SOLUCIONES DE SEGURIDAD FLEXIBLES PARA EMPRESAS

El panorama de amenazas actual era inimaginable hace una década. Los cibercriminales han adaptado sus técnicas para eludir las defensas tradicionales y acechan sin ser detectados en sistemas durante meses o incluso años. Ha llegado el momento de que la seguridad empresarial se adapte a esa situación con un enfoque inteligente a varios niveles en cuanto a la seguridad de IT.

"La inteligencia es la capacidad de adaptarse a los cambios."
– Stephen Hawking.

SOLUCIONES DE SEGURIDAD FLEXIBLES PARA EMPRESAS

Las amenazas persistentes avanzadas (APT), los ataques dirigidos y el malware sofisticado son solo algunas de las nuevas amenazas en constante evolución a las que la empresa debe hacer frente. Los cibercriminales son muy conscientes de las limitaciones de la seguridad tradicional basada en el perímetro: es su primera escala cuando buscan grietas en las defensas empresariales.

Si los atacantes cambian de forma constantemente, es justo decir que varias tecnologías empresariales proporcionan una adecuada red de vectores de ataque: los dispositivos móviles, las aplicaciones web, el almacenamiento portátil, la virtualización y las tecnologías basadas en la nube presentan una oportunidad para los cibercriminales a la que no puede dar respuesta la seguridad tradicional, basada en "impedir y bloquear".

Es necesario un nuevo enfoque integrado y más flexible basado en los pilares de la predicción, prevención, detección y respuesta.

LOS CUATRO PILARES DE LA SEGURIDAD EMPRESARIAL ADAPTABLE

Predicción: nadie tiene una bola de cristal, pero las empresas con acceso a las últimas tendencias e inteligencia de amenazas están en mejor posición para anticiparse a los incidentes y evitarlos. La formación de los empleados para reconocer las tácticas utilizadas en los ataques aumenta el análisis predictivo, igual que la capacidad de aprender de los errores mediante un análisis forense de las brechas; las pruebas de penetración, por su parte, pueden ayudar a destapar puntos débiles.

Prevención: un objetivo fundamental es reducir la superficie de los ataques (ya sea con antimalware tradicional basado en firmas, con controles de dispositivo o por medio de parches de vulnerabilidades de las aplicaciones). El fortalecimiento de los sistemas y la interposición de tantos obstáculos en el camino de los atacantes como sea posible son tan solo dos componentes de un enfoque integral que incluye limitar la capacidad de los ataques de propagarse y reducir su impacto.

Detección: como demuestran las investigaciones realizadas por Kaspersky Lab en APT de alto perfil, los ataques sofisticados pueden pasar desapercibidos durante años. Se calcula que un ataque empresarial medio pasa desapercibido durante más de 200 días[1]; cuanto antes se descubra un incidente, tanto mejor. Las tecnologías de detección respaldadas por el mejor análisis de amenazas aumentan la detección: a medida que evoluciona el ritmo de las amenazas, la mejor estrategia de detección se basa a menudo en la capacidad de detectar comportamientos y secuencias de eventos que indican que se ha producido una brecha.

Respuesta: la seguridad empresarial eficaz tiene la capacidad de responder a los efectos de una brecha y mitigarlos. En un nivel, eso puede implicar una política de tipo condicional para los procedimientos que puedan automatizarse, como los parches. En otro nivel, podría incluir análisis posteriores a la detección de brechas o el uso de equipos de respuesta a incidentes especializados para detener, mitigar e investigar ataques, brechas y otros incidentes de seguridad.

Para ser eficaces, esas capacidades deben funcionar juntas como un sistema con varios niveles. Basada en inteligencia, centrada en las amenazas, integrada, integral y estratégica: estas son las características principales de una completa arquitectura de seguridad empresarial adaptable. Kaspersky Lab ocupa una posición única para ofrecer una plataforma de seguridad empresarial adaptable. Echemos un vistazo a algunos de sus elementos.

