

RATIOS DE INFECCIONES EN SISTEMAS CON PROTECCIÓN ANTI-MALWARE

Estudio de Investigación de **PandaLabs**
pandalabs.pandasecurity.com

Índice

1 Resumen	3
2 Introducción al estudio	4
3 Metodología	5
4 Estudio en el sector de consumo	7
4.1 Evolución de las infecciones de malware	7
4.2 Información sobre la muestra estadística	8
4.2.1 Máquinas por estado de la protección anti-malware	8
4.2.2 Máquinas por sistema operativo	9
4.2.3 Máquinas por país	10
4.3 Infecciones por malware en máquinas protegidas	11
4.3.1 Infecciones por tipo de malware	12
4.3.2 Infecciones de malware por solución anti-malware	13
5 Estudio en el sector corporativo	14
5.1 Información sobre la muestra estadística	14
5.1.1 Empresas por país	14
5.1.2 Estaciones por sistema operativo	15
5.1.3 Estaciones por estado de la protección anti-malware	16
5.2 Infecciones de malware en redes protegidas	17
5.2.1 Infecciones de malware por red analizada	17
5.2.2 Infecciones por tipo de malware	18
5.2.3 Infecciones por solución anti-malware	19
6 Conclusiones	20
7 Apéndice – Detección y prevalencia de malware en julio	22
8 Referencias	24

1. Resumen

Si existe más cantidad de malware que nunca y los laboratorios antivirus no pueden crear firmas con la suficiente rapidez como para proteger a los usuarios, parece lógico pensar que exista **un número significativo de usuarios infectados, pese a que dispongan de una solución de seguridad actualizada con el último archivo de firmas de virus.**

Hemos llevado a cabo un proyecto de investigación con el objetivo de descubrir la auténtica situación del malware en ordenadores reales con protección actualizada. El estudio, que aún continúa, se realizó entre mayo y julio de 2007 en **ordenadores domésticos** y redes corporativas de todo el mundo. De los ordenadores domésticos analizados, con diferentes soluciones de seguridad instaladas y archivos de firmas actualizados, **más del 23% se encontraba infectado con código malicioso cargado en la memoria.** De todas las empresas analizadas que ejecutaron nuestra auditoría de seguridad en más de 100 estaciones con protección anti-malware activa y actualizada, **el 72% presentaba infecciones por malware.**

Como conclusión de esta investigación hemos descubierto que usuarios que son clientes activos y que pagan el servicio de sus soluciones antivirus o anti-malware están sufriendo infecciones de malware sin saberlo. Parece que en algunos casos el software de seguridad proporciona una falsa sensación de seguridad. Esta impresión es conocida por la industria anti-malware. Incluso se potencia desde la misma, en algunos casos proporcionando a los usuarios "certificaciones de producto" que perciben como una certificación de calidad cuando en realidad sólo prueban que la solución es capaz de detectar una parte del porcentaje de malware que está en circulación.

Se necesita de nuevas formas de cooperación entre los miembros de la industria así como de nuevos enfoques tecnológicos sobre protección anti-malware para proporcionar protección contra el panorama actual del malware. Este estudio de investigación se ha llevado a cabo con la esperanza de que sirva para realizar un análisis de las barreras para la innovación, como los estándares empleados para los tests antivirus, los estándares de calidad y los estándares de certificación de productos, que mantienen esta situación oculta bajo la alfombra.

2. Introducción al estudio

El objetivo de esta investigación, que sigue en marcha, es proporcionar estadísticas sobre las infecciones de malware activo en sistemas protegidos por soluciones de seguridad o anti-malware con el último archivo de firmas instalado. El objetivo final de este estudio es mostrar la evolución de los índices de infección con el fin de analizar la efectividad de las diferentes tecnologías de protección.

Pese a que existen encuestas basadas en usuarios que intentan mostrar investigaciones similares¹, no hemos sido capaces de encontrar ninguna que mostrase conclusiones científicas y verificables basadas en:

- *Datos recopilados automáticamente que puedan ser divididos según usuarios con y sin protección anti-malware.*
- *Infecciones por malware en sistemas protegidos con las últimas actualizaciones y motores anti-malware.*
- *Una muestra amplia de población que refleje la situación en diferentes lugares geográficos.*
- *Estadísticas que muestren los índices de infección específicamente y de forma separada para el mercado de consumo y corporativo.*

Nuestro proyecto tiene como objetivo recoger datos de forma automática de cientos de miles de ordenadores en todo el mundo, dándonos la oportunidad de ofrecer una visión mucho más realista de la situación real de la seguridad. Durante el curso de esta investigación hemos sido capaces de recopilar otra serie de estadísticas significativas que han arrojado un poco de luz sobre la situación real de los PCs de los usuarios.

3. Metodología

Se llevaron a cabo dos estudios diferentes analizando físicamente ordenadores de consumo y de empresas en más de 80 países. Las máquinas analizadas incluían protección de más de 40 fabricantes diferentes de seguridad. El análisis fue realizado utilizando diferentes sistemas online y herramientas de auditoría con millones de firmas de malware y goodwill y capacidad para analizar desde la nube:

Estudio en el sector doméstico:

- Los consumidores analizaron sus PCs empleando un scanner online especial.
- Los consumidores que analizaron sus PCs varias veces sólo se cuentan una vez.
- Sólo se toma en consideración el resultado del primer análisis.

Estudio en el sector corporativo:

- Las auditorías tuvieron lugar físicamente en redes corporativas de todo el mundo utilizando una herramienta de auditoría de malware especialmente creada con el objetivo de descubrir malware no detectado.
- Las empresas que realizaron varias auditorías sólo se cuentan una vez.
- Sólo se toma en consideración el resultado de la primera auditoría de cada PC.

Criterios de infección:

- **Se considera que un PC está infectado** cuando encontramos malware (troyanos, adware, virus, gusanos, etc.) ejecutándose de forma activa en memoria.
- **Se considera que un PC NO está infectado** si sólo tiene malware latente (malware en bases de datos de correo electrónico, guardado en el disco duro) que no esté ejecutándose de forma activa, ejecutándose en la memoria, registrado como un BHO o activo de cualquier otra forma.
- **Se considera que un PC NO está infectado** si sólo tiene tracking cookies, jokes u otras aplicaciones no maliciosas.

Criterios para definir un sistema protegido:

- Consideramos que un PC está protegido cuando tiene una solución anti-malware o de seguridad instalada y actualizada con el último archivo de firmas de virus.
- Las estadísticas sobre el estado de la solución anti-malware o de seguridad instalada (driver residente activo o inactivo) y la información sobre el archivo de firmas (actualizado o desactualizado) se obtiene directamente de Microsoft Windows Security Center en Windows XP SP2 y Windows Vista. Algunas empresas de seguridad no aparecen en nuestras estadísticas ya que no quedan registradas o no comparten información con Microsoft Windows Security Center.

Para determinar si un PC está infectado o no, hemos creado un sistema capaz de detectar de forma positiva todos los ejemplares de malware conocidos (y una gran parte de los desconocidos), independientemente de que dispongamos o no de firmas de detección para ellos en nuestros productos estándar.

