



INTELIGENCIA COLECTIVA: LA EVOLUCIÓN DEL MODELO DE SEGURIDAD TRADICIONAL

Technology Paper de **Panda Research**
research.pandasecurity.com

Índice

1 Resumen	3
2 El panorama del malware	4
2.1 Los laboratorios antivirus, objeto de ataque	4
2.2 Técnicas y diseño de malware	5
2.2.1 Ataques dirigidos: Por debajo del radar	5
2.2.2 Control de calidad del malware	5
2.2.3 Rootkits y técnicas de detección por "Sandbox"	6
2.2.4 Empaquetadores en tiempo de ejecución	7
2.2.5 Botnets	8
2.2.6 Vectores de infección por fases	8
2.2.7 "Malware 2.0"	8
3 Evolución de la tecnología de Panda	10
3.1 Primera generación: los programas antivirus	10
3.2 La segunda generación: las tecnologías anti-malware	10
3.3 La tercera generación: las tecnologías proactivas	11
3.3.1 Técnicas de desenmascaramiento	11
3.3.2 Análisis de comportamiento TruPrevent	12
3.3.3 Bloqueo por comportamiento TruPrevent	14
3.3.4 Tecnología heurística de análisis genético	14
3.4 La Inteligencia Colectiva	16
3.4.1 Aprovechamiento del conocimiento colectivo	16
3.4.2 Proceso automático de protección frente al malware	17
3.4.2.1 Recopilación automática de malware	17
3.4.2.2 Clasificación automática del malware	18
3.4.2.3 Remediación automática del malware	18
3.4.3 Obtención de conocimiento sobre las técnicas de malware	19
3.4.4 Distribución de Servicios de Seguridad "desde la nube"	19
3.4.5 Un comentario sobre las listas blancas	19
4 Conclusión	21
5 Referencias	22

1. Resumen

Existen más amenazas de malware en circulación que nunca y las empresas antivirus que se basan en la detección por firmas no dan abasto para crear firmas que protejan a los usuarios con la suficiente rapidez.

Como hemos sido capaces de demostrar en un estudio reciente¹, incluso los usuarios protegidos con soluciones de seguridad y anti-malware con el último archivo de firmas se pueden ver infectados por malware activo. Se hace necesario desarrollar e implementar enfoques y tecnologías complementarias para aumentar la eficacia de estas soluciones hasta niveles aceptables.

El presente documento presenta la cuarta generación de tecnologías de seguridad desarrollada por Panda Security, bautizadas con el nombre de Inteligencia Colectiva. La Inteligencia Colectiva nos permite maximizar nuestra capacidad de detección reduciendo al mínimo el consumo de recursos y ancho de banda de los sistemas protegidos.

El concepto de Inteligencia Colectiva supone un modelo de seguridad completamente diferente de los modelos actuales. Se trata de un modelo basado en una base de conocimiento exhaustiva, remota, centralizada y accesible en tiempo real sobre malware y aplicaciones no-maliciosas mantenida a través del procesamiento automático de todos los elementos analizados.

Una de las ventajas de este modelo es la automatización de todo el ciclo de protección y detección de malware (recogida, análisis, clasificación y solución). Sin embargo, la automatización en y por sí misma no es suficiente para responder al juego del gato y el ratón que plantea el malware. Las grandes cantidades de malware vienen acompañadas de ataques dirigidos y el tiempo de respuesta en este tipo de escenario no puede depender sólo de la automatización del proceso de generación del archivo de firmas.

La otra gran ventaja de la Inteligencia Colectiva es que proporciona mayor visibilidad y conocimiento de los procesos que se ejecutan en los ordenadores que analiza. Esta visibilidad de la comunidad, junto con la automatización, es lo que nos permite responder no sólo a los grandes volúmenes de nuevo malware sino también a los ataques dirigidos.

Escrito y revisado por:
Pedro Bustamante, Senior Research Advisor
Iñaki Urzay, Chief Technology Officer
Luis Corrons, Director Técnico de PandaLabs
Josu Franco, Director de Desarrollo Corporativo

2. El panorama del malware

Es un hecho sabido por todos los profesionales de la seguridad que hoy en día existen más ejemplares de malware infectando ordenadores que nunca.

Los creadores de malware se han dado cuenta de que pueden ganar mucho dinero con la distribución de códigos maliciosos. El cambio en cuanto a 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.

Esta nueva dinámica del malware, que supone un tipo de ataque dirigido, se ha convertido en la próxima gran plaga tanto para los usuarios como para las empresas. Gartner 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 las defensas de host y perimetrales tradicionales².

2.1 Los laboratorios antivirus, objeto de ataque

Hoy en día los laboratorios antivirus están sometidos a ataques constantes y cada vez más frecuentes de denegación de servicio distribuida. El sector de la seguridad se encuentra literalmente saturado por la aparición de miles de nuevos ejemplares de malware todos los días. Cada uno de estos ejemplares tiene que ser examinado por un analista experto en ingeniería inversa para crear una firma, lo cual resulta caro y re-

quiere muchos recursos desde un punto de vista corporativo y empresarial.

Algunas empresas tratan de solucionar el problema aumentando el número de analistas en los laboratorios³ o abogando por una aplicación más contundente⁴ de la ley⁵, que perseguiría a los creadores de malware más activos y reduciría la carga de trabajo.

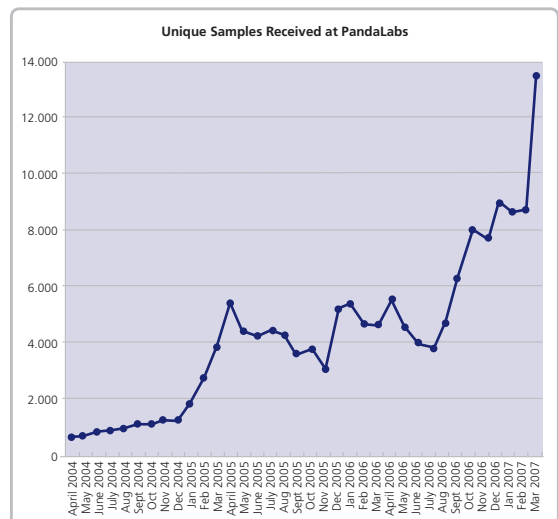


Figura 1: Ejemplares únicos recibidos en PandaLabs de 2004 a 2007

Las iniciativas para conseguir que las autoridades se involucren más en esta lucha son algo positivo. Sin embargo y desgraciadamente, estas soluciones no resultan demasiado realistas, debido a que el número de variantes no deja de aumentar y en la mayor parte de los casos sólo se consigue detener a las "mulas" y "script kiddies".

Los autores de malware más experimentados, que son los que más se benefician de la venta de sus códigos a los spammers, las mafias y los delincuentes, se están hacien-

do cada vez más escurridizos y difíciles de atrapar. Además, la falta de recursos en la mayoría de agencias de seguridad de todo el mundo, unida a la falta de la necesaria cooperación y coordinación entre ellos, hacen que sea misión imposible arrestar, y mucho más condenar, a un sospechoso o conocido delincuente informático.