[1] https://www.siliconrepublic.com/enterprise/2014/04/11/advanced-cyberattacks-can-go-undetected-for-typically-229-days

SEGURIDAD EMPRESARIAL. BASADA EN INTELIGENCIA.

Kaspersky Lab acumula una larga trayectoria en el descubrimiento de algunas de las amenazas más importantes y de más alto perfil, incluidas:

- Carbanak: el ciberrobo bancario más grande del mundo
- Dark Hotel: dirigido específicamente a viajeros de negocios de alto standing
- The Mask/Careto: dirigido a empresas, gobiernos y empresas de capital privado, entre otros
- Wild Neutron: dirigido a corporaciones internacionales y otras empresas
- Icefog: atacó la cadena de suministro de empresas
- Red October: exploit de sistemas empresariales para realizar operaciones de vigilancia en masa

Más de un tercio de nuestros empleados trabaja en investigación y desarrollo y se centra exclusivamente en el desarrollo de tecnologías para combatir y anticiparse a las amenazas en constante evolución que los equipos especializados de investigadores de inteligencia y análisis de Kaspersky Lab analizan a diario.

Los conocimientos de Kaspersky Lab sobre el funcionamiento interno de algunas de las amenazas más sofisticadas del mundo nos han permitido desarrollar una cartera de servicios y tecnologías de seguridad estratégicos y en varios niveles capaces de ofrecer un enfoque totalmente integrado y adaptable en cuanto a la seguridad. Con nuestra experiencia, Kaspersky Lab ha conseguido más primeros puestos en pruebas independientes de detección y mitigación de amenazas que cualquier otra empresa de seguridad de IT.

PREDICCIÓN

Las capacidades de predicción y las estrategias de mitigación que resultan de ellas son fundamentales en todas las actividades de Kaspersky Lab, desde nuestro equipo especializado en análisis e investigación global (GReAT) hasta Kaspersky Security Network (KSN) y nuestra cartera Security Intelligence Services (SIS):

Kaspersky Security Network: uno de los componentes más importantes de la plataforma en varios niveles de Kaspersky Lab, Kaspersky Security Network es una arquitectura distribuida y compleja basada en la nube que se dedica a la recopilación y análisis de inteligencia de amenazas de seguridad en millones de sistemas en todo el mundo.

Kaspersky Security Network es un eficaz laboratorio global de amenazas en la nube que detecta, analiza y gestiona las amenazas y las fuentes de ataques online desconocidas o avanzadas en cuestión de segundos, y distribuye dicha inteligencia directamente a los sistemas del cliente. Para empresas con preocupaciones muy concretas sobre la privacidad de datos, Kaspersky Lab ha desarrollado una opción denominada Kaspersky Private Security Network.

Security Intelligence Services: pocas empresas cuentan con los recursos necesarios para desarrollar los altos niveles de inteligencia de seguridad estratégica requeridos para seguir el ritmo de las amenazas sofisticadas en constante evolución. Por ese motivo, Kaspersky Lab ha desarrollado una amplia cartera de servicios de inteligencia.

Educación y formación: desde principios básicos generales de ciberseguridad hasta técnicas forenses digitales avanzadas, análisis de malware y formación sobre ingeniería inversa, Kaspersky Lab ofrece amplios programas de formación y sensibilización para empresas, tanto in situ como online. Además de juegos interactivos, evaluaciones de conocimientos y promoción general de la ciberseguridad, también ofrecemos cursos de dos a cinco jornadas de duración, incluidos algunos de los siguientes temas:

- **Principios básicos de la ciberseguridad:** entender las amenazas y utilizar la tecnología de manera segura.
- **Ciencia forense digital general:** crear un laboratorio de análisis forense digital, reconstrucción de incidencias, herramientas.
- **Análisis general de malware e ingeniería inversa:** crear un entorno seguro de análisis de malware, realizar análisis urgentes.
- **Ciencia forense digital avanzada:** análisis detallados del sistema de archivos, recuperación de archivos eliminados, reconstrucción de la escala de tiempo de los incidentes.
- **Análisis avanzado de malware e ingeniería inversa:** análisis del shellcode de exploits, malware no Windows, uso de mejores prácticas globales.

