Micro-ordinateurs, informations, idées, trucs et astuces

Utiliser Kaspersky, Version 5

Auteur : François CHAUSSON Date : 11 septembre 2008 Référence : utiliser Kaspersky.doc

Préambule

Voici quelques informations utiles réunies ici initialement pour un usage personnel en espérant qu'elles puissent aider d'autres utilisateurs de micro-informatique.

Ces informations sont présentées sans démarche pédagogique ; si un niveau de détail était nécessaire sur un sujet particulier, ne pas hésiter à me demander.

Ce document

Il fait partie de l'ensemble documentaire *Micro-ordinateurs, informations, idées, trucs et astuces* qui couvre ces sujets :

- 1. La micro-informatique, en 2 tomes
- 2. *L'Internet*, en 2 tomes



- 3. Des Trucs HTML et Javascript
- 4. Des notices d'utilisation de divers logiciels¹

Tout commentaire à propos de ce document pourrait être adressé à : pcinfosmicro@francois.chausson.name

Ce document est régulièrement mis à jour sur : <u>http://fcfamille.free.fr/</u> 2

Ce document est protégé par un Copyright ; sa propriété n'est pas transmissible et son utilisation autre que la lecture simple doit être précédée d'un accord explicite de son auteur.

¹ ZoneAlarm, AVG, ...

² Site à accès contrôlé

Infos, idées, trucs et astuces

Table des matières

PREAMBULE Ce document	2 2
ANTI-VIRUS KASPERSKY	4
INSTALLATION	4
Chargement	4
Installation	4
Post-installation	4
UTILISATION	4
Lancement	4
En manuel	4
En automatique	5
En exécution	6
Un virus	6
Des virus	
MISES A JOUR	10
A la demande	10
Automatiquement	10
UNE BONNE PRECAUTION	11
ATTENTION	11
ANNEXES	12
En savoir plus	12
Kaspersky et la protection contre les attaques réseau	12
Le besoin	12
La démarche	12
Importance de la mise à jour d'un anti-virus	15
La détection	15
L'alerte	16

Anti-Virus Kaspersky

Kaspersky est considéré comme le meilleur anti-virus ; son utilisation pour usage personnel est payante, après une période d'essai.

Installation

Chargement

Télécharger d'abord depuis le site :

• <u>http://www.kaspersky.com</u>

et choisir la version 5.

Installation

Cliquer sur le fichier reçu³ et suivre les instructions données par le logiciel.

A la fin, aucune icône n'est créée sur le Bureau ; par contre, une petite icône en forme de **K** est créée en bas à droite.

Post-installation

Bien considérer le sujet présenté à « Kaspersky et la protection contre les attaques réseau », p.12.

Utilisation

Kaspersky, c'est :

- Une partie résidente en mémoire RAM qui teste en permanence les programmes actifs
- Une autre partie qui teste les fichiers présents sur les disques durs/disquettes : à la demande ou de manière planifiée
- Une troisième partie qui contrôle les mails entrants et sortants
- …⁴

Lancement

L'exécution de Kaspersky peut être demandée :

- en manuel
- en automatique

En manuel

L'utilisateur peut demander un test :

- clic droit sur la petite icône en bas à droite en forme de K
- sélectionner Ouvrir Kaspersky anti-virus

³ auto-exécutable

⁴ j'en oublie ?

Infos, idées, trucs et astuces



• clic sur le lien Analyser le poste de travail

En automatique

Avec ce paramétrage initial :

• clic sur le lien, à droite, *modifier l'horaire*

K Configuration de l'analyse programmée	×
O Analyser avec un intervalle de jours	
Analyser les jours définis de la semaine	
O Ne pas analyser	
Paramètres d'analyse	
Sélection des jours de la semaine :	
🗖 Lundi 🗹 Vendredi	
🗖 Mardi 🛛 🗖 Samedi	
🗖 Mercredi 🚺 Dimanche	
🗖 Jeudi	
Début de l'analyse :	
17:00	
Mode économie d'energie	
Charge minimum de la bacterie pour la cer i analyse programmee	
 30 <u>⇒</u> %	
Aide <u>Ok</u> <u>Annuler</u>	

• choisir la périodicité et l'horaire

Kaspersky s'exécutera en arrière plan sans fenêtre apparente.