Además, los autores de malware se están haciendo cada vez más sofisticados y descompilar algunas de las últimas amenazas más comunes requiere de mucho más tiempo y conocimientos que antes. En consecuencia, ya no es posible contratar "en masa" a ingenieros antivirus para que creen cientos de miles de firmas cada pocos meses.

2.2 Técnicas y diseño de malware

La principal diferencia entre los virus del pasado y el malware actual es que su ciclo de vida se ha reducido considerablemente y los objetivos han cambiado: robo de identidad, uso de ordenadores como bots para lanzar spam, robo de credenciales de servicios bancarios online, datos de tarjetas de crédito, contraseñas de acceso a sitios web, etc.

Y lo más importante, hoy en día el malware está diseñado para no generar ningún tipo de alarma. A diferencia del pasado, cuando los virus y los gusanos se diseñaban para propagarse por el mayor número posible de ordenadores sin la intervención del usuario, armando mucho revuelo y llamando la atención de los medios, el malware delictivo actual trata de pasar lo más desapercibido posible.

Con el fin de alcanzar su objetivo, el malware actual utiliza técnicas avanzadas para eludir la detección y "volar bajo".

2.2.1 Ataques Dirigidos: por debajo del radar

Una de las principales estrategias empleadas por los Ataques Dirigidos para permanecer fuera del radar es distribuir pocas copias de muchas variantes⁶. En el pasado, un solo virus o gusano era el responsable de infectar a cientos de miles o incluso millones de ordenadores. La visibilidad de estas situaciones era muy obvia para los laboratorios antivirus.

Sin embargo, hoy en día, el malware sólo infecta a unos pocos cientos de ordenadores antes de actualizarse con una nueva variante indetectable y así eludir a las firmas antivirus ordinarias. La cuestión de fondo es ¿cómo puede un laboratorio antivirus darse cuenta de que existe una infección si solo afecta a unos pocos usuarios?

2.2.2 Control de calidad del malware

Otra técnica cada vez más utilizada por el malware actual es la realización de pruebas de control de calidad. Estas pruebas consisten en analizar cada variante con las firmas antivirus más habituales para asegurarse de que pasan inadvertidas para la mayoría de ellas. Esta tarea se ha simplificado enormemente gracias a servicios de análisis online como Jotti, VirusTotal e incluso los propios servicios de análisis online de las empresas antivirus⁷.

Los creadores de malware cuentan también con herramientas personalizadas para automatizar el análisis del nuevo malware mediante firmas, análisis heurístico e incluso tecnologías de análisis de comportamiento. Con estas herramientas, los autores de malware pueden comprobar la calidad de

sus creaciones offline, sin arriesgarse a que el ejemplar llegue a los laboratorios antivirus a través de los servicios de análisis online mencionados anteriormente.

El objetivo de las pruebas de control de calidad del malware no es tanto evitar la detección por parte de todos los escáners y técnicas proactivas (firmas genéricas, heurística, análisis de comportamiento, bloqueo por comportamiento, etc.) sino conseguir eludir a la mayoría de ellas. Dado que su objetivo es permanecer "fuera del radar", no merece la pena crear el ejemplar de malware más difícil de detectar si sólo va a durar unas horas o unos días.

2.2.3 Rootkits y técnicas de detección de "sandbox"

Otro de los procedimientos para eludir la detección cada vez más utilizado⁸ es el uso de técnicas de rootkit incluidas en troyanos y spyware. Una vez empleados por el malware, los rootkits crean una barrera más para evitar ser detectados, sobre todo porque todavía no se han implantado las últimas tecnologías de detección de rootkits en todas las soluciones de seguridad fabricadas en serie.

Esto significa también que los laboratorios antivirus tienen que pasar más tiempo analizando drivers en modo kernel que ejemplares en modo usuario. Por ejemplo, LinkOptimizer, que ha estado activo en los últimos meses, es capaz de determinar si la máquina a la que va a infectar tiene instaladas herramientas de seguridad, depuración o monitorización del sistema.

También comprueba si se está ejecutando en un entorno de Máquina Virtual. Si el resultado de estas comprobaciones es posi-

vo, termina de forma silenciosa y no lleva a cabo ninguna acción. Los laboratorios que dependen de VM tendrán que llevar a cabo un largo proceso para poder instalar algunos ejemplares de LinkOptimizer y poder analizarlos en profundidad.

En el momento de escribir este paper pocas suites de seguridad y anti-malware cuentan con tipos básicos de detección de rootkits, como vistas cruzadas (cross-view) de accesos a bajo nivel frente a llamadas a nivel de API. La mayoría no han incorporado todavía las técnicas de detección y desactivación más avanzadas que se pueden encontrar en utilidades anti-rootkit autónomas y gratuitas⁹.

En términos generales, podría decirse que el uso de rootkits por parte de los creadores de malware sigue creciendo continuamente. El uso de rootkits se ha convertido en un problema para los laboratorios antivirus que enfocan la ingeniería inversa de malware de modo tradicional y necesitan analizar los ejemplares uno a uno.

Sin embargo, no son solo los laboratorios antivirus los que tienen problemas con los rootkits, sino que también las empresas están empezando a experimentar sus efectos negativos en sus negocios, especialmente cuando se utilizan para espionaje corporativo¹⁰.

Con el objeto de obtener una visión más clara del problema en las máquinas reales de los usuarios, hemos recopilado todas las detecciones de rootkits conocidos y desconocidos que realizó nuestra utilidad gratuita Panda Anti-Rootkit¹¹ entre los meses de diciembre de 2006 y junio de 2007.

A continuación, hemos correlacionado la distribución de los rootkits con el malware in-the-wild. En la figura 2, se muestra el resulta-

Top Rootkit	User-mode	Kernel-mode	Prevalence
1 Beagle.Fu		x	6.20%
2 NaviPromo	x		5.73%
3 Rustock.A		x	1.20%
4 Flush.K	x		1.01%
5 Oddysee.B		x	0.20%

Figura 2: Principales rootkits in-the-wild detectados por Panda Anti-Rootkit entre diciembre de 2006 y junio de 2007

do del "Top 5 rootkits". Como se puede apreciar, se ha producido un gran aumento en el uso de rootkits en modo kernel.

2.2.4 Empaquetadores en tiempo de ejecución

Tal vez el procedimiento más frecuente para tratar de eludir la detección por parte de los productos anti-malware sea el uso de empaquetadores en tiempo de ejecución que empleen técnicas de antidepuración y antivirtualización.

Este tipo de herramientas pueden modificar y comprimir un archivo ejecutable encriptando y modificando su forma respecto a su formato original. El resultado final es un ejecutable modificado que, cuando se ejecuta, hace lo mismo que el código original, mostrando por fuera una forma completamente distinta.

Estos códigos pueden eludir la detección por firmas salvo que el motor antivirus posea el algoritmo de desempaquetado o sea capaz de desempaquetarlo de forma genérica.

