Tutorial GMER

GMER est un des meilleurs scanner rootkit. Voici donc un tutorial pour GMER démystifier le programme.

Quelques liens relatifs à Gmer et Rootkit :

- Le danger et fonctionnement des Rootkits
- Gmer Scanner Rootkit efficace »>Fiche de GMER dans les programmes utiles
- Les Anti-Rootkit / Scanner Rootkit
- Supprimer les rootkits sous Windows

DISLAIMER : GMER est un outil puissant...

Cette page est destinée aux personnes ayant un minimum de connaissance sur le fonctionnement de Windows. Si vous n'avez pas de connaissances, n'utilisez pas GMER.

Ce n'est pas la peine de scanner avec GMER et demander de l'aide sur le forum pour analyser le rapport. On utilise pas un programme si on ne comprend pas le rapport ou pour le plaisir ou par excès de paranoïa.

Téléchargement de GMER

L'adresse du site officiel de GMER est : http://www.gmer.net

Le téléchargement du programme se fait à partir du menu *Files* à gauche.

GMER est disponible au format ZIP (*gmer.zip*) ou via un EXE avec un nom aléatoire (*Download EXE*), ceci permet l'exécution sur des PC avec des infections bloquant l'exécution de fichiers portant le nom GMER.

elsiks	Carl Caracter	GI	MER our rectigits are belong to us [*]
Start	Download		1/(PALLERA VA
News Rootkit Logs	The latest version of GMER 1.0.15.14939 GMER runs only on Windows NT/W2K/XP/VISTA	1	2 AND
Files	GMER application	Download EXT	(or ZIP archives gmor.nip (284kB)
FAQ	It's recommended to download randomly named EXE	Nek apove buttan i	ecause some malware doesn't let gmer.exe laun
Contact	Userland rootkit detector	Varia	(25kB)
	Example of rootkit scanning and removal	gins r. winv	(87kB Windows Media Video 9 codec)
Donate	Sample of undetectable rootkin	100LWIIIV	(950kB Windows Media Video 9 codec)
	Gromozon rootkit unhooking i	gromozon.wmv	(0,6MB Windows Media Video 9 codec)
	Log samples	Rustock.B, Grem	ozon, Haniloor, hudef, BadRRDemo
	IceSword + DarkSpy + GMER + pe386 rootkit :	pe386.wmV	(0,5MB Windows Media Video 9 codec)
	Thanks to MR Team, CastleCops,		

Avant toute utilisation de GMER, veuillez désactiver votre antivirus, antispyware sous peine de vous prendre un BSOD.

L'exécution de GMER se fait simplement en double-cliquant sur le fichier téléchargé. Le programme se lance alors... si un rootkit est détecté dès le lancement du programme, une popup vous en informe.



Onglet GMER

Processes

L'onglet Processes permet de lister les processus démarrés et éventuellement afficher les processus considérés comme rootkités.

Les boutons :

- Kill Process permet de tuer le processus sélectionné
- *Kill All* tue tous les processus et services, Windows ne tourne alors qu'avec le stric minimum (voir application plus bas).
- *Restart* redémarre l'ordinateur (à utiliser après Kill All par exemple)
- *Files* permet de naviguer dans les dossiers pour démarrer une application.

Dans la partie basse GMER affiche les libraries et Thread (si le

bouton Libraries à droite est coché).

GMER ne permet pas de manipuler ces derniers, Process Explorer permet cela, reportez-vous à la page virtumonde VS Process Explorer

