INTELIGENCIA COLECTIVA: LA EVOLUCIÓN DEL MODELO DE SEGURIDAD TRADICIONAL

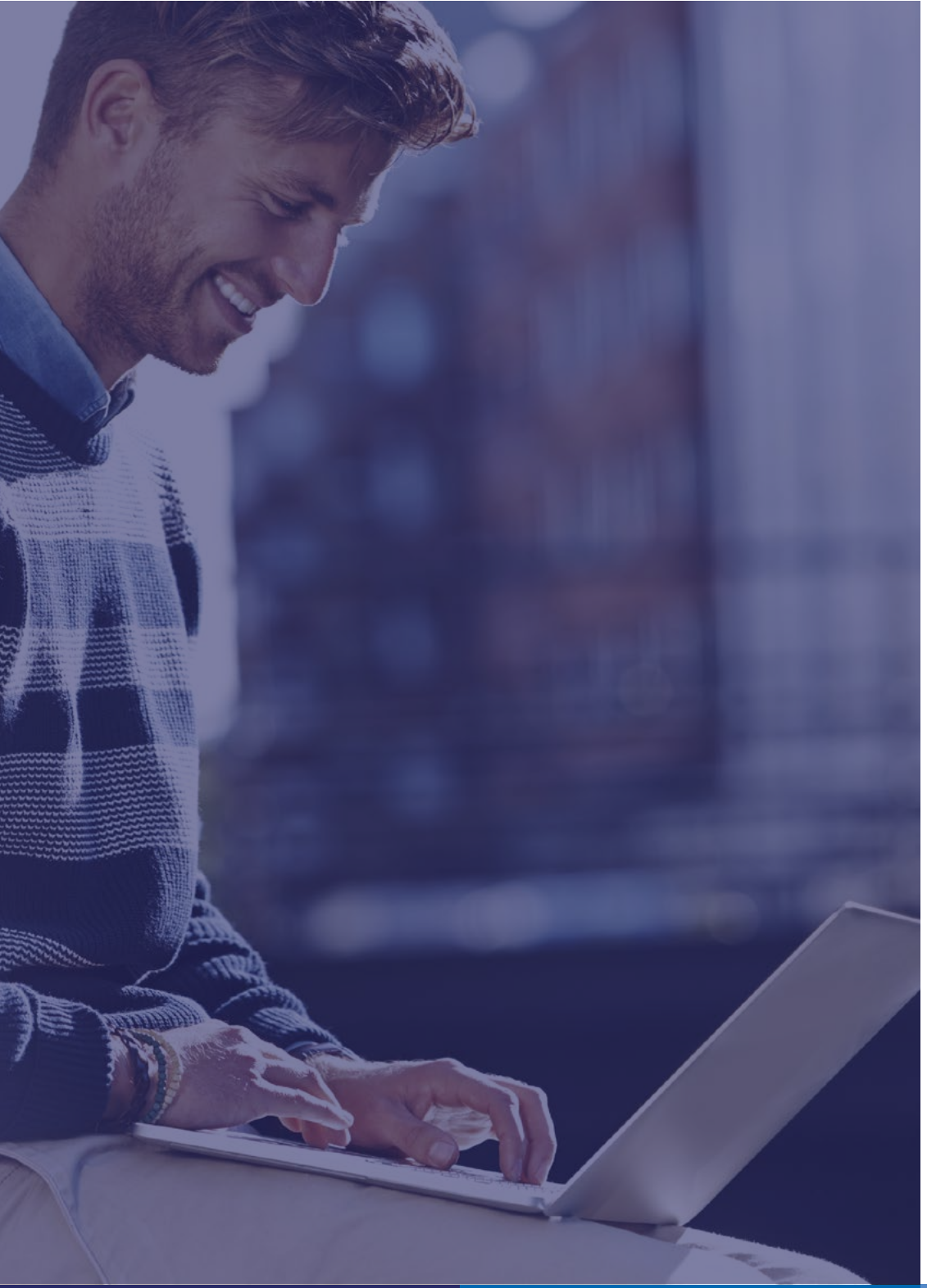
panda

pandasecurity.com

01 Resumen

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

Como hemos sido capaces de demostrar en un estudio reciente[1], 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 si misma no es suficiente para responder aljuego 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.

02
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 este año, 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 tradicionales[2].

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

Algunas empresas tratan de solucionar el problema aumentando el número de analistas en los laboratorios o abogando por una aplicación más contundente[4] de la ley[5], que perseguiría a los creadores de malware más activos y reduciría la carga de trabajo.