Evaluación de la seguridad:

- **Pruebas de penetración:** comprensión de la infraestructura de seguridad desde el punto de vista del atacante y cumplimiento de estándares de seguridad como PCI DSS.
- **Pruebas de seguridad de aplicaciones:** análisis de aplicaciones web (incluidas la banca online y aplicaciones web con WAF activado), aplicaciones móviles, clientes pesados

Inteligencia frente a amenazas:

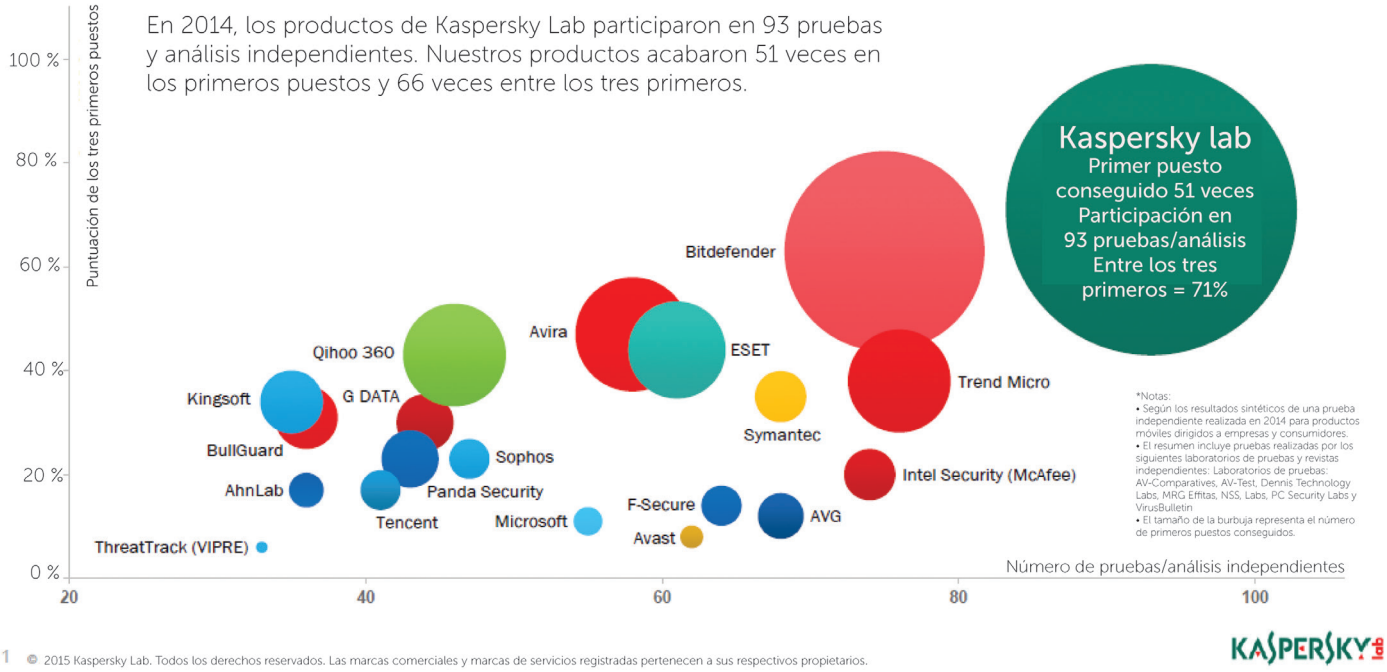
- Un sistema de alerta anticipada, impulsado por los conocimientos especializados del equipo GReAT y respaldado por KSN, que incluye fuentes de datos de amenazas, seguimiento de botnets e informes de inteligencia. El acceso temprano a archivos de configuración relacionados con APT y muestras de malware, junto con la integración con SIEM (HP Arcsight), ayudan a las empresas a desarrollar completos datos de inteligencia.