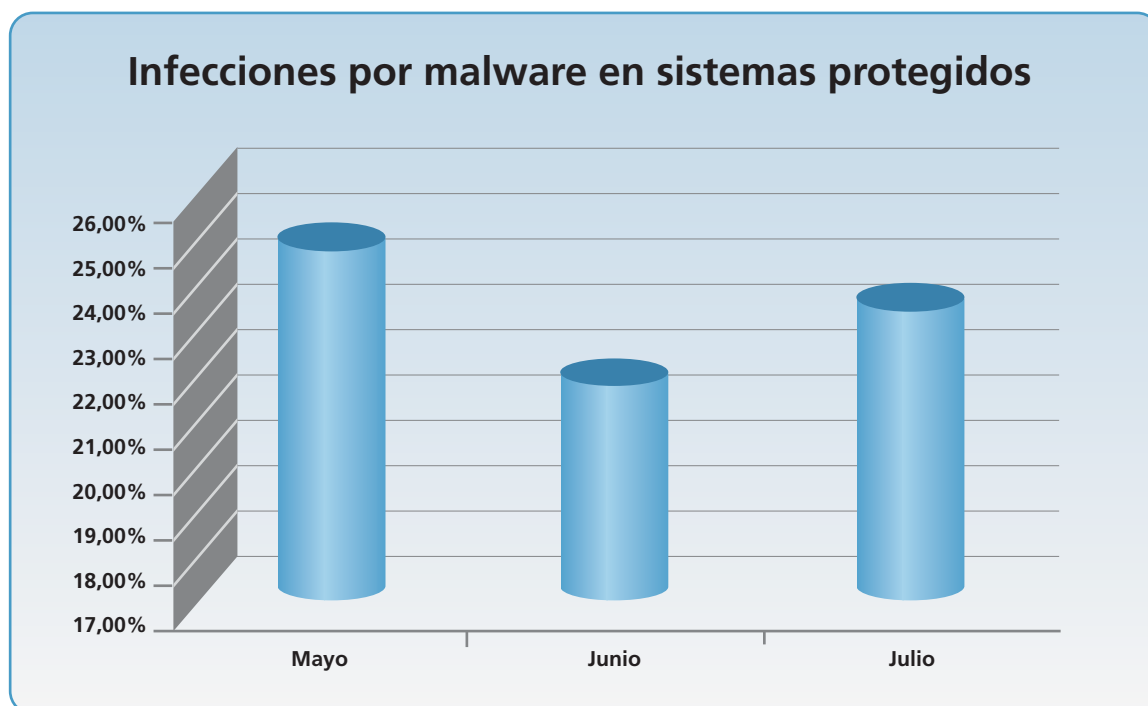
Hemos conseguido esto con una plataforma que llamamos Inteligencia Colectiva, que consiste en un sistema online alojado en varios Centros Operativos de Red que automatiza los procesos de recogida, clasificación y detección de malware y correlaciona los resultados de los análisis procedentes de todos los usuarios, siendo por lo tanto capaz de detectar también ataques dirigidos. Analizar desde la nube proporciona otras ventajas, como poder utilizar tecnologías de análisis mucho más avanzadas y con más recursos, sin los límites que presenta un único PC en cuanto a memoria RAM o CPU.

La Inteligencia Colectiva de Panda es un nuevo concepto en protección anti-malware que se beneficia en tiempo real de la información proporcionada por la comunidad de usuarios y la automatización de los procesos de recogida de muestras, procesamiento y solución con el fin de aumentar su capacidad de detección².

4. Estudio en el sector doméstico

Los datos de esta parte del estudio estadístico se obtuvieron de 1,48 millones de usuarios que analizaron sus PCs con uno de nuestros scanners online de Inteligencia Colectiva desde mayo de 2007. De estos 1,48 millones sólo nos interesaron aquellos que (a) tenían sistemas anti-malware o de seguridad instalados activos y actualizados y (b) tenían infecciones por malware activo. Los PCs que cumplen estos dos criterios son, de media, el 23% de todos los PCs analizados, tal y como se muestra a continuación.

4.1 Evolución de las infecciones de malware



Periodo de estudio	Usuarios analizados	Ratio de infección en sistemas desprotegidos	Ratio de infección en sistemas protegidos
Mayo 2007	730.237	34,85%	24,17%
Junio 2007	443.214	31,25%	21,78%
Julio 2007	306.836	33,74%	22,97%
TOTAL	1.480.287	33,28%	23,21%

Es importante destacar que los índices de infección que nos interesan son los “*índices de infección en sistemas protegidos*”, que son sistemas con soluciones de seguridad anti-malware o de seguridad instaladas y actualizadas. El índice de infección en las máquinas desprotegidas es obviamente superior, tal y como se muestra en la página anterior.

En las secciones siguientes analizaremos en profundidad los datos de la parte final del estudio, que corresponde a julio de 2007.

4.2 Información sobre la muestra estadística

Como este es un estudio que aún sigue en marcha y que se publicará regularmente, hacemos un seguimiento de los índices de infección en los sistemas con protección anti-malware (sección 4.1 anterior) y un análisis de los datos pertenecientes a la última parte del estudio, que corresponde a esta sección (4.2).

El estudio realizado en julio de 2007 se refiere a un número total de 306.836 PCs distintos analizados. Los datos fueron recogidos desde el 1 de julio al 20 de julio de 2007.

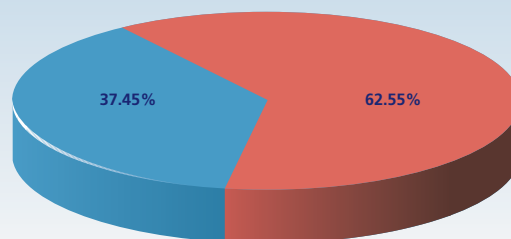
En los siguientes apartados desgranaremos estos datos por sistema operativo, país, estado de la protección, índices de infección en los sistemas protegidos, infecciones por tipo de malware e infecciones por fabricante.

