Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes

EN SAVOIR PLUS OK!

News Rootkits **FAQ**

Contact

GMER is an application that detects and removes rootkits .

It scans for:

 hidden processes hidden

threads hidden modules

 hidden services hidden files

 hidden disk sectors (MBR)

hidden Alternate Data Streams hidden

registry keys drivers hooking SSDT drivers

hooking IDT drivers hooking IRP calls

inline hooks

■ GMER 2.0.18323 WINDOWS 6.1.7600 ×64 Rootkit/Malware >>> Type Name Value ✓ System C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdD3Transition] ▼ Sections [ffff80000b9b840] \SystemRoot\system32\kdcom.dll [.text] C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdD0Transition] IAT [fffff80000b9b834] \SystemRoot\system32\kdcom.dll [.text] ✓ IAT/EAT IAT C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdReceivePacket] [fffff80000b9b920] \SystemRoot\system32\kdcom.dll [.text] ▼ Devices [fffff80000b9b918] \SystemRoot\system32\kdcom.dll [.text] IAT C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdSendPacket] ▼ Trace I/O C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdRestore] C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdSave] [fffff80000b9b90c] \SystemRoot\system32\kdcom.dll [.text] IAT [fffff80000b9b900] \SystemRoot\system32\kdcom.dll [.text] ✓ Modules IAT C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdDebuggerInitialize0] [fffff80000b9b8e4] \SystemRoot\system32\kdcom.dll [.text] IAT ▼ Processes IAT C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdDebuggerInitialize1] [ffff80000b9b8f0] \SystemRoot\system32\kdcom.dll [.text] 굣 Threads C:\Windows\system32\hal.dll[KDC0M.dll!KdRestore] [fffff80000b9b90c] \SystemRoot\system32\kdcom.dll [.text] IAT C:\Windows\system32\kdcom.dll[ntoskrnl.exe!HalPrivateDig ✓ Libraries IAT IAT C:\Windows\system32\kdcom.dll[ntoskrnl.exe!atol] ✓ Services C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KeFindConfig IAT ✓ Registry IAT C:\Windows\system32\kdcom.dll[ntoskrnl.exelMmMaploSp ▼ Files IAT C:\Windows\system32\kdcom.dll[ntoskrnl.exel_strupr] WARNING !!! IAT C:\Windows\system32\kdcom.dll[ntoskrnl.exe!InbvDisplayS ✓ Quick scan IAT C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KdDebugge GMER has found system modification caused by ROOTKIT activity. □ C:V C:\Windows\system32\kdcom.dll[ntoskrnl.exe!strstr] IAT IAT C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KeBugCheck C:\Windows\system32\kdcom.dll[HAL.dll!HalQueryRealTim IAT IAT C:\Windows\system32\kdcom.dll[HAL.dll!KdComPortInUse] OK \Driver\atapi \Device\Ide\IdeDeviceP0T0L0-0 Devi. ✓ ADS \Driver\atapi -> DriverStartlo \Device\Ide\IdePort0 Devi... \Driver\atapi -> DriverStartlo \Device\Ide\IdePort1 fffffa800156d480 Devi... fffffa800156d480 \Driver\atapi -> DriverStartlo \Device\Ide\IdeDeviceP1T0L0-2 Devi... Show all fffffa800156d480 \Driver\atapi -> DriverStartIo \Device\ScsiPort0 Devi... fffffa800156d480 Devi... \Driver\atapi -> DriverStartlo \Device\ScsiPort1 Scan Trace ntoskrnl.exe CLASSPNP.SYS disk.sys >>UNKNOWN [0xfffffa800156d6c0]<< fffffa800156d6c0 1 ntllofCallDriver -> \Device\Harddisk0\DR0[0xfffffa8001354790] fffffa8001354790 Trace Сору 3 CLASSPNP.SYS[fffff8800190443f] -> ntllofCallDriver -> \Device\Ide\IdeDeviceP0T0L0-0[0... fffffa80012ba680 Trace \Driver\atapi[0xfffffa800156be70] -> IRP_MJ_CREATE -> 0xfffffa800156d6c0 fffffa800156d6c0 Trace Save. Disk \Device\Harddisk0\DR0 TDL4@MBR code has been found Disk \Device\Harddisk0\DR0 sector 0: rootkit-like behavior GMER 2.0.18323 WINDOWS 6.1.7600 ×64 Exit

GMER runs on XP/VISTA/7/8/10

You can download GMER here.