PREVENCIÓN

Kaspersky Lab detecta 325 000 nuevos elementos de malware *cada día*. Incluso un solo punto porcentual en los índices de detección puede traducirse en la detección de cientos de miles de elementos de malware. Los resultados de pruebas independientes demuestran consistentemente que Kaspersky Lab ofrece la mejor protección del sector. Tan solo en 2014, participamos en 93 pruebas y análisis independientes, en los que conseguimos el primer puesto 51 veces y uno de los tres primeros puestos un 71 % de las veces.[2] Esta es solo una de las razones por las que los OEM, incluidos Microsoft, Cisco Meraki, Juniper Networks y Alcatel Lucent, confían en Kaspersky Lab para proporcionar la seguridad que incluyen en sus propios productos.

[2] Para obtener información más detallada sobre las pruebas y las métricas, visite: http://media.kaspersky.com/en/business-security/TOP3_2013.pdf
El nuevo enlace del informe actualizado es: http://media.kaspersky.com/en/business-security/TOP3_2014.pdf.

KASPERSKY LAB OFRECE LA MEJOR PROTECCIÓN DEL SECTOR*



Nuestra cartera de seguridad empresarial combina antimalware líder del sector con varias tecnologías para reducir las superficies de ataque en una combinación única de tecnologías centradas en la inteligencia.

Las amenazas conocidas, desconocidas y avanzadas pueden evitarse gracias al uso de varios niveles de protección, incluidos:

Network Attack Blocker: analiza todo el tráfico de la red mediante el uso de firmas conocidas para detectar y bloquear ataques basados en la red, incluidos ataques de análisis de puertos y de denegación de servicio (DoS). Para disponer de un nivel de protección adicional, Kaspersky DDoS Protection (KDP) está disponible como una solución para protegerse contra los ataques de denegación de servicio distribuidos (DDoS). Es una solución completa e integrada de prevención y mitigación de DDoS, que incluye análisis las 24 horas del día e informes posteriores a los ataques.