4.2.1 Máquinas por estado de la protección anti-malware

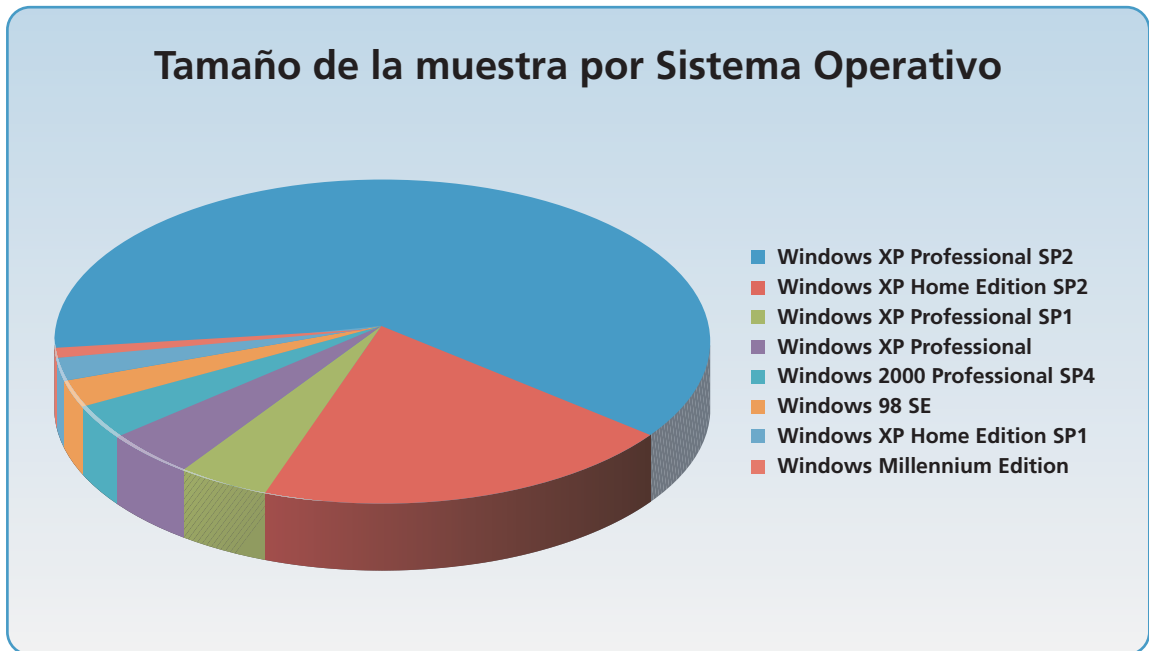
Como ya se ha mencionado anteriormente, este estudio se centra en determinar el índice de infecciones por malware en sistemas que se encuentren protegidos activamente con soluciones anti-malware actualizadas. En este estudio, solo el 37,45% de los sistemas analizados tenían protección activa y actualizada. El 62,55% restante o bien tenían firmas desactualizadas y el driver residente desactivado; o firmas desactualizadas y el driver residente activado, o no disponían de ningún anti-malware instalado.

Tamaño de la muestra en base al estado de la protección

- Anti-malware actualizado y activo
- Anti-malware desactualizado o sin protección



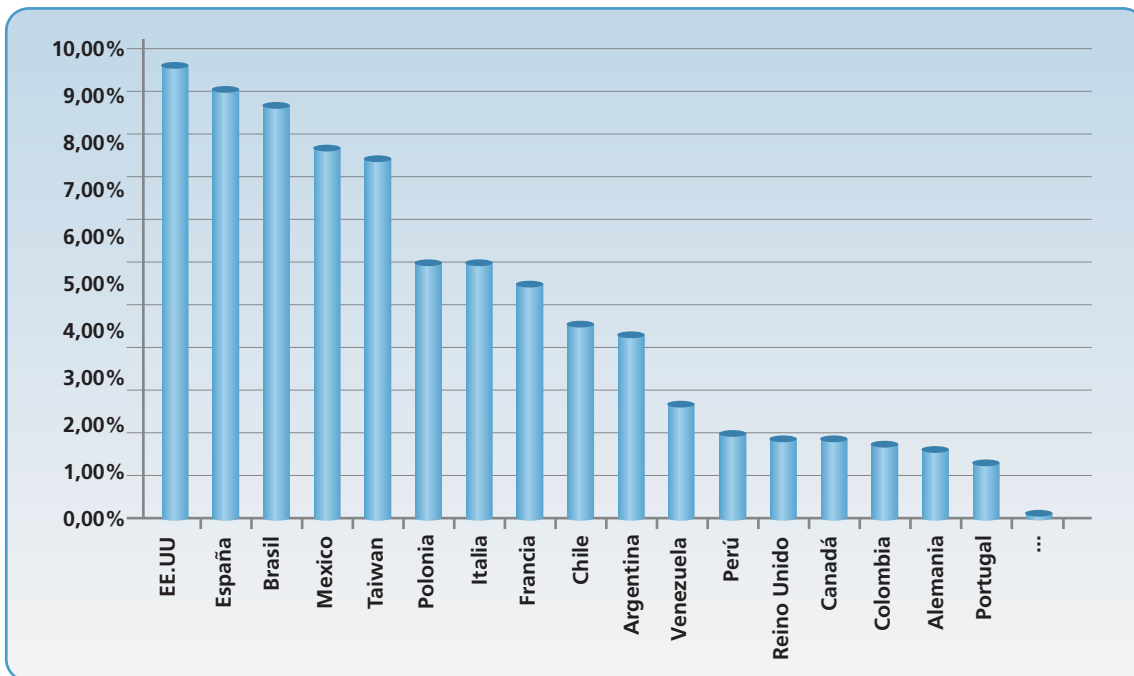
4.2.2 Máquinas por sistema operativo



Sistema operativo analizado	Cuota de mercado de la muestra
Windows XP Professional SP2	59,16 %
Windows XP Home Edition SP2	20,74 %
Windows XP Professional SP1	4,01 %
Windows XP Professional	3,66 %
Windows 2000 Professional SP4	3,55 %
Windows 98 SE	2,74 %
Windows XP Home Edition SP1	1,45 %
Windows Millennium Edition	1,03 %

* Datos obtenidos sobre el número total de PCs analizados.

4.2.3 Máquinas por país



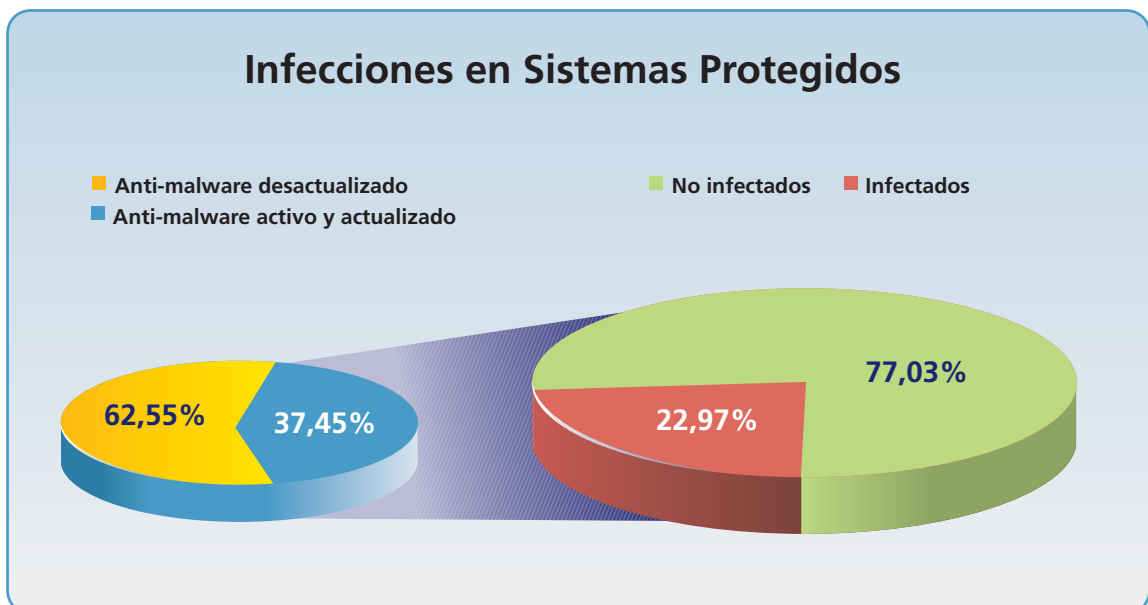
Distribución por país	Cuota de mercado de la muestra
Estados Unidos	9,60 %
España	9,12 %
Brasil	8,70 %
Mexico	7,83 %
Taiwan	7,55 %
Polonia	5,14 %
Italia	5,08 %
Francia	4,61 %
Chile	3,80 %
Argentina	3,67 %
Venezuela	2,68 %
Perú	2,11 %
Reino Unido	1,96 %
Canadá	1,93 %
Colombia	1,88 %
Alemania	1,75 %
Portugal	1,39 %
...	...