Please see the FAQ section and feel free to send any comments here .

Download

The latest version of GMER 2.2.19882

GMER runs only on Windows NT/W2K/XP/VISTA/7/8/10

GMER application:

GMER.exe SHA256:

Download EXE

or ZIP archive: gmer.zip (372kB)

E8A3E804A96C716A3E9B69195DB6FFB0D33E2433AF871E4D4E1EAB3097237173

It's recommended to download randomly named EXE (click button above) because some malware won't let gmer.exe launch.

Avast! antivirus integrated with GMER

o avast!

aswMBR - antirootkit with avast! AV engine

actively protecting over 230 million PCs

aswMBR.exe

Thanks to: MR Team, CastleCops, ...

Version History:

This is list of changes for each release of GMER:

- 2.2
- Added support for Windows 10
- Improved files & disk scanning
- Added third-party software component scan
- Improved services scanning
- Improved registry scanning - Fixed Windows 8 x86 lock issue
- 2.0
- Added support for Windows 8
- Added full support for Windows x64
- Added Trace I/O function
- Added disk "Quick scan" function
- 1.0.15

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes

EN SAVOIR PLUS

- Improved "delete file" function
- Added disk browser
- Added registry browser and editor
- Added registry exportsAdded "Kill file" and "Disable service" options to help remove stubborn malware
- Added new option "gmer.exe -nodriver"
- Added new option "gmer.exe -killfile"

gmer.exe -killfile C:\WINDOWS\system32\drivers\runtime2.sys

gmer.exe -killfile C:\WINDOWS\system32:pe386.sys

- Simplified displaying of device hooks
- Added detection and removal of MBR rootkit
- 1.0.13
- Added kernel & user IAT hooks detection
- Added AttachedDevice hooks detection
- Added detection of hooks outside code sections
- Added button "Save ..." log
- Added kernel & user mode code sections scanning (inline hooks)
- Added code restoring
- Improved "GMER Safe Mode"
- Improved hidden process scanning
- 1.0.11
- Added "Simple mode"
- Added threads tab
- Added hidden Alternate Data Stream (NFTS Stream) scanning
- Added hidden threads scanning
- Improved hidden process scanning
- Improved hidden modules scanning
- Improved hidden files scanning
- Fixed devices scanning
- 1.0.10
- English version
- Improved process monitoring
- Added Autostart tab
- Added "GMER Safe Mode"Added "Files" window
- Added full path of process
- Added loaded libraries
- Added hidden libraries scanning
- 1.0.9
- Improved hidden services scanning.
- Improved ROOTKIT scanning.
- Improved "Kill all" and "Restart".
- Added hidden services scanning.
- Added hidden services deletion.
- Added hidden files deletion.
- Added restoring SSDT table.
- Added Interpretation of the rootkit scanning.
- Added CMD tab executing shell commands
- Fixed showning registry keys
- Fixed tracing library loading.
- Improved hidden files scanning.
- Added "Services" tab.
- 1.0.6
- Fixed hidden registry keys scanning.
- 1.0.5
- Added online antivirus scanning.
- Fixed scanning of rootkits that hooks devices' IRP calling
- 1.0.4
- Added rootkit scanning.
- Added loading devices monitoring.
- Added log.
- Fixed NTVDM.EXE tracing.
- 1.0.2
- Added processes tab
- Added "Kill all" function.
- Added "Shell" option in the "Process" section, that executes an application other than Explorer.exe

[Process] Shell=gmer.exe

- 1.0.1
- First release.

News

2013.01.04

pcworld.com: Detect and remove rootkits with GMER

2013.01.03

New version 2.0.18327 with full x64 support has been released.

2011.03.18

New version 1.0.15.15565 has been released.

2010.11.24

New version 1.0.15.15530 has been released.

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OF

ALWIE SOILWATE HAS TELEASED AVAST 4.0 COILCAINING AND TOOLKIL DASED ON GMEK LECHNOLOGY.

2008.01.18

Version 1.0.14.14116 released.