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 haciendo 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.

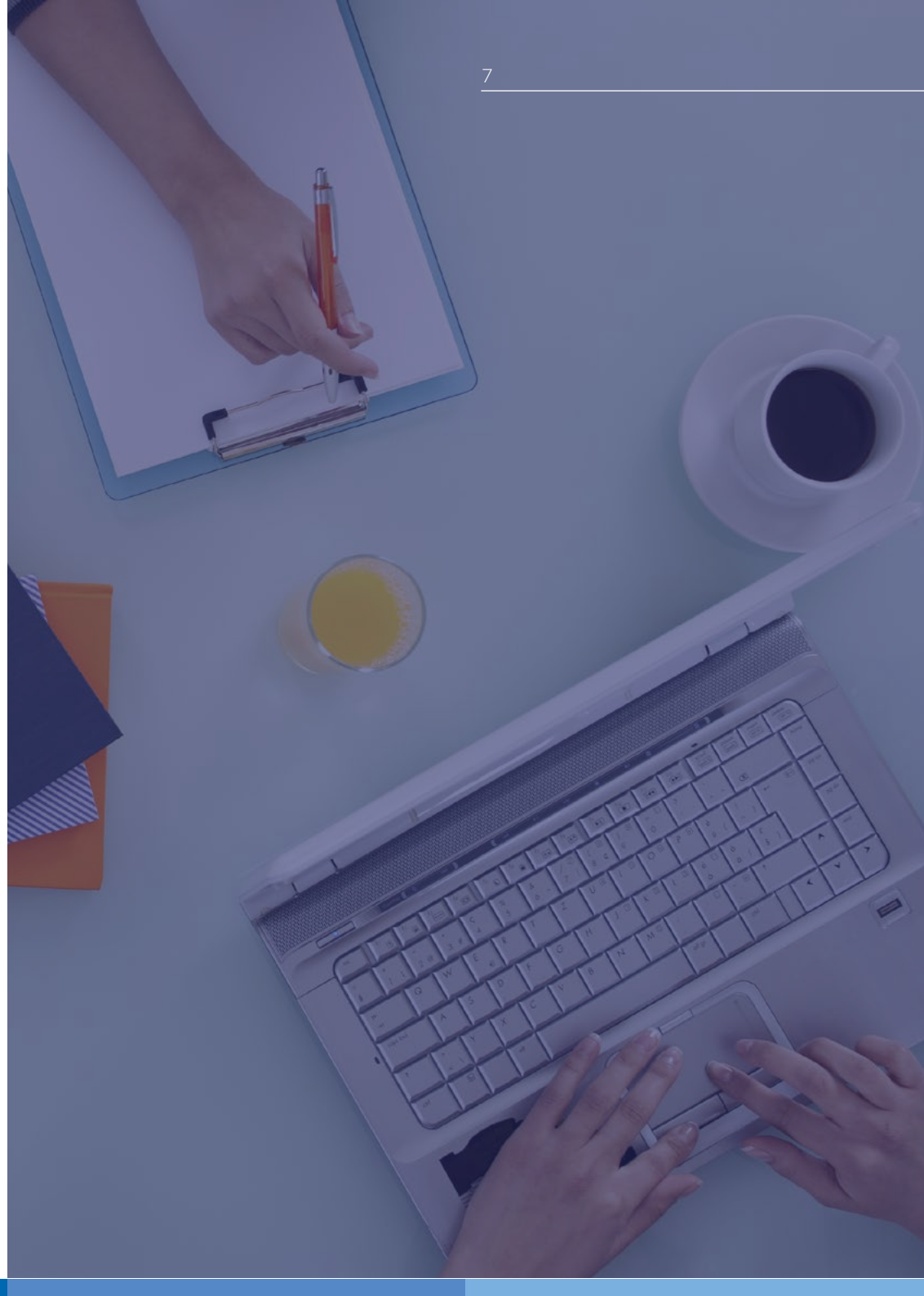
Técnicas y diseño de malware

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”.



1. ATAQUES DIRIGIDOS: POR DEBAJO DEL RADAR

Una de las principales estrategias emplea das por los Ataques Dirigidos para permanecer fuera del radar es distribuir pocas copias de muchas variantesó. 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 de antivirus darse cuenta de que existe una infección si solo afecta a unos pocos usuarios?

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 antivirus[7].

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.