I GMER 1.0.15.14939								- 0
ocesses Modules Services Files Registry Roothil/	Malware Autostat	CHD	1					
topess	Parameters	PID	Memory	Threads	Handles	User time	Kilme	and a
VProgram Files/Adobe/Acrobat 7.0\Reader/veader_sl.exe		1168	2780	3	42	0.078	NA POL	ACT 1
//Program Files/Ultrav/NC/winvnc.exe //Program Files/Ultrave/Ultrave Tools/Ultrave/Service.exe		172	4368	3	61	0.078	Ki a	4
"Program Files"\/Mware/\/Mware Tools\//MwareTray.eve		1040	3832	2	51	0.078	ITT Barbar	een.
Program Files/WMware/WMware Tools/WMwareUser.exe		1049	3256	2	44	0.140	P PROTOR	220
WWNDOWSV3129837 eve		1144	6512 150ch	10	190	242,734		
WNDOWS/asten32/cous.exe		644	1656	14	378	10,109	Rept	at .
WINDOWS\system32\sass.exe		728	760	15	333	0.468		
WNDDWS/upten32/services.exe		716	4532	24	299	0.468	12223733	
'WINDOWS'susten32'sychost eve		292	3728	6	36	0.453	M Libraries	E.,
WINDOWS\system32\sychost.exe		308	5614	2h	264	0.200		
WINDOWS/system32/uvchost.exe		305	4460	CI,	212	0.295		
WINDOWS/autenci2/uvchost.eve		1228	20	12	129	0.109		
WINDOWS\system32\system32\system32		1.55	6	0	129	0.062		
/WINDOWS/system32/winlogon.exe		3	•(500	24	523	0,734	Files	-
sulen.	105	4	301	41	518	0.000		
ystem Ide	ale.	0	16	1	0	0.000 -		
4	0.				- 1		-	
Acure: Threads								
Name		Size		Address			1	
://winDdw5/TEMP\8N2.trp		0,00	017000	0x05000000	100	1.10	1	
://wiNDOWS/apsten/32/vtdl.dl		0,00	0800080	0x7C900000	1	1.1	1	
2/WINDOWS/system/32/kenel32.dl //WINDOWS/system/22/USEB/32.4l		0.00	094000	0x7C800000				
://wiNDDW5/apstern32/GDI32.dll		0.00	046000	0x77F10000	1			
://wiNDOW5/apten32/SHELL32.dl		0,00	814000	Dx7C9C0000	1			
2. WINDOWS lapites 32 visivel. dl		0600	058000	0677010000		-	1	
rocesses 25 (hidden 1)		Com	nand [B	un
							-	

Modules

Affiche les modules chargés dans le kernel Windows. Aucune opération n'est possible, ceci est une fenêtre de consultation.

horana Module	R. Raminer Bler, Bassim Reefit Malaura Autority	lon 1			the local data
Name	File	Eddens	Gas		-
CPI sur	ACR and	E9E5C000	100416		
director in	Murturys	E871E000	100910		
ed type	capterin voor capterin ac varvers verd sys	F0F1E000	45052		
Contract of the	agreed by	ESPERADO	90000		
ange oys	12 ontani Rosti contane 2% DRE/EREL in which do some	FA.896000	4/166		
and and the second	V200 VD001IME=1VMALEKA=1U 000 S=1VTannol as and	F2054000	81900		
ATTC SVS	ValMORalSimulan 200 BUEBS/BATTC SVS	E4203000	16384		
ant SVS	Victor Rout Conten 20 Disard Raas SVS	EA3C3000	R192		
DOTVID 4	Vu/ND/WStoreten 23800T/dD dl	FA288000	12288		
44 51/5	VSurtan Broth Surtan 20 Disearch Cills SVS	FAGREGOO	201303		
vience met	VSector/Regimentar/2008/ERSU-dots tor	EPERROOO	5304R		
LASSEND SVS	Va/MD/Va/Structure/SV/20/EBS//D ASSEND SVS	ESEEBOOD	6304B		
West and	Ventee Root exteen 20 DRIVERS/Consult one	EA352000	16384		
conductions	complete sex optimized activity of the labor light	EA28ED00			
ing our	dais not	ESEEB000	- Cl ·		
man and	disio sus	FIFTHERE	COLUMN AND		
indexed over	depload san	04381000	R192		
and staticas	Sustan Rout/Sustan 20 Divers/Johann atari on	104700	98304		
Amn WMEIRS	Sustem Root/Sustem 20 Discent/stemp WMEIR SVS	101000	R182		
wate put	(Sustant Root/Sustant 2) divers/Duani on	FREREDOO	12288		
buth start	Sustan Rock Sustan Oldinavidur on	BE9C1000	73728		
active sup	SustenRoot/Susten32\divers\dathit av	EA/995000	4096		
AVE WHEN	VSustemPlace/Sustem22/Deluer/Factor	F8300000	143360		
Sc out	VSusten/Roof/uniten/32/DR//ERS/stdc.uni	FA16BDDD	28672		
ion SYS	\SustenRoot\Sustem32\Driven\Fpx SYS	FA05B000	36864		
Dedak ava	\SustemBoot\usstem32\DRIVERSVlpadak.sus	FA1A3000	20460		
Max.sec	filling and	F9DB7000	126976		
4 Rec St/S	\SustenRoot\Sustem32\Drivers\Fr Rec SYS	FA3C1000	8192		
disk ove	fidek eve	F9E2C000	126976		
al dil	Wr/NDOw/Stouten32Vial dl	BORE COOD	131968		
042pit sas	\SustemPool/upsten/32\DRIVERS\8042pit.ppt	F9F68000	53248		
velde avs	intelide pyp	FA3AF000	87.92		
velopm over	\SusteniPool/custen32\DRIVERS\intelpon.cus	F9FA8000	36864		
00ec.899	\SystemPoor/system32\DRI//ERS\psec.sps	F87C0000	77824		
HOND BYS	inaprip. ityl	FSEAE000	36864		
bdclass.sys	\SystemRoot\system32\DRIVERS\bbdclass.sys	FA158000	24576		
					-
				OK	Cancel