2008.01.11

bbc.co.uk: Warning on stealthy Windows virus

2008.01.08

washingtonpost.com: New Nasty Hides From Windows, Anti-Virus Tools

2008.01.02

Stealth MBR rootkt found in the wild!

You can read about it here: [1], [2]

2007.06.26

Version 1.0.13.12540 released.

2007.03.14

Just another DDoS story - One Person's Perspective by Paul Laudanski

"... Around the middle of February 2007, CastleCops itself became the target of a large scale DDoS. Not new to this kind of attack, it is the first time CastleCops experienced such a large throughput at nearly 1Gbit/s ..."

2007.03.09

Andy Manchesta added catchme into SDFix tool.

2007.02.26

Thanks to Marco Giuliani for preparing Italian version of help!

http://www.pcalsicuro.com/main/2007/02/guida-a-gmer/

2007.02.21

New version of catchme with Windows Vista support released.

Catchme has been integrated with ${f combofix}$ developed by ${f sUBs}$. Keep up the good fight ${f sUBs}$!.

2007.01.20

After over a month of fight my web page is up and running.

 $Thank \ you \ Paul \ Vixie \ and \ ISC, \ Matt \ Jonkman, \ guys \ from \ register.com, \ MR \ Team \ and \ everyone \ who \ helped \ me.$

Special thanks to $\mbox{\bf Paul Laudanski}$ who won this battle.

You can read about it here: [1], [2]

2006.12.13

My doman DDoS-ed for the first time.

2006.12.06

I developed sample rootkit "test.sys" which hides its file from all public rootkit detectors:

- BlackLight
- Sophos ARK
- RootkitRevealer
- IceSword
- DarkSpySVV
- 500

GMER

Rootkit doesn't create hooks (SSDT, IRP, SYSENTER, IDT, inline, FSF) and its modifications are not visible.

You can see it in action in these movies: test.wmv, test2.wmv (0.9MB, 0.7MB Windows Media Video 9 codec).

The detection of this type of rootkit will be added into the next version.

2006.11.28

Version 1.0.12.12011.

2006.10.17

New tool - catchme released.

2006.06.20

washingtonpost.com: New Rootkit Detectors Help Protect You and Your PC

FAQ

Frequently Asked Questions

Question: Do I have a rootkit?

Answer: You can scan the system for rootkits using GMER. Run gmer.exe, select Rootkit tab and click the "Scan" button.

If you don't know how to interpret the output, please **Save** the log and send it to my email address.

Warning! Please, do not select the "Show all" checkbox during the scan.

Question: How to create "3rd party" log?

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS

Answer: Just delete the exe file.

Question: My computer is infected and GMER won't start:

Answer: Try to rename gmer.exe to iexplore.exe and then run it.

Question: How do I remove the Rustock rootkit?

Answer: When GMER detects hidden service click "Delete the service" and answer YES to all questions.

Туре	Name	Value	
SYSENTER Code text text text text text text text Thread	? F7E 4AA5E ntoskml.exelKei386E oiHelper + 1269 tcpip.sys! PTransmit + 4279 tcpip.sys! PTransmit + 9433 tcpip.sys! PTransmit + 18018 wanarp.sys [noname] (**** hidden ****) 4:1040	F7E 4BFAF plofCallDriver 804D8DF0 3 Bytes F7D97CFA 6 Bytes F7D9911C 6 Bytes F7D9B2A5 6 Bytes F9BF73FD 7 Bytes F7E 47000 F7E 4A08A	·
Service ADS	D:\WINDOWS\system32:lzx32.sys (*** hidden ***)	[SYSTEM] pe386	Restore SSDT
	D:\WINDOWS\system32:lzx32.sys		11030010 3301
			Restore Code
			Delete the service
			Delete file
			Kill process

Question: How do I show all NTFS Streams?

Answer: On the "Rootkit Tab" select only: Files + ADS + Show all options and then click the Scan button.

Question: Can I launch GMER in Safe Mode?

Answer: Yes, you can launch GMER in Safe Mode, however rootkits which don't work in Safe Mode won't be detected.

Question: I am confused as to use delete or disable the hidden "service".

Answer: Sometimes "delete the service" option wont work because the rootkit protects its service. So, in such case use: 1) "disable the service", 2) reboot your machine, and 3) "delete the service".

Contact

Use the following address: info@gmer.net

Copyright (c) GMER 2004 - 2016