

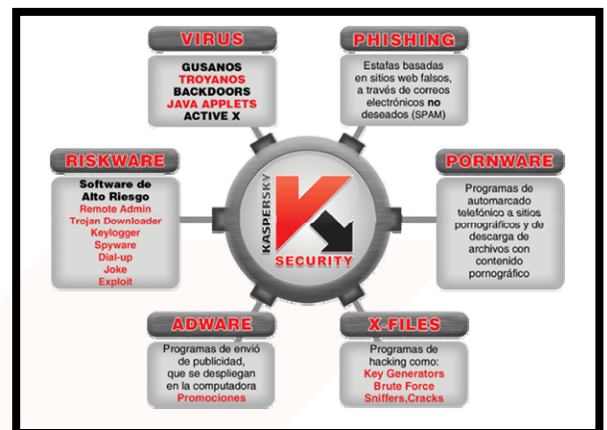


El propósito de este documento es conocer a Kaspersky Antivirus como la mejor solución Antivirus en el mercado. Se incluyen referencias técnicas y comerciales que le ayudaran a los usuarios a conocer más a fondo a Kaspersky.

Cada día que pasa los distribuidores y Usuarios están cambiando a Kaspersky por ser el único antivirus en el mundo que se actualiza cada hora y tiene el tiempo de respuesta mas rápido ante una amenaza, además de contar con la capacidad de poder detectar desde el virus mas antiguo hasta el mas reciente, ya que no recorta su base de firmas de detección de virus.

En este documento toda la información esta debidamente respaldada poniendo la fuente de información, en algunas comparativas no se incluyen todos los antivirus que actualmente se encuentran en México, como es el caso de Hauri, que no es considerado en el CheckMark y Panda que hace tiempo que no participa en el VirusBulletin y en ocasiones no participa en AV-comparatives.org.

- Kaspersky Antivirus es el Antivirus que los expertos recomiendan por su gran capacidad de detección, de virus, spyware, riskware, phishing, adware, pornware, rootkits y herramientas de hackeo.
- Permite el escaneo en más de 1,200 formatos de compresión de archivos.
- **2do.** Lugar ExpoComm 2006 “ Mejor Tecnología PyMES
- Kaspersky ofrece protección para Teléfonos inteligentes y PDA, Estaciones de trabajo, servidores de Archivos y Correos, Firewall, Proxies, además de protección AntiSpam.



Contenido de este documento

1. Conociendo a Kaspersky Antivirus
2. Soluciones Kaspersky Antivirus
 - Kaspersky Corporate Suite
 - Kaspersky AntiSpam
 - Kaspersky SOS (Second Opinión Solution)
 - Kaspersky Internet Security 6.0
 - Kaspersky Productos BETA
3. Kaspersky en el Mercado Mexicano
 - Encuesta Infochannel 2006 (Las favoritas del Canal)
4. Premios y Certificaciones
 - Premios del Virus Bulletin
 - Certificación ICSA Labs
 - Certificación CheckMark
 - Microsoft Antivirus Partners
5. Comparativas
 - Comparativa de av-comparatives.org
 - Comparativa de Virus.gr <http://www.virus.gr/english/fullxml/default.asp?id=82>
6. AOL distribuye gratuitamente Active Virus Shield, con tecnología Kaspersky
7. Compañías que utilizan Ingeniería de Kaspersky Antivirus
 - Alcatel, Juniper, Sybari (Una Compañía de Microsoft), Optenet, Nokia, BlueCoat, SonicWall, etc.
8. VirusTotal un Portal que ofrece escaneo de mas de 20 Antivirus en Línea
 - <http://blog.hispasec.com/laboratorio/43>
9. Caso de Éxito
 - http://www.tecnologiaempresarial.info/busqueda.asp?id_notas=11822&seccion
10. Problemas de Detección



1.- Conociendo a Kaspersky Antivirus

Fundados en 1997 en Moscú, Rusia, Kaspersky Antivirus rápidamente se ha convertido en el antivirus más recomendado por los usuarios, debido a gran eficiencia contra las nuevas amenazas en Internet.

Actualmente la Ingeniería de Kaspersky esta integrada en productos de seguridad que protegen a más de 200 millones de usuarios a nivel mundial, como NetScreen, Nokia, SonicWall, BlueCoat, Sybari, Optenet, Astaro

Kaspersky cuenta con distribuidores en todo el mundo. Rusoft es el distribuidor exclusivo para México, con oficinas en México D.F. y Monterrey.

