executable
C:\WINDOWS\system32\drivers\Deg39.sys 178688 bytes executable

scan completed successfully
hidden processes: 0
hidden services: 1
hidden files: 2

file zipped: C:\WINDOWS\system32\drivers\symavc32.sys -> catchme.zip -> symavc32.sys ( 178688 bytes )
PE file "C:\WINDOWS\system32\drivers\symavc32.sys" killed successfully
file zipped: C:\WINDOWS\system32\drivers\Deg39.sys -> catchme.zip -> Deg39.sys ( 178688 bytes )
PE file "C:\WINDOWS\system32\drivers\Deg39.sys" killed successfully
```

Previous version - catchme 0.2

---

catchme 0.2 is the rootkit scanner that detects all userland rootkits including gromozon, hexdef, vanquish and AFX. It cannot detect kernel mode rootkits like Rustock (PE386), Haxdoor, etc.

How to scan:

- Download **catchme.exe** (25kB) to your desktop.
- Double click the **catchme.exe** to run it
- Open **catchme.log** to see results

Samples:

- gromozon rootkit

```
catchme 0.1 W2K/XP - userland rootkit detector by Gmer, 17 October 2006
http://www.gmer.net

detected NTDLL code modification:
ZwQueryDirectoryFile, ZwQuerySystemInformation

Scanning hidden processes ...

Scanning hidden services ...

Scanning hidden autostart entries ...

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
  AppInit_DLLs = \\?\D:\WINDOWS\com4.exg

Scanning hidden files ...

D:\WINDOWS\com4.exg
D:\WINDOWS\wgifi1.dll

scan completed successfully
hidden processes: 0
```

```
hidden services: 0
hidden files: 2
```

- hxdef rootkit

```
catchme 0.1 W2K/XP - userland rootkit detector by Gmer, 17 October 2006
http://www.gmer.net

detected NTDLL code modification:
ZwEnumerateKey, ZwEnumerateValueKey, ZwQueryDirectoryFile, ZwQuerySystemInformation

Scanning hidden processes ...

  hxdef100.exe [1416]

Scanning hidden services ...

HKLM\SYSTEM\CurrentControlSet\Services\HackerDefender100
  Type = 16
  Start = 2
  ErrorControl = 63
  ImagePath = C:\rootkits\hxdef100\hxdef100.exe
  DisplayName = HXD Service 100
  ObjectName = LocalSystem
  Description = powerful NT rootkit

HKLM\SYSTEM\CurrentControlSet\Services\HackerDefenderDrv100
  ErrorControl = 63
  ImagePath = \??\C:\rootkits\hxdef100\hxdefdrv.sys
  Start = 3
  Type = 1

Scanning hidden autostart entries ...

Scanning hidden files ...

C:\rootkits\hxdef.txt
C:\rootkits\hxdef100
C:\rootkits\hxdef100\hxdef100.2.ini
C:\rootkits\hxdef100\hxdef100.exe
C:\rootkits\hxdef100\hxdef100.ini
C:\rootkits\hxdef100\hxdefdrv.sys
C:\WINDOWS\Prefetch\HXDEF100.EXE-351601D2.pf

scan completed successfully
hidden processes: 1
hidden services: 2
hidden files: 7
```

- vanquish rootkit

```
catchme 0.1 W2K/XP - userland rootkit detector by Gmer, 17 October 2006
http://www.gmer.net

Scanning hidden processes ...

Scanning hidden services ...

HKLM\SYSTEM\CurrentControlSet\Services\vanquish
  Type = 272
  Start = 2
  ErrorControl = 1
  ImagePath = "C:\WINNT\vanquish.exe"
  DisplayName = Vanquish Autoloader v0.2.1
  ObjectName = LocalSystem

Scanning hidden autostart entries ...

Scanning hidden files ...

C:\vanquish.log
C:\WINNT\vanquish.dll
C:\WINNT\vanquish.exe

scan completed successfully
```

```
hidden services: 1
hidden files: 3
```

- AFX rootkit

```
catchme 0.1 W2K/XP - userland rootkit detector by Gmer, 17 October 2006
http://www.gmer.net

detected NTDLL code modification:
ZwEnumerateKey, ZwEnumerateValueKey, ZwQueryDirectoryFile, ZwQuerySystemInformation

Scanning hidden processes ...

  root.exe [1556]

Scanning hidden services ...

HKLM\SYSTEM\CurrentControlSet\Services\rewt
  Type = 272
  Start = 2
  ErrorControl = 63
  ImagePath = C:\rootkits\rewt\root.exe
  ObjectName = LocalSystem

Scanning hidden autostart entries ...

Scanning hidden files ...

C:\rootkits\rewt
C:\rootkits\rewt\hook.dll
C:\rootkits\rewt\ReadMe.txt
C:\rootkits\rewt\root.exe

scan completed successfully
hidden processes: 1
hidden services: 1
hidden files: 4
```