KASPERSKY lab

EL PODER DE LA PROTECCIÓN

LOS RIESGOS FUTUROS: PROTÉJASE

Informe especial de nuestro equipo de análisis e investigación global sobre estrategias de mitigación de amenazas sofisticadas

kaspersky.com/enterprise
#EnterpriseSec

ÍNDICE

Amenazas persistentes avanzadas y el panorama de amenazas 3

La gran empresa es un objetivo 5

¿Por qué es tan importante la mitigación? 6

Principales estrategias de mitigación 7

Otras estrategias altamente eficaces 9

El enfoque de Kaspersky Lab:
Protección en varios niveles contra amenazas conocidas, desconocidas y sofisticadas 11

¿Por qué Kaspersky Lab? 12

Kaspersky Lab: la mejor protección del sector 13

AMENAZAS PERSISTENTES AVANZADAS Y EL PANORAMA DE AMENAZAS

La ciberseguridad no es en absoluto un juego de números. Se necesita una sola brecha en la seguridad para causar graves daños a su empresa y defenderse de la mayoría de los ataques no es suficiente.

Por eso lo mejor es centrar nuestra atención en las amenazas más peligrosas a las que nos enfrentamos, en lugar de aquellas a las que nos enfrentamos con más frecuencia.

El "ecosistema" de malware se divide en amenazas **conocidas** (70 %), amenazas **desconocidas** (29 %) y amenazas **sofisticadas** (1 %).

Es relativamente fácil defenderse de las amenazas conocidas, que representan cerca del 70 % del malware. En la medida en que reconocemos el código malicioso, se puede bloquear: los métodos tradicionales basados en firma normalmente pueden hacerle frente.

Asimismo, un 29 % del malware se recopila en el marco de las "amenazas desconocidas". La lucha contra estas amenazas requiere herramientas más sofisticadas. Pero mediante el uso de métodos que van más allá del software antivirus estándar, como los análisis exhaustivos y el marcado dinámico en lista blanca, también podemos luchar contra estas.

Luego está el restante 1 %. Las amenazas sofisticadas que son ataques polivalentes, continuados y dirigidos. Diseñados para introducirse en una red, merodear de forma invisible y recopilar datos confidenciales, una vez introducidos pueden pasar desapercibidos durante años.

Una APT conocida como "Darkhotel" utilizó el Wi-Fi en hoteles de lujo para robar los datos de los huéspedes durante siete años antes de que se descubriera. Esta fue una APT especialmente interesante, ya que tenía un objetivo muy específico (los altos ejecutivos y directores ejecutivos) e ilustraba de forma muy clara el reto que se presenta a la seguridad de IT cuando los endpoints (portátiles y tablets empresariales) operan fuera del perímetro de seguridad de la red de la empresa.

Una APT conocida como "Darkhotel" utilizó el Wi-Fi en hoteles de lujo para robar los datos de los huéspedes durante siete años antes de que se descubriera.

Aunque algunas empresas muy destacadas se han convertido en víctimas de APT, no es necesario ser objeto de la mirada pública para estar en el punto de mira de los cibercriminales. Las empresas deben ser capaces de mitigar el riesgo que suponen las APT y las consecuencias que podrían derivarse de un ataque, ya sea que la pérdida de datos, un prolongado periodo de inactividad o el daño a la reputación. Y como las APT operan de forma silenciosa y sigilosa, la prevención es, a largo plazo, mucho menos costosa que las acciones correctivas posteriores a un ataque (ya que el ataque se puede haber producido hace algún tiempo y haber hecho un daño incalculable durante meses o incluso años).

No existe una solución para este problema. Aunque son útiles, las tecnologías que utilizamos para luchar contra las amenazas conocidas y desconocidas no son las más adecuadas para luchar contra las APT por sí solas. Un panorama de amenazas cada vez más sofisticado y complejo exige un enfoque de seguridad en varios niveles en el que una combinación de tecnologías integradas proporciona detección y protección completas contra el malware conocido, desconocido y sofisticado, y otras amenazas.

Este informe está diseñado para ayudarle a estar mejor preparado para luchar contra las APT.