Este planteamiento atrajo a muchos autores de malware. Hoy en día estamos viendo creadores que emplean versiones modificadas de empaquetadores conocidos, o bien crean rutinas de empaquetado en tiempo de ejecución específicas para su malware¹².

Con objeto de enfrentarse a este problema, los ingenieros de Panda han creado detectores genéricos de empaquetadores y rutinas genéricas de desempaquetado que puedan detectar empaquetadores desconocidos e intentar desempaquetarlos.

Sin embargo, una solución más eficaz sería al menos marcar como sospechosos todos los empaquetadores en tiempo de ejecución nuevos. Algunas soluciones perimetrales estándar hacen ya esto por defecto. Incluso algunas soluciones de seguridad basadas en host utilizan este procedimiento marcando estos ejemplares como maliciosos, como así lo indican claramente los diferentes nombres de detección utilizados por los distintos motores anti-malware¹³

Sin embargo, este tipo de enfoque para la detección proactiva de empaquetadores supone un coste. En las conversaciones mantenidas con otros proveedores de soluciones anti-malware durante el International Antivirus Testing Workshop celebrado en 2007 en Islandia, quedó claro que, en el caso de los entornos corporativos, éste resultaba un enfoque acertado. Sin embargo, los proveedores con una alta base instalada en el mercado de consumo podrían encontrarse con una cantidad tan grande de falsos positivos que podrían hacer que la solución fuera peor que el problema.

2.2.5 Botnets

Según algunos estudios, aproximadamente el 11% de los ordenadores de todo el mundo están infectados por bots, responsables del 80% del spam que se envía¹⁴. Una buena parte del dinero que consiguen los delincuentes informáticos procede de los botnets.

El control de estas grandes redes de ordenadores infectados se vende o alquila para llevar a cabo delitos informáticos: envío de spam, ataques de denegación de servicio distribuida, venta de proxies, etc. PandaLabs ha sido testigo de guerras online entre diferentes bandas de bots para hacerse con los PCs secuestrados.

Hay pruebas que sugieren que existen muchos PCs de empresas pertenecientes al índice Fortune 500 que son controlados de forma remota por bot herders para el envío de spam¹⁵.

Aunque los botnets tradicionales son controlados vía IRC, hay botnets nuevos basados en P2P y HTTP que utilizan técnicas de encriptación de comunicaciones más potentes y se están haciendo populares entre los delincuentes informáticos para evadir la detección.

2.2.6 Vectores de infección por fases

No es nuevo que la mayoría del malware actual tiende a utilizar ataques en dos fases como principal técnica de infección, ya sea explotando vulnerabilidades conocidas o del tipo día cero, o utilizando pequeños "downloaders" que cambian muy rápidamente para evitar la detección.

Mientras en el pasado aprovecharse de una vulnerabilidad como principal vector de infección podía llevar semanas o incluso meses a los autores del malware, hoy en día es normal ver exploits in-the-wild que se aprovechan de vulnerabilidades dos días después de que se hagan públicas. Aplicaciones maliciosas automatizadas, como Web-Attacker¹⁶ y MPack¹⁷ están explotando, por ejemplo, vulnerabilidades GDI, de cursores animados y VML para aprovecharse de usuarios desprevenidos o sin parches e infectarles con un troyano.

Los downloaders se están convirtiendo también en herramientas habituales en las técnicas de infección en dos fases. En primer lugar, se ejecuta un pequeño fichero mediante una descarga conducida del navegador o un exploit similar. El objetivo de este archivo es el siguiente: descargar un segundo archivo desde una URL y ejecutarlo. Este segundo archivo es el verdadero troyano que termina infectando al sistema.

Estos downloaders han evolucionado mucho. SecuriTeam organizó recientemente un concurso para crear el downloader más pequeño del mundo¹⁸. Más recientemente, hemos visto surgir miles de herramientas gráficas que simplifican el trabajo de creación de downloaders¹⁹, incluso con técnicas de empaquetamiento personalizadas para eludir la detección.

2.2.7 "Malware 2.0"

Una de las tendencias actuales en la creación de malware es que el binario que infecta al PC del usuario sea "tonto" y la inteligencia esté "en la nube". El código que reside en el PC posee funciones simples que transfiere a un servidor compinchado remotamente. El servidor, entonces,

devuelve instrucciones sobre lo que es preciso hacer. Tomando prestado el término (tal vez usado en exceso) "2.0" que define la tendencia actual de Internet, nos referimos al "*Malware 2.0*" como *el tipo de malware que separa su código de su capacidad*.

PandaLabs ha detectado el método "2.0" en troyanos utilizados en ataques bancarios dirigidos. Estos troyanos controlan de forma remota los hábitos de navegación de los usuarios y, en función de la página web bancaria y su esquema de autenticación, inyecta tipos de código HTML distintos. Troyanos bancarios famosos, como Limbo (alias NetHell) o Sinowal (alias Torpig), utilizan mucho estas técnicas²⁰.

Otras técnicas "2.0" empleadas recientemente por el malware son la "compilación en el lado del servidor", en la que el servidor web re-compila un nuevo binario cada pocas horas. Por último, los botnets están empleando redes DNS fast-flux para mejorar su resistencia a la desinfección. Estas últimas técnicas aparecen en casos como los de los recientes ataques protagonizados por Storm/Nuwar.

3. Evolución de la tecnología de Panda

Desde hace ya un tiempo los planteamientos tradicionales basados en firmas no han resultado eficaces a la hora de enfrentarse a esta situación creada por el malware. Resulta absolutamente imprescindible para una solución de seguridad medianamente aceptable contar con un completo Sistema de Prevención de Intrusiones basado en Host (HIPS) con heurística avanzada, firewall de inspección profunda de paquetes, bloqueo por comportamiento, análisis de comportamiento y securización de sistemas y aplicaciones. Sin embargo, la triste realidad es que prácticamente la mitad de las soluciones disponibles en el mercado no disponen aún de estas tecnologías.²¹

En Panda, nos encargamos de la investigación y desarrollo del 100% de nuestras principales tecnologías anti-malware. Esta dedicación a la innovación es la que nos ha permitido estar a la cabeza en cuanto a tecnologías de seguridad proactivas en el mercado.

Siguiendo una filosofía de defensa en profundidad, que podría resumirse como la integración de diferentes capas de protección en distintas capas de la infraestructura, Panda Research, un equipo dedicado al desarrollo de nuevas tecnologías de seguridad, ha desarrollado un nuevo enfoque de la seguridad basado en el concepto de **Inteligencia Colectiva**.

Este concepto responde al deseo de complementar el sistema integrado de protección de escritorio, servidor y pasarela de Panda a fin de enfrentarse a la dinámica

actual del malware y proporcionar el complemento definitivo al modelo ideal de protección de Panda.

Antes de pasar a explicar en profundidad la Inteligencia Colectiva, vamos a hacer un pequeño recorrido por las distintas tecnologías sobre las que se ha construido.