* Datos obtenidos sobre el número total de PCs analizados. Sólo se muestran los países de los que se obtuvieron más datos.

4.3 Infecciones por malware en máquinas protegidas

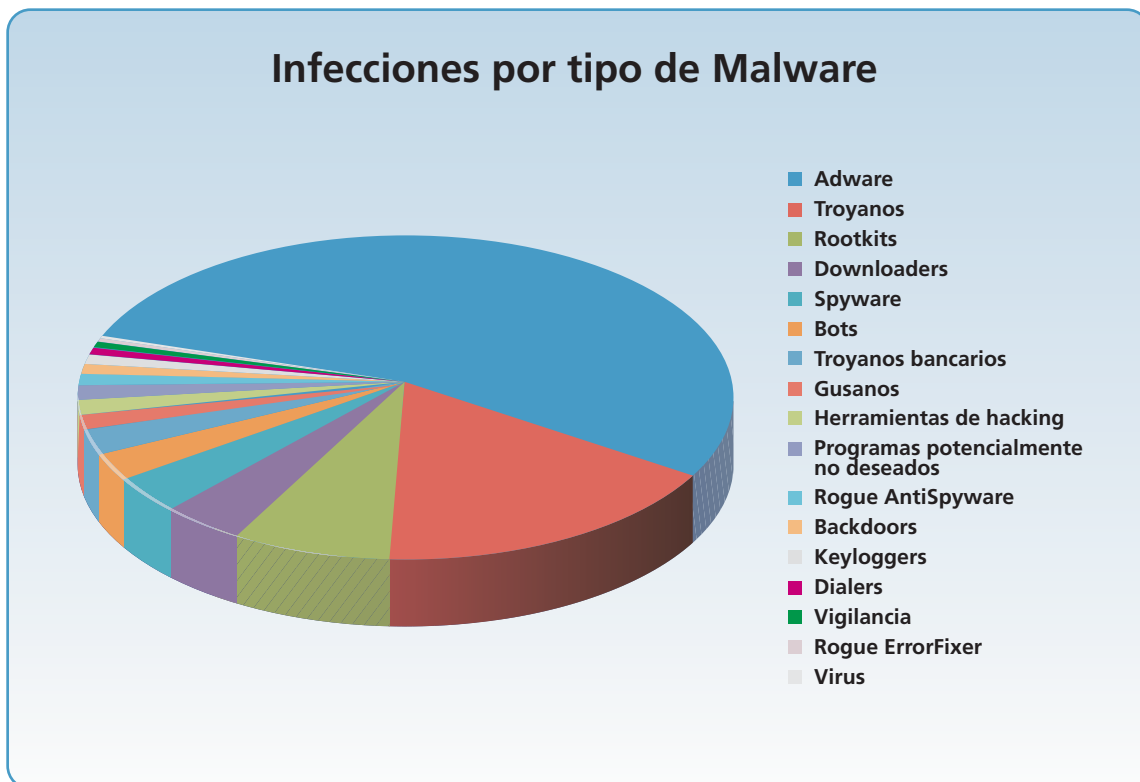
Descubrimos que, del 37,45% de sistemas analizados que disponían de protección anti-malware activa y actualizada, el 22,97% estaba infectado con código malicioso.

Estado de la protección	Tamaño de la muestra	No infectado	Ratios de inf. con malware activo
Anti-malware desactualizado y deshabilitado	55,32 %	66,46 %	33,54 %
Anti-malware activo y desactualizado	7,23 %	64,75 %	35,25 %
Anti-malware actualizado y activo	37,45 %	77,03 %	22,97 %



4.3.1 Infecciones por tipo de malware

La tabla siguiente muestra el porcentaje de PCs protegidos e infectados por malware activo según el tipo de malware encontrado. Un PC puede tener varios tipos de malware.



Tipo de malware	Encontrado en x % de PCs*
Adware	54.50 %
Troyanos	15.46 %
Rootkits	7.21 %
Downloaders	5.20 %
Spyware	4.80 %
Bots	2.65 %
Troyanos bancarios	2.22 %
Gusanos	2.21 %
Herramientas de hacking	1.06 %

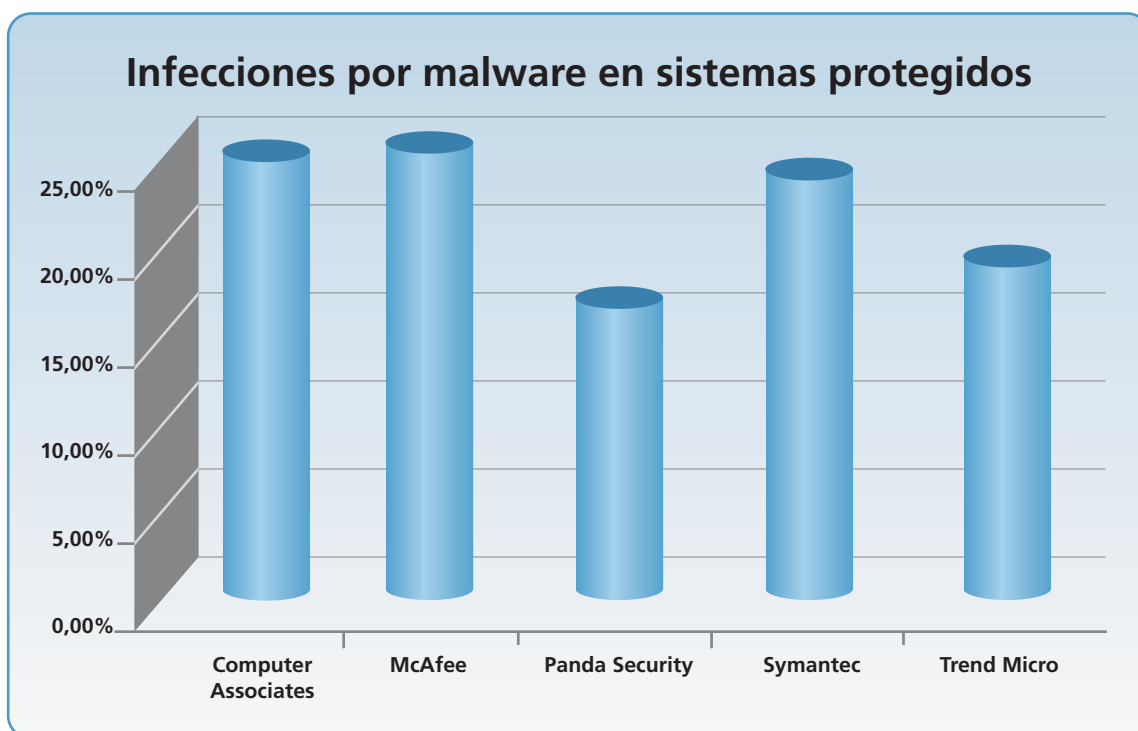
Tipo de malware	Encontrado en x % de PCs*
Programas potencialmente no deseados	1.03 %
Rogue AntiSpyware	0.96 %
Backdoors	0.86 %
Keyloggers	0.56 %
Dialers	0.45 %
Vigilancia	0.40 %
Rogue ErrorFixer	0.26 %
Virus	0.18 %