El promedio de costes de un incidente de malware es de 56 000 dólares para las pymes y de 649 000 dólares para las grandes empresas.[1]

Las APT pueden tener consecuencias muy graves. En 2014, Kaspersky Lab ayudó a descubrir el funcionamiento de Carbanak. Este complejo ataque permitió que un grupo internacional de criminales robara 1000 millones de dólares de varias instituciones financieras. Después de infectar la red de un banco, el grupo pudo registrar todo lo que sucedía en las pantallas de los empleados y aprender a transferir dinero sin ser detectado.

[1] El alto coste de una brecha en la seguridad, Kaspersky Lab.

LA GRAN EMPRESA ES UN OBJETIVO: 5 PUNTOS CLAVE

Como propietario de una empresa grande, es consciente de las amenazas de seguridad de IT a las que se enfrenta. Estas amenazas son cada vez más selectivas y sofisticadas.

1 El primer paso para crear una estrategia adecuada para hacer frente a las APT es entender que usted es un objetivo potencial. La verdad es que, tanto si se trata de propiedad intelectual, datos de contacto o información financiera, su empresa dispone de información que los criminales podrían aprovechar. Incluso si no son sus datos los que persiguen, pueden utilizar su red como una manera de llegar a sus partners o clientes (como fue el caso de Darkhotel).

2 En segundo lugar, necesitamos desarrollar una mayor concienciación sobre la vulnerabilidad. En las empresas en las que un gran número de empleados trabaja desde varios dispositivos, aplicaciones y plataformas, puede ser difícil mantenerse un paso por delante de todos los riesgos y posibles "vectores de ataque" que los cibercriminales pueden explotar. Las APT van dirigidas a las vulnerabilidades, humanas o técnicas, por lo que cuanto más grande y compleja sea una empresa, más puntos de entrada potenciales existirán.

3 El aumento de la adopción de las iniciativas BYOD y el horario flexible de trabajo solo aumentan la complejidad del reto. Además de ser vulnerables por sí mismos, los teléfonos y tablets se utilizan con frecuencia para conectarse a redes no seguras. Para empeorar las cosas aún más, a menudo es mucho más difícil saber si un dispositivo está infectado, especialmente aquellos con sistemas operativos como iOS de Apple. Una fuerza de trabajo móvil es como un objetivo en movimiento; los dispositivos que operan fuera del perímetro de seguridad son más difíciles de controlar, lo que convierte la seguridad para endpoints efectiva en un componente importante de su estrategia de seguridad.

4 Esta amplia variedad de endpoints, junto con el número de métodos que pueden utilizar los cibercriminales para infectar una red, se traduce en que las medidas de seguridad singulares por sí mismas no son suficientes. En cambio, las medidas de mitigación potentes necesitan combinar inteligencia de amenazas, políticas de seguridad y tecnología especializada que no solo bloqueen las amenazas entrantes reconocidas, sino que también reconozcan otras nuevas, a la vez que se utilizan medidas como el marcado en lista blanca para evitar la ejecución de amenazas aún desconocidas.

5 La mitigación necesita un enfoque renovado centrado en el endpoint. Los cibercriminales explotan las vulnerabilidades y lo más habitual es que el punto más débil de la empresa sean los endpoints, en los que la seguridad habitualmente se ve comprometida no solo por los dispositivos en sí, sino por el comportamiento negligente del empleado o los entornos carentes de seguridad en los que se utilizan. Si los endpoints no disponen de protección en varios niveles, toda la empresa puede verse en situación de riesgo.

¿POR QUÉ ES TAN IMPORTANTE LA MITIGACIÓN?

La mitigación es el punto en el que las empresas necesitan comenzar, y la prevención es mucho más eficaz y rentable que las acciones correctivas posteriores a un ataque.

Los actores de amenazas que desarrollan APT están altamente cualificados y decididos, y disponen de los recursos que necesitan. No obstante, al igual que todos los cibercriminales (con algunas notables excepciones), todavía encuentran atractivo el objetivo de menor resistencia. Por lo tanto, si bien no se puede garantizar la inmunidad ante las APT, existen medidas que puede aplicar para dificultar el éxito de un ataque.

Al igual que las APT a menudo son amenazas en varios niveles, una respuesta eficaz ante las APT también debe estar basada en un enfoque en varios niveles. Las herramientas de seguridad simples sencillamente no son suficientes.