3.1 Primera generación: los programas antivirus

La primera generación de productos antivirus se basaba exclusivamente en la detección por firmas. Esta generación comprendió la mayor parte de los años noventa e incluía motores polimórficos, así como sistemas de análisis heurísticos basados en reglas sencillas para MS-DOS, Win32, Macro y, más tarde, de scripts. Este periodo también se vio marcado por la aparición de los primeros troyanos win32 utilizados de forma masiva, como NetBus y BackOrifice.

3.2 La segunda generación: las tecnologías anti-malware

A partir del año 2000 comenzaron a surgir nuevos tipos de malware, con los gusanos de paquete de red y el spyware como principales protagonistas, debido a las epidemias masivas y notorias que provocaban.

Se produjo una evolución en los motores antivirus básicos, que pasaron a integrar firewalls personales, capaces de detectar y blo-

quear gusanos de red basándose en firmas de paquetes, y limpiadores de sistema que restauraban modificaciones en la configuración del Sistema Operativo, como entradas de registro, archivos de HOST, Browser Helper Objects, etc. Fue en esta etapa cuando Panda Security incluyó en el motor antimalware la funcionalidad SmartClean, concebida para desinfectar y restaurar el Sistema Operativo tras una infección provocada por spyware o troyanos de puerta trasera.

3.3 La tercera generación: las tecnologías proactivas

Panda lanzó al mercado las tecnologías de análisis de comportamiento TruPrevent en 2004 tras más de tres años de intensos trabajos de investigación y desarrollo

Desde entonces, TruPrevent ha evolucionado hasta convertirse en un conjunto de tecnologías de análisis de comportamiento sustancialmente más eficaces para bloquear de forma proactiva el malware del tipo día cero sin depender de firmas de virus que ningún otro esfuerzo realizado hasta el momento en esa dirección. TruPrevent se adapta continuamente a las nuevas técnicas de malware.

TruPrevent se diseñó como una capa de protección adicional al motor antimalware. En la actualidad, más de 5 millones de ordenadores cuentan con esta tecnología. Estos ordenadores funcionan también como honeypots de alta interacción que se encargan de informar a PandaLabs de cualquier nuevo ejemplar de malware que TruPrevent designa como sospechoso y que no detecta las firmas antivirus ordinarias.

El método de TruPrevent consiste en analizar todos los elementos o amenazas poten-

ciales mediante distintas técnicas, llevando a cabo inspecciones complementarias en profundidad en las diferentes capas de la infraestructura. La implementación de TruPrevent responde a un planteamiento modular que puede, por tanto, aplicarse tanto a escritorios como a servidores (HIPS) para convertirse en un sistema HIPS (Sistema de prevención de intrusos en host) totalmente integrado.

Como prueba de efectividad, aproximadamente dos terceras partes de las muestras de malware que recibe PandaLabs de nuestros usuarios proceden actualmente de los envíos automáticos procedentes de TruPrevent.

Técnicamente, TruPrevent consta de dos tecnologías principales: **el análisis de comportamiento** y el **bloqueo por comportamiento**, también conocido como securización de sistemas y aplicaciones. Antes de entrar de lleno en cada una de ellas, vamos a analizar la capa de desenmascaramiento que hace que el malware pueda ser detectado por estas tecnologías de análisis de comportamiento.

3.3.1 Técnicas de desenmascaramiento

A medida que ha evolucionado el malware, también lo han hecho las técnicas que sirven para eludir la detección y ocultarse de miradas indiscretas.

Para combatir estas técnicas existe una capa base de tecnologías de desenmascaramiento común a todos los productos de Panda. Las técnicas que se presentan a continuación son capaces de inspeccionar cualquier elemento con la profundidad necesaria, incluso aunque dicho elemento uti-

lice técnicas de ocultamiento, y transferir los resultados a las tecnologías de análisis y de monitorización:

- *Inspección profunda de código*
- *Desempaquetamiento genérico*
- *Acceso nativo a ficheros*
- *Heurística de rootkits*

3.3.2 Análisis de comportamiento TruPrevent

Denominado en código Proteus, actúa como verdadera última línea de defensa contra los nuevos ejemplares de malware que estén ejecutándose en una máquina y que hayan sido capaces de superar la protección por firmas, los análisis heurísticos y el bloqueo por comportamiento. Proteus intercepta, durante el tiempo de ejecución, las operaciones y las llamadas a los APIs efectuadas por cada programa y las correlaciona antes de permitir que el proceso se ejecute de forma completa. Esta correlación en tiempo real permite o deniega la ejecución de un proceso basándose en su comportamiento.

Nada más ejecutarse el proceso, Proteus monitoriza de forma silenciosa todas sus operaciones y llamadas a los APIs, reuniendo información sobre el comportamiento del proceso. Proteus analiza el comportamiento de forma exhaustiva y está diseñado para bloquear malware tan pronto como comienza a realizar acciones maliciosas.

Si se determina que un proceso es sospechoso, se bloquea y elimina antes de que pueda actuar, y se evita que pueda volver a ejecutarse.

A diferencia de otras tecnologías de análisis de comportamiento, Proteus es autónomo

y no plantea cuestiones técnicas al usuario final ("¿Desea permitir que el proceso xyz inyecte un hilo en explorer.exe o en la dirección de memoria abc?"). Si Proteus considera que un programa es malicioso, lo bloqueará sin requerir la intervención del usuario.

La mayoría de los usuarios no pueden tomar decisiones fundamentadas en lo que respecta a la seguridad. Algunas soluciones de análisis de comportamiento lanzan opiniones no deterministas, o indecisiones de comportamiento, cuya eficacia depende de que el usuario seleccione la opción correcta. Una de las funcionalidades clave de cualquier tecnología de análisis de comportamiento es que sea capaz de tomar decisiones sin la intervención del usuario. Lo contrario constituirá una fuente potencial de fallo.

Nuestras estadísticas internas demuestran que esta tecnología por sí sola es capaz de detectar más del 80 por ciento del malware "in the wild", sin firmas y sin generar falsos positivos.

Esta tecnología no requiere de actualizaciones de firma, ya que se basa exclusivamente en el comportamiento de las aplicaciones. Un bot no sería un bot si no se comportara como tal, pero si lo hace, esta tecnología lo detectará, independientemente de su forma o de su nombre.

Se han llevado a cabo varios exámenes de TruPrevent por parte de terceros. Sin embargo, la realización de exámenes de tecnologías de análisis de comportamiento, como TruPrevent, utilizando ejemplares reales de malware lleva mucho tiempo y exige tener mucha experiencia en este campo. Indudablemente, resulta mucho más complejo que realizar exámenes de programas antivirus comparándolos con una colección de virus.

