

White Paper

Cómo comprobar el nivel de seguridad de su empresa



La información incluida en este documento representa el punto de vista actual de Panda Software International, S.L. sobre las cuestiones tratadas en el mismo, en la fecha de publicación. Este documento es de carácter informativo exclusivamente. Panda Software International, S.L. no ofrece garantía alguna, explícita o implícita, mediante este documento.

El cumplimiento de las leyes que rigen el copyright es responsabilidad del usuario. De acuerdo con los derechos de copyright queda totalmente prohibida la reproducción total o parcial de este documento, así como su almacenamiento o introducción en un sistema de recuperación. Asimismo, queda prohibida la distribución de este documento por cualquier forma o medio (electrónico, mecánico, fotocopia, grabación u otros) o por razón alguna, sin previo consentimiento escrito de Panda Software International, S.L.

Panda Software International, S.L. puede tener patentes, aplicaciones de la patente, marcas registradas, derechos de autor o cualquier otro derecho de propiedad intelectual sobre la información contenida en este documento. Salvo previo acuerdo escrito con Panda Software International, S.L. la posesión de este documento no proporciona derecho alguno sobre dichas patentes, marcas registradas, copyrights u otra forma de propiedad intelectual.





Índice

La falsa percepción de seguridad en las empresas	2
El spam como nueva pesadilla económica de las compañías.....	4
El mal uso de Internet como riesgo de pérdidas económicas	4
La realidad sobre el tratamiento preventivo de las amenazas	5
La reducción de la ventana de riesgo	7
La situación de riesgo ¿percepción o realidad?	8
¿Por qué probar una solución perimetral?	13

La falsa percepción de seguridad en las empresas

Actualmente la mayoría de las compañías perciben que están protegidas de una forma u otra contra las amenazas informáticas. Sin embargo, cuando la seguridad se analiza por expertos, los datos muestran que esta percepción no es correcta en absoluto. La seguridad empresarial es un espejismo que puede causar daños nefastos en la mayoría de las empresas.

La nueva dinámica del malware

La motivación de los creadores de aplicaciones maliciosas ha cambiado en los últimos años. Han pasado de tener un carácter lúdico, en el que se perseguía la fama personal, a tener una motivación puramente económica. Ahora, las amenazas de malware suponen una importante fuente de ingresos.

Esto provoca que el malware sea mucho más específico y dirigido, de tal modo que en ocasiones sólo es efectivo en determinadas zonas geográficas o sólo se activa en determinados tipos de empresas. Esta situación dificulta la detección de los nuevos tipos de malware dirigido y, por tanto, la protección a través de herramientas tradicionales.

Las amenazas emergentes

La existencia de amenazas dirigidas y especializadas no ha acabado con las amenazas masivas. El objetivo de los hackers es saturar a los laboratorios para que no puedan hacer frente a todo el malware y desviar la atención de las nuevas amenazas. De hecho, el número de amenazas presentes en el mercado crece de forma exponencial y su repercusión en la calidad de las protecciones tradicionales ya se puede apreciar.