*Datos obtenidos sobre el número total de PCs analizados.

4.3.2 Infecciones de malware por solución anti-malware

Cada vez que se analiza un sistema consultamos a Windows Security Center por la solución anti-malware instalada, el firewall instalado, el estado del sistema y el estado de las actualizaciones. Esta información es almacenada y correlacionada con el estado de infección.

En la gráfica y la tabla que aparecen a continuación podemos ver los índices de infección de los sistemas en relación a la solución instalada y actualizada. Pese a que hemos reunido y correlacionado información de más de 40 empresas anti-malware y de seguridad, las que aparecen a continuación corresponden a las principales empresas por cuota de mercado mundial según Gartner. Esta información no debe ser tomada como un análisis comparativo ya que su objetivo es poner de manifiesto la existencia de un problema, común a toda la industria, relativo al estado actual de las soluciones anti-malware. De hecho, existen otros fabricantes en una lista que sobrepasa las 40 empresas con índices de infección superiores e inferiores a los mostrados a continuación³.



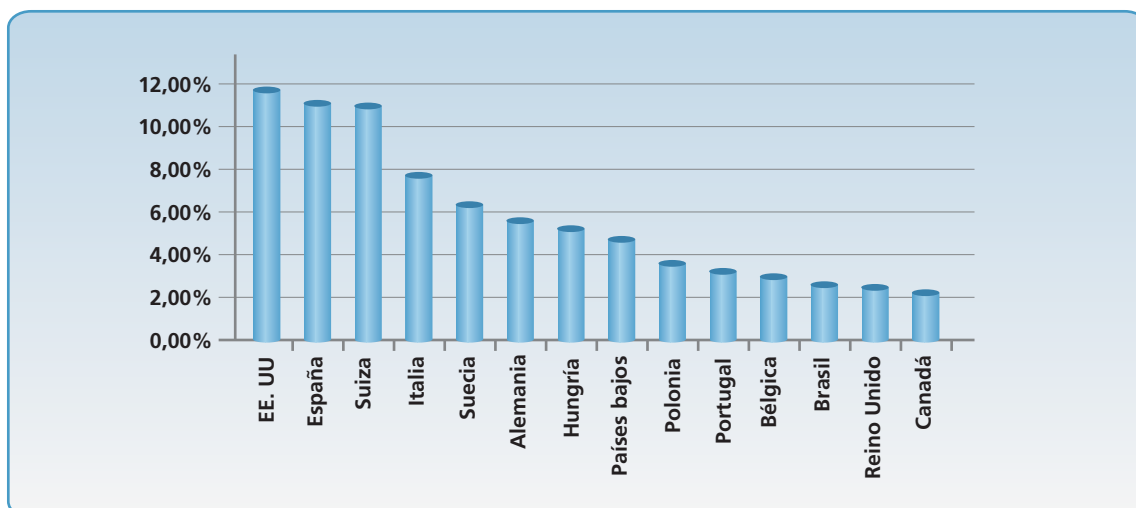
Fabricante	Ratio de infecciones en sistemas protegidos
Computer Associates	23,32 %
McAfee	24,18 %
Panda Security	15,54 %
Symantec	22,20 %
Trend Micro	17,08 %

5. Estudio en el sector corporativo

5.1 Información sobre la muestra estadística

Datos recopilados desde abril a julio de 2007 de un total de 1206 empresas. Número total de ordenadores analizados: 17.809.

5.1.1 Empresas por país



País	Cuota de mercado de la muestra
EEUU	11,77%
España	11,19%
Suiza	11,03%
Italia	7,96%
Suecia	6,05%
Alemania	5,47%
Hungría	4,81%

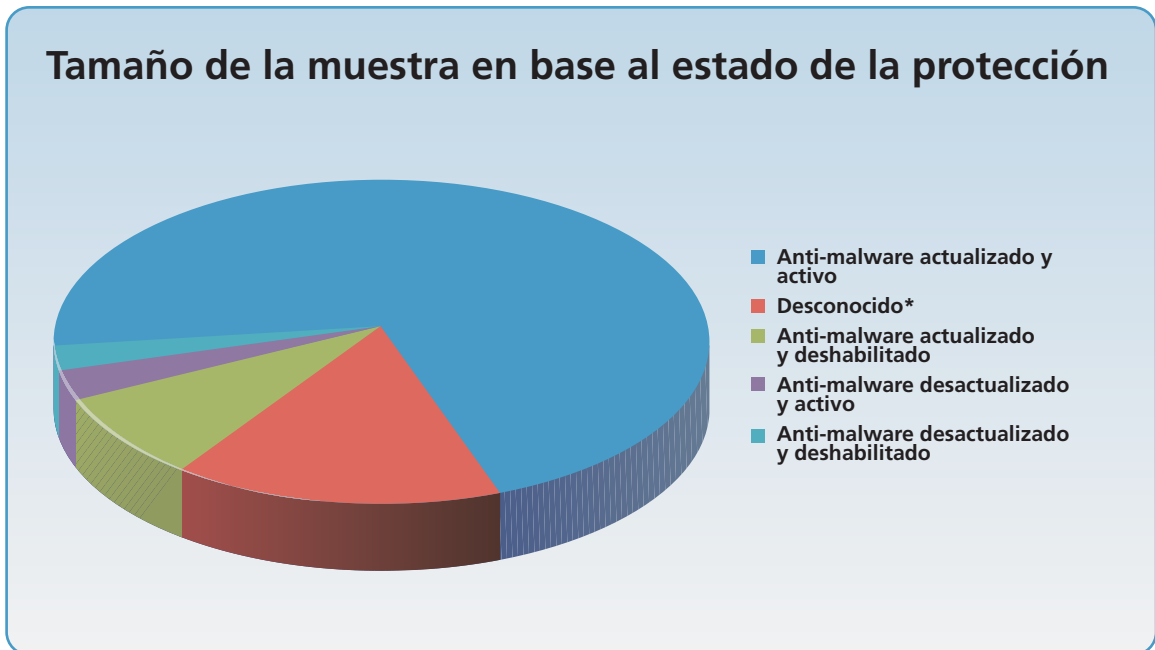
País	Cuota de mercado de la muestra
Países Bajos	4,56%
Polonia	3,57%
Portugal	3,23%
Bélgica	3,07%
Brasil	2,40%
Reino Unido	2,24%
Canadá	2,07%
...	...