¿Y en qué consiste este enfoque? La agencia Australian Signals Directorate ha desarrollado lo que Kaspersky Lab considera una lista ampliada y completa de las estrategias para mitigar las amenazas sofisticadas. Creemos que estas estrategias también se pueden aplicar a las empresas y son un buen punto de partida.

Estas estrategias se dividen en cuatro categorías principales:

1 POLÍTICAS DE SEGURIDAD Y FORMACIÓN

La seguridad de IT no depende solo de IT. Los errores humanos son una gran ayuda para los cibercriminales. Al ofrecer formación amplia y periódica sobre las cuestiones de seguridad, fomentar los comportamientos adecuados e implementar políticas pertinentes y realistas puede reducir la posibilidad de que los empleados introduzcan las ciberamenazas en su empresa.

2 SEGURIDAD DE LA RED

La estructura de la red puede ayudar en gran medida a reducir el impacto potencial de una infección. Existen varias estrategias de seguridad de la red que pueden reducir el riesgo y mitigar las amenazas; por ejemplo, la separación de determinadas partes de la red puede reducir el número de endpoints que pueden acceder a información confidencial, disminuyendo exponencialmente su nivel de riesgo.

3 ADMINISTRACIÓN DE SISTEMAS

El control y, por supuesto, la restricción de los privilegios de administración del usuario mediante políticas de seguridad pueden reducir considerablemente el número de vulnerabilidades que debe tratar. Y, por encima de todo, el aprovechamiento de las funciones de seguridad incorporadas en los programas que utiliza marca una gran diferencia. La desactivación de las funciones innecesarias implica que puede aprovechar al máximo el software a la vez que cierra las vías que podrían explotarse.

La desactivación de la ejecución de código Java en el navegador es un gran ejemplo de cómo puede eliminar vulnerabilidades de los recursos que utilizan sus empleados.

4 SOLUCIONES DE SEGURIDAD ESPECIALIZADAS

Además de estas medidas, las funciones específicas de software especializado pueden agregar niveles de protección incalculables. No obstante, la integración de soluciones no tiene que implicar una gran inversión o cientos de horas de trabajo de los empleados. De hecho, las tres soluciones de seguridad especializadas que se muestran a continuación, junto con la restricción de derechos de administración (consulte la estrategia de administración de sistemas descrita anteriormente), mitigan aproximadamente el 85 % de las amenazas a la seguridad. Las tres principales soluciones de seguridad especializadas son las siguientes:

- Uso del control de aplicaciones, el marcado en lista blanca y el modo de denegaciones predeterminadas
- Aplicación de parches a las aplicaciones que habitualmente reciben ataques
- Aplicación de parches a las vulnerabilidades de los sistemas operativos

PRINCIPALES ESTRATEGIAS DE MITIGACIÓN

Existen varias estrategias de mitigación que cualquier empresa ya debería estar aplicando o, por lo menos, tener en cuenta.

CONTROL DE APLICACIONES Y MARCADO EN LISTA BLANCA

El marcado en lista blanca es una potente herramienta que puede mitigar considerablemente las APT y otros ataques. En lugar de preguntar si una aplicación puede ser perjudicial, el marcado en lista blanca pregunta si estamos seguros de que el elemento es legítimo. Esto pone el control en manos del administrador, independientemente del comportamiento de los usuarios. Se crea una lista blanca de aplicaciones conocidas y fiables, y solo se permite la ejecución de las aplicaciones incluidas en esta lista. El malware se manifiesta a menudo como un archivo ejecutable de algún tipo, que con este enfoque se bloqueará y no podrá ejecutarse. Este es el enfoque opuesto al de las "listas negras" de antivirus tradicionales, que solo evitan que una aplicación se inicie si aparece en una lista de "delincuentes conocidos".

Llevado a su extremo más seguro, los administradores pueden configurar un escenario de "denegaciones predeterminadas" por el que solo se ejecutarán las aplicaciones que los administradores hayan aprobado previamente, lo que limita drásticamente la exposición. Aunque esta es una manera eficaz de mantener el malware fuera de la red, necesita garantizar que no está bloqueando herramientas que sus compañeros realmente necesitan utilizar para trabajar con más eficacia. Con el uso de un control más detallado en las aplicaciones y el marcado dinámico en lista blanca, dispondrá de más herramientas de control. Puede bloquear o controlar el uso de aplicaciones por categoría de software, unidad de negocio, usuarios individuales y otros factores.