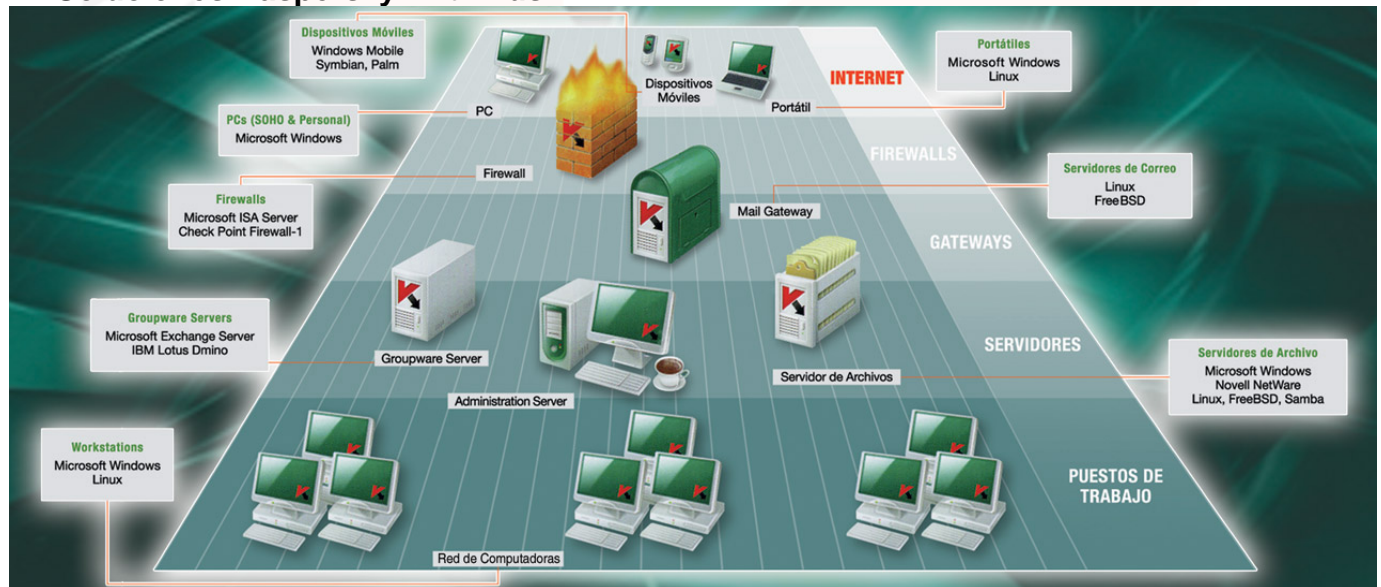
El Laboratorio de Virus

La exitosa detección e interceptación de virus depende de su constante investigación. **Kaspersky mantiene una de las más grandes colecciones de definiciones de virus en el mundo, con más de 210,115 (Julio 2006) registros** y que cada día aumentan. **Tamaño de las Actualizaciones entre 20Kb y 60 KB, en forma incremental.**

Innovadora tecnología y rápida respuesta

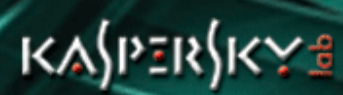
Kaspersky es reconocido por su rápida respuesta a las nuevas amenazas de virus, mientras nuestra tecnología de punta ha ganado muchos premios. Líderes en la venta de software certifican nuestros productos y hemos participado en numerosos programas de socios, tales como el "Microsoft Gold Certified Security Solutions Program" (Programa de Certificación Microsoft para Soluciones de Seguridad) o el "Novell Sure Partner Program" (Programa de Socios de aseguramiento Novell).

2.- Soluciones Kaspersky Antivirus



Kaspersky Corporate Suite

- Windows Workstations
- Linux Workstations
- Windows File Servers
- Linux File Servers
- Novell Network
- MS Exchange Server 2003
- Lotus Notes/Domino
- MS ISA Server 2000
- MS ISA Server 2004 Standard Edition
- MS ISA Server 2004 Enterprise Edition
- Check Point Firewall
- Administration Kit
- Security for PDAs
- Linux / Unix Mail Servers





Kaspersky AntiSpam

Filtración de múltiples niveles

El programa analiza y filtra correos entrantes de una gran variedad de maneras, revisando tanto la estructura del mensaje y sus datos adjuntos

Administración flexible

Un módulo incorporado de administración basado en una interfaz web permite al administrador modificar configuraciones del programa desde cualquier nodo de la red. i.e. cambiar los parámetros de la base de datos spam o agregar firmas directamente.