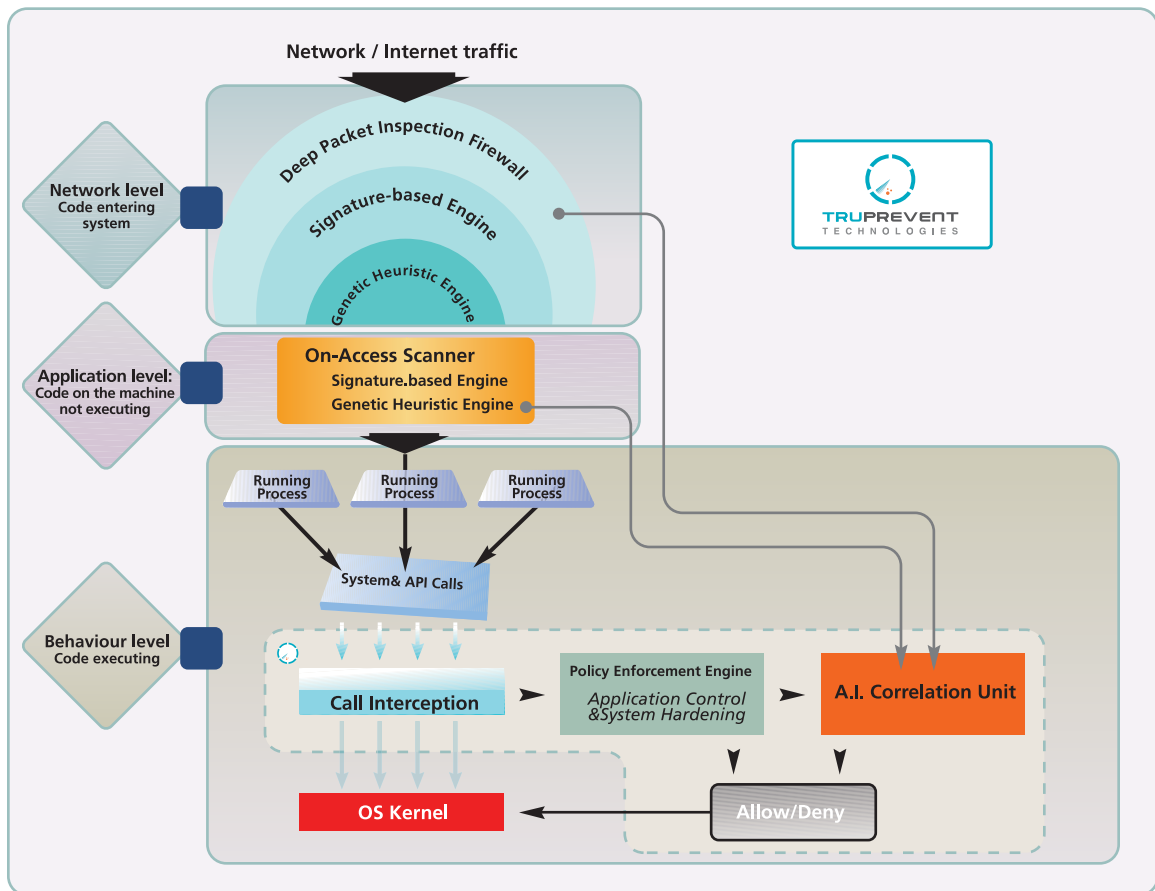


Figura 3: Seguridad integrada para endpoints de Panda

El primer examen fue encargado por Panda a ICSALabs, una división de CyberTrust Corporation, en el otoño de 2004. ICSALabs examinó las tecnologías tomando como referencia un conjunto de aproximadamente 100 ejemplares reales de malware. El primer examen fue diseñado para comprobar si las tecnologías resultaban eficaces frente a distintos tipos de malware, más que para comprobar la efectividad general de las tecnologías a lo largo del tiempo.

Al mismo tiempo, ICSALabs examinó TruPrevent tomando como base varios

grupos de aplicaciones legales, desde juegos a programas para compartir archivos (P2P). No se produjo ni un solo falso positivo a pesar de los intentos en este sentido.

Otro de los "primeros" análisis, realizado esta vez por la revista PC Magazine USA, concluyó que²² "TruPrevent ha conseguido bloquear las dos terceras partes de una muestra de gusanos, virus y troyanos recientes basándose exclusivamente en el comportamiento. No ha bloqueado ningún programa legal ni ha tenido un impacto reseñable en el rendimiento del sistema."

3.3.3 Bloqueo por comportamiento TruPrevent

El segundo componente principal de TruPrevent es el denominado KRE (Kernel Rules Engine), al que se conoce también como Application Control & System Hardening o Resource Shielding (Securización de Sistemas y Control de Aplicaciones o Escudo de Protección de Recursos).

Los hackers y el malware abusan de los privilegios de las aplicaciones legales para atacar a los sistemas mediante la inyección de código. Con el fin de evitar este tipo de ataques de forma genérica, resulta muy económico utilizar una tecnología de bloqueo basada en reglas que permitan restringir las acciones que las aplicaciones autorizadas pueden llevar a cabo en un sistema.

KRE consta de un conjunto de normas definidas por una serie de reglas que describen las acciones que una aplicación concreta puede realizar o no. Las reglas pueden configurarse para controlar el acceso por parte de la aplicación a los ficheros, a las cuentas de usuario, al registro, a los objetos COM, a los servicios de Windows o a los recursos de red.

A pesar de ofrecer un alto grado de granularidad a los administradores para crear normas personalizadas, el módulo Application Control & System Hardening (KRE) se suministra con un conjunto de normas configuradas por defecto. Estas normas son gestionadas y actualizadas por PandaLabs. Dichas normas ofrecen protección frente a ataques que aprovechan vulnerabilidades comunes de instalaciones estándar o completamente parcheadas de los sistemas operativos de Windows.

Un ejemplo reciente de la eficacia que ofrece este bloqueo proactivo es la intermina-

ble oleada de vulnerabilidades de formato de Microsoft Office que están siendo aprovechadas para ocultar código malicioso²³. Estas vulnerabilidades han sido utilizadas recientemente para realizar ataques dirigidos sobre determinadas empresas.

En un estudio sobre exploits que aprovechen vulnerabilidades conocidas (parcheadas) y del tipo día cero (sin parchear) de Microsoft Office, los motores antivirus examinados alcanzaron una tasa promedio de detección de dichos exploits mediante firmas del 50%. Eso representa un 50% de probabilidades de ser infectado al abrir un documento de Excel, PowerPoint o Word de Microsoft cuya vulnerabilidad haya sido aprovechada.

Por el contrario, las tecnologías de bloqueo por comportamiento, como TruPrevent, evitan de forma proactiva que Word, PowerPoint, Excel, Access, Acrobat Reader, Windows Media Player u otras aplicaciones ejecuten o instalen cualquier tipo de código ejecutable en el sistema. A diferencia de los antivirus basados en firmas, TruPrevent ofrece protección real frente a cualquier amenaza del tipo día cero que intente aprovecharse de vulnerabilidades de Microsoft Office, conocidas o desconocidas.

3.3.4 Tecnología heurística de análisis genético

Las tecnologías "genéticas" se inspiran en el campo de la biología genética y en su utilidad para comprender cómo se diferencian los diferentes organismos y la forma en que se asocian unos con otros. Estas tecnologías se basan en el proceso e interpretación de "genes digitales", que en nuestro caso se refiere a unos pocos cientos de características propias de cada uno de los archivos analizados.

