



Forum: Dépannage

Topic: Roguekiller

Subject: Re: Roguekiller

Publié par: Eddy713

Contribution le : 26/10/2014 17:51:44

Bonjour speddycool,

Voilà avec l'ancienne version de roguekiller, ça marche.

J'essaye de joindre le rapport en pdf ou en txt mais ça marche pas, donc copier coller :

RogueKiller V10.0.3.0 [Oct 22 2014] par Adlice Software

Mail : <http://www.adlice.com/contact/>

Remontées : <http://forum.adlice.com>

Site Web : <https://www.surlatoile.org/RogueKiller/>

Blog : <http://www.adlice.com>

Système d'exploitation : Windows XP (5.1.2600 Service Pack 3) 32 bits version

Démarrage : Mode normal

Utilisateur : Administrateur [Droits d'admin]

Mode : Recherche -- Date : 10/26/2014 17:42:01

Processus malicieux : 0

Entrées de registre : 0

Tâches planifiées : 0

Fichiers : 0

Fichier HOSTS : 0 [Too big!]

Antirootkit : 11 (Driver: CHARGE)

[Filter(Kernel.Filter)] Driveratapi @ Unknown : DriverCdrom @ DeviceCdRom1

(SystemRootsystem32DRIVERSNic1394.sys)

[Filter(Kernel.Filter)] Driveratapi @ Device 000006b : DriverCdrom @ DeviceCdRom0

(SystemRootsystem32DRIVERSNic1394.sys)

[Filter(Kernel.Filter)] Driveratapi @ Device 000006a : DriverDisk @ DeviceHarddisk1DR1 (ViPrt.sys)

[Filter(Kernel.Filter)] Driveratapi @ DeviceHarddisk1DR1 : DriverPartMgr @ Unknown (videX32.sys)

[Filter(Kernel.Filter)] Driveratapi @ Device 0000069 : DriverDisk @ DeviceHarddisk0DR0 (ViPrt.sys)

[Filter(Kernel.Filter)] Driveratapi @ DeviceHarddisk0DR0 : DriverPartMgr @ Unknown (videX32.sys)

[Filter(Kernel.Filter)] DriverDisk @ DeviceHarddisk1DR1 : DriverPartMgr @ Unknown (videX32.sys)

[Filter(Kernel.Filter)] DriverDisk @ DeviceHarddisk0DR0 : DriverPartMgr @ Unknown (videX32.sys)

[IAT:Addr] (explorer.exe @ sti.dll) CFGMGR32.dll - CM_Reenumerate_DevNode :

C:WINDOWSsystem32SETUPAPI.dll @ 0x779526a5

[IAT:Addr] (explorer.exe @ sti.dll) CFGMGR32.dll - CM_Get_DevNode_Status :
C:WINDOWSsystem32SETUPAPI.dll @ 0x778ec6eb
[IAT:Addr] (explorer.exe @ sti.dll) CFGMGR32.dll - CM_Get_Parent :
C:WINDOWSsystem32SETUPAPI.dll @ 0x77957a5d

▣▣▣ Navigateurs web : 0 ▣▣▣

▣▣▣ MBR Verif : ▣▣▣

+++++ PhysicalDrive0: ST380011A +++++

--- User ---

[MBR] 7f8d4fe88249d7512f9fec981f904b18

[BSP] 59f0acc5c5820b736ff9bbc523cbbb9b : Windows XP MBR Code

Partition table:

0 - [ACTIVE] NTFS (0x7) [VISIBLE] Offset (sectors): 1824103 | Size: 75421 MB

User = LL1 ... OK

User = LL2 ... OK

+++++ PhysicalDrive1: ST380011A +++++

--- User ---

[MBR] 9f329404286bffc3418c5a275a32eba5

[BSP] 82d3d7ba8f8a2ba891a5e3684f3a2973 : Legit.Unknown MBR Code

Partition table:

0 - [XXXXXX] NTFS (0x7) [VISIBLE] Offset (sectors): 63 | Size: 76308 MB

User = LL1 ... OK

User = LL2 ... OK

=====

RKreport_DEL_10262014_111532.log - RKreport_DEL_10262014_162504.log -

RKreport_SCN_10262014_111108.log - RKreport_SCN_10262014_112037.log

RKreport_SCN_10262014_123730.log

Merci de votre aide

Fichier(s) attaché(s):

-

[RKreport_SCN_10262014_174201.pdf](#) Taille: 47.32 KB; Hits: 659