5.1.2 Estaciones por sistema operativo



Sistema operativo analizado	Cuota de mercado de la muestra
Windows XP Professional SP2	65,94 %
Windows 2000 SP 4	17,93 %
Windows Server 2003 SP1	4,01 %
Windows XP Professional SP 1	3,91 %
Windows 2000 Server SP4	2,46 %
Windows Server 2003 SP2	2,24 %
Windows Vista	0,92 %
Windows 2000 SP3	0,57 %
Windows XP Home Edition SP2	0,47 %
Windows XP Professional	0,43%
Windows 2000 SP2	0,23%
Windows NT 4.0 Server SP6	0,13%
Windows 98 Second Edition	0,06%
Otros	0,70%

5.1.3 Estaciones por estado de la protección anti-malware



Estado de la protección	% de PCs analizados
Anti-malware actualizado y activo	69,34 %
Desconocido*	14,50 %
Anti-malware actualizado y deshabilitado	9,25 %
Anti-malware desactualizado y activo	4,49 %
Anti-malware desactualizado y deshabilitado	2,43 %

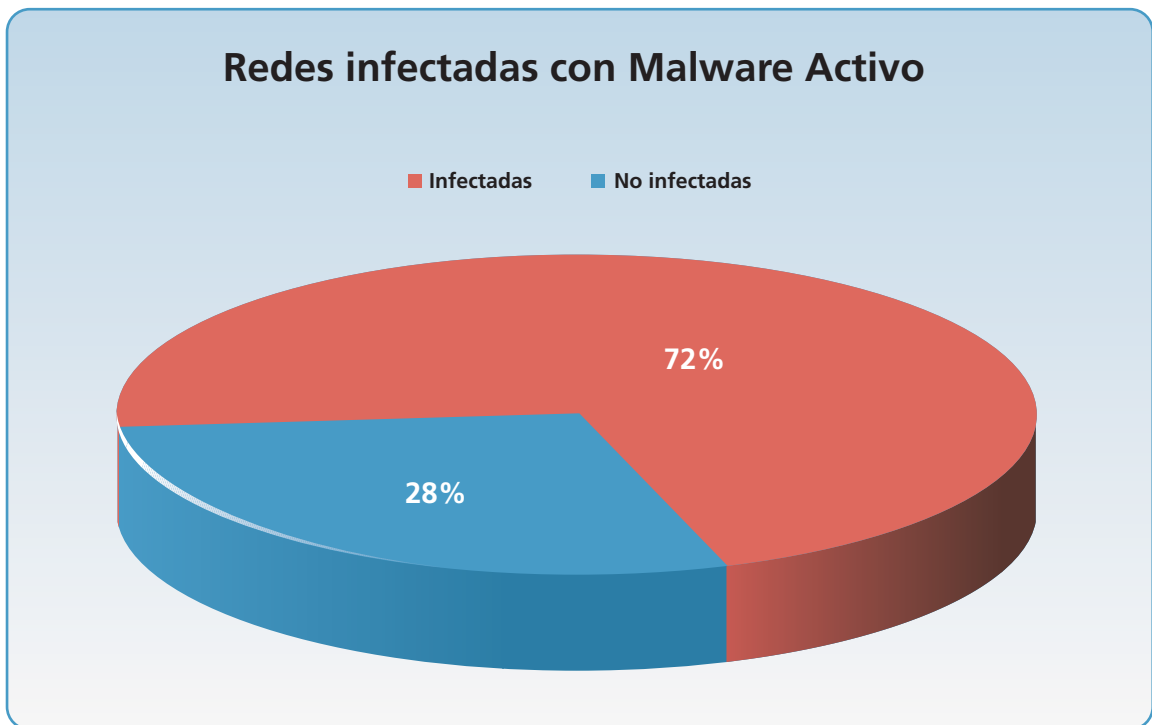
* "Desconocido" se refiere a PCs con sistemas operativos distintos de Windows XP SP2 y Windows Vista sin Windows Security Center, y/o ordenadores en los que se produjeron errores durante el proceso de recogida de datos.

5.2 Infecciones de malware en redes protegidas

Pese a que realizamos el estudio en más de 1.200 empresas distintas de todo el mundo, nos centraremos en las empresas que realizaron la auditoría de seguridad en más de 100 PCs. De esta forma reflejamos de forma más exacta la situación en el segmento que más nos interesa del mercado corporativo. Las empresas que realizaron auditorías en menos de 100 PCs se consideran auditorías departamentales o no relevantes para este estudio.

5.2.1 Infecciones de malware por red analizada

El siguiente gráfico muestra el porcentaje de empresas en las que se encontraron infecciones de malware durante la auditoría en al menos una estación dentro de la red corporativa.



Tamaño de la red	Ratio de redes infectadas
Menos de 50 estaciones	36,63 %
De 51 a 100 estaciones	62,26 %
Más de 100 estaciones	71,79 %