Por supuesto, antes de poder utilizar el marcado en lista blanca eficazmente, es necesario que sepa cuáles son las aplicaciones que ya se están ejecutando en sus equipos. Por lo tanto, la realización de un inventario es fundamental. Después de todo, no puede controlar algo si no sabe que está presente.

FUNCIÓN DE KASPERSKY LAB: CONTROL DE APLICACIONES CON MARCADO DINÁMICO EN LISTA BLANCA

La base de datos de aplicaciones legítimas con marcado en lista blanca de Kaspersky Lab ya contiene bastante más de mil millones de elementos e incluye el 97,5 % de todo el software relacionado con el sector empresarial. Nuestro módulo Kaspersky Security Network actualiza constantemente en la nube nuestra inteligencia continua frente a amenazas.

Nuestro control de aplicaciones va más allá de la simple funcionalidad de "detención/inicio". Cuando una aplicación debe bloquearse, permitimos que todos los componentes sin modificar del sistema operativo se ejecuten de forma normal. Esto significa que puede poner fin a los ataques sin interrumpir las actividades de los usuarios. Kaspersky Lab también facilita en gran medida la implementación de un modo de denegaciones predeterminadas ya que proporcionamos un modo de prueba para ayudarle a ver de antemano si habrá complicaciones cuando se apliquen.

FUNCIONES DE KASPERSKY LAB: VALORACIÓN DE LAS VULNERABILIDADES Y GESTIÓN DE PARCHES

La base de datos que utiliza nuestra tecnología para detectar vulnerabilidades es muy amplia: Kaspersky Endpoint Protection for Business buscará e instalará automáticamente las actualizaciones de Microsoft, así como las actualizaciones (renovaciones) de las aplicaciones que no son de Microsoft. Esto significa que puede mantener actualizados todos los sistemas operativos y aplicaciones sin necesidad de tener que dedicar las valiosas horas de trabajo de los empleados.

"En el modo de denegaciones predeterminadas, solo los programas fiables se pueden ejecutar en el ordenador y le puedo garantizar que la inmensa mayoría del malware utilizado en los ataques de APT proviene de aplicaciones no fiables o a las que no se han aplicado los parches adecuados".

Costin Raiu, director del equipo de análisis e investigación global, Kaspersky Lab.

APLICACIÓN DE PARCHES A LAS VULNERABILIDADES DE LAS APLICACIONES Y LOS SISTEMAS OPERATIVOS

Tanto las aplicaciones como los sistemas operativos presentan vulnerabilidades que los criminales pueden explotar. Es importante estar al tanto de estas brechas de seguridad y cerrarlas antes de que código malicioso se introduzca por ellas. Además, son las aplicaciones más populares las que a menudo presentan vulnerabilidades cuando no se les han aplicado los parches adecuados.

Las herramientas de gestión de parches son fundamentales para la seguridad de IT en varios niveles, ya que pueden automatizar la tarea de mantener actualizadas las aplicaciones en numerosos endpoints. Como resultado, puede asegurarse de que los puntos potenciales de entrada para un ataque se cierran tan pronto como sea posible.

Una vez más hay que destacar que no hay métodos infalibles para protegerse de las APT.

No obstante, si se implementa correctamente, una combinación de estas cuatro estrategias (privilegios de administración, control de aplicaciones, gestión de parches y gestión de sistemas operativos) puede proteger contra el 85 % de los incidentes relacionados con ataques dirigidos. Juntas dificultan la ejecución u actividad no detectada de código malicioso porque activan varias líneas de defensa.

En 2014, las vulnerabilidades en Oracle Java, los navegadores más populares y Adobe Reader representaron el 92 % de exploits de malware.[2]

[2] Boletín de seguridad de Kaspersky 2014, Kaspersky Lab

OTRAS ESTRATEGIAS ALTAMENTE EFICACES

Como hemos afirmado al principio de este documento, la ciberseguridad no es un juego de números. Aunque puede protegerse contra la mayoría de las intrusiones mediante las estrategias de mitigación que ya hemos repasado anteriormente, necesita para ir un poco más allá.