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 por que 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 positivo, 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 algu nos ejemplares de LinkOptimizer y poder analizarlos en profundidad.

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 es tán empezando a experimentar sus efectos negativos en sus negocios, especialmente cuando se utilizan para espionaje corporativo[10].

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 empaquetador es 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 po sea 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 malware[12]. 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-malware[13].

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 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.

5. BOTNETS

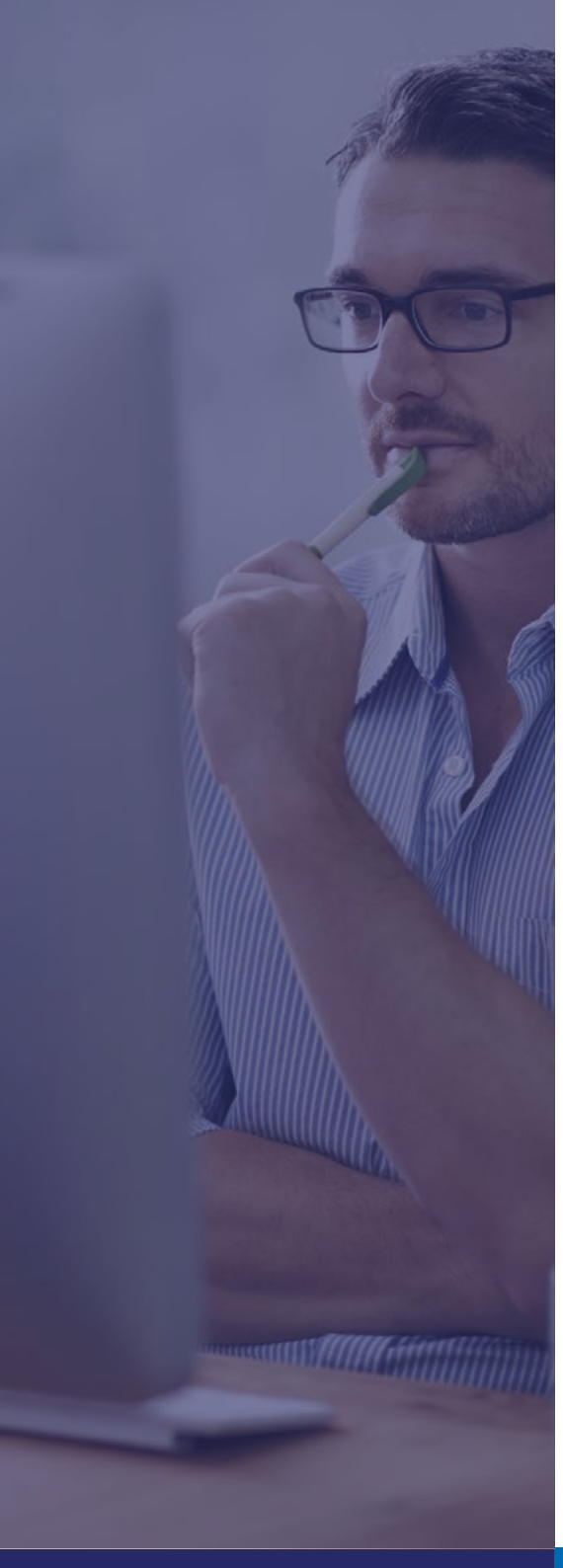
Hoy en día, una de las mayores amenazas son las redes de bots, y de hecho los bots son responsables de gran parte de las infecciones que se producen. Más del 90% del spam que se envía proviene de estos ordenadores infectados con bots. El control de estas grandes redes de ordenadores infectados se vende o alquila para llevar a cabo delitos informáticos: envío de spam, ataques de denegación de servicio, venta de proxies, robo de credenciales, etc.

En 2010 PandaLabs protagonizó el cierre de una de las mayores redes de bots de la historia. Esta red, conocida como Mariposa, controlaba millones de equipos a lo largo de 190 países, afectando a empresas, organismos públicos y usuarios particulares. Para hacernos una idea de la gravedad de la infección, más de la mitad de empresas pertenencientes al índice Fortune 1000 tenían equipos comprometidos por esta red. Aunque las botnets tradicionales son controlados vía IRC, en los últimos años hemos visto una gran evolución, utilizando canales como el P2P o el HTIP, e incluso redes sociales, como Twitter, como medio de control de las mismas.

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 MPack17 y Icepack26. 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 mundo[18].

Más recientemente, hemos visto surgir miles de herramientas gráficas que simplifican el trabajo de creación de downloaders[19] incluso con técnicas de empaquetamiento personalizadas para eludir la detección.