5.2.2 Infecciones por tipo de malware



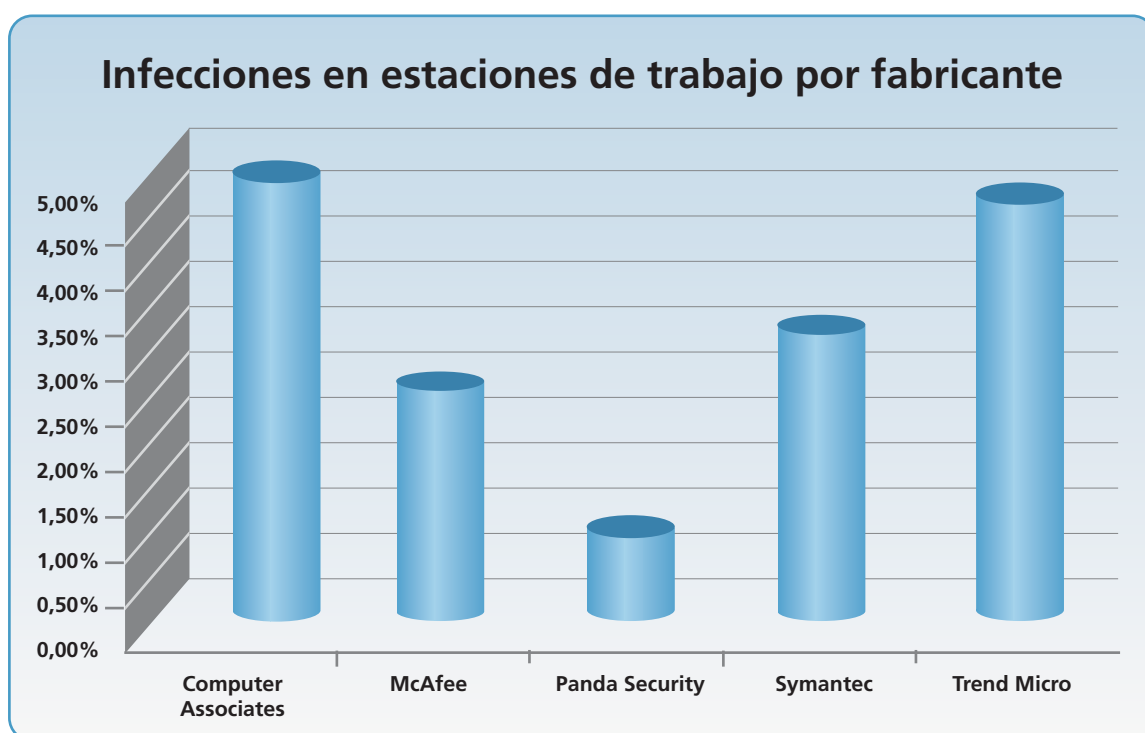
Tipo de malware	Porcentaje de detecciones*
Adware	63,04 %
Troyanos	12,57 %
Rootkits	4,50 %
Spyware	3,75 %
Backdoors	2,44 %
Troyanos bancarios	2,44 %
Bots	2,44 %
Downloaders	1,69 %
Gusanos	1,69 %
Keyloggers	1,50 %
PUPs	1,13 %
Virus	0,94 %
Rogue ErrorFixer	0,75 %
Dialers	0,75 %
Rogue AntiSpyware	0,19 %
Herramientas de hacking	0,19 %

* Detecciones sobre la base del total de detecciones de malware.

5.2.3 Infecciones por solución anti-malware

Como una red corporativa puede tener diferentes soluciones anti-malware en diferentes máquinas, la gráfica y la tabla que aparecen a continuación muestran los índices de infección del total de estaciones auditadas de acuerdo a la solución anti-malware instalada y actualizada.

Pese a que hemos recopilado y correlacionado información de muchos fabricantes de soluciones de seguridad y anti-malware para empresas, las que aparecen a continuación corresponden a las principales empresas por cuota de mercado mundial según Gartner. Esta información no debe ser tomada como un análisis comparativo, ya que el objetivo de estos datos es poner de manifiesto la existencia de un problema, común a toda la industria, relativo al estado actual de las soluciones anti-malware. De hecho, existen otros fabricantes en la lista completa de fabricantes que presentan índices de infección superiores e inferiores a los aquí mostrados.



Fabricante	Ratio de infecciones por malware activo
Computer Associates	4,55 %
McAfee	2,28 %
Panda Security	0,73 %
Symantec	2,80 %
Trend Micro	4,30 %

6. Conclusiones

El cambio en la motivación para la creación de malware, junto con el uso de técnicas avanzadas, ha originado un crecimiento exponencial de la cantidad de malware creado profesionalmente con fines delictivos y distribuido para infectar a usuarios desprevenidos. Según AusCERT, el 80% del malware nuevo consigue derrotar a las defensas antivirus⁴.

También conocida como ataques dirigidos, esta nueva dinámica del malware se ha convertido en la próxima gran plaga tanto para los usuarios como para las empresas. Se calcula que, para finales de 2007, el 75% de las empresas se verán infectadas por malware dirigido, no detectado, y creado para obtener beneficio económico, que habrá conseguido eludir sus defensas tradicionales de host y perimetrales⁵.

La consecuencia es que los laboratorios antivirus están sometidos a ataques constantes y cada vez más frecuentes de denegación de servicio distribuida. Nos vemos literalmente bombardeados por miles de nuevos ejemplares de malware todos los días. Algunas empresas de antivirus han intentado solucionar el problema o bien aumentando el número de analistas en los laboratorios⁶, o pidiendo la participación⁷ de las autoridades⁸ para que persigan a los creadores de malware más activos y se reduzca la carga de trabajo. Las iniciativas para conseguir que las autoridades se involucren más en esta lucha son positivas. Sin embargo y desgraciadamente, no son suficientes. Como desarrolladores y distribuidores de soluciones de seguridad debemos continuar asumiendo nuestra responsabilidad de proteger a los usuarios.

Por otro lado, los fabricantes de soluciones de seguridad y antivirus están haciendo grandes esfuerzos e inversiones para desarrollar y proporcionar mejores tecnologías de seguridad, como HIPS y análisis y bloqueo por comportamiento, que protejan mejor a los usuarios. La industria está realizando muchos esfuerzos para mejorar la WildList⁹, las certificaciones de producto y las metodologías de los análisis comparativos¹⁰.

Sin embargo, el problema continúa y no parece tener una solución fácil. Un número significativo de los clientes que pagan sus soluciones están infectados con malware a pesar de estar protegidos con los últimos y más avanzados productos de seguridad de los diferentes fabricantes. Por supuesto, tener una solución anti-malware o de seguridad instalada es mucho mejor que no tener ninguna. Sin embargo, tener una solución de seguridad no garantiza estar "totalmente protegido" de las amenazas actuales de Internet, los ciberdelitos, el robo de identidad o los ataques maliciosos.

La pregunta que deberíamos hacernos a continuación es la siguiente: “¿Cuál es la solución a este problema?”. Como sabemos, la seguridad de la información es más efectiva según va incorporando diversas capas de técnicas de protección. El estándar mínimo de protección actual consiste en tener un HIPS¹¹ integrado que incorpore como mínimo un antivirus basado en firmas, heurística avanzada, firewall de inspección profunda de paquetes, control de acceso a la red, prevención de explotación de vulnerabilidades, bloqueo por comportamiento y análisis de comportamiento. Sin embargo, tal y como hemos demostrado en este estudio, un HIPS integrado sigue sin ser suficiente para mantener a todos los usuarios protegidos de las infecciones.

La industria necesita desarrollar y proporcionar nuevas capas de protección que, junto con el actual estado de la tecnología, sean capaces de enfrentar el problema del incremento exponencial del malware, las técnicas que permiten evadir la detección por firmas y los ataques dirigidos. En nuestro caso estamos avanzando en el uso de la Inteligencia Colectiva de Panda¹², un nuevo concepto de seguridad completamente diferente al enfoque tradicional y que está demostrando ser muy efectivo es sus fases iniciales de implementación.