Services

Liste les services, le mode de démarrage (colonne Start), le driver et la description. Pour plus d'informations sur les services Windows, se rendre à la page Dossier sur les processus et les services Windows

hoceases	Modules	Services	Files Registry Rootkit/Malware Autostart D	10	
Name		Start	File name	Description	
chicedok.		DISABLED			
sbp480n5		DISABLED			
ACPI		BOOT	system32VDRIVERSVACPLays	Microsoft ACPI Dever	
ACPIEC		DISABLED			
adpu160m		DISABLED			
NFD		SYSTEM	\SystemRoot\System32\drivers\ald typ	AFD Networking Support Environment	
tgp440		BOOT	system32\DRIVERS\agp440.sys	Intel AGP Bus Filter	
Aha154x		DISABLED			
aic78u2		DISABLED			
aic78xx		DISABLED			
Alerter		DISABLED	%SystemRoot%\system32\system33sses	Notifies selected users and computers of adminis	
ALG		MANUAL	%SystemRoot%System32%alg.eve	Application Layer Gateway Service	
Ailide		DISABLED		•	
AendK7		SYSTEM	system32\DRIVERS\amdk7.sys	AMD K7 Put MetaDever	
anviel .		DISABLED		.011	
AppMgmt		MANUAL	%SystemRoot%uystem32\avchost.exe & netsvos	April: accordingement	
anc		DISABLED			
atc3350p		DISABLED			
asc.3950		DISABLED	VO		
AsyncMac		MANUAL	system32\DRIVER5\asyncmac.eve	RAS Asynchronous Media Driver	
al api		BOOT	system32\DR/VERS\atapi sys	Standard IDE/ESDI Hard Disk Controller	
Abdelik.		DISABLED	-11		
Amapo		MANUAL	system32\DRIVERS\assaccivit	ATM ARP Client Protocol	
AudioStv		AUTO	3SystemRoot%System35/avchost.exe ik netovos	Windows Audio	
duning .		MANUAL	system32\DRIVERS\&ubitsb.sys	Audio Stub Dever	
BattC					
Beep		SYSTEM			
BITS		MANUAL	%SystemRoot%\system32\svohost.exe & netsvos	Transfers data between clients and servers in th	
Browner		AUTO	3SystemRoot3System32System32SystemRoot3SystemRoot3System32SSystem32System33System33System33System33System33System33System33System33System33System33System33System33System33System3	Maintains an updated list of computers on the ne	
obid/2k		DISABLED			
od20ent		DISABLED			
Cdaudo		SYSTEM			
Cdfs		DISABLED			
Cdiom		SYSTEM	system32%DRIVERS\cdom.sys	CD-ROM Driver	
Dianger		SYSTEM			
CISVC		MANUAL	3SystemRoot2/system32/cirvc.exe	Indexing Service	

Voici deux services appartenant à des rootkits (plus d'infos sur new_drv.sys/Trojan-PSW.Win32.Small.bs)