A continuación se indican algunas otras técnicas que puede utilizar para añadir niveles de defensa adicionales:

MITIGACIÓN DE EXPLOITS DEL SISTEMA OPERATIVO

Aunque las tecnologías nativas pueden ayudarle mucho a la hora de mitigar los exploits genéricos en los sistemas operativos, las soluciones especializadas pueden hacer todavía más. Y hay un motivo de peso para ello. Por ejemplo, incluso si aplica parches constantemente a las aplicaciones y los sistemas operativos, aún está potencialmente desprotegido contra un ataque que utiliza una vulnerabilidad de día cero.

FUNCIÓN DE KASPERSKY LAB: PREVENCIÓN AUTOMÁTICA CONTRA EXPLOITS (AEP)

La prevención automática contra exploits (AEP, del inglés "Automatic Exploit Prevention") lleva a cabo una serie de comprobaciones de seguridad y presta especial atención a los programas que normalmente son objetivo de ataques, como Internet Explorer, Microsoft Office y Adobe Reader. Supervisa continuamente los procesos de la memoria y es capaz de discernir patrones de comportamiento sospechoso característicos de los exploits, que son muchos menos en comparación con la cantidad de exploits que existen. Este enfoque permite que la AEP de Kaspersky Lab detenga incluso los ataques de día cero.[3]

[3] Según una prueba independiente de MRG Effitas, la AEP fue capaz de proteger los endpoints probados contra los ataques basados en exploits en el 95 % de las pruebas con todos los demás mecanismos de defensa desactivados.

Por eso es tan importante disponer de una solución que detecte y neutralice las amenazas conocidas, pero que también detecte anomalías y comportamientos sospechosos, protegiéndole así de las amenazas desconocidas. De esta manera, incluso puede defenderse contra los ataques completamente nuevos.

PREVENCIÓN DE INTRUSIONES BASADO EN HOST

Como se ha demostrado, las APT son malware sigiloso y pueden permanecer ocultas durante meses e incluso años. Por lo tanto, un perímetro de defensa no es suficiente: ¿qué ocurre si ya hay código malicioso al acecho dentro de su empresa? Lo que se necesita es una tecnología que reconozca y evite las actividades del programa que son "demasiado arriesgadas", incluso si no son exactamente maliciosas. Los sistemas de prevención de intrusiones basados en host (HIPS, del inglés "Host-based Intrusion Prevention systems") restringen las actividades de las aplicaciones dentro del sistema en función de su nivel de fiabilidad. HIPS detecta "anomalías de ejecución", esto es, aplicaciones que realizan funciones o actividades que están fuera de contexto y también sugerir la existencia de riesgo. La mejor manera de conseguirlo es inmediatamente después de la instalación de las aplicaciones (es decir, antes de que un sigiloso ataque de malware las pueda dañar).

FUNCIÓN DE KASPERSKY LAB: SUPERVISOR DEL SISTEMA Y CONTROL DE PRIVILEGIOS EN LAS APLICACIONES

Con estas dos funciones, los eventos que se producen en sus sistemas informáticos se pueden supervisar y registrar, garantizando así que las aplicaciones no intentan llevar a cabo acciones maliciosas. El supervisor del sistema y su subsistema de restauración pueden deshacer los cambios no deseados, y el control de privilegios en las aplicaciones evita que estos cambios se produzcan si los han iniciado aplicaciones con un bajo nivel de confianza.

ANÁLISIS DINÁMICO DEL CONTENIDO DE LOS CORREOS ELECTRÓNICOS Y LAS PÁGINAS WEB

Al igual que un enfoque basado en firma no puede luchar contra los ataques de día cero, el uso de "análisis estáticos" tradicionales para comparar el contenido de los correos electrónicos y las páginas web con una base de datos de malware conocido no puede protegerle contra las nuevas amenazas.

Este es el motivo por el que el análisis dinámico es tan importante. Necesita una solución que pueda buscar características sospechosas codificadas en páginas web y correos electrónicos, como que traten de buscar y modificar programas ejecutables, y bloquearlas antes de que se ejecuten.

Un ataque de "día cero" es aquel que tiene como objetivo una vulnerabilidad no reconocida previamente en un sistema operativo o una aplicación antes de que un parche esté disponible.