Denominado en código Nereus, el motor de análisis heurístico genético (Genetic Heuristic Engine), fue introducido por primera vez en el año 2005. El objetivo del GHE es correlacionar las características genéticas de los ficheros mediante un algoritmo propietario. Estas características genéticas determinan el potencial del software para llevar a cabo acciones maliciosas o inofensivas cuando se ejecuta en un ordenador. GHE es capaz de concluir si un fichero es inofensivo, o es un gusano, spyware, un troyano, un virus, etc., correlacionando las distintas características de cada elemento analizado.

Es posible definir la sensibilidad del GHE como baja, intermedia o alta, con el lógico reajuste entre las tasas de detección y falsos positivos. Los distintos niveles de sensibilidad están diseñados para ser aplicados en diferentes entornos dependiendo de la probabilidad de que exista malware en cada uno de ellos.

Por ejemplo, la probabilidad de que un archivo ejecutable sea malware en pasarelas SMTP de red es muy alta. Por lo tanto, hemos implementado una alta sensibilidad en las soluciones de análisis de correo electrónico en la capa de red. Sin embargo, en las capas de almacenamiento (o de aplicación), en las que la mayor parte del código ejecutable procede de aplicaciones legales, hemos implementado una sensibilidad intermedia en el GHE.

Gracias a esta configuración, hemos podido maximizar las tasas de detección de malware desconocido con una tasa mínima de falsos positivos.

Hasta ahora, los resultados del GHE han sido magníficos. Desde su introducción, aproximadamente un tercio (acumulativo) de las nuevas variantes de malware

recibidas en PandaLabs procedentes de las máquinas reales de usuarios ha sido enviado por el GHE.

3.4 La Inteligencia Colectiva

Hoy en día hay diez veces más malware en circulación que hace dos años. La conclusión obvia es que una solución de seguridad debe ser capaz de detectar diez veces más malware para ofrecer una protección adecuada a los usuarios.

Aunque una solución HIPS completa detecta y bloquea la mayoría de este malware con tecnologías proactivas, sigue existiendo la posibilidad de que malware desconocido pueda saltarse estas defensas.

Aunque el 80 o el 90 % de eficacia de la protección proactiva es en términos relativos una excelente cifra, en términos absolutos puede significar que cientos o miles de ejemplares de malware no se detecten, ya que una pequeña fracción de un número grande sigue siendo una cantidad "enorme".

El concepto de Inteligencia Colectiva surgió por primera vez a finales de 2006 en fase experimental con el objetivo de "detectar diez veces más de lo que detectamos actualmente con 10 veces menos esfuerzo". La Inteligencia Colectiva funciona como una plataforma de seguridad como servicio (SaaS) online y en tiempo real. Con más de dos años de investigación y desarrollo a sus espaldas y millones de dólares de inversión, esta tecnología ha empezado ya a producir beneficios gracias al:

1. Aprovechamiento del conocimiento "colectivo" para proteger de forma proactiva a otros.

2. Automatización y mejora de la recopilación, clasificación y eliminación de malware.

3. Adquisición de conocimientos sobre técnicas para mejorar las tecnologías existentes.

4. Utilización de una nueva generación de tecnologías proactivas desde la nube.

5. Distribución de una nueva generación de servicios proactivos desde la nube.

3.4.1 Aprovechamiento del conocimiento colectivo

La arquitectura de las soluciones de seguridad tradicionales se basa en una filosofía en la que el PC es el centro. Esto significa que el PC es tratado como una unidad independiente en el tiempo y que cualquier ejemplar de malware detectado en ese PC se considerará al margen de los demás ejemplares detectados en otros millones de PCs.

Las empresas de seguridad tradicionales no saben en qué PC se detectó por primera vez un ejemplar de malware, ni tampoco saben cómo ha evolucionado ese malware a lo largo del tiempo en los distintos ordenadores.

Y lo que resulta aún más importante, los demás ordenadores no pueden beneficiarse de forma automática de las detecciones proactivas de malware realizadas en otros PCs. Tienen que esperar a que el laboratorio antivirus reciba el ejemplar concreto, cree la firma, garantice su calidad, la distribuya y finalmente proteja a los usuarios.

El resultado es que los enfoques tradicionales resultan excesivamente lentos para combatir al ágil malware actual.

Una de las virtudes fundamentales de la Inteligencia Colectiva, además de la eficacia derivada de la automatización del ciclo de

eliminación de malware, son las ventajas automáticas y en tiempo real que ofrece a los usuarios de la Comunidad de la Inteligencia Colectiva.

Tan pronto los servidores de Inteligencia Colectiva detecten un proceso sospechoso en el PC de un usuario (ya sea mediante análisis heurísticos del sistema, emulaciones, sandboxing, análisis de comportamiento, etc.), el resto de usuarios de todo el mundo se beneficiarán en tiempo real de esa detección. Esto produce una detección casi en tiempo real no sólo de los brotes iniciales de malware, sino también de los ataques dirigidos de baja intensidad cuyo objetivo es infectar a un número pequeño de usuarios para no ser detectados.

3.4.2 Proceso automático de protección frente al malware

Una de las principales barreras para elevar los ratios de detección fiable de malware es la cantidad de tiempo que lleva la creación de una firma para un solo ejemplar. Es necesario que un usuario afectado u otro investigador envíen al laboratorio el ejemplar de malware. A continuación, los técnicos del laboratorio tienen que descifrarlo, lo que supone a su vez la necesidad de crear una firma de detección y una rutina de desinfección para ese ejemplar. Después, deben asegurarse de la calidad de dicha firma y rutina de desinfección, cargarlas en los servidores de producción, replicarlas a nivel mundial y finalmente ser descargadas y aplicadas por los clientes.

El proceso entero es fundamentalmente manual en la mayoría de los casos, y puede llevar desde minutos hasta horas, días o

incluso semanas, dependiendo de la carga de trabajo de los ingenieros del laboratorio o de otros factores, como la prioridad de la muestra, su distribución, su capacidad para causar daño, su repercusión mediática, etc.

El proceso puede demorarse incluso más tiempo si es necesario actualizar la información o la funcionalidad de los motores de análisis de comportamiento o anti-malware. Normalmente los proveedores de soluciones anti-malware ofrecen actualizaciones una o dos veces al año, porque cada actualización supone un proceso costoso de testeo y distribución a los clientes corporativos.

Gracias a la infraestructura de la Inteligencia Colectiva, todo el proceso de recopilación, clasificación y eliminación del malware puede automatizarse y realizarse online en cuestión de segundos para la gran mayoría de muestras.

Vamos a hacer un recorrido por el proceso desde el punto de vista de un ordenador con una vulnerabilidad que ha sido aprovechada y que ha resultado infectado por un código malicioso.

3.4.2.1 Recopilación automática de malware

El agente de Inteligencia Colectiva (IC) reúne información de los procesos y objetos de memoria y realiza consultas a los servidores centrales de IC, que se encargan de realizar una serie de comprobaciones.

Si se cumplen determinadas condiciones, el archivo sospechoso o partes del mismo que se consideren como tales se cargarán automáticamente en los servidores de IC, donde serán procesadas.