Compatibilidad

Kaspersky Anti-Spam es compatible con todos los sistemas de correo facilitando la integración de la solución en configuraciones de red existentes sin importar el sistema operativo.

La solución es lo suficientemente flexible debido a que funciona como filtro separado o en un servidor de correo empresarial de gran escala soportando Sendmail, Qmail, ComminGate Pro, Postfix o Exim.

Actualizaciones de la base de datos de lingüística

Uno de los elementos claves del programa es una base de datos de lingüística que contiene firmas spam. Actualizaciones de la misma son lanzadas cada dos horas. Actualizaciones de Kaspersky Anti-Spam incluyen versiones actualizadas del kernel de lingüística.

Protección contra Virus

Protección en Correos.

Escaneo todo el tráfico de correos, entrante (POP3, IMAP y NNTP) saliente (SMTP) en cualquier programa de correo. Es compatible con Microsoft Outlook y Microsoft Outlook Express.

Escaneo de tráfico de Internet.

Escaneo en tiempo real de todo el tráfico de internet (HTTP), asegurando que objetos infectados no sean descargados o escritos en el disco duro, compatible con Microsoft Internet Explorer.

Protección Proactiva.

KIS monitorea la actividad de los programas y procesos que son ejecutados en la memoria RAM, avisa a el usuario de procesos ocultos (Rootkit), peligrosos o sospechosos, evitando cambios en el sistema, protege el registro.

Protección contra Spyware.

Asegura la confidencialidad de su información, como password, números de cuentas bancarias y tarjetas de crédito, detecta mensajes de phishing y deshabilita la conexión a sitios de phishing.

Navegación Segura en Internet.

KIS evita la ejecución de programas scripts que son lanzados de sitios web, y bloquea ventanas popup, y banners de publicidad, Bloqueo automático de Programas de Automarcado

Protección contra Hackers

Bloqueo contra ataque de red.

El Intrusión detection system (IDS) monitorea cualquier actividad de red que tenga las características de un ataque de un hacker. KIS bloquea las conexiones de la computadora que lo esta atacando.

Control total sobre la actividad de la red.

KIS controla todas las peticiones a websites, de acuerdo con el juego de reglas predefinidas, monitoreando todo el tráfico de paquetes que entran y salen.

Modo invisible.

Esta tecnología permite a la computadora ser invisible a usuarios externos, previniendo efectivamente de todo tipo de ataque de Denegación de Servicios (DoS)





Protección contra SPAM

Protección Integral contra SPAM

La combinación de varios métodos aseguran el mas alto nivel de detección de spam, incluyendo listas blancas y negras de direcciones IP y combinación de palabras, y un algoritmo de autoaprendizaje, KIS puede también escanear características de spam en imágenes graficas

- Microsoft Windows 98 (SE): Intel Pentium 133 MHz , 64 Mb RAM
- Microsoft Windows ME: Intel Pentium 150 MHz , 64 Mb RAM
- Microsoft Windows NT Workstation 4.0 (Service Pack 6a): Intel Pentium 133 MHz , 64 Mb RAM
- Microsoft Windows 2000 Professional (Service Pack 2 or higher): Intel Pentium 133 MHz, 64 Mb RAM
- Microsoft Windows XP Home Edition or XP Professional (Service Pack 1 or higher): Intel Pentium 300 MHz, 128 Mb RAM
- Microsoft Windows XP 64bit Edition: Intel Pentium 300 MHz , 128 Mb RAM

Kaspersky Corporate 6.0 (Beta)

Esta solución integra todas las características de funcionalidad de Kaspersky Antivirus Personal 6.0, permite la administración Remota a través de la consola de Administración (Administration Kit) <http://www.kaspersky.com.mx/descargas/BETA/>

Kaspersky SOS Second Opinion Solution (Beta)

Kaspersky SOS 5.0 (Second Opinion Solution), es recomendado para usarse en estaciones de trabajo en las cuales esta instalado y funcionando otro antivirus. Esta solución no instala ningún componente residente en tiempo real, con lo cual se evitan conflictos cuando están instalados dos antivirus en una misma computadora. Kaspersky no recomienda utilizar KAV SOS como único antivirus en la computadora.

Kaspersky SOS permite detectar y eliminar los virus o código malicioso que no fueron detectados por el antivirus principal.