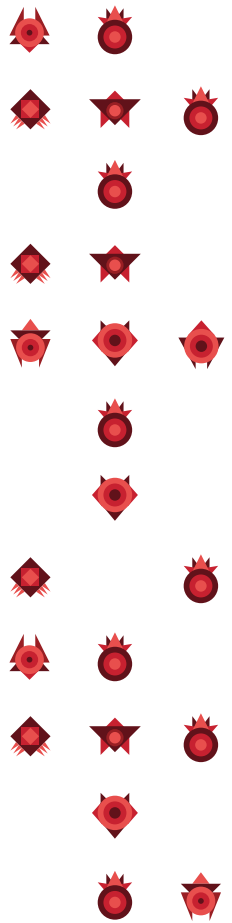
7. "MALWARE 2.0"

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 por el malware son la "compilación en el lado del servidor", en la que el servidor web recompila un nuevo binario cada pocas horas.

Por último, los botnets están empleando red es DNS fast-flux para mejorar su resistencia a la desinfección. Estas últimas técnicas aparecen en casos como los de los ataques protagonizados por Storm/ Nuwar.



03 Evolución de la tecnología de Panda

En Panda, nos encargamos de la investigación y desarrollo del 100% de nuestras principales tecnologías antimalware. 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.

Desde hace ya un tiempo los planteamientos tradicionales basados en firmas no han resultado eficaces a la hora de enfrentarse a esta situación creadapor 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].

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.

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.

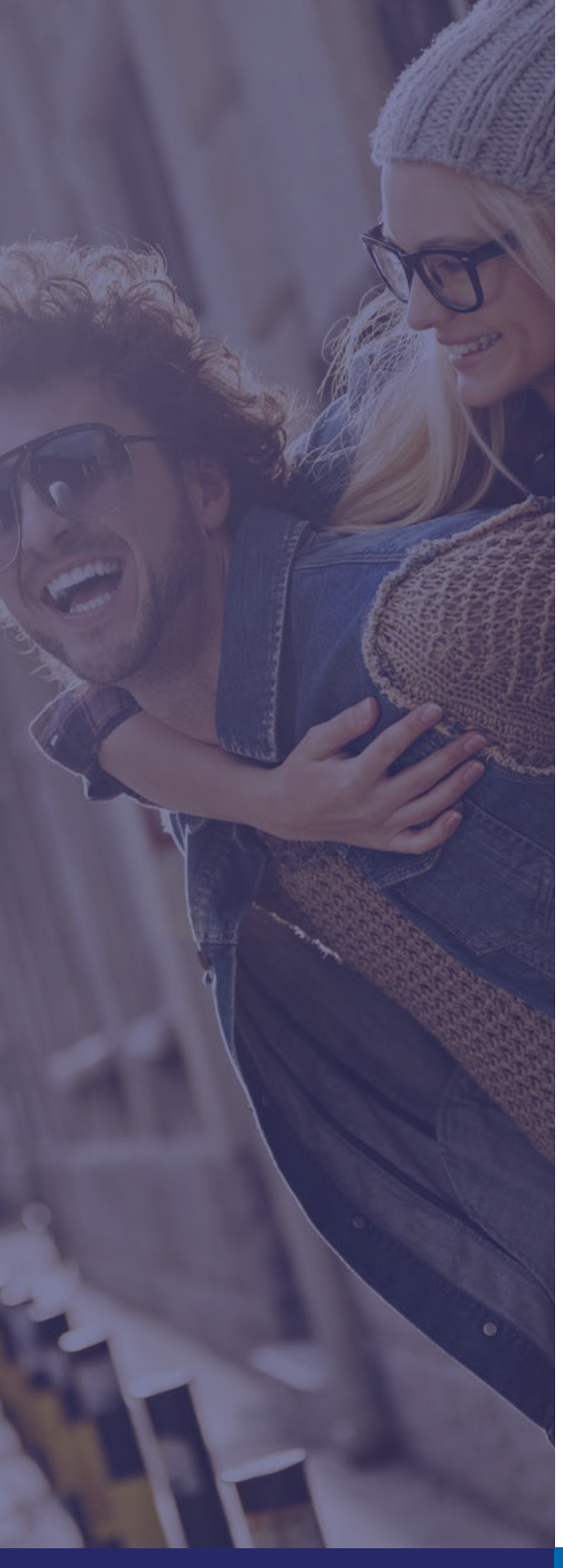
Este periodo también se vio marcado por la aparición de los primeros troyanos win32 utilizados de forma masiva, como NetBus y BackOrifice.