Dado que los procesos cargados en la memoria no están sujetos a muchas de las técnicas de ocultación y se “desenmascaran ellos solos”, el agente no necesita incluir demasiada información ni rutinas de desenmascaramiento. Esto permite que el agente sea muy ligero.

Panda ha creado una enorme base de datos de ejemplares de malware, recopilados automáticamente, lo que a su vez proporciona al servicio web de IC información en tiempo real de los nuevos ejemplares de malware.

3.4.2.2 Clasificación automática del malware

El procesamiento basado desde la nube no se encuentra condicionado por las limitaciones de memoria o de CPU de los ordenadores personales. Por consiguiente, las rutinas de análisis en los servidores de IC se someten a un procesamiento más profundo utilizando tecnologías más sensibles (análisis heurístico sensible y análisis de firmas, emulación, sandboxing, virtualización, listas blancas, etc.) para alcanzar una clasificación final.

Es importante observar que la potencia de análisis de los servidores de IC solo se ve limitada por las posibilidades de escalamiento de la banda ancha y del hardware, a diferencia de lo que sucede con los PCs, ordenadores de escritorio o servidores. Así pues, ahora es posible utilizar de forma generalizada muchas de las técnicas proactivas que emplea PandaLabs y que ofrecen las tasas de detección más altas sin tocar apenas los valiosos recursos de memoria y de CPU del cliente

Con este método, la mayoría de los nuevos ejemplares de malware se pueden analizar

y clasificar de forma automática en cuestión de minutos.

PandaLabs gestiona los servidores de IC y, por lo tanto, los ejemplares que no se pueden clasificar de forma automática son examinados en última instancia por un analista del laboratorio.

3.4.2.3 Remediación automática del malware

El módulo de remediación de IC se encarga de crear de forma automática firmas de detección y eliminación para los ejemplares analizados previamente por el módulo de clasificación y procesamiento. Estas firmas a su vez son utilizadas por la comunidad de usuarios de la Inteligencia Colectiva de forma proactiva para detectar y eliminar nuevos ataques, incluso los ataques dirigidos que cuentan con un número muy bajo de hosts infectados.

Las soluciones HIPS y anti-malware tradicionales han comenzado también a beneficiarse de la Inteligencia Colectiva. Durante los 3 primeros meses de funcionamiento, el módulo de remediación ha creado firmas para unos cuantos cientos de miles de ejemplares de malware, que hemos ido implementando de forma gradual en nuestros productos.

Uno de los principales beneficios del concepto de Inteligencia Colectiva es que no hace falta descargar estas firmas a cada cliente, ya que se encuentran disponibles desde la nube. Esto, sin embargo, no significa que la máquina cliente no deba mantener su conjunto de firmas actualizado.

Una de las principales amenazas para este enfoque está en la disponibilidad de los servidores de Inteligencia Colectiva.

No obstante, nuestro planteamiento a la hora de integrar la tecnología de Inteligencia Colectiva en nuestras soluciones actuales es su diseño como una capa de protección complementaria. Por lo tanto, en el caso de que por alguna razón no estuviese disponible dicha plataforma, la protección de seguridad recurriría a la solución HIPS ordinaria, que proporciona una protección por encima de la media.

3.4.3 Obtención de conocimiento sobre las técnicas de malware

Otra de las principales ventajas de esta característica comunitaria de la Inteligencia Colectiva es que proporciona a nuestros ingenieros la oportunidad de conocer nuevas técnicas de malware y puntos de entrada. Preguntas como dónde se detectó por primera vez un ejemplar de malware y su forma de propagación nos permiten obtener más conocimiento sobre familias de malware específicas o incluso creadores de variantes concretas de malware.

La aplicación de técnicas de extracción y almacenamiento de datos a las detecciones de malware realizadas por la comunidad nos proporciona un conocimiento significativo sobre cómo se llevan a cabo los ataques dirigidos y los ataques por malware. Los conocimientos obtenidos con este método resultan muy útiles para hacer un seguimiento de los orígenes de las infecciones, lo cual a su vez puede tener aplicaciones y ventajas interesantes en la persecución de delitos informáticos.

3.4.4 Distribución de Servicios de Seguridad “desde la nube”

Nosotros hemos desarrollado y estamos

distribuyendo ya algunos servicios que funcionan exclusivamente en base a la plataforma de la Inteligencia Colectiva. Estos servicios online están diseñados para realizar auditorías exhaustivas de los ordenadores y detectar malware no detectado por las soluciones de seguridad instaladas.

Para los consumidores y ordenadores autónomos hemos desarrollado NanoScan (www.nanoscan.com), que analiza los PCs en busca de malware activo en ejecución, y TotalScan (www.pandasecurity.com/totalscan), que realiza un análisis completo del ordenador, incluyendo discos duros, memoria, email, etc.

En el frente corporativo, los requisitos para la realización de una auditoría exhaustiva de malware son más exigentes. Por este motivo hemos creado un servicio gestionado específico llamado Malware Radar (www.malwareradar.com). Gracias a este servicio, las empresas pueden realizar rápidamente auditorías completas de los puntos finales de su red con el fin de comprobar su nivel de seguridad, encontrar focos de infección no detectados o descubrir máquinas que hayan sufrido ataques dirigidos.

3.4.5 Un comentario sobre las listas blancas

Desde el año 2004 han surgido muchas empresas prometiendo “resolver el problema de los virus para siempre” con el método de las listas blancas. Aunque entonces pudiera haber parecido una idea interesante, los problemas que plantean las soluciones que se basan en las listas blancas son muy variados.

A continuación presentamos algunos de los principales defectos de los métodos que se basan exclusivamente en el uso de listas blancas:

1. En la actualidad, existen miles de millones de ficheros goodware frente a unos pocos millones de ficheros malware. Para que las listas blancas sean eficaces, resultaría necesario analizar una cantidad ingente de ficheros que no son malware.
2. Siempre que sea preciso añadir un fichero a la lista blanca, hay que analizarlo para asegurarse de que no es malicioso. Añadir archivos a la lista blanca sin analizarlos haría fracasar su utilidad. Si no, ¿cómo puede evitarse la inclusión de malware en las listas blancas?
3. Cada vez que se pone disponible una actualización en forma de Service Pack o de Hotfix para Microsoft Windows, Office, QuickTime, Adobe, Java, etc., habrá que volver a analizar los archivos de las listas blancas y crearlas de nuevo.
4. La gestión de las listas blancas en cada ordenador de una red es un trabajo manual y tedioso para el que no disponen de tiempo los administradores de red.
5. Si los laboratorios antivirus que cuentan con cientos de ingenieros no dan abasto para analizar el malware, ¿qué inversión de capital y recursos necesitaría hacer una empresa dedicada a la gestión de listas blancas para analizar 100 veces más cantidad de goodware?
6. Las actualizaciones de las tecnologías anti-malware se entregan a los clientes a través de archivos de firmas de considerable tamaño. No obstante, las actualizaciones de las listas blancas serían mucho más voluminosas. ¿Cómo podrían ser entregadas a los ordenadores de escritorio y a las compañías?
7. ¿Qué sucede cuando hay aplicaciones nuevas o actualizadas que necesitan ser ejecutadas por un usuario o una compañía y que no están incluidas en las listas blancas? ¿Quién se encargará de llevar a cabo la ingeniería inversa y el análisis del programa supuestamente benigno, así como de sus archivos asociados, a fin de determinar si son realmente inofensivos?
8. ¿Qué sucedería si un virus o un gusano consiguiese infectar el paquete de instalación –incluido en una lista blanca- de una compañía acreditada dentro del sector? Esta situación se ha producido ya unas cuantas veces en el pasado.