GMER 1.0.1	5,14939			- 0
hocesses Module	d Services	Files Registry Rootkit/Malware Autostat CMD		
Varie	Staft	File name	Description	
lasMan lemoteAccess ichedule eclogon ENS havedAccess havedAccess havedAccess havedAccess havedacess havedacess apSin heress isbWs visit heress istaged visit wedarPmSN Visit iscove nuosenv V2CSVC enlprov Inscache IPS SS	MANUAL DISABLED AUTO AUTO DISABLED MANUAL AUTO MANUAL AUTO AUTO AUTO AUTO AUTO AUTO AUTO AUTO	SystemFloot/System32/svchoot.exe 4: netword SystemFloot/System32/svchoot.exe	Creates a network connection Differs routing services to businesses in local are Task Scheduler Seconday Logon System E vent Notification Windows Frewal/Internet Connection Sharing (J., Provides notifications for AutoPlay hardware even Performs system restore functions. To stop servi Telephony Provides user experience theme management. Distbuted Link Tracking Clen? Windows Time Brivides a common interface and object model L. Pervides to even insuber of any portable medi Undows Management Instrumentation Driver E. Monitors system security settings and configurati Enables the download and installation of Window. Provides automatic configuration for the 882:11 Network Provisioning Service Resolves and caches Domain Name System [D., Unitersupplie Power Supply Walkes Studeus Core	
euroth	AUTO	122/C/WINDOWS1 at a 191 122/C/WINDOWS1 at a 2/drivers1 securentin. (y)		
VgaSave CDMSysApp SvPtv ImapService memory MSDTC MSDTC MSDTC MSDEven RDSexMgr EventSystem TextSv WmitpSvv	SYSTEM MANUAL MANUAL MANUAL MANUAL MANUAL MANUAL DISABLED MANUAL	SystemRoot/System32/diversivgs.tys C W/INDOWS/system32/diversivgs.tys C W/INDOWS/system32/dihost eve /Processid IDDEFF3F8.9 C W/INDOWS/system32/mapic eve C W/INDOWS/system32/mapic eve	Manages the configuration and Itacking of Com Manages software based volume shadow copie Manages CD recording using Image Mastering A Enables an authorized user to access this comp Coordinates transactions that span multiple reso Windows Installer Manages and controls Remote Ausistance. If thi, Supports System Event Notification Service (SE Enables a remote user to log on to this computer. Provides performance likewy information hom W	

Un clic droit sur le service sélectionné permet de modifier le mode de démarrage (AUTO, MANUAL, DISABLED etc)... ou supprimer (bouton Delete)



mais bien souvent cela ne fonctionne pas et GMER affiche un message d'erreur. La suppression d'un service appartenant à un rootkit ne peut se faire si ce dernier est actif sur le système (se reporter plus bas).



Files

L'onglet Files est un explorateur de fichiers qui permet en autre d'afficher des fichiers rootkités. Les boutons :

- Delete : Supprime le fichier sélectionné
- *Copy :* Copie le fichier sélectionné (ce qui peut être pratique pour récupérer un fichier rootkité)
- Kill : Détruit la structure du PE, le fichier n'est pas supprimé mais endommagé, il devient alors non exécutable (erreur Win32 lors de l'exécution).



Dans la capture ci-dessous, le fichier twext.exe (variante Trojan.Zbot/Zeus) est rouge car il est rootkité.

Si vous jetez un coup d'oeil à l'explorateur de fichiers plus bas, vous verrez que ce dernier n'apparaît pas, il est donc caché de l'utilisateur et du système.

Le bouton *Only Hidden* permet d'afficher que les fichiers considérés comme rootkités (en rouge).



Registry

De même que l'onglet Files, GMER intègre un éditeur du registre Windows qui permet aussi de visualiser les clefs du registre rootkitées.

Le bouton *Export* permet d'exporter une clef vers un fichier reg. En double-cliquant sur une clef, il est possible de modifier les valeurs, la clef se grise et vous devez cliquer sur le bouton *Save* à droite pour enregistrer les modifications.

NOTE : J'ai déjà planté un ordinateur en effectuant des modifications du registre Windows via GMER (voir la FAQ Microsoft : Comment faire pour récupérer Windows XP à partir d'un Registre endommagé qui empêche le démarrage du système). Avant de jouer avec GMER, il est conseillé de faire une copie du registre (dossier C:\Windows\System32config) ou un export via ERUNT (se reporter au tutorial ERUNT)



AutoStart

Liste les divers points de chargement du registre Windows et leurs contenus.

Le bouton *Copy* permet d'effectuer un copier/coller du contenu du rapport.