FUNCIONES DE KASPERSKY LAB: CONTROL WEB Y ANTIVIRUS WEB

Nuestra tecnología de control web le permite decidir si se permite a los usuarios acceder a sitios, tanto por categoría de usuarios individuales como por la clasificación del tipo de sitio web (por ejemplo, un sitio de apuestas, etc.). Mediante la supervisión del tráfico HTTP(S) puede asegurarse de que los recursos web a los que se accede a través de los endpoints coinciden con los elementos de la lista blanca.

Mientras tanto, nuestro antivirus web utiliza análisis dinámicos para detectar código malicioso distribuido por protocolos HTTP(S) y FTP, lo que se traduce en protección contra las APT que utilizan infecciones por descargas o descargas ocultas para introducirse en un sistema.

FUNCIÓN DE KASPERSKY LAB: ANTIVIRUS PARA EL CORREO ELECTRÓNICO Y SECURITY FOR MAIL SERVER

Mediante el uso de una combinación de análisis exhaustivos y análisis estáticos y dinámicos, Kaspersky Endpoint for Business ayuda a bloquear las amenazas transmitidas por correo electrónico. Al emular cómo podrían comportarse los archivos adjuntos, nuestra tecnología puede detectar en los archivos adjuntos de correos exploits que se basen en archivos.

Kaspersky Security for Mail Server, con su opción de prevención de pérdidas de datos (DLP, del inglés "Data Loss Prevention"), también puede detener la filtración de información importante. Haciendo que los archivos "no se puedan compartir", puede asegurarse de que esta información no sale de su empresa a través de archivos adjuntos de correo electrónico.

EL ENFOQUE DE KASPERSKY LAB: PROTECCIÓN EN VARIOS NIVELES

El panorama de amenazas a la seguridad es complejo y evoluciona rápidamente. En Kaspersky Lab, trabajamos con grandes empresas en una estrategia con un enfoque en varios niveles, desde la mitigación hasta los servicios de inteligencia sobre amenazas.

Como una empresa impulsada por la tecnología, hemos desarrollado las herramientas que necesita para crear una estrategia de mitigación completa. Y como todas ellas se han diseñado a partir de la misma base de código, se integran a la perfección, lo que le permite formular una estrategia de seguridad integral sin que haya brechas innecesarias en su sistema de protección.

El núcleo de nuestro enfoque lo componen nuestros galardonados firewall para los endpoints y tecnología antimalware. Juntas bloquean las amenazas **conocidas**, que representan el 70 %. Con herramientas más **avanzadas** como análisis del comportamiento, análisis exhaustivos, control de aplicaciones con marcado dinámico en lista blanca y control web, protegemos contra las amenazas **desconocidas**. Y para las amenazas sofisticadas añadimos otro nivel de protección para ayudarle mediante el uso de herramientas avanzadas como la prevención automática contra exploits de Kaspersky y el supervisor del sistema.

INTELIGENCIA Y DETECCIÓN PARA IDENTIFICAR RÁPIDAMENTE LOS ATAQUES "DIRECTOS"

A pesar de que un enfoque exhaustivo es fundamental para la mitigación, su estrategia contra APT también debería incluir medidas que garanticen que se puede detectar un ataque "directo" sin causar falsas alarmas que exijan mucho tiempo. Además, su estrategia debería incluir tecnologías que puedan bloquear un ataque rápidamente y minimizar el daño que su empresa pueda sufrir.

Nuestro enfoque recomendado incluye detección en los endpoints, detección en la red, tecnología sandbox inteligente y una amplia base de datos de eventos.

Recientemente, la detección en la red ha captado la imaginación de varios proveedores de IT, y muchos de ellos han diseñado dispositivos especializados para la detección en la red. No obstante, creemos que una solución alternativa que utiliza una arquitectura de sensores distribuidos puede ofrecer importantes ventajas. La colocación de sensores en puntos clave de la red que envíen datos a un punto central puede ayudar a mejorar la detección. Además, puede permitir una mayor escalabilidad y ayudar a reducir los costes cuando se deben proteger complejas redes de nivel empresarial.

MÁS ALLÁ DE LA TECNOLOGÍA: SERVICIOS DE INTELIGENCIA SOBRE AMENAZAS

Aunque la mitigación reducirá considerablemente los riesgos para cualquier empresa, no es posible que una solución de seguridad pueda garantizar el 100 % de protección.