Confiar únicamente en tecnologías basadas en listas blancas puede tener sentido en ambientes muy restringidos, como centros de llamadas, cajeros automáticos y parecidos. Pero este no es el caso en la gran mayoría de ambientes corporativos.

Últimamente, ha habido debates^{24 25} muy animados y activos sobre los pros y los contras de las listas blancas. Debates promovidos especialmente por las empresas que se dedican a ellas, y basados en el rumor de que “los programas antivirus han muerto y la solución son las listas blancas”.

No obstante, el planteamiento de las listas blancas no debe descartarse totalmente ya que plantea muchas oportunidades interesantes en la lucha contra el malware. Sin embargo, creemos que ofrece muchas más ventajas cuando se combina con el método de las listas negras y otras metodologías proactivas.

Tal y como hemos visto en la explicación sobre la plataforma de la Inteligencia Colectiva, el componente de las listas blancas resulta fundamental para complementar y mejorar la detección mediante listas negras y, en particular, reducir los falsos positivos y los tiempos de procesamiento.

4. Conclusión

Los últimos avances protagonizados por las comunidades de ciberdelincuentes se están aprovechando de las debilidades inherentes a la industria de la seguridad: (a) los laboratorios se ven inundados por la gran cantidad de malware que aparece cada día; (b) como las amenazas son invisibles, los usuarios no perciben la necesidad de una protección adicional, y (c) los ataques dirigidos que infectan a muy pocos usuarios son más efectivos que las epidemias que infectan a millones de usuarios.

Según avanzan las técnicas del malware en este juego del gato y el ratón, las empresas de seguridad necesitan añadir más capas de protección para mantener seguros a los clientes. La necesidad de protección adicional se manifiesta por el hecho de que una gran parte de los usuarios con soluciones de seguridad actualizadas están también infectados.

Para enfrentarnos a la situación actual se necesitan nuevas capas de protección que se aprovechen de la automatización del ciclo de protección contra el malware: recogida de muestras, análisis, clasificación y solución. Pero la automatización por sí misma no es suficiente. Se necesita también tener visibilidad sobre lo que pasa en los PCs para detectar los ataques dirigidos de forma más eficaz y obtener una ventaja competitiva sobre los creadores de malware.

El enfoque desarrollado por Panda Security, la Inteligencia Colectiva, ofrece todas las ventajas de una capa adicional de defensa que proporciona una respuesta y protección efectiva contra las amenazas actuales de malware. Además, es capaz de detectar los ataques dirigidos y obtener información y conocimiento gracias a la correlación de todas las detecciones realizadas por la comunidad de usuarios.

5. Referencias

1. Research Study: Active Infections in Systems Protected by Updated AntiMalware Solutions. Panda Research. August 2007. <http://research.pandasecurity.com>
2. Gartner's 10 Key Predictions for 2007. Gartner. December 2006. <http://www.eweek.com/article2/0,1895,2072416,00.asp>
3. The Zero-Day Dilemma. Security IT Hub. January 2007. http://www.security.ithub.com/article/The+ZeroDay+Dilemma/199418_1.aspx
4. Welcome to 2007: the year of professional organized malware development. F-Prot's Michael St. Neitzel at Hispasec. February 2007. <http://blog.hispasec.com/virustotal/16>
5. Call the cops: We're not winning against cybercriminals. ComputerWorld. February 2007. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010041>
6. 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
7. List of online scanners. CastleCops Wiki. http://wiki.castlecops.com/Online_antivirus_scans
8. Kernel Malware. F-Secure. February 2007. <http://www.f-secure.com/weblog/archives/archive-022007.html#00001118>
9. Antirootkit.com List of Rootkit Detection & Removal Software. <http://www.antirootkit.com/software/index.htm>
10. Rootkit used in Vodafone Phone Tapping Affair. July 2007. <http://www.antirootkit.com/blog/2007/07/12/rootkit-used-in-vodafone-phone-tapping-affair/>
11. Panda Anti-Rootkit. April 2007. http://research.pandasoftware.com/blogs/research/archive/2007/04/27/New-Panda-Anti_2D00_Rootkit-_2D00_-Version-1.07.aspx
12. Packing a punch. Panda Research. February 2007. <http://research.pandasoftware.com/blogs/research/archive/2007/02/12/Packing-a-punch.aspx>
13. AV performance statistics. OITC & MIRT. Real-time feed of antivirus zero-day detection. <http://winnow.oitc.com/avcentral.html>
14. Attack of the Zombie Computers Is Growing Threat. The New York Times. January 2007. <http://www.nytimes.com/2007/01/07/technology/07net.html?ex=1325826000&en=cd1e2d4c0cd20448&ei=5090>
15. 30 Days of Bots Inside the Perimeter. Support Intelligence. March-April 2007. <http://blog.support-intelligence.com>
16. Web-Attacker Exposed. Websense. November 2006. <http://www.websense.com/securitylabs/blog/blog.php?BlogID=94>
17. MPack Uncovered, May 2007. <http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf>
18. The World's Smallest Downloader. Symantec. December 2006. http://www.symantec.com/enterprise/security_response/weblog/2006/12/worlds_smallest_downloader.html
19. Packing a punch (II). Panda Research. March 2007. http://research.pandasoftware.com/blogs/research/archive/2007/03/20/Packing-a-Punch-_2800_III_2900_.aspx
20. Banking Targeted Attack Techniques. Panda Research. March 2007. <http://research.pandasoftware.com/blogs/images/Panda-eCrime2007.pdf>
21. PHost-Based Intrusion Prevention Systems (HIPS) Update: Why Antivirus and Personal Firewall Technologies Aren't Enough. Gartner. January 2007. http://www.gartner.com/teleconferences/attributes/attr_165281_115.pdf
22. Panda TruPrevent Personal 2005. PC Magazine USA. November 2004. <http://www.pcmag.com/article2/0,1759,1727653,00.asp>
23. Panda TruPrevent Personal 2005. PC Magazine USA. November 2004. <http://www.pcmag.com/article2/0,1759,1727653,00.asp>
24. The Last Great Security Crisis. eWeek February 2007. <http://www.eweek.com/article2/0,1895,2095118,00.asp>
25. Comments on "The Decline of Antivirus and the Rise of White-Listing". The Register. June 2007. http://www.theregister.co.uk/2007/06/27/whitelisting_v_antivirus/comments/
25. "More on White-listing". Kurt Wismer. June 2007. <http://anti-virus-rants.blogspot.com/2007/06/more-on-whitelisting.html>

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-PSD-01