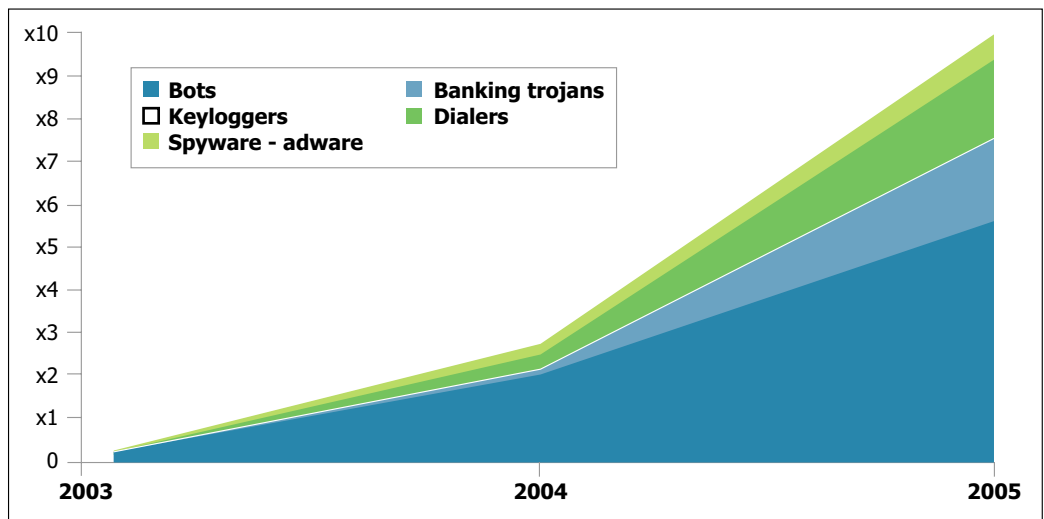


Fig. 1.-Crecimiento del malware por tipo de amenaza - Fuente: Pandalabs

Los ataques silenciosos

Las nuevas tácticas utilizadas por los hackers para lanzar sus ataques dificultan su detección. Se apoyan en redes de ordenadores robots (botnets) que lanzan ataques sin que sus propietarios sean conscientes. También utilizan técnicas evasivas que evitan las protecciones tradicionales y no dejan huella tras el ataque. Incluso aplican tácticas de suplantación de la identidad para atacar a otras redes o empresas.