Si el ataque tiene éxito, su empresa tendrá que determinar:

- Cuáles son los datos exactos que se han robado con el fin de que pueda tomar las medidas oportunas para limitar los daños ocasionados por la pérdida
- Cómo se activó el ataque, para que pueda solucionar las vulnerabilidades y brechas de seguridad específicas

Por eso es importante que disponga de los mejores recursos en análisis de ciencia forense, preparados para que pueda acceder rápidamente a la experiencia en seguridad necesaria.

Kaspersky Lab ofrece una amplia variedad de servicios de inteligencia, y puede elegir el nivel de servicio que mejor se adapte a su empresa:

- Análisis de malware, para los clientes que dispongan de su propio equipo de ciencia forense
- Servicios de ciencia forense digital, incluido el análisis de malware
- Servicios de respuesta completos ante incidentes, incluida la ciencia forense

¿POR QUÉ KASPERSKY LAB?

Kaspersky Lab es una de las empresas que están a la vanguardia de la lucha contra las APT. Nuestro equipo de análisis e investigación global (GReAT, del inglés "Global Research and Analysis Team") ha participado en el descubrimiento de muchas de las amenazas más peligrosas y complejas del mundo, desde Octubre Rojo a "Equation Group", la herramienta de ciberespionaje recientemente descubierta.

Desafortunadamente para los cibercriminales, la escala no es un gran problema. Una vez desarrolladas las ciberarmas avanzadas, los demás grupos de criminales no tardan mucho en volver a configurarlas para atacar objetivos empresariales. Eso quiere decir que incluso las armas que se hayan desarrollado secretamente a cambio de grandes costes por parte de los países pueden terminar en manos de bandas criminales.

Lo reconocemos. Este es el motivo por el que estamos moviendo ficha para que haya un equilibrio en el campo de juego. Utilizamos la información recopilada de las investigaciones de las APT para asesorar a los gobiernos sobre cómo defenderse de los ciberataques. Pero no nos detenemos aquí. Utilizamos todo lo que aprendemos de nuestro trabajo como creadores de soluciones que sean eficaces y prácticas a nivel empresarial.

Con este objetivo, combinamos nuestra inigualable inteligencia de seguridad con la innovación tecnológica. Tenemos una proporción bastante mayor de nuestros empleados trabajando en investigación y desarrollo en comparación con cualquiera de nuestros competidores.

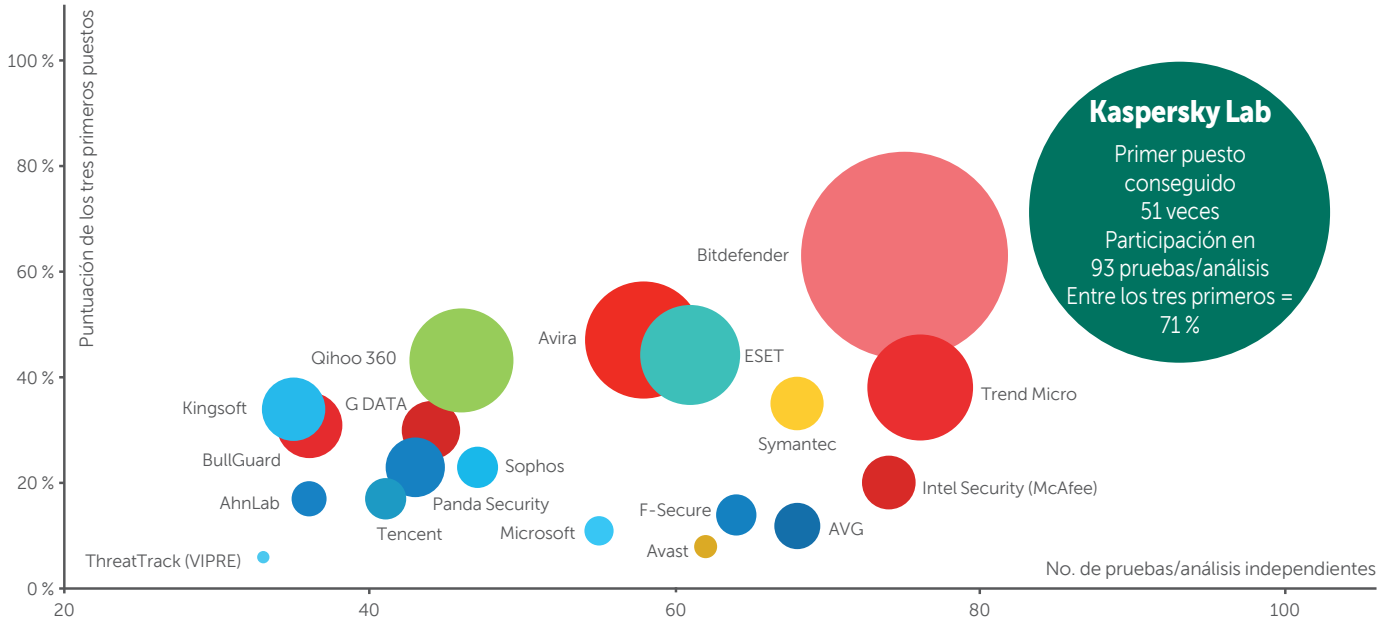
El resultado es un enfoque en varios niveles para la seguridad empresarial, que puede contribuir a formar los pilares para cualquier empresa que desee diseñar una estrategia de mitigación contra APT.