En exécution

Lorsqu'un test s'exécute, ce panneau est mis à jour en temps réel :

🔀 Analyse 0%		
	L'analyse est	en cours
Début de la tâche :	08/02/2005 22:07:22	
Fin de la tâche :	Calcul en cours	
Objet courant :	svchost.exe\comsvcs.dll	
Statistiques Rapport	Paramètres	1
Objets analysés :	707	
Virus détectés :	0	
Virus neutralisés :	0	
Objets supprimés :	0	
Objets mis en quaran	taine : 0	
Eteindre l'ordinateur	à la fin de l'analyse.	<u>xamen de la guarantaine</u>
Aide		Pause Arrêt

A la fin :

🔀 100% - L'analyse est terminée					
Ro.	Aucun objet dangereux n'a été découvert				
	Durée de l'analyse :	03:44:10	Objets réparés :	0	
	Objets analysés :	293930	Objets supprimés :	0	
	Objets dangereux découverts :	0	Objets mis en quarantaine :	0	
Aide			Pause Eermer	*	

Un virus

Kaspersky permet de :

- détecter un virus
- éradiquer ce virus

A la détection d'un virus, Kaspersky affiche un panneau caractéristique

🔀 Kasp	persky Anti-Virus Personal	×
	Attention ! Un scénario dangereux a été découvert.	
W	Application: C:\Program Files\Internet Explorer\iexplore.exe	:
	La page http://www.mature-bitches.com / contient le code malveillant Trojan-Downloader.VBS.Small.e. L'exécution de ce scénar a été bloquée automatiquement.	io
🗖 Ne j	plus afficher ce message lors de cette session	_
0	Aide 🧐 Son OFF Ok	

ou bien celui-ci :

K Kasp	ersky Anti-Virus Personal	×
	Attention ! Votre ordinateur a été attaqué via Internet.	
•	L'attaque de réseau Lovesan depuis l'adresse 82.216.139.233 a été repoussée.	
⊠ Ñe j	plus afficher ce message lors de cette session	
0	Aide Son OFF]

Des virus

Dans le stock :

bjet	État	Date de mise en do	Chemin 🗸	Restaurer
MOINVED1.DOC	Infecté	24/04/2006 19:47:52	D:\fran\MAISON(1 Mormoiron\inventaire\MOINVE01.DOC	
Domaine ChaussonFamille.doc	Infecté	24/04/2006 19:47:46	D:\fran\FINANCE\achats\achats micro\Domaine ChaussonFamile.doc	Supprimer
Faits Marguants - INT- PTM	Infecté	24/04/2006 19:45:33	D:\fran\EMPLOI\INDEPEND\TRAVAILL\projets\65ilca\Perso\Faits marguants\annee 2006\02 Fev06\originaux\Fe	
Faits Marguants - INT- PTM	Infecté	24/04/2006 19:44:52	D:\fran\EMPLOI\INDEPEND\TRAVAILL\projets\65ilca\Perso\Faits marguants\annee 2006\03 Mar06\Faits Margu	
ie0601a[1].jar	Infecté	06/04/2006 19:50:06	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\HF7RST8E\je0601a[1].j;	
pluginst[1].htm	Infecté	27/03/2006 18:24:22	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\SHYN8L23\pluginst[1].ht	
xxx.dataseeq[1].htm	Infecté	18/10/2005 22:23:53	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\KTUFW1UN\xxx.datase	
MSWINSCK.OCX	Infecté	20/09/2005 19:35:49	C:\WINNT\system32\M5WIN5CK.OCX	
pictureheaven[1]	Infecté	18/09/2005 22:07:50	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\TZVJDPOE\pictureheave	
classload[1].jar	Infecté	31/08/2005 07:25:01	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\4PUNSHAR\classload[1]	
msjid[1].jar	Infecté	31/08/2005 07:15:54	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\J3LB39G5\msild[1].jar	
ccurs[1].ani	Infecté	31/08/2005 02:08:40	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\ZIS73D4T\ccurs[1].ani	
Script_0379d000.html	Infecté	19/07/2005 15:44:11	C:\Documents and Settings\Fran\Local Settings\Temp\Script_0379d000.html	
countme[1].htm	Infecté	19/07/2005 15:43:52	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\4XWXA38Hcountme[1].	
counter[1].htm	Infecté	19/07/2005 15:43:51	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\4XWXA38H(counter[1].	
index[8].htm	Infecté	19/07/2005 15:43:43	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\4PUNSHAR\index[8].htn	
counter[1].htm	Infecté	19/07/2005 15:43:42	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\6L0RAT65\counter[1].h	
test[1].htm	Infecté	19/07/2005 08:38:18	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\4PUNSHAR\test[1].htm	
ierknao[1].htm	Infecté	18/07/2005 14:34:08	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\J3LB39G5\terknoo[1].ht	
dir6783226[1].htm	Infecté	18/07/2005 14:21:25	C:\Documents and Settings)Fran\Local Settings)Temporary Internet Files\Content.IES\2X9UBIT0\dir6783226[1	
pavload[1].ani	Infecté	18/07/2005 13:03:50	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\Y8132LDW\pavload[1].a	
image[3].gif	Infecté	18/07/2005 13:02:43	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IES\FGOISKUD\image[3].of	
input[1].php	Infecté	12/06/2005 22:44:01	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\DZG427VC\input[1].php	
xxxxgatewav[1]	Infecté	01/06/2005 19:50:38	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\Y8I32LDW\xxxxgateway	
xxxgateway[1]	Infecté	14/05/2005 07:58:27	C:\Documents and Settings\Fran\Local Settings\Temporary Internet Files\Content.IE5\DZG427VC\xxxgateway	
dir87534238[1].htm	Infecté	12/05/2005 21:59:40	C:\Documents and Settings\Administrateur\Local Settings\Temporary Internet Files\Content.IE5\MI8O89X9\dri	
msild[1].iar	Infecté	12/05/2005 21:58:48	C:\Documents and Settings\Administrateur\Local Settings\Temporary Internet Files\Content.IES\SHU75L68\ms	
sh[1].htm	Infecté	19/04/2005 13:15:51	C:\Documents and Settings\Administrateur\Local Settings\Temporary Internet Files\Content.IES\632R6LIF\shf	
sh[1].htm	Infecté	19/04/2005 13:06:42	C:\Documents and Settings\Administrateur\Local Settings\Temporary Internet Files\Content.IES\SVNJA8T1\shf	
sh[1].htm	Infecté	19/04/2005 12:55:36	C:)Documents and Settings)Administrateur)) ocal Settings)Temporary Internet Files)Content (FS)(0063C148)sh	
Cette boîte de dialogue	Infecté présente	19/04/2005 12:55:36 les copies de sauvegarde	CLDocuments and Settinos/AdministratourLocal Settinos/Tencorary Internet Fles/Content.IES/0063CL48bt	
2 Aide				Fermer