7. Apéndice – Detección y prevalencia de malware en julio

Nombre del malware	Tipo de malware	Prevalencia en PCs
Application/MyWebSearch	Adware	14773
GenericMalware	Troyano	4536
Adware/VideoActiveXObject	Adware	3073
Trj/Downloader.MDW	Downloader	2283
Spyware/Virtumonde	Spyware	1977
Generic Trojan	Troyano	1799
Adware/SaveNow	Adware	865
Adware/VideoActiveXAccess	Adware	709
Adware/SweetBar	Adware	691
Trj/Lineage.BZE	Rootkit	675
Application/DriveCleaner	Herramienta Hacking	547
Adware/ActiveSearch	Adware	545
Adware/PurityScan	Adware	536
Adware/DriveCleaner	Adware	500
Trj/Clicker.WM	Rootkit	494
Application/MyWay	Adware	485
W32/MSNWorm.K.worm	Gusano	472
Adware/SecurityError	Adware	372
Adware/Spylocked	Adware	354
Adware/OneStep	Adware	347
W32/IrcBot.AYK.worm	BOT	342
Adware/WebSearch	Adware	339
Adware/Zango	Adware	327
Spyware/New.net	Spyware	321
Adware/Comet	Adware	309
Application/FunWeb	Adware	308
Adware/VirusProtectPro	Adware	250
Adware/SpywareNo	Adware	241
Application/Messengerskinner	Adware	236
Trj/Mitglieder.OW	Rootkit	232
Adware/GoodSearchNow	Adware	214
Adware/IST	Adware	203
Adware/BaiduBar	Adware	197
Adware/VideoExtension	Adware	190
Application/Winantivirus2006	Falso AntiSpyware	187
Adware/Borlander	Adware	184
Adware/NaviPromo	Rootkit	182
Application/MSNContentPlus	Adware	181
Trj/Banker.FWD	Troyano bancario	174

Nombre del malware	Tipo de malware	Prevalencia en PCs
Adware/PopupSearches	Adware	165
Application/ViewPoint	PUP	165
Adware/Lop	Adware	160
Adware/Starware	Adware	160
Adware/Gator	Adware	25
Trj/Multidropper.BPX	Troyano	8
Adware/WUpd	Adware	6
Application/ErrorSafe	Falso parche	6
W32/Spamta.QO.worm	Bot	6
Bck/Hupigon.KMV	Backdoor	5
Application/ServUBased.A	Backdoor	4
Generic Adware	Adware	4
Trj/Keylog.LO	Keylogger	4
Trj/VB.OO	Troyano	4
W32/UsbStorm.A.worm	Gusano	4
Adware/DeluxeComunications	Adware	3
Adware/Exact.BargainBuddy	Adware	3
Trj/Banker.HDQ	Troyano bancario	3
Trj/Nabload.ACN	Rootkit	3
Trj/Rizalof.ABS	Troyano	3
W32/MadCoffee.C.worm	Gusano	3
W32/Virutas.G	Virus	3
Adware/123Mania	Adware	2
Adware/Alexa-Toolbar	Adware	2
Adware/CommanderToolbar	Adware	2
Adware/DelFinMedia	Adware	2
Adware/Maxifiles	Adware	2
Adware/WebBuying	Adware	2
Application/MediaPipe	Adware	2
Dialer.BCI	Dialer	2
W32/SdBot.KGP.worm	Bot	2
...

* Los datos mostrados se refieren a la identidad y tipo de malware con más presencia en ordenadores distintos en el estudio del sector de consumo y corporativo. No mostramos la lista completa de detecciones, ya que contiene una larga ristra final de malware con un nivel bajo de presencia.

8. Referencias

- ¹ AOL survey finds rampant online threats, clueless users. AOL. October 2004.
<http://www.computerworld.com/securitytopics/security/story/0,10801,96918,00.html>
- Know Your Enemy: Tracking Botnets. German HoneyNet Project. March 2005.
<http://project.honeynet.org/papers/bots/>
- Study says over 1m Windows PCs compromised. Sydney Morning Herald. March 2005.
<http://www.smh.com.au/news/Breaking/Study-says-over-1m-Windows-PCs-compromised/2005/03/18/1111085984429.html>
- Symantec Internet Security Threat Report, Volume XI.
http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xi_keyfindings_03_2007.en-us.pdf
- US tops spam relaying and malware leagues of shame. The Register. January 2007.
<http://www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en>
- Microsoft Security Intelligence Report. Microsoft Corporation. October 2006.
<http://www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en>
- ² Technology Paper: From Traditional AV to Collective Intelligence. Panda Research. August 2007.
http://research.pandasoftware.com/blogs/research/archive/2007/08/27/Technology-Paper_3A00_-From-AV-to-Collective-Intelligence.aspx
- ³ Market Share: Security Software Worldwide, 2006. Gartner.
<http://www.gartner.com>
- ⁴ Eighty percent of new malware defeats antivirus. ZDNet Australia. July 2006.
http://www.zdnet.com.au/news/security/soa/Eighty-percent-of-new-malwaredefeats_antivirus/0,130061744,39263949,00.htm
- ⁵ Gartner's 10 Key Predictions for 2007. eWeek. December 2006.
<http://www.eweek.com/article2/0,1895,2072416,00.asp>
- ⁶ The Zero-Day Dilemma. Security IT Hub. January 2007.
http://www.security.ithub.com/article/The+ZeroDay+Dilemma/199418_1.aspx
- ⁷ Welcome to 2007: the year of professional organized malware development. Michael-St. Neitzel at Hispasec. February 2007.
<http://blog.hispasec.com/virustotal/16>
- ⁸ Call the cops: We're not winning against cybercriminals. ComputerWorld. February 2007.
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010041>
- ⁹ The Disconnect Between the WildList and Reality. Panda Position Paper for Anti Virus Product Developer (AVPD) Confidential. January 2007.
- ¹⁰ Security Vendors Challenge Antivirus Tests. IDG News. June 2007.
<http://www.pcworld.com/article/id,133409-page,1/article.html>
- ¹¹ HIPS Update: Why Antivirus and Personal Firewall Technologies Aren't Enough. Gartner. January 2007.
http://www.gartner.com/teleconferences/attributes/attr_165281_115.pdf
- ¹² Technology Paper: From Traditional AV to Collective Intelligence. Panda Research. August 2007.
http://research.pandasoftware.com/blogs/research/archive/2007/08/27/Technology-Paper_3A00_-From-AV-to-Collective-Intelligence.aspx
- ¹³ The Long Tail: malware's business model. Panda Research. January 2007.
http://research.pandasoftware.com/blogs/research/archive/2007/01/08/The-Long-Tail_3A00_-malware_2700_s-business-model.aspx

PANDA SECURITY

Delegación Bilbao

Buenos Aires, 12
48001. Bilbao. ESPAÑA
Tlf: 94 425 11 00 - Fax: 94 424 46 97

Delegación Madrid

Ronda de Poniente, 17
28760. Tres Cantos. Madrid. ESPAÑA
Tlf: 91 806 37 00 - Fax: 91 804 35 29

Delegación Barcelona

Avda. Diagonal, 420 - 2º, 1
08037. Barcelona. ESPAÑA
Tlf: 93 208 73 00 - Fax: 93 458 59 00

Delegación Valencia

Doctor Zamenhof, 20 Bajo
46008. Valencia. ESPAÑA
Tlf: 96 382 49 53 - Fax: 96 385 93 80

902 365 505
www.pandasecurity.com

© Panda 2007. Todos los derechos reservados. 0907-WP-PSDRS-01