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 bloquear 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 Smartelean, concebida para desinfectar y restaurar el Sistema Operativo tras una infección provocada por spyware o troyanos de puerta trasera.



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 proteccion 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 en cargan de informar a Pandalabs de cualquier nuevo ejemplar de malware que TruPrevent designa como sospechoso y que no detectan las firmas antivirus ordinarias.

El método de TruPrevent consiste en analizar todos los elementos o amenazas potenciales mediante distintas técnicas, llevando a cabo inspecciones complementarias en profundidad en las diferentes capas de la infraestructura. La implementación de Tru Prevent 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.

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 utilice 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

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 abe?"). 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 respecto 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 si sola es capaz de detectar más del 80 por ciento del malware "in the wild", sin firmas y sin generar fal sos 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.

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.

El tiempo, no obstante, ha demostrado que la innovación que supusieron en su día las tecnologías TruPrevent era el inicio del camino a seguir, y año tras año numerosos análisis independientes han seguido de mostrando la eficacia de estas tecnologías.Por mencionar varios de los resultados más recientes:

- AV-C omparatives realizó en Mayo de 2010 una "prueba retrospectiva", consistente en desactivar las actualizaciones y el acceso a Internet del AV, y probar con malware aparecido un mes más tarde de la última actualización permitida. Obviamente, en estas circunstancias la única posibilidad de un AV de detectar malware se basa en sus tecnologías y firmas proactivas. En esta prueba, Panda Antivirus Pro obtuvo la primera posición (junto a TrustPort) con un 61% de capacidad de detección, más de un 20% por encima de la media[27].

- La revista alemana c't magazine realizó el mismo mes una prueba de detección "0- day ", es decir, exponiendo los AVs a muestras de malware recién aparecidas y que por tanto no han podido ser detectadas de forma reactiva por las compañías de seguridad. Panda Cloud Antivirus obtuvo la primera posición, con un 99,10% de detección.

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 atacaralos 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 interminable oleada de vulnerabilidades en el formato PDF, afectando principalmente a Acrobat Reader, que están siendo aprovechadas para distribuir malware. Además también hemos visto casos de ataques dirigidos a determinadas empresas utilizando estas técnicas. El ratio de detección de ficheros que explotan estas vulnerabilidades utilizando tecnologías tradicionales, como las firmas, es muy bajo, no llegando en la mayoría de los casos al 50%.

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.

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 proc eso e interpretación de “genes digitales”, que en nuestro caso se refiere a unos pocos cien tos de características propias de cada uno de los archivos analizados.

Denominado en código Nereus, el motor de análisis heurístico genético (Genetic Heur istic 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 probablidad 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 implemanta do 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.

La cuarta generación: la Inteligencia Colectiva

Como venimos diciendo durante los últimos años, el número de malware está aumentando de forma significativa año tras año. Frente a otro tipo de métricas. en las que los valores ofrecidos por la industria de seguridad parecen reflejar más una "guerra de números" que una información objetiva, algo en lo que todas las empresas del sector coincidimos -expresado de diferentes maneras, aunque con el mismo mensaje- es en poner de relevancia el hecho de que cada año recibimos y detectamos tanto malware como en la suma de los dos años anteriores.

Eso se traduce en que una solución de seguridad debe ser capaz de detectar 40 veces más malware que hace sólo cinco años, o tres veces más que hace sólo dos años. 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. Si bien alcanzar un 80 o 90% de eficacia de la protección proactiva es en términos relativos una excelente cifra, en términos absolutos puede suponer que, en 2010, decenas de miles de ejemplares de malware al mes queden sin detectar, ya que una pequeña fracción de un número grande sigue siendo una cantidad "enorme".

Por otro lado, este volumen de aparición de nuevo malware no se traduce en un volumen similar de presencia de malware activo en cada momento. La estrategia de los creadores de malware ha cambiado, y salvo excepciones, no se centran tanto en crear malware destinado a infectar masivamente y perdurar en el tiempo, sino en distribuir muy rápidamente y de forma segmentada malware nuevo, que en breve será sustituido por una nueva variante, a menudo antes de que las tecnologías tradicionales de detección por firma lleguen a detectarlo.

