PANDA**ADVANCED**PROTECTION**SERVICE**

CERRANDO LAS GRIETAS EN LA DETECCIÓN DEL MALWARE

¿CREES QUE TU ORGANIZACIÓN ESTÁ PROTEGIDA CONTRA ATAQUES DIRIGIDOS O ZERO-DAY?

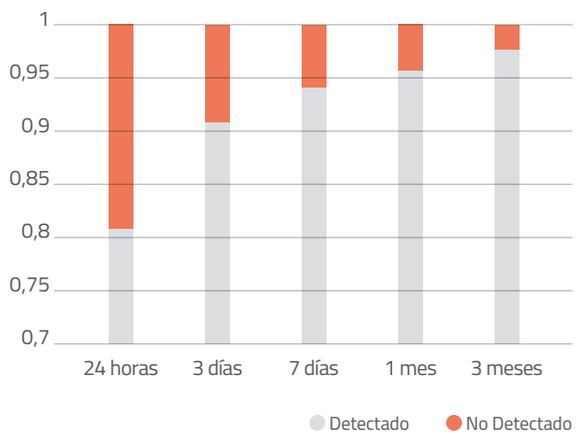
Más de 200 mil nuevas muestras de virus son descubiertas a diario. De entre todas ellas ha emergido **un nuevo tipo de ataque muy sofisticado,** dirigido específicamente contra empresas y capaz de funcionar por debajo del radar de antivirus y cortafuegos tradicionales.

Este "malware de nueva generación" **denominado APTs (Advanced Persistent Theats)** utiliza múltiples vectores de infección de forma simultánea en periodos muy dilatados en el tiempo, permaneciendo escondido durante meses gracias a sus capacidades polimórficas. Una vez infectada la red del cliente, el espionaje industrial y el robo de datos se convierten en sus objetivos prioriarios.

Panda Advanced Protection Service es un nuevo modelo de seguridad basado en la supervisión, control y clasificación del comportamiento y la naturaleza de cada una de las aplicaciones ejecutadas para **ofreciendo una garantía de protección robusta y completa, permitiendo únicamente la ejecución de aplicaciones lícitas (goodware).**

La posibilidad de incorporarse a la infraestructura existente del cliente coexistiendo con antivirus tradicionales e integrándose en la solución **SIEM** utilizada por la empresa, sumado a su capacidad de desinfección de virus hacen de Panda Advanced Protection Service la herramienta corporativa completa y definitiva contra todo tipo de malware, incluyendo ataques dirigidos y de zero-day.

VENTANA DE OPORTUNIDAD DEL MALWARE



Fuente: Panda Research. Enero-Junio 2014, con más de 10 millones de muestras.

Los antivirus tradicionales no llegan a detectar el 18% del nuevo malware en sus 24 primeras horas de aparición y al cabo de 3 meses todavía un 2% del malware continúa sin ser descubierto

VISIBILIDAD
Visualiza en tiempo real cada acción realizada por las aplicaciones en ejecución.

DETECCIÓN
Clasifica cada fichero y proceso de la red mediante **técnicas Machine Learning en entornos Big Data.**

RESPUESTA
Desinfección con herramientas especializadas en malware de nueva generación y análisis forense para investigar en profundidad cada intento de ataque.

PREVENCIÓN
Bloquea aplicaciones y aísla los sistemas para prevenir futuros ataques.

PANDA**ADVANCED**PROTECTION**SERVICE**

CERRANDO LAS GRIETAS EN LA DETECCIÓN DEL MALWARE

PANDA**ADVANCED**PROTECTION**SERVICE**

LA ÚNICA SOLUCIÓN QUE GARANTIZA LA SEGURIDAD DE TODAS LAS APLICACIONES EJECUTADAS.

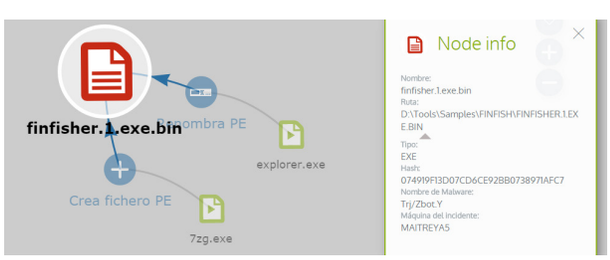
GARANTÍA DE PROTECCIÓN ROBUSTA Y COMPLETA

El **Modo Bloqueo Básico** solo permite la ejecución de las aplicaciones catalogadas como goodware y de las aplicaciones todavía no catalogadas por los sistemas automatizados y los expertos de Panda Security.
El **Modo Bloqueo Extendido** únicamente permite la ejecución de aplicaciones catalogadas como goodware. El bloqueo extendido es la solución perfecta para empresas que tengan objetivos de seguridad de tipo **"riesgo cero".**

INFORMACIÓN FORENSE

Visualiza mediante **Grafos de ejecución** los eventos desencadenados por el malware.Obtén información visual del destino de las comunicaciones del malware, los ficheros creados y mucho más con los **Mapas de Calor.** Localiza el software con vulnerabilidades conocidas instalado en la red.

Mapas de calor con el destino de las comunicaciones.



Grafo de ejecución con acciones desencadenadas por malware.

DESINFECCIÓN DE MALWARE

Elimina el malware escondido en la red que las soluciones tradicionales de seguridad utilizadas no han sido capaces de detectar.

PROTECCIÓN DE SISTEMAS VULNERABLES

Debido a la ausencia de actualizaciones, los sistemas no soportados por el proveedor original (como Windows XP) se convierten en blanco automático de ataques zero-day y de nueva generación que aprovechan las vulnerabilidades del sistema. Protégelos con nuestra solución de seguridad.

INFORMACIÓN CONTINUADA DEL ESTADO DE LA RED

Recibe alertas inmediatas en el momento en que se identifique malware en la red, con un informe completo detallando su localización, máquinas infectadas y acciones realizadas por el malware. Obtén informes por e-mail con la actividad diaria del servicio.

SERVICIO 100% GESTIONADO

Olvídate de invertir recursos en personal técnico para gestionar cuarentenas, ficheros sospechosos o desinfecciones y reinstalaciones de los equipos infectados. Panda Advanced Protection Service clasifica todas las aplicaciones de forma automática mediante **técnicas de Machine Learning en nuestros entornos Big Data** bajo la continua supervisión de los técnicos especializados de **PandaLabs,** que controlan en todo momento el proceso.

MÓDULO SIEM DISPONIBLE

Panda Advanced Protection Service se integra con productos **SIEM** (QRadar, ArcSight…) agregando información detallada sobre la actividad de todas las aplicaciones ejecutadas en los puestos.

Para aquellos clientes que no dispongan de un SIEM, **Panda Advanced Protection Service** incorpora su propio sistema de almacenamiento y gestión de eventos de seguridad. De esta forma es posible representar de forma gráfica **patrones de comportamiento y tendencias** encontradas en la red del cliente, fruto del análisis en tiempo real de toda la información recogida.

CERTIFICACIONES PANDA SECURITY

REQUERIMIENTOS TÉCNICOS

CONSOLA WEB (solo monitorización)
- Conexión a Internet
- Internet Explorer 7.0 o superior
- Firefox 3.0 o superior
- Google Chrome 2.0 o superior

AGENTE
- Sistemas operativos (estaciones): Windows XP SP2 o superior (Vista, Windows 7, 8 y 8.1).
- Sistemas operativos (servidores):Windows Server 2003, Windows Server 2008, Windows Server 2012.
- Conexión a Internet (directa o mediante proxy)