CMD

L'onglet CMD permet d'exécuter des commandes CMD lorsque l'onglet CMD.EXE est coché.

Tapez la commande dans la partie haute et cliquez dur *Run* à droite, le résultat de la commande apparaît dans la partie basse de la fenêtre.

Le bouton *Copy* permet de récupérer le résultat dans un copier/coller.



En cochant l'onget *REGEDIT.EXE*, il est possible d'exécuter des commandes reg pour modifier le registre Windows.





Scanner Rootkit de GMER

L'onglet Rootkit/Malware permet de lancer un scan anti-rootkit.

Dans la partie droite, vous pouvez choisir les éléments du système à scanner (IE/EAT, Modules, processus, Registre etc). Notez que pour les fichiers, vous pouvez déterminer les partitions à scanner. Eventuellement ne scanner que la partition système pour gagner du temps.

Les informations sur le scan s'affichent alors, les éléments détectés comme rootkit apparaissent en rouge dans chaque section.

Le bouton *Copy* permet de récupérer le résultat pour effectuer un copier/coller.

Le bouton *Save* permet l'enregistrement du rapport sur votre disque au format texte.



Voici quelques exemples de logs, encore une fois GMER peut afficher des informations sur des éléments légitimes puisque le rapport ne se contente pas de lister des éléments néfastes mais afficher les éléments chargés dans le système et surtout la manière dont ils se chargent... GMER peut donc lister des éléments néfastes comme des éléments légitimes. Il convient donc d'effectuer une recherche sur le nom de fichier

sur Google par exemple (voir le sujet Mieux Utiliser les moteurs de recherche), si vous avez un doute:

Exemple de SSDT Hook (les API apparaîssent à droite) :

SSDT SystemRootSystem32DRIVERSavpe32.sys ZwCreateProcess SSDT SystemRootSystem32DRIVERSavpe32.sys ZwCreateProcessEx SSDT SystemRootSystem32DRIVERSavpe32.sys ZwOpenProcess SSDT SystemRootSystem32DRIVERSavpe32.sys ZwQueryDirectoryFile SSDT SystemRootSystem32DRIVERSavpe32.sys ZwQuerySystemInformation

Certains programmes de sécurité peuvent effectuer des hook comme vsdatant.sys (ZoneAlarm), klif.sys (Kaspersky) etc.

Exemple de Devices..... ci-dessous des devices attachées aux drivers runtime2.sys (malware)

-- Devices - GMER 1.0.12 --

Device FileSystemNtfs Ntfs IRP_MJ_CREATE [F82048FE] runtime2.sys Device FileSystemNtfs Ntfs IRP_MJ_DIRECTORY_CONTROL [F820498A] runtime2.sys Device DriverTcpip DeviceIp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys Device DriverTcpip DeviceTcp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys Device DriverTcpip DeviceUdp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys Device DriverTcpip DeviceRawIp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys Device DriverTcpip DeviceIPMULTICAST [F8D6EA92] runtime.sys Device DriverTcpip DeviceIPMULTICAST IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys ... et ici légitime vsdatant.sys étant le driver de ZoneAlarm

Device DriverTcpip DeviceIp IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys Device DriverTcpip DeviceIp IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys Device DriverTcpip DeviceTcp IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys Device DriverTcpip DeviceTcp IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys Device DriverTcpip DeviceUdp IRP MJ CLOSEIRP MJ READ [BA437E90] vsdatant.sys Device DriverTcpip DeviceUdp IRP MJ INTERNAL DEVICE CONTROL [BA437E90] vsdatant.sys Device DriverTcpip DeviceRawIp IRP MJ CLOSEIRP MJ READ [BA437E90] vsdatant.sys Device DriverTcpip DeviceRawIp IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys Device DriverTcpip DeviceIPMULTICAST IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys Device DriverTcpip DeviceIPMULTICAST IRP MJ INTERNAL DEVICE CONTROL [BA437E90] vsdatant.svs Device DriverAFD DeviceAfd IRP MJ CREATE [BA431B50] vsdatant.sys Device DriverAFD DeviceAfd IRP MJ CLOSEIRP MJ READ [BA431B50] vsdatant.sys Device DriverAFD DeviceAfd IRP_MJ_INTERNAL_DEVICE_CONTROL [BA431B50] vsdatant.sys