Autoriser un programme à s'exécuter

Dans Kaspersky :

🔀 Kaspersky Anti-Virus 7.0		
Kaspersky Anti-Virus	Votre o	rdinateur est protégé
Antivirus Fichiers Antivirus Courrier Antivirus Internet Défense Proactive	Protection Kaspersky Anti-Virus garantit la fordinateur contre les virus, les malicieux.	protection complète de Spywares et autres programmes
Analyse	Etat de la protection de votre ou	rdinateur
- Hindiyse	La protection de votre ordinateu	r : en exécution
🔗 Mise à jour	Analysés / découverts :	74892 / 31
	Stop Pause Configuration	
Rapports	Applusor los soctours critiquos	
	Dernière exécution :	12/01/2008 19:22:14
	Etat : l'exécu	tion de la tâche est interrompue
Assistance Technique	Configuration Planification	
	Mettre à jour les bases	
	Date de publication :	10/09/2008 11:56:32
	Etat :	les bases sont à jour
	Configuration Retour aux bases antéri	eures
Aide Configuration		

• bouton *Configuration*



• dans Exclusions, bouton Zone de confiance

Zone de confiance Règles d'exclusion Applications de confian	:e]	_ 🗆 ×
Objet G (:\Program Files\RingThree\BIM\Rin C (:\WINDOWS\system32\services.exe C (:\WINDOWS\system32\services.exe G (:\Download\Opera_952_10108_in) C (:\WINDOWS\System32.exe)	Type de me (Invader Hidden object Hidden object Invader	Ajouter Modifier Supprimer
Description (cliquez sur les paramètres souil L'objet ne sera pas analysé lorsque les cor Objet : <u>Gitcopy(XnView-win.exe</u> Type de menace : <u>Invader</u> Composant : <u>précisez : Défense Proactive</u>	gnés pour les modifi nditions suivantes se	er) : rront remplies :
🖗 <u>Aide</u>	Ōĸ	Annuler

Mises à jour

Kaspersky peut être mis à jour :

- à la demande
- automatiquement si la demande lui en a été faite au préalable

A la demande

Dans le panneau d'accueil :

• clic sur le lien Mettre à jour maintenant

🔀 Mise à jour de	es bases antivirus (0%)	
?	Etablissement de la connexion avec le serveur de jour des bases antivirus.	e mises à
Taille de la mise à	jour : 0,00 Ko	
Téléchargement :	0,00 Ko	
🗹 Fermer la fené	ŝtre à la fin de la mise à jour	
🕐 Aide	[Arrêter

Les données reçues sont utilisées pour mettre à jour la base des profils de virus.