Nuestra confianza en nuestras soluciones nos ha llevado a participar en más pruebas independientes que cualquier otro proveedor. Hemos alcanzado índices de detección de malware de más del 99 % y, de las 93 pruebas independientes en las que participamos en 2014, obtuvimos uno de los tres primeros puestos en 66 y el primer puesto en 51[4]. Ninguno de nuestros competidores se acerca siquiera a estos resultados. La tecnología de Kaspersky Lab también se utiliza y cuenta con la confianza de más de 130 partners de OEM, por lo que hoy en día ya podría estar utilizando Kaspersky Lab.

[4] http://media.kaspersky.com/en/business-security/TOP3_2014.pdf

KASPERSKY LAB: LA MEJOR PROTECCIÓN DEL SECTOR*

Durante 2014, los productos de Kaspersky Lab participaron en 93 pruebas y revisiones independientes. Nuestros productos acabaron en 51 primeros puestos y 66 veces entre los tres primeros.



*Notas:
Según los resultados sintéticos de una prueba independiente realizada en 2014 para productos dirigidos a empresas, consumidores y dispositivos móviles.

El resumen incluye pruebas realizadas por los siguientes laboratorios y revistas independientes:
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin.
El tamaño de la burbuja representa el número de primeros puestos obtenidos.

PROTEGEMOS EL PRESENTE PARA ASEGURAR EL FUTURO

Un panorama de amenazas cada vez más sofisticado y complejo exige una plataforma de seguridad en varios niveles que proteja contra amenazas conocidas, desconocidas y sofisticadas.

Visite **kaspersky.com/enterprise** para obtener más información sobre la experiencia exclusiva de Kaspersky Lab y Security Solutions for Enterprise.

MÁS INFORMACIÓN

ÚNASE A LA CONVERSACIÓN

#EnterpriseSec

Véanos en YouTube

Síganos en Facebook

Síganos en Twitter

Únase a nosotros en LinkedIn

Revise nuestro blog

Únase a nosotros en Threatpost

Véanos en Securelist

ACERCA DE KASPERSKY LAB

Kaspersky Lab es el mayor proveedor privado de soluciones de protección de endpoints del mundo. La empresa figura entre los cuatro proveedores principales de soluciones de seguridad para usuarios de endpoints.* A lo largo de sus más de 17 años de historia, Kaspersky Lab se ha mantenido como una empresa innovadora en seguridad de IT y suministra eficaces soluciones de seguridad digitales para grandes empresas, pymes y particulares. Kaspersky Lab, cuya sociedad de cartera está registrada en el Reino Unido, opera actualmente en casi 200 países y territorios de todo el mundo, y brinda protección a más de 400 millones de usuarios en todo el mundo. Más información en www.kaspersky.es.

* La empresa logró el cuarto puesto en el índice de IDC de ingresos de seguridad para endpoints en todo el mundo por proveedor de 2013. Este índice se publicó en el informe de IDC "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (Previsión de seguridad mundial de endpoints 2014-2018 y acciones de los proveedores en 2013) (IDC núm. 250210, agosto de 2014). En el informe se clasifican los proveedores de software según los ingresos de ventas de soluciones de seguridad para endpoints en 2013.