3.- Kaspersky en el Mercado Mexicano

3.1 En una encuesta realizada a distribuidores en el Mes de Julio por la revista Infochannel, Kaspersky Antivirus Obtuvo el 4to lugar en preferencia de antivirus por los distribuidores a nivel nacional. <http://www.infochannel.com.mx/images/docs/pdf/software2006.pdf>

3.2 ExpoComm 2006 **2do Lugar** "Mejor Tecnología PyMES"

4.- Premios y Certificaciones

4.2.- Certificaciones de ICSA Labs (Estados Unidos)

ICSA Labs Una de las certificaciones más importantes es sin duda la que otorga ICSA Labs, en seguida enlistamos los antivirus, que han logrado conquistar dicha certificación. [https://newlabs.icsalabs.com/icsa/product.php?tid=dfgdf\\$gdhkkjk-kkkk](https://newlabs.icsalabs.com/icsa/product.php?tid=dfgdf$gdhkkjk-kkkk)

Certificados		No Certificados
Kaspersky	McAfee	Hauri
NOD32	Trend Micro	
Symantec	Panda	

Porque Hauri no tiene la certificación de ICSA Labs?





4.3.- Certificaciones de CheckMark Labs (Inglaterra)

Checkmark es un sistema el cual prueba y certifica productos de seguridad con estándares del mundo real. El sistema de Checkmark es un servicio de calidad bien establecido, con estándares independientes. Es un servicio global, que beneficia tanto a los desarrolladores y compradores de sistemas de seguridad y también las personas que toman la decisión.

<http://www.westcoastlabs.org/checkmarkcertification.asp>

Porque Hauri no tiene la certificación de ICSA Labs?

TECHNOLOGY GROUPS

- Content Security
- Anti-Virus Level 1
- Anti-Virus Level 2
- Trojan
- Email Filtering
- Web Filtering
- Anti-Spyware Gateway
- Anti-Spyware Installed
- Anti-Spyware Desktop
- Anti-Spam
- Perimeter Security
- Firewall Level 1
- Firewall Level 2
- PC Firewall
- Intrusion Detection
- VPN
- Vulnerability Assess

BUYERS INFORMATION

- Product Info

SERVICES

- Checkmark Newswire
- Press Releases
- Contact Us

Company Product Information: Please Choose ...

	AhnLab	✓ Testing History
	Computer Associates	✓ Testing History
	Equinet	✓ Testing History
	ESET	✓ Testing History
	Internet Security Systems	✓ Testing History
	Kaspersky Labs	✓ Testing History
	McAfee	✓ Testing History
	McAfee Consumer	✓ Testing History
	Panda Software International	✓ Testing History
	SOFTWIN	✓ Testing History
	SOPHOS	✓ Testing History
	Symantec Corporation	✓ Testing History
	Trend Micro Inc.	✓ Testing History

5.- Comparativas

5.1- Comparativa del Virus Bulletin Agosto 2006 – Inglaterra <http://www.virusbtn.com/>

El Virus Bulletin es una de las más antiguas instituciones en realizar pruebas de detección de Antivirus, desde 1998 se han realizado diferentes comparativas desde el viejo MSDOS hasta llegar en la actualidad a Linux y Windows 2003 Server 64 bits

	Windows Server 2003 Enterprise X64 version Dec 2005	Windows NT 4.0 Workstation Feb 2006	Red Hat Linux 9 Apr 2006	Windows XP Jun 2006	Netware 6.5 Aug 2006	Total de Premios
Eset						39
Kaspersky						34
Symantec						33
McAfee						27
Trend Micro						14
AhnLab						5
Hauri						1
Microsoft OneCare						1
Panda						1

1.- El reconocimiento del 100%: Detección del 100% de virus en el campo (sin incluir código malicioso)

2.- Fallar la prueba:

- Dejar de detectar cuando menos un virus en el campo
- Reportar cuando menos un **Falso Positivo**
- No finalizar el escaneo, presentar mensaje de error, para el escaneo

3.- No Participar: En este caso los Antivirus prefieren no participan si consideran que su antivirus no es bueno o no tienen un producto para el sistema operativo que se esta evaluando.

- Los virus en el campo que se utilizan en esta

comparativa se basa en el WildList <http://www.wildlist.org/WildList/RTWL.htm>

- Las 7 empresas antivirus establecidas en México, participan activamente en el Virus Bulletin y el WildList.
- La comparativa se realiza cada dos meses con diferentes Sistemas Operativos.
- Actualmente el Antivirus con el mayor número de premios ganados del Virus Bulletin es NOD32 y en segundo lugar se encuentra Kaspersky, y en último lugar se encuentra **Panda y Hauri**.