Inline Hook (en mode userland) faite par l'infection Haxdoor :

User code sections : .text C:WINDOWSgmer.exe[504] ntdll.dll!LdrLoadDll 7C9161CA 5 Bytes JMP 00010016 .text C:WINDOWSgmer.exe[504] USER32.dll!GetDlgItemTextA + 2 77D8AC08 5 Bytes JMP 000102B3 .text C:WINDOWSgmer.exe[504] WS2_32.dll!gethostbyname + 2 71A54FD6 5 Bytes JMP 00010C14 .text C:WINDOWSgmer.exe[504] WININET.dll!InternetConnectA 771B44DB 5 Bytes JMP 00010F44 .text C:WINDOWSgmer.exe[504] WININET.dll!HttpOpenRequestA + 2 771B4AC7 5 Bytes JMP 000110B9 .text C:WINDOWSgmer.exe[504] WININET.dll!InternetOpenA + 2 771B6D2C 5 Bytes JMP 00011042 .text C:WINDOWSgmer.exe[504] WININET.dll!HttpSendRequestA + 2 771B76BA 5 Bytes JMP 10001000 C:\Windows\System32bmtdhh.dll

Exemple de log avec une librairie bmtdhh.dll cachée (hidden) chargée dans divers processus :

-- Processes - GMER 1.0.11 --

Process C:\Windows\System32winlogon.exe (*** hidden ***) 484 Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @ C:\Windows\System32winlogon.exe [484] 0×1000000 Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @ C:WINDOWSgmer.exe [504] 0×1000000 Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @ C:\Windows\System32cmd.exe [672] 0×1000000 Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @ C:\Windows\System32bmtdhh.dll (*** hidden ***) @

Service considéré comme rootkité, le type de démarrage est indique entre []:

—- Services – GMER 1.0.11 —-Service C:\Windows\System32bmtdhk.sys [BOOT] bmtdhk <– ROOTKIT !!!

Fichiers considérés comme rootkités :

-- Files - GMER 1.0.11 --

File C:\Windows\System32bmtdhh.dll File C:\Windows\System32bmtdhk.sys <- ROOTKIT !!! File C:\Windows\System32klgcptini.dat File C:\Windows\System32rd.dll File C:\Windows\System32rd.sys

spdt (Daemon Tools, Alchohol 120% etc)

Le cas spXX.sys où X sont des lettres aléatoires avec le service spdt – Les programmes Dameon Tools, Alcohol 120% etc installent un driver commençant par sp et un driver aléatoire. Beaucoup de scanner rootkit d'éditeur de sécurité détectent ce dernier comme étant un rootkit alors qu'il est tout à fait légitime.

Voici un rapport GMER complet : http://www.malekal.com/fichiers/GMER/GMER_spdt.txt

Dans le rapport ci-dessus le driver est spjp.sys et le driver aléatoire est ascafl5y.SYS On reconnait facilement ces derniers aux devices relatifs au SCSI :

-- Devices - GMER 1.0.15 ---

Device Driversptd Device1875799320 spjp.sys Device Driverascafl5y DeviceScsiascafl5y1Port3Path0Target0Lun0 82D171F8 Device Driverascafl5y DeviceScsiascafl5y1 82D171F8

En outre pour la partie Registry du scan GMER nous indique clairement entre parenthèses que le service spd appartient à Daemon Tools.

Type de Scan

Dans l'onglet Rootkit/Malware en effectuant un clic droit sur la fenêtre, il est possible de choisir le type de scan.



La dernière option « *Only non MS files* » permet un scan rapide de l'ordinateur et ne lister que les fichiers non Microsoft.

Vous aurez donc aussi les fichiers de vos applications en cours d'exécution. Cela peut donner un rapide aperçu de ce qui tourne sur la machine et donc les malwares comme le montre la capture ci-dessus (pour un oeil averti).

L'avantage est que le scan dure 15s contrairement à un scan complet GMER mais permet tout de même de lister une bonne partie voire la totalié des malwares en cours d'exécution.