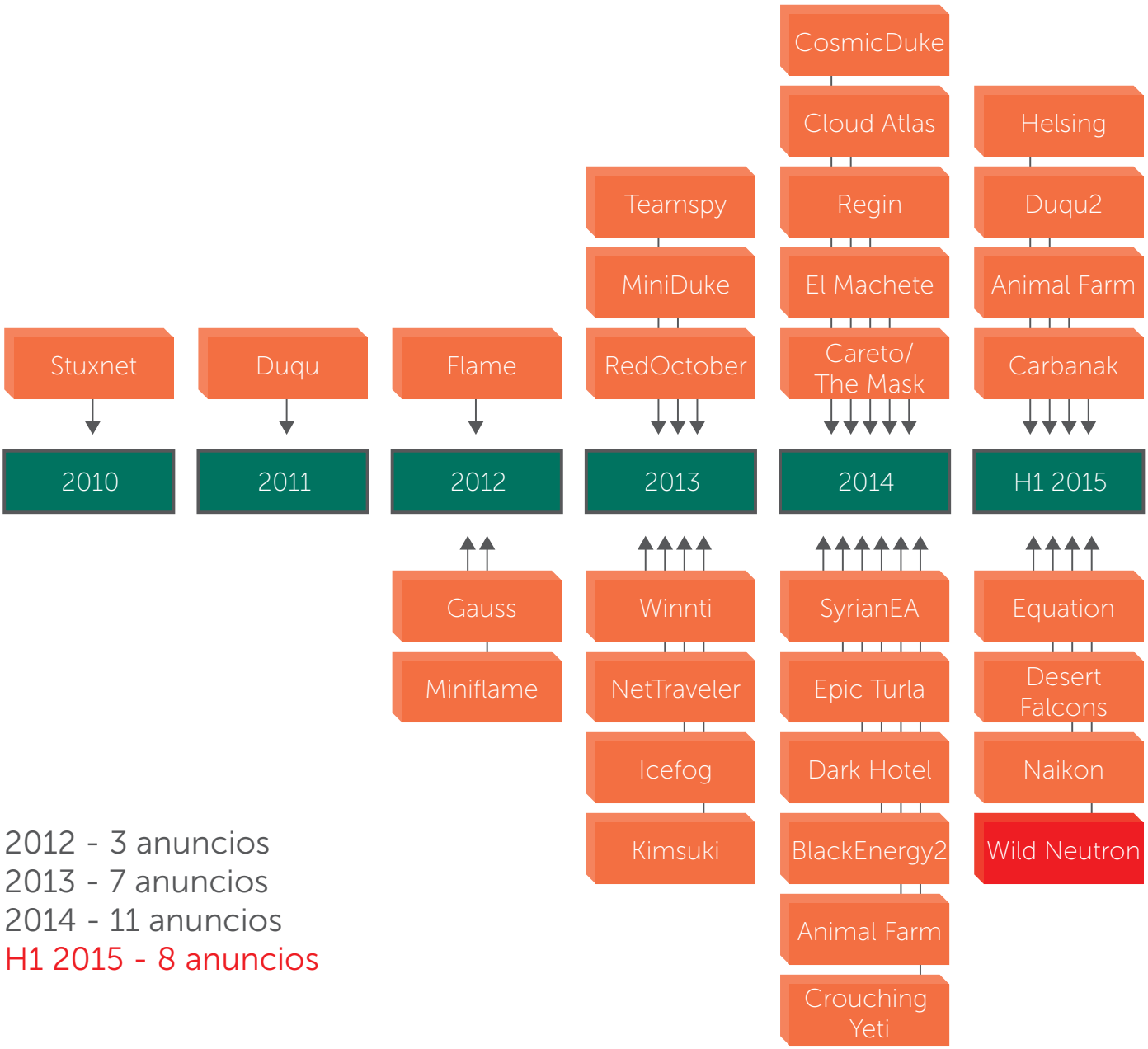
Antiphishing exhaustivo: capaz de prevenir algunas de las últimas técnicas de ataque de phishing gracias a la búsqueda de pruebas adicionales de actividad sospechosa, con una eficacia mucho mejor que los enfoques tradicionales en cuanto al phishing, basados en bases de datos. Control de aplicaciones y marcado dinámico en lista blanca: El control de aplicaciones bloquea o autoriza el uso de las aplicaciones especificadas por el administrador. Se basa en el marcado dinámico en lista blanca, las listas constantemente actualizadas de categorías de software y aplicaciones de confianza de Kaspersky Lab.

Sistema de prevención de intrusiones basado en host (HIPS): ayuda a controlar el comportamiento de las aplicaciones y restringe la ejecución de programas potencialmente peligrosos sin afectar al rendimiento de las aplicaciones seguras y autorizadas.

DETECCIÓN

La incomparable experiencia de Kaspersky Lab en la detección de algunas de las amenazas más sofisticadas del mundo influye directamente en nuestras capacidades de detección de amenazas empresariales. Desde 2008, nuestros investigadores han descubierto algunos de los más sofisticados ataques multicomponente del mundo. Estos conocimientos e inteligencia se aprovechan en el desarrollo de nuestros productos; además de nuestra capacidad para detectar sofisticados ataques centrados en la empresa, Kaspersky Lab ha utilizado los conocimientos adquiridos a partir de la detección de importantes actores en las amenazas financieras, como Carbanak, para desarrollar soluciones orientadas exclusivamente a la detección del fraude financiero.

ANUNCIOS DE APT DE KASPERSKY LAB



2012 - 3 anuncios
2013 - 7 anuncios
2014 - 11 anuncios
H1 2015 - 8 anuncios

RESPUESTA

En una arquitectura de seguridad adaptable, la capacidad de respuesta a las amenazas es tan importante como la capacidad de predecirlas y evitarlas, y supone un ahorro de tiempo y dinero para las empresas. También hay que tener en cuenta que una consecuencia directa de la mejora