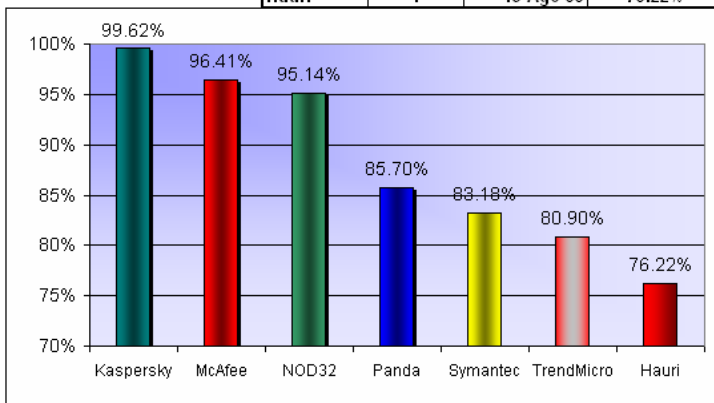


5.2- Comparativa del Virus.gr Agosto 2006

<http://www.virus.gr/english/fullxml/default.asp?id=82>

COMPARATIVA AGOSTO 2006			
Antivirus	Version	Actualizacion	% Deteccion
Kaspersky	6.0.0.303	15-Ago-06	99.62%
McAfee	10.0.217	15-Ago-06	96.41%
NOD32	2.51.30	15-Ago-06	95.14%
Panda	10.01.02	15-Ago-06	85.70%
Symantec	12.1.0.20	15-Ago-06	83.18%
TrendMicro	14.10.1051	15-Ago-06	80.90%
Hauri	4	15-Ago-06	76.22%

Esta prueba fue realizada entre el 15 y 25 de Agosto del 2006, se utilizaron **147,184** muestras de virus y todos los programas fueron actualizados con su ultima versión y firma de virus, y con su mejor configuraron, no se utilizo la configuración de default.

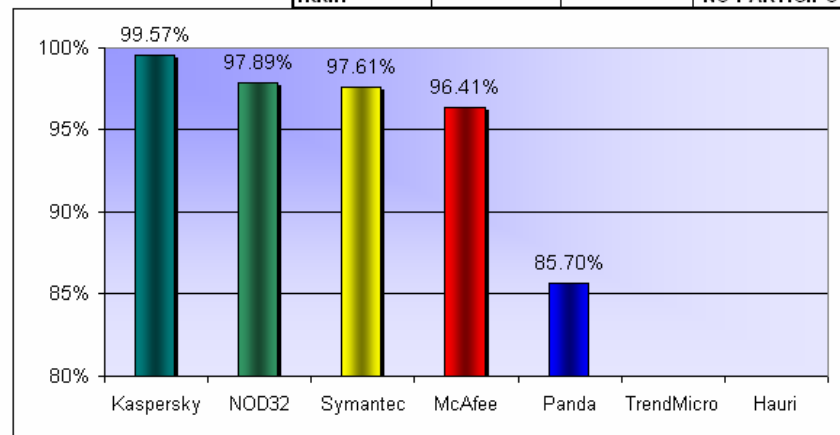


5.3.- Febrero 2006 Detección de código malicioso Escaner (On- Demand)

http://www.av-comparatives.org/seiten/ergebnisse_2005_09.php

Todos los Antivirus fueron actualizados hasta el día 06 de Febrero del 2006, y se les puso su mejor configuración

On Demand Detection of Malicious Software			
Antivirus	Version	Actualizacion	% Deteccion
Kaspersky	5.0.391	06-Feb-05	99.57%
NOD32	2.51.20	06-Feb-06	97.89%
Symantec	12.1.0.20	06-Feb-06	97.61%
McAfee	10.0.21	06-Feb-06	96.41%
Panda	10.01.02	06-Feb-06	85.70%
TrendMicro	-----	-----	NO PARTICIPO
Hauri	-----	-----	NO PARTICIPO





5.4.- Tiempo de Respuesta Promedio

Average response time	2005	2004
0 to 2 hours	Kaspersky Lab	-
2 to 4 hours	BitDefender, Dr. Web, F-Secure, Norman, Sophos	Kaspersky Lab , BitDefender
4 to 6 hours	AntiVir, Command, Ikarus, Trend Micro	AntiVir, Dr. Web, F-Secure, Panda Software, RAV
6 to 8 hours	F-Prot, Panda Software	Quickheal, Sophos
8 to 10 hours	AVG, Avast, CA eTrust-Inoculan, McAfee, VirusBuster	AVG, Command, F-Prot, Norman, Trend Micro, VirusBuster
10 to 12 hours	Symantec	Avast, CA eTrust-CA
12 to 14 hours	-	Ikarus, McAfee
14 to 16 hours	-	CA eTrust-VET, Symantec
16 to 18 hours	-	-
18 to 20 hours	CA eTrust-VET	-

Source: Ranking Response Times for Anti-Virus Programs (Andreas Marx of Av-Test.org); http://blogs.washingtonpost.com/securityfix/2005/12/antivirus_resea.html.