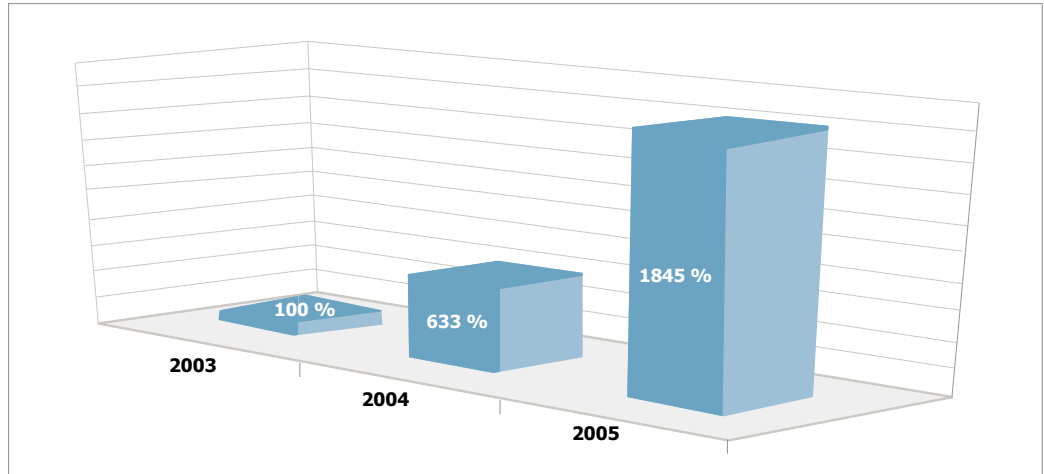


Fig. 2.-Crecimiento de nuevas muestras de bots detectadas - Fuente: Pandalabs

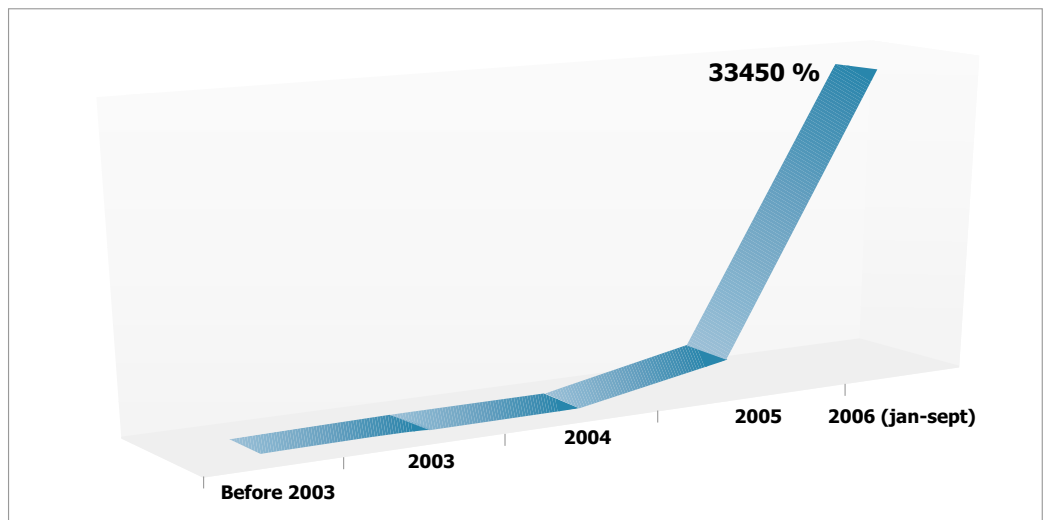


Fig. 3.- Crecimiento del malware usando técnicas de suplantación - Fuente: Pandalabs

En definitiva, los riesgos a los que se exponen las compañías siguen creciendo y las protecciones han de estar preparadas para combatirlos en el menor tiempo posible. La **protección tradicional es insuficiente** si no se apoya en un método de **prevención** y detección rápida de **nuevas amenazas**. No todas las compañías de seguridad pueden ofrecer este enfoque.



El spam como nueva pesadilla económica de las compañías

De forma análoga a lo que ocurre con el malware, la amenaza del spam o correo basura se multiplica continuamente.

Durante el primer trimestre de 2007, el 87,5% del correo analizado era spam. Este dato corresponde al informe de la plataforma de Servicio Premium de Protección de correo de Panda.

Esto quiere decir que únicamente alrededor de un 12% del correo recibido es de interés o su recepción se ha autorizado por el usuario.

Los datos económicos son alarmantes. Según un estudio de la universidad de Amsterdam (fuente JournalduNet) "...el coste del spam ronda los 300 euros por empleado al año".

El mal uso de Internet como riesgo de pérdidas económicas

Internet es una herramienta de utilidad innegable para las compañías y la necesidad de acceso a esta red está fuera de duda. Internet es la principal fuente de información entre las empresas.

Sin embargo, la variedad de contenidos de las páginas web a disposición de los usuarios es un riesgo para las empresas. Causa pérdidas de productividad de los empleados, al malgastar su tiempo navegando por páginas con contenidos negativos, violentos, obscenos o no relacionados con su trabajo.

Los datos del mal uso de Internet explican el riesgo que supone la navegación web no controlada.

- Entre el **30 y el 40%** del uso de Internet tiene carácter **no laboral**.
- Al menos el **60% de los empleados navegan** por Internet desde el trabajo **con fines personales** (chats, subastas, compras online...).
- El 70% de las visitas a páginas web con pornografía se realizan durante el horario laboral.

La realidad sobre el tratamiento preventivo de las amenazas

En Panda se optó por la prevención hace tiempo. Por eso desarrollamos herramientas de detección de nuevas posibles amenazas sin necesidad de un fichero de firmas. Así se acelera el proceso de creación de vacunas adecuadas a tales amenazas.

Hoy, millones de ordenadores en todo el mundo utilizan las tecnologías Tru-Prevent, que detectan y envían las nuevas amenazas a PandaLabs inmediatamente. Esto confiere una presencia global al laboratorio de Panda ante amenazas emergentes. Los remedios a nuevas amenazas se incluyen tan rápidamente que, en ocasiones, los ficheros de firmas se actualizan incluso antes de que la amenaza sea reconocida por el resto de laboratorios.

El incremento del número de detecciones a partir de técnicas preventivas es altamente significativo, como se observa en la siguiente tabla:

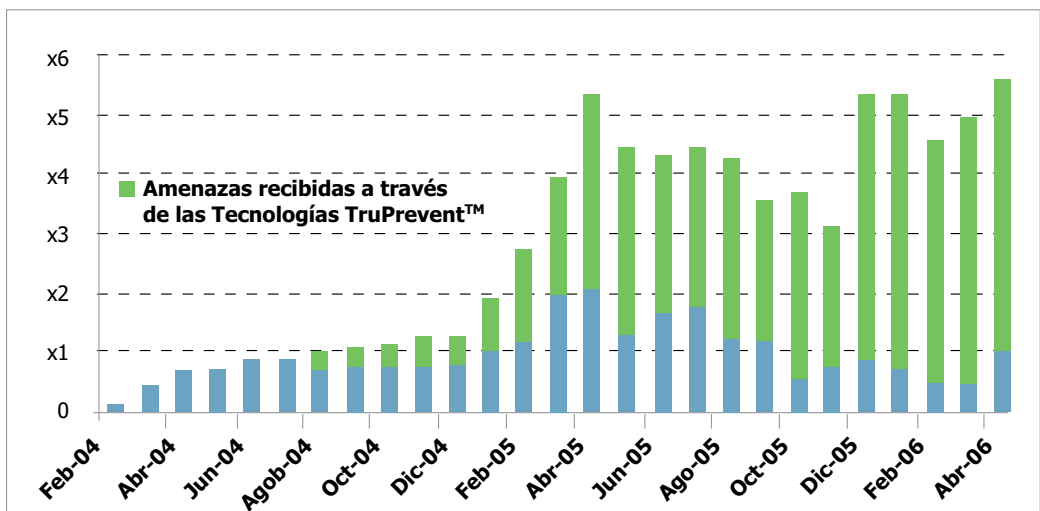


Fig. 4.-Comparación de amenazas detectadas por técnicas reactivas y preventivas - Fuente: Pandalabs

Gracias a la apuesta de PandaLabs por la prevención, la detección de malware anual se ha incrementado exponencialmente en los últimos tiempos.

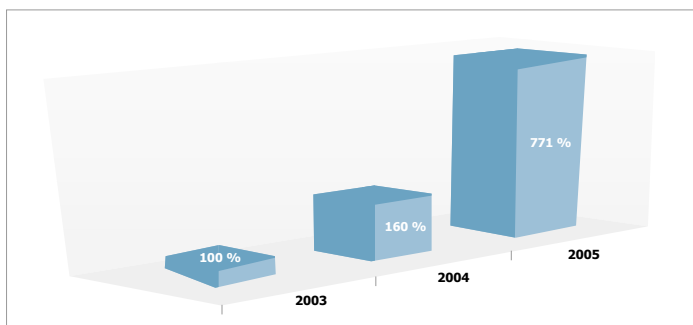


Fig. 5.- Evolución del nuevo malware detectado por años
Fuente: Pandalabs

Detectar un mayor número de amenazas, en cualquier punto del planeta y en el menor tiempo posible, es un factor diferenciador de Panda frente a sus competidores.



La reducción de la ventana de riesgo

La ventana de riesgo es el tiempo que transcurre desde que una amenaza aparece hasta que su vacuna se distribuye en los ficheros de firmas. Reducir la ventana de riesgo es el reto de toda compañía de seguridad. Las protecciones reactivas Panda también se benefician del alto nivel de prevención, ya que la solución a las nuevas amenazas se incluye en los ficheros de firmas lo antes posible.

En Panda, se detectan las amenazas de forma instantánea y es más probable conseguir un remedio en menor tiempo. Incluir nuevas técnicas de inteligencia artificial permite clasificar antes las nuevas amenazas y generar firmas en tiempo récord. Un proceso que tradicionalmente supone horas en otros laboratorios se reduce a segundos en PandaLabs.

Así, los ficheros de firmas se actualizan continuamente y las soluciones Panda reducen la ventana de riesgo. Por ejemplo, los appliances de protección perimetral actualizan las firmas cada 15 minutos. Además, disponen de un potente heurístico genético que detecta y bloquea posibles nuevas amenazas durante este periodo.

La situación de riesgo ¿percepción o realidad?

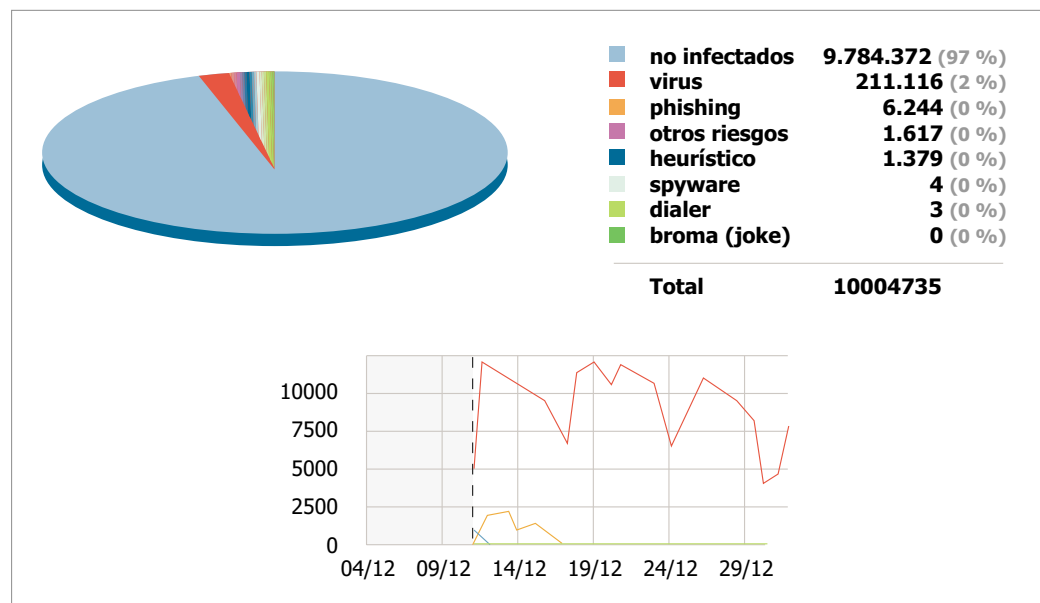
La percepción de protección de las compañías o la idea de que algunas redes no son objetivo de las amenazas es un error extendido en empresas de todo tamaño. Basta con instalar una protección perimetral temporalmente para ver que esa percepción no es cierta. Es la forma adecuada para salir de dudas y comprobar el riesgo al que la red está sometida. A continuación se muestran algunos ejemplos de informes extraídos de los appliances Panda GateDefender instalados a modo de prueba en diferentes empresas:

Ejemplo 1 - Compañía de 900 usuarios

Se instaló un dispositivo GateDefender Performa durante 1 mes con las protecciones Anti-malware y Anti-spam activas y el resultado del informe fue concluyente:

Malware detectado en un mes:

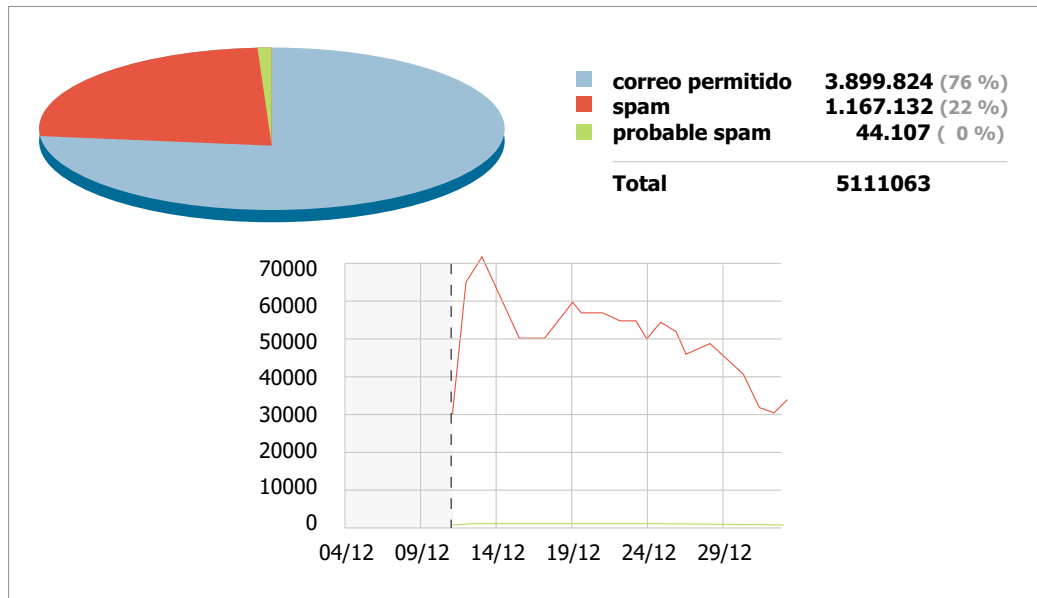
- Un 3% del tráfico soportado
- Esto es un total de 220.363 amenazas detectadas
- Lo que supone una media de más de 7000 ficheros peligrosos al día





Spam detectado en un mes:

- La cuarta parte del correo recibido es Spam o Probable spam
- Es un total de 1.211.239 mensajes que saturarían el tráfico de la red interna

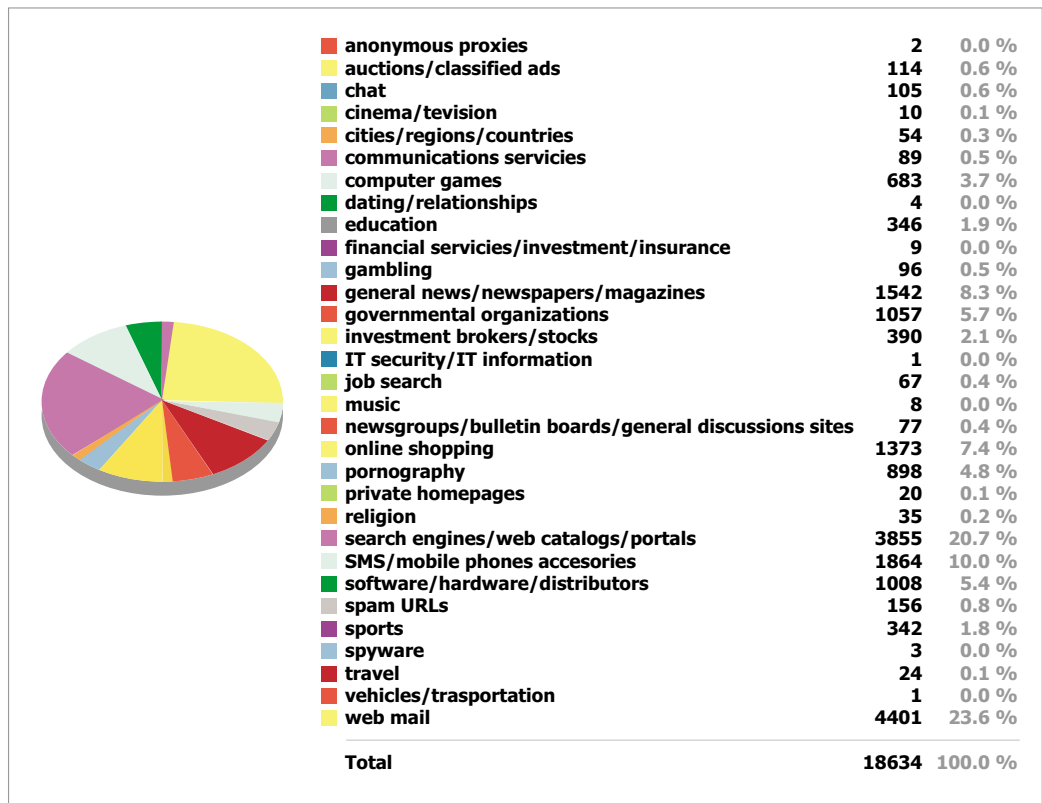


Ejemplo 2 - Compañía de 200 usuarios

Se instaló un dispositivo GateDefender Performa durante 4 días para analizar las visitas a páginas web improductivas y el resultado del informe fue el siguiente:

Acesos web no autorizados en 4 días:

- Detectados 18.634 accesos a páginas prohibidas
- Corresponde a una media de 4765 intentos diarios
- Destacan los accesos a servicios webMail y consultas de catálogos web



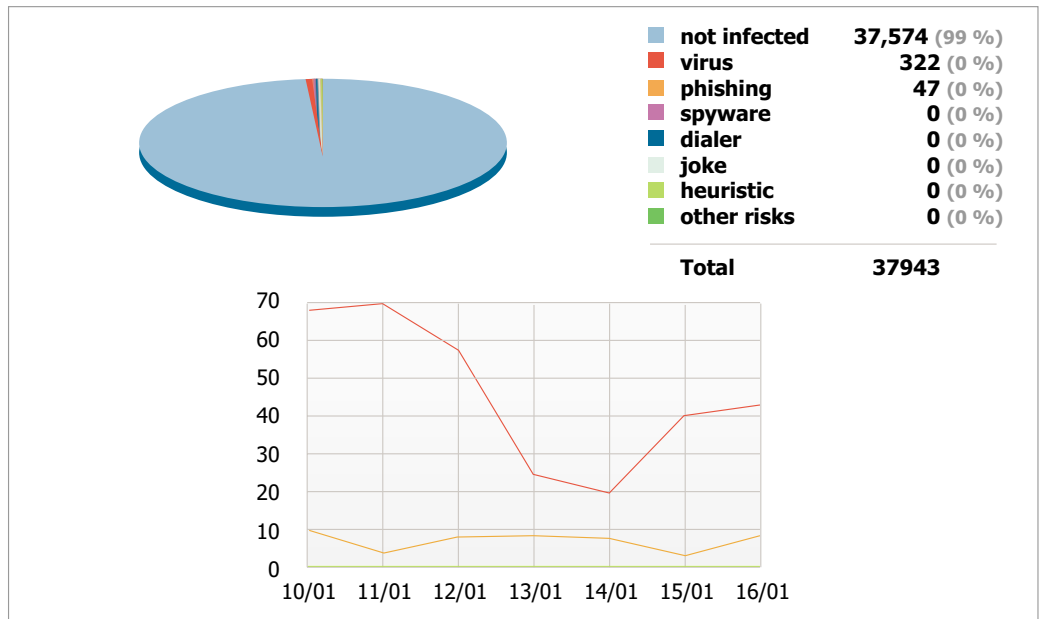


Ejemplo 3 - Compañía de 15 usuarios

Se instaló un dispositivo GateDefender Performa durante 1 semana con las protecciones Anti-malware y Anti-spam activadas y el resultado del informe fue el siguiente:

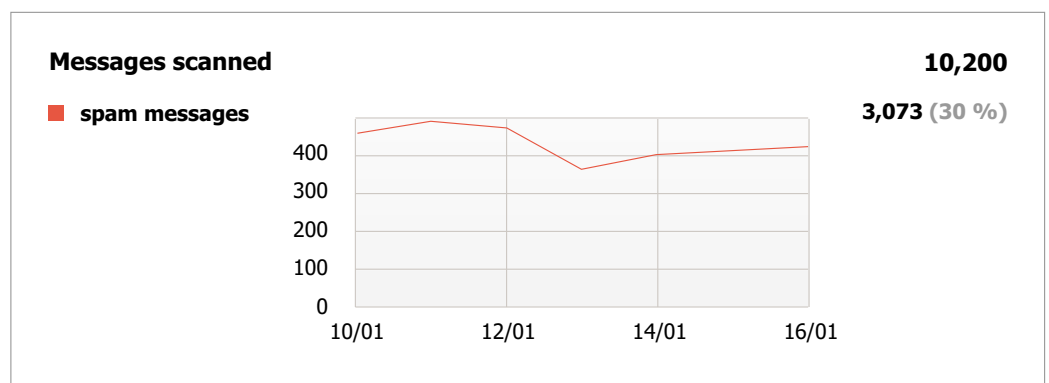
Malware detectado en 1 semana:

- 367 amenazas detectadas



Spam detectado en una semana:

- 3.073 mensajes clasificados como spam
- Suponen el 30% del tráfico de correo total

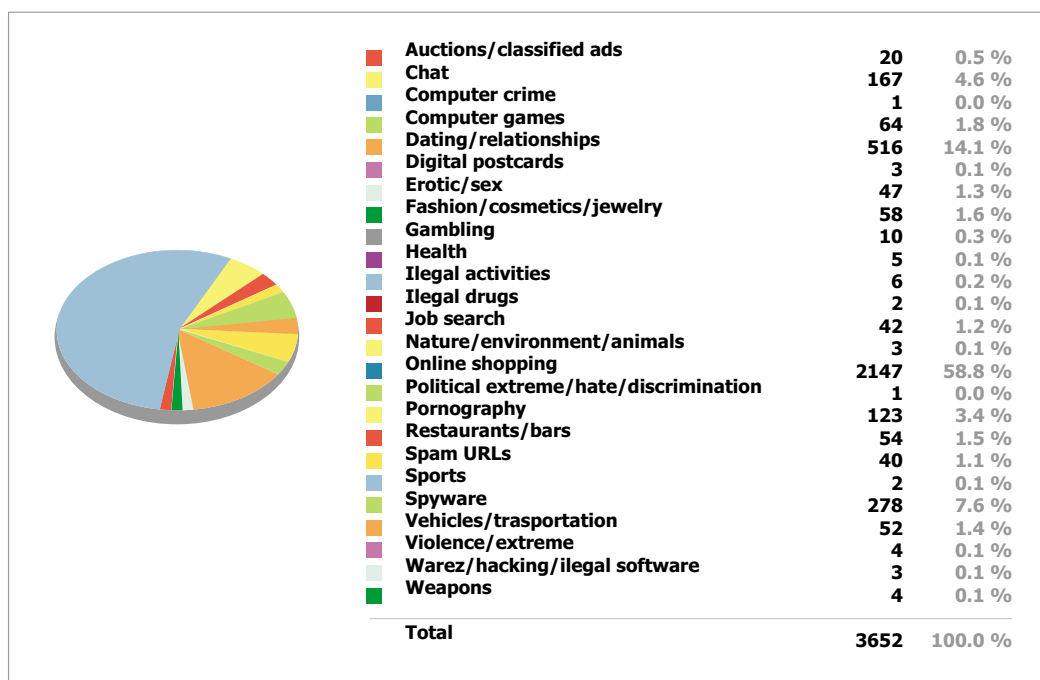


Ejemplo 4 - Compañía de 85 usuarios

Se instaló un dispositivo GateDefender Performa durante 3 semanas para analizar las visitas a páginas web improductivas. Aunque contaba con otra protección Anti-malware y Anti-spam, también se activaron estos módulos y el resultado del informe fue el siguiente:

Accesos web no autorizados en 3 semanas:

- 3652 accesos neutralizados
- Corresponde a una media de 174 intentos diarios
- Destacan los accesos a páginas de Ventas Online
- Además se detectaron 9566 mensajes de spam y 5 códigos maliciosos



Estos ejemplos corresponden a empresas reales de distintos tamaños y países, que quisieron comprobar el resultado de instalar una protección perimetral Panda en su red. Se comprobó que mejoró el nivel de su seguridad incluso cuando se instaló como complemento a otras protecciones de las que ya disponían.

Los informes gráficos se extraen directamente desde los dispositivos. Son suficientemente auto-explicativos como para comprender, a primera vista, la mejora en la seguridad global de la red al instalar una protección perimetral.



¿Por qué probar una solución perimetral?

■ Porque se miden los riesgos a los que se expone la red.

Los datos de detección durante la prueba no son estadísticos sino que se refieren a tráfico real de la red de la compañía.

■ Porque cada día crece el número de Nuevas amenazas.

La sensación de que hay menos ataques se debe a que las amenazas son cada vez más silenciosas, pero el malware aumenta cada día. Una protección perimetral actualiza las firmas contra amenazas cada 15 minutos, reduciendo la ventana de riesgo al máximo.

■ Porque las protecciones deben anticiparse a las amenazas.

Incluso en una pequeña ventana de riesgo de tan sólo 15 minutos, el motor heurístico detectará y bloqueará las amenazas y evitará que lleguen al interior de la red.

■ Porque todas las redes son atacadas.

Las redes de todos los tamaños son objetivo de todo tipo de amenazas. Las soluciones perimetrales de Panda se adaptan en prestaciones requeridas y precio a empresas de cualquier tamaño.

■ Porque el consumo innecesario de recursos es un problema creciente.

Evitar el tráfico de correo basura y de contenidos peligrosos mejora el funcionamiento de la red porque libera a servidores y estaciones de trabajo de una carga innecesaria.

■ Porque merece la pena comprobar los beneficios que aporta.

- Tranquilidad frente a nuevas amenazas
- Aumento de la productividad de los usuarios
- Maximización de la eficiencia de los dispositivos internos de la red
- Optimización de la inversión en sistemas de seguridad
- Bajo Coste Total de Propiedad
- Rápido Retorno de Inversión