Esta estrategia se traduce en que el periodo de vida medio de una gran parte del malware es sumamente corto, de días o incluso horas, frente al anteriormente habitual de semanas o meses. Para un enfoque de protección basado en actualizaciones de ficheros de firmas, con una frecuencia de publicación típica de una actualización cada 24 horas, supondría que los usuarios están desprotegidos durante gran parte del tiempo en que cada ejemplar de malware va a estar activo.

La respuesta de Panda a estos dos grandes retos que supone la nueva dinámica del malware (volúmenes cada vez mayores de nuevo malware, combinado con una distribución limitada y tiempos de vida muy cortos} fue la Inteligencia Colectiva.

1. FUNCIONALIDADES

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 de lo que detectamos ac tualmente con diez 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 preliminar, y otros tantos de explotación y evolución como sistema productivo, esta tecnología ha producido resultados espectaculares en cuanto a la cantidad de malware recibido, analizado y detectado, así como en cuanto al tiempo de respuesta ofrecido desde la recepción de dicho malware.

Bajo el concepto de Inteligencia Colectiva se agrupan diversos bloques funcionales, encargados de proporcionar servicios de naturaleza complementaria:

- Red de sensores en tiempo real.
- Recopilación automática de malware.
- Procesamiento y clasificación automática de malware.
- Remediación automática del malware.

A continuación incluimos una descripción de dichos bloques, aclarando de antemano que no pretendemos ofrecer una visión téc nica de la arquitectura del sistema, sino una visión de alto nivel de las distintas funciona lidades que se realizan.

a. Red de sensores en tiempo real

Gracias a la presencia de sensores avanzados en nuestros productos, el agente de Inteligencia Colectiva reúne información de los procesos y objetos de memoria y realizan consultas a los servidores centrales de la IC, que se encargan de almacenar y correlacionar la información que, en tiempo real, se está recibiendo de las máquinas de nuestros usuarios.

Esto nos ofrece una gran visibilidad sobre los patrones de aparición y comportamiento de nuevos ejecutables en las máquinas de nuestra comunidad, dando lugar a la identificación de posibles procesos sospechosos. Esa identificación de un fichero como sospechoso pasa a estar disponible de forma inmediata para toda la comunidad, evitando tener que realizar análisis similares en otros PCs, y no dando por tanto oportunidad al malware a propagarse a otras máquinas antes de su detección.

b. Recopilación automática de malware

Si se cumplen determinadas condiciones que conviertan un archivo en sospechoso, dicho archivo o partes del mismo que se consideren relevantes se cargarán automáticamente en los servidores de la IC para su procesamiento.

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. De forma adicional, prácticamente la totalidad de las empresas de la industria de seguridad, así como los analistas más relevantes, proceden a intercambios periódicos de muestras de malware, de forma que entre todos consigamos mantener bajo control la propagación de malware en el mundo. Los sistemas de captura de malware de la IC permiten a Panda automatizar estos intercambios, mejorando así nuestros tiempos de procesa miento, y la calidad de la información que recibimos de, y enviamos a, otros proveedores de seguridad.

c. Procesamiento y clasificación automática de malware

El procesamiento basado en 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 la IC se someten a un procesamiento más profundo utilizando tecnologías más sensibles de Inteligencia Artificial (análisis heurístico sensible y análi sis de firmas, emulación, sandboxing, virtualización, comprobación contra listas blancas, etc.) para alcanzar una clasificación final.

Es importante observar que la potencia de análisis de los servidores de la IC sólo se ve limitada por las posibilidades de escalado de las líneas de comunicación 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 tasas de detección más altas sin tocar apenas los valiosos recursos de memoria y 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 la IC y, por tanto, los ejemplares que no se pueden clasificar de forma automática son examina dos en última instancia por un analista del laboratorio.

d. Remediación automática del malware

El módulo de remediación de la IC se encarga de crear de forma automática firmas de detección y eliminación para los ejemplares analizados previamente por el módulo de clasificación, y que se hayan determinado como maliciosos. Estas firmas son a su vez 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 se benefician también de de la Inteligencia Colectiva. El módulo de remediación ha creado centenares de miles de ejemplares de malware, que hemos ido implemen tando de forma gradual en nuestros productos.