Automatiquement

Kaspersky déclenche automatiquement la mise à jour en fonction des critères spécifiés dans le panneau d'accueil à l'onglet *Paramètres*



• clic sur le lien *Mises à jour* ...

K Configuration des mise	es à jour 🔀		
🗹 Activer la mise à jour aut	comatique		
Fréquence des mises à	Toutes les trois heures 🔹		
🔲 M'alerter avant le dét	out de la mise à jour automatique		
Type de mise à jour			
Type de mise à jour :	via Internet, bases standard 💽		
Mettre les modules	s du logiciel à jour		
Les paramètres repris dans MS Internet Explorer seront utilisés pour la connexion à Internet. Vous pouvez <u>modifier la configuration du serveur proxy</u> .			
Aide	<u>Ok</u> nnuler		

• choisir la périodicité et l'horaire

Une bonne précaution

Comme un anti-virus n'est pas infaillible, il est utile de charger⁵ un ou deux autres anti-virus⁶ et de les conserver en réserve.

S'il apparaît un jour que AVG ne peut pas, soit détecter, soit éradiquer un virus, alors l'utilisation ponctuelle d'un de ces autres anti-virus pourra être utile⁷.

Attention

Comme un anti-virus est de nature très méfiant, ne jamais faire fonctionner deux anti-virus en même temps ; ils pourraient se bloquer mutuellement.

Toujours désinstaller l'anti virus à remplacer avant d'installer le nouveau anti virus.

⁵ et de tenir raisonnablement à jour

⁶ comme Avast, Kaspersky, ...

⁷ sans avoir à aller d'abord les chercher sur Internet

Annexes

En savoir plus

Dans le panneau d'accueil, à l'onglet Support technique :

• clic sur le lien *Aide*



Kaspersky et la protection contre les attaques réseau

Le besoin

Cette fonction entre en conflit avec tout Firewall ; dans le cas de ZoneAlarm, le conflit provoque un Reboot du système en cas de tentative de connenxion RTC.

La démarche

Dans l'Aide :



- Entrer dans Kaspersky :
- Clic sur l'onglet *Paramètres*



• Clic sur le lien *Protection en temps réel*

K Configuration de la protection en temps réel	×
Niveau de protection	
- - Recommandé	
Ce niveau de protection en temps réel est recommandé par les experts de Kaspersky Lab car il représente la configuration optimale au niveau de la vitesse d'analyse des objets.	
A ce niveau, l'analyse porte sur tous les objets qui peuvent être infectés ainsi que sur le courrier sortant et entrant. Les archives auto-extractibles et les autres archives ne sont pas analysées.	
En cas de tentative d'accès à un objet infecté :	
 Interdire l'accès et confirmer l'action auprès de l'utilisateur 	
O Interdire l'accès et exécuter l'action recommandée	
O Interdire l'accès et supprimer les objets infectés	
O Interdire l'accès et consigner les informations dans le rapport	
Attention ! Quelques exclusions ont été définies. Cela peut réduire le niveau général de la protection en temps réel. Vous pouvez <u>restaurer</u> la configuration par défaut.	
Configuration de la zone protégée	
<u>Aide</u> <u>Aide</u> <u>Aide</u>]

• Clic sur le lien *Configuration de la zone protégée*

Configuration de la zone protégée
Désactiver la protection en temps réel :
Désactiver la protection en temps réel des fichiers
Désactiver la protection en temps réel du courrier
Désactiver la protection en temps réel des scénarios
Désactiver la protection contre les attaques de réseau
Protection des fichiers
Ne pas vérifier les secteurs d'amorçage du disque
Arrêter si l'analyse dure plus de (s.)
Activer la liste des objets exclus
Modifier
Protection contre les attaques de réseau
Ne pas m'avertir en cas d'attaque de réseau
🗖 Bloquer l'ordinateur attaquant pendant (m)
Utiliser le mode furtif
Ne pas activer la protection contre les attaques de réseau lors du démarra
<u>Qk</u> <u>Annuler</u>

- Cocher la case Désactiver la protection contre les attaques réseau
- Cocher la case Ne pas activer la protection contre les attaques réseau lors du démarrage

Importance de la mise à jour d'un anti-virus

Un délai très court peut s'écouler entre l'apparition d'un virus et sa manifestation.