5.5.- Detección en Archivos compactados

- support for over 1,200 archiving and compression utility formats puts Kaspersky Internet Security 6.0 completely beyond the reach of competing solutions in terms of detection of viruses in compressed files. Most contemporary malicious programs are packed with one compression utility or another. This prompted experts at IBM Virus CERT to conduct a test in October 2005, in which the notorious Nimda.A virus was packed by 20 different packers using default settings and then scanned by 13 popular antivirus products. Results of this analysis are provided in the table below.

	Sym	Trm	McA	Sop	KL	NOD	CA	Nor	Bit	Pan	AVG	DrW	Hau
Detected by the monitor	5	11	9	12	17	1	2	2	12	4	5	9	2
%	24%	52%	43%	57%	81%	5%	10%	10%	57%	19%	24%	43%	10%
Detected by the on demand scanner	7	12	14	12	19	1	4	15	16	12	7	11	4
%	33%	57%	67%	57%	90%	5%	19%	71%	76%	57%	33%	52%	19%
Total detected	12	23	23	24	36	2	6	17	28	16	12	20	6
Overall %	29%	55%	55%	57%	86%	5%	14%	40%	67%	38%	29%	48%	14%

Source: ANTIVIRUS IN THE WILD (IBM Virus CERT) <http://www.malwareblog.com/>

6.- AOL distribuye gratuitamente Active Virus Shield con Tecnología Kaspersky.

AOL Premium Services ofrecerá en línea a sus usuarios un nuevo producto "Active Virus Shield", una solución antivirus **gratuita** con buena ingeniería, alto nivel, funcionalidad de antivirus y acceso a las actualizaciones de firmas de virus.

FREE for Everyone! A new service courtesy of AOL

Comprehensive Anti-Virus Protection
Helps Protect Your PC from Viruses & Spyware

Introducing Active Virus Shield

- Advanced detection technology to help stop known and new viruses, spyware and other malware before they attack you.
- Always-on, automatically checks for updates every hour, providing real-time scanning and protection against real threats.
- Easy-to-install, works with most Windows® operating systems. (Windows 95, 2000, ME & XP)
- Free to everyone- No AOL subscription required.

Get FREE Anti-Virus Today!
Click Here to DOWNLOAD

Is Your Virus Protection Working? Find out!

*Powered by Kaspersky Lab, one of the largest antivirus providers, worldwide.

"Concluir una sociedad con uno de los principales proveedores internacionales de Internet es un paso importante para Kaspersky Lab elevando el perfil de nuestra marca en Norteamérica. AOL tiene alrededor de 18 millones de suscriptores a sus servicios en todo el mundo, y 80% de ellos están localizados en Estados Unidos. Desde que el proyecto se lanzó, apenas hace una semana, ya hemos recibido varias propuestas de compañías Americanas, ofreciendo distribuir nuestro software en la región," comentó Natalya Kaspersky.

Para mayor información acerca del software de Active Virus Shield, por favor visite: <http://www.kaspersky.com.mx>
<http://www.activevirusshield.com/antivirus/freeav/index.asp?>



7.- Compañías que utilizan Ingeniería de Kaspersky Antivirus.



Actualmente la Ingeniería de Kaspersky esta integrada en productos de seguridad que protegen a más de 200 millones de usuarios a nivel mundial.



Actualmente la Ingeniería de Kaspersky esta integrada en productos de seguridad que protegen a más de 200 millones de usuarios a nivel mundial.





8.- VirusTotal un Portal que ofrece escaneo de más de 25 Antivirus en Línea

VirusTotal es un servicio gratuito de análisis de archivos, mediante el uso de múltiples Antivirus

El envío de archivos sospechosos puede realizarse de dos maneras:

- 1.- En el sitio de Virus Total <http://www.virustotal.com> se selecciona el archivo sospechoso y se pulsa el botón de enviar y se recibe el resultado
- 2.- Enviando un correo electrónico a analiza@virustotal.com
 - Poner en el asunto únicamente ANALIZA (o ANALIZA- en el caso de que no quiera que su muestra se envíe a casas antivirus).
 - Adjuntar en el mensaje el archivo que desea analizar con Virustotal.
 - El archivo no deberá sobrepasar el tamaño máximo de 5 MB. En caso de superarlo el mensaje será automáticamente descartado.
 - Recibirá en su e-mail un reporte detallado del análisis. La velocidad de respuesta dependerá de la carga a la que esté sometido el servicio en ese instante. Colaboradores:

Se recomienda utilizar este servicio en caso de tener duda si un archivo esta infectado y su actual antivirus no lo detecta.