Process	P10	CPU D	escription	Company Name			
il System Idle Process	0	33.33	Second and the				
[interupts	n/-	GMER	1 0 15 14944				
DIPCs	n/-	OMEN	Thurballesee				- 1-1
Sjotem .		Processes	Modules Services Files	Registry Rootkit/Makwar	Autodat CMD		
Cirisi eve	48	Tupe	Name		a second a second s	Value +	E Custom
E 📓 winkogon exe	51×	Process	CADDOLIME~TYMALEK	ATIVLOCALSTIVTemplany24	inp.	1952	- System
E tervices.exe	63	Library	C'\DOCUME-T'MALEK	A-1\LOCALS-1\Temp\arv24	the	0x004000	Sections
svchost.exe	- 90	Process	C-\DOCUME~TWALER	A-1/LOCALS-7/Temp/anvEl	8.tmp	2012	IT IAT/EAT
svchost.exe	33	Library	C:\DOCUME~T\MALEK	A~1\L0CALS~1\Temp\anvEl	B. trip	0x004000	T Devices
svchost.exe	116	Process	C:\Program Files\\/Mwa	e/WMware Tools/WMwareTray	exe (/MvareTray//Hware, Inc.)	2028	W Modules
svohost.exe	123	Library	C: Program Filed WMwa	eWMware Tools/WMwareTray	cese (/MwareTray//Mware, Inc.)	0x004000	FT P
svchost.exe	137	Provent	CAProyan Fler/Whee	Withman Trode Withmani Ine	ever followed liser Althouse liser 1	2040	M Phocesses
poolsv.eve	158	Library	C/Program Files/WMwa	e/Whware Tools/WMwareUse	exe (VMwareUser/VMware, Inc.)	0x004000	Threads
White Service.exe	178	Library	C:\Program Files\\\Mwa	re'///Mware Tools/hook.dll		0x100000	V Libraries
Datt eve	63	Process	C://wINDOWS/ayaten/3	2\sychost.exe (Generic Host P	topess for Win32 Services/Microsoft Corp	3092	GT Cardena
A explorer exe	138	Library	C/DOCUME~1/MALEK	A~1\LOCALS~1\Temp\ntdl6	HT	0x100000	1* SELATES
20 VMware Trap ever	202	Process.	C:/WINDOWS/apitent3	Zurychost ever [Generic Hour P	edget for Win32 Services/Microsoft Corp	3104	Registry
VMwareUser.exe	204	Discess	C/WINDOWS Scoretan 7	A TILULALS TIT EIEPEOR	4.08	3116	F Files
proceed: exe	106	Library	C/WINDOWS/system3	Zucerni eue		0-004000	Dich
a film a Dai mar		Library	C:\DOCUME~1\MALEK	A-11LOCALST TTene/mount	B. koots	0x100000	MUS
WindSCP.exe	103	Process.	C\Documents and Setti	ngs/Naki & hote/Desktoply	h25ypo7.exe	3232	
senanarbribribribribcibobolo e	179	Library	C:\Documents and Site	rigerMalekal_monelDesktop/y	h25ypo7.exe	0x004000	
hobybdddodododod ak	122	Process	C/WINDOWS/aprilate3	2V0hdl32.exe (Run a DLL as)	an App/Microsoft Corporation)	3496	
bijmananbocpdgenetit exe	87	Decay	C/WINDOWS BONGON	g.cli	Annual Include 22 Carrieras Mercanol Com	02100000	
- Statistics and		Library	CADOCUME "TYMALEK	A "IN DEALS" IN employed	All	0,100000	55 405
CAN BUR		Process	C/Documents and Setti	ngs'Malekal mote'Malekal m	ofe eve	4048	ALLS
Construction of the second		Service	C/WINDOWS\System3	2\DRIVERS\gner.tys IGMER	Driver http://www.gnet.net/GMER]	[MANUAL	R Shew al
rtil_thet.exe	104	Service				[MANUAL	-
Evchost.exe	303	Service	C:/wINDOWS/apstens3	2\DRIVERS\pontpol5.yv (ND	IS 5.0 driver/AMD Inc.)	IMANUAL -	Scan
Landing eso	242			A MARCHARD CONTRACTOR	and the second		Free
	422						robh
Twencer.exe	400						Save
	143						
					1	OK	Carcel
and the second second second							
C Province of the local		A COLUMN TO A COLUMN					

Suppression de Rootkit avec GMER

Se reporter à la page : Supprimer les Rootkits sous Windows

[Translate]