La détection

La détection locale a été faite le 6 Fév 07 :

🔏 44% - Anal	yse en cours				- 🗆 🗵				
P	Objet actuel : D:\\Apps\APP09988\src\MSWorks\PFiles\MSWorks\WKSv7std.sb								
	Temps restant :		00:35:18	Objets réparés :	0				
	Objets analysés :		179510	Objets supprimés :	1				
	Objets dangereux d	écouverts :	1	Objets mis en quarantaine :	0				
Rapport St	atistiques Paramètres								
Jack susself	Addamara CE Darram	Résultat du tra	aitement	nen heité	<u>D</u> =				
iles\Lavasoft	lies\Lavasoft\Ad-Aware SE Person protege par un mot de passe, non traite								
iles\Lavasoft	illes Lavasoft Ad-Aware SE Person protégé par un not de passe, non traité								
iles\Lavasoft	iles (Lavasoft Ad-Aware SE Person protégé par un mot de passe, non traité								
iles\Lavasoft	iles\Lavasoft\Ad-Aware SE Person protégé par un mot de passe, non traité								
S\system32\	TFTP5356	est un cheval	de Troie Trojan	-Downloader.Win32.Agent.bft	07				
S\system32\	TFTP5356	Placé dans le	dossier de sauv	/egarde	07				
S\system32\	TFTP5356	supprimé			07				
I					<u>ک</u>				
Eteindre l'a	ordinateur à la fin de l'ana	lyse.		Examen de la g	<u>uarantaine</u>				
Aide				Pause A <u>r</u> rêt	*				

L'alerte

La première alerte sur le Web date du 30 Jan 07 :

🖉 Viruslist.com - Trojan-Downloader.Win32.Agent.bft - Windows Internet Explorer										
🚱 🕘 👻 🕒 http://www.viruslist.com/en/viruses/encyclopedia?virusid=149375 🔹 4 🗙 Google										
Canon Easy-WebPrint -) Imprimer 🛛 🤬 Impress	ion rapide 🛛 🕵 Aperçu	a 🛛 😴 Optio	ns 📄 Recto	verso 📔 Afficher I	a liste d'impressions				
🚖 💠 🔡 🚽 🄏 http://fcfamillewc.free	.fr/ 😑 Viruslist.c	om - Trojan-Dow 🗙] 🐔) • 🗟 • 🖶 • 🗄	} <u>P</u> age →) Outils → 3				
Viruslist.com	All Threats	Viruses	Subscript Hackers	ions <u>RSS Fe</u> Spam	eds <u>Discussions</u> Whole site	Polls <u>Site Map</u>				
Virus Encyclopedia Riskware	Alerts	Analysis		News	Glossary	Weblog				
Malware Environment Malware Descriptions • Network Worms • Classic Viruses • Troian Drograms • Backdoors • General Trojans • ESW Trojans • Trojan Ockers • Trojan Ockers • Trojan Ockers • Trojan Deventoaders • Trojan Deventoaders	Hone / Viruse / Virus Downloaders Trojan-Do Detection added Update released Behavior Currently there is n As many viruses a check the descript will be listed at the	Encyclopedia / Malwar WINICACIET.V Jan 30 2007 04:01 (0 Jan 30 2007 05:28 (0 TrojanDownloader to description availat nd worms are molimar progra top of the page.	e Descriptions / Vin32.A EMT de for this pro cations of ear ms. If such d	gent.bft gent.bft gram. lier versions, if	r may help you to available, they					
Trobust Toxism Our virus analysts work hard to ensure that descriptions of the commonest and most potentially dangerous software are available to users. The Virus Encyclopedia is updated on a regular basis. Who Creates Malware If you cannot find the description you need, please check back later, or contact us on webmaster@viruslist.com.										
Malware Trends If Your Computer Is Infected					ternet	(A) 100%				

soit un délai de 6 jours entre les deux dates.

Bibliographie « Utiliser ... »

Ces différents documents constituent l'ensemble documentaire Utiliser

La liste complète est disponible sur http://fceduc.free.fr/documentation.php.

François CHAUSSON

17/09/08 21:09

W:\Fran\micro\notices utilisation\avance\utiliser Kaspersky.doc