Este es el resultado completo de analizar el archivo "Importante_Atenci_n_al_cliente_S" que VirusTotal ha recibido el día 31.08.2006 a las 17:31:51 (CET). ESTADO: FINALIZADO

Antivirus	Version	Actualización	Resultado
AntiVir	6.35.1.11	31.08.2006	no ha encontrado virus
Authentium	4.93.8	31.08.2006	no ha encontrado virus
Avast	4.7.844.0	31.08.2006	no ha encontrado virus
AVG	386	31.08.2006	no ha encontrado virus
BitDefender	7.2	31.08.2006	no ha encontrado virus
CAT-QuickHeal	8.00	31.08.2006	no ha encontrado virus
ClamAV	devel-20060426	31.08.2006	no ha encontrado virus
DrWeb	4.33	31.08.2006	no ha encontrado virus
eTrust-InoculateIT	23.72.111	31.08.2006	no ha encontrado virus
eTrust-Vet	30.3.3052	31.08.2006	no ha encontrado virus
Ewido	4.0	31.08.2006	no ha encontrado virus
Fortinet	2.77.0.0	31.08.2006	no ha encontrado virus
F-Prot	3.16f	31.08.2006	no ha encontrado virus
F-Prot4	4.2.1.29	31.08.2006	no ha encontrado virus
Ikarus	0.2.65.0	31.08.2006	no ha encontrado virus
Kaspersky	4.0.2.24	31.08.2006	Trojan-Spy.HTML.Bankfraud.qa
McAfee	4842	31.08.2006	no ha encontrado virus
Microsoft	1.1560	31.08.2006	no ha encontrado virus
NOD32v2	1.1733	31.08.2006	no ha encontrado virus
Norman	5.90.23	31.08.2006	no ha encontrado virus
Panda	9.0.0.4	31.08.2006	no ha encontrado virus
Sophos	4.09.0	31.08.2006	no ha encontrado virus
Symantec	8.0	31.08.2006	no ha encontrado virus
TheHacker	5.9.8.202	31.08.2006	no ha encontrado virus
UNA	1.83	31.08.2006	no ha encontrado virus
VBA32	3.11.1	30.08.2006	no ha encontrado virus
VirusBuster	4.3.7.9	31.08.2006	no ha encontrado virus



9.- Soluciones Antivirus Certificadas por Microsoft

La ingeniería de Kaspersky Antivirus es utilizada en **7 de las 27** soluciones certificadas por Microsoft.

<http://www.microsoft.com/security/partners/antivirus.asp>



Aladdin (Ingeniería Kaspersky)	Frisk (F-prot)	Panda Software
Cat Computer Services	BullGuard Ltd.	Proland Software
F-Secure (Ingeniería Kaspersky)	Computer Associates	Sophos
GFI (Ingeniería Kaspersky)	ESET	Sybari (Ingeniería Kaspersky)
Symantec	GRISOFT	Zero-Knowledge Systems Inc.
Trend Micro, Inc.	HAURI	DialogueScience, Inc.
VirusBuster Ltd.	Kaspersky Lab	MicroWorld (Ingeniería Kaspersky)
AhnLab, Inc.	McAfee	http://www.microsoft.com/security/partners/antivirus.asp
ALWIL Software	Norman	

• **6 de 27** Microsoft Antivirus Partners utilizan la Ingeniería de Kaspersky.

Sybari
A Microsoft Subsidiary

FRONTBRIDGE
A Microsoft Subsidiary

KASPERSKY Lab

10.- Kaspersky Incluido en Desktop Boards de Intel.

<http://support.intel.com/design/motherbd/software/kav/>

US Home | Intel Worldwide | Where to Buy | Training & Events | Contact Us | About Intel

Resource Centers | Products | Solutions & Services | Technologies & Trends | Support & Downloads

Hardware Design | Hardware Design | Design Components & Products | Intel® Desktop Boards | Value Added Software | Kaspersky® Anti-Virus Business Optimal

Intel® Desktop Boards

Kaspersky® Anti-Virus Business Optimal

Offered with all Intel® Desktop Boards, Kaspersky® Anti-Virus Business Optimal provides virus protection for small and medium businesses. Featuring cutting-edge technologies, user-friendly management tools and a flexible licensing policy, Kaspersky Anti-Virus Business Optimal produces a highly versatile security solution for your business, offering an excellent return on investment.

Kaspersky Anti-Virus Business Optimal is fully scalable, supports a wide range of operating systems and applications, and protects even the most complex networks. Centralized management and installation tools ensure ease of use.

Comprehensive protection

Kaspersky Anti-Virus Business Optimal detects malicious programs without false positives. The comprehensive virus database, updated every three hours, supports accurate identification. The application also protects all network components and equipment which can serve as entry points for malicious programs: workstations, file servers, mail systems, and Internet gateways.



KASPERSKY Lab



10.- Casos de Éxito.



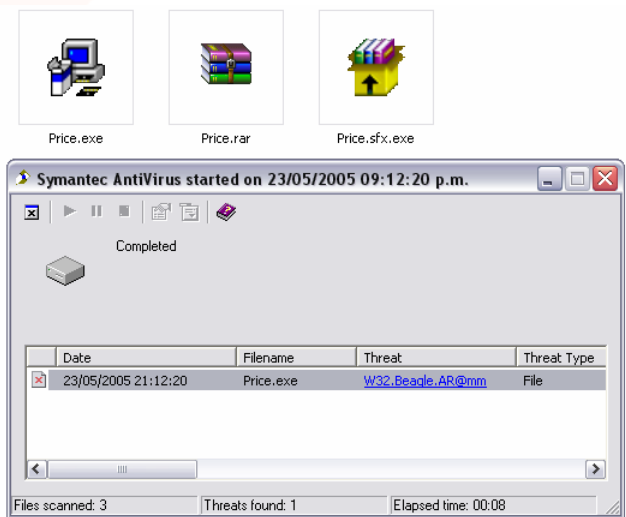
4 Años consecutivos que renuevan su confianza con Kaspersky Antivirus

8.- Problemas de detección en Antivirus

El 17 de Febrero del 2005, Hispasec publico una noticia donde preguntaba ¿Por qué la mayoría de antivirus no han detectado al "nuevo" Mydoom? <http://www.hispasec.com/unaaldia/2308> , enseguida se explica la razón por la cual algunos Antivirus no pudieron detectar esta nueva variante.

“Una de los ejemplos consistió en "modificar" un troyano para hacerlo invisible al motor antivirus de TrendMicro (le tocó en este caso, como le ocurrió a otros motores en el resto de ejemplos). Como muestra se optó por el reconocido y veterano BackOrifice, un troyano de puerta trasera con bastante solera, detectado por todos los antivirus. Le pasamos un compresor de ejecutables, y conseguimos una copia del troyano, con las mismas funcionalidades, pero al estar su código comprimido no era reconocido por la firma de TrendMicro “.

Otros problemas derivados de este tipo de prácticas es que cuando se ejecuta un archivo bajo ese formato la descompresión se hace en RAM, y queda fuera del alcance de los monitores residentes antivirus que interceptan y analizan sólo cuando existen accesos al disco. Ya no hablamos de los motores situados en el perímetro, como por ejemplo en el servidor de correos, que no tienen opción a ejecutar las muestras.





Esa "transformación" en un troyano nuevo, no detectable por el antivirus, se consiguió con dos clicks de ratón, literalmente, como pudo verse en directo.

Pues lo ocurrido con la nueva versión de Mydoom es similar a lo que se pudo ver en la charla. Se trata de la variante que apareció en julio del año pasado, que en aquella ocasión fue comprimida con UPX, y que alguien la ha tratado con un nuevo compresor, en este caso MEW."

- En esta prueba se tienen 3 Archivos infectados con el virus bagle, con difentes formatos:

- Price.exe : Es el virus bagle
- Price.rar: Es el virus bagle comprimido con el compresor Winrar.
- Price.sfx.exe: Es el virus Bagle comprimido y ejecutable con el compresor Winrar.

- Solo Symantec y TrendMicro no detectaron los tres archivos infectados, si vemos con detalle las graficas notaremos que ambos escaners reportan 3 archivos escaneados pero

- Symantec solo reporta infectado el archivo "Price.exe" con el virus bagle.
- TrendMicro reporta infectados el archivo "Price.exe" y "Price.rar", sin poder detectar el virus en "Price.sfx.exe"

En esta grafica podemos ver la detección del virus Bagle con Kaspersky Antivirus.