2. BENEFICIOS

a. Uso de la comunidad

La arquitectura de las soluciones de seguridad tradicionales se basa en una filosoffa 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 más importante, los demás ordenadores no pueden beneficiarse de forma automática de las detecciones proactivas de malware realizadas en otros PCs. Gracias a la tecnología de la IC, toda evidencia de la presencia de malware obtenida en cualquiera de los PCs de nuestros usuarios es inmediatamente aprovechada por el resto, de forma que el conjunto de usuarios de Panda actúa como una red de alerta temprana, dando lugar a un conocimiento global muy superior al alcanzable mediante el análisis individual y aislado de cada PC.

b. Mayor capacidad de procesamiento de malware en nuestro laboratorio

Una de las principales barreras para elevar los ratios de detección fiable de malware era la cantidad de tiempo que lleva la creación de una firma para un solo ejemplar. Es nece sario que un usuario afectado u otro investi gador envíen al laboratorio el ejemplar de malware. A continuación, los técnicos del laboratorio tienen que descifrarlo, lo que su pone a su vez la necesidad de crear una firma de detección y una rutina de desinfección para ese ejemplar.

Hasta la puesta en marcha de los módulos de procesamiento, clasificación y remediación automática de malware, el proceso era fundamentalmente manual en la mayoría de los casos, y podía 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. Era un proceso laborioso, pero no olvidemos que debía realizarse así para cada ejemplar. Multipliquemos ese esfuerzo por decenas de miles de ejemplares nuevos diarios, y nos daremos cuenta de que es absolutamente imposible abarcar de esta forma la oleada de malware a la que nos enfrentamos actualmente.

Gracias a la infraestructura de la Inteligencia Colectiva, todo el proceso puede automatizarse y realizarse masivamente on-line en cuestión de segundos para la mayoría de las muestras, reservando la capacidad de los ingenieros del laboratorio para el análisis de ejemplares particularmente complejos, o para la creación de rutinas de detección avanzadas que aporten mayor proactividad y capacidad de generalización.

c. Ahorro de consumo de an cho de banda y de espacio en disco

Uno de los principales beneficios del concepto de Inteligencia Colectiva es que no hace falta descargar las firmas a cada cliente, ya que se encuentran disponibles desde la nube. Dado el ingente número de detecciones creadas por la Inteligencia Colectiva para todo el malware aparecido desde su puesta en marcha, si se quisiera volcar todo ese conocimiento a ficheros de firmas construidos de la manera tradicional, serían necesarios aproximadamente 250 MB, una cifra excesiva tanto por el coste de manejo de esas firmas, como de actualizaciones diarias.

Gracias al conocimiento disponible en nuestros servidores, podemos permitirnos mantener unos ficheros de firmas de un tamaño considerablemente inferior, que sin embargo albergan la información

suficiente sobre el malware actualmente en activo como para ofrecer una protección efectiva incluso en el caso de que el ordenador de un usuario no disponga de conexión a Internet en un momento dado.

d. Incremento de la velocidad de reacción frente a nuevo malware

Como ya hemos comentado, en el enfoque tradicional se analiza cada PC como una entidad aislada. Esto no sólo se traducía en un conocimiento global sobre el malware en circulación menor, sino que llevaba también a unos tiempos efectivos muy superiores desde la aparición de un malware hasta que su detección está accesible para todos los usuarios.

Según ese esquema, los usuarios 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 el 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. Tan pronto como los servidores de Inteligencia Colectiva determinen que un ejecutable es malicioso, ese conocimiento está accesible para toda la base instalada, que se encuentra por tanto protegida en cuestión de minutos, frente a los ciclos cercanos a 24h de la mayoría de enfoques tradicionales.

e. Obtención de conocimiento sobre las técnicas de malware

Otra de las principales ventajas de la 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 diri gidos y los ataques por malware. El conocimiento obtenido con este método resulta muy útil para hacer un seguimiento de los orígenes de las infecciones, lo cual a su vez tiene aplicaciones y ventajas interesantes en la persecución de delitos informáticos.

3. ALGUNOS DATOS SORPRENDENTES DE LA INTELIGENCIA COLECTIVA

Cada día, este sistema recibe más de 17 millones de peticiones de información de los usuarios de soluciones Panda. Procesa más de 75.000 ficheros nuevos, nunca vistos anteriormente, y determina si son malware o no.

La media de nuevo malware aparecido diariamente se sitúa en estos momentos en 55.000. El total de ejemplares de malware catalogados actualmente supera los 40.000.000. El 0,6% que el sistema no es capaz de determinar de forma automática si es malicioso, es analizado por el equipo técnico de la compañía. En estos momentos, la base de datos principal de Inteligencia Colectiva ocupa 2.5 TB de disco (contabilizando sólo malware clasificado) y genera 190 Gb de logs diarios. La Base de Datos de la Inteligencia Colectiva cuenta con más de 1.000.000.000.000 de registros.

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 usuarios domésticos hemos desarrollado Panda Cloud Antivirus Pro que analiza los PCs en busca de malware y 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. 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.

04
Conclusión

Los últimos avances protagonizados por las comunidades de ciberdelincuentes se están aprovechando de las debilidades inherentes a la industria de la seguridad:

- Los laboratorios se ven inundados por la gran cantidad de malware que aparece cada día;
- Como las amenazas son invisibles, los usuarios no perciben la necesidad de una protección adicional;
- 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 establece que 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.

05 Referencias

1. Research Study: Active Infections in Systems Protected by Updated AntiMalware Solutions. Panda Research. http://research.pandasecurity.com

2. Gartner's 10 Key Predictions for 2007. Gartner. http://www.eweek.com/article2/0,1895,2072416,00.asp

3. Toe Zero-Day Dilemma. Security IT Hub J. http://www.security.ithub.com/article/The+ZeroDay+ Dilemma/1994 18_1.aspx

4. Welcome to 2007: the year of professional organized malware development. F-Prot's Michael St. Neitzel at Hispasec. http://blog.hispasec.com/virustotal/16

5. Call the cops: We' re not winning against cybercriminals. ComputerWorld. http://www.computerworld. com/action/article.do?command=viewArticleBasic&articleId=9010041

6. Toe Long Tail: malware's business model. Panda Research. http://research.pandasoftware.com/blog/research/archive/2007 /O 1/ 08/rhe-Long-Tail_3AOO_-malware_2700_s-business-model.aspx

7. List of online scanners. CastleCops Wiki. http://wiki.castlecops.com/Online_antivirusans

8. Kernel Malware. F-Secure. http://www.f-secure.comlweblog/archivesfarchive- 022007.html#00001118

9. Antirootlcit.com List of Rootlcit Detection & Removal Software. http://www.antirootkit.com/software/index. htm

10. Rootkit used in Vodafone Phone Tapping Affair. http://www.antirootkit.com/blog/2007/07/12/rootlcit-used-in-vodafone phone-tapping-affair

11. Panda Anti-Rootlcit. http://research. pandasoftware.com/blog/research/archive/2007/041 27/New-Panda-Anti_2DOO_Rootlcit-_2DOO_-Version-1.07.aspx

12. Packing a punch. Panda Research. http://research. pandasoftware.com/blogsfresearch/archive/2007/02/ 121Packing-a-punch.aspx

13. AV performance statistics. OITC & MIRT. Real-timefeed of antivirus zero-dar detection. http://w1nnow. oitc.com/avcentral .html

14. Attack of the Zombie Computers Is Growing Threat. The New York Times. http://www.nytimes.com/2007/01/07/technology/07net.html?eX=1325826000&en=cd1 e2d4c0cd20448&ei =5090

15. 30 Days of Bots Inside the Perimeter. Support Intelligence. http://blog.support-intelligence.com

16. Web-Attacker Exposed. Websense. http://www.websense.com/securitylabslblog/blog. php?BlogID=94

17. MPack Uncovered. http://blogs,pandasoftware.com/blogs/images!Pandal.abs/2007/05/1 1/MPack.pdf

18. The World's Smallest Downloader. Symantec. http://www.symantec.com/enterprise/security_response/weblog/200 6112/worlds_smallesLdownloader.html

19. Paclcing a punch (11). Panda Research. http://research.pandasoftware. com/blogstresearch/archive/2007/03/ 20/Packing-a-Punch-_)_800_11L2900_.aspx

20. Banking Targeted Attaclc Techniques. Panda Research. http://research.pandasoftware. com/blogsfimages!Panda eCrime2007 .pdf

21. PHost-Based Intrusion Prevention Systems (HIPS) Update: Why Antivirus and Personal Firewall Technologies Aren't Enough. Gartner. http://www.gartner.comfteleconferences/attributes/attr_ 165281_11 5.pdf

24. The Last Great Security Crisis. 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. http://www.theregister. eo.uk/2007/06/27/whitelisting_v_antivirus/commentst

26. "More on White-listing•. Kurt Wismer. http://anti-virurrants.blogspot.comfl007/0fJ/more-on-whitel isting.html

27. http://pandalabs.pandasecurity.com/blogs/images/Pandalabs/200 7112118/lcepack.pdf

28. http://www.av compartives.org/images/storiesftest/ondret/avc_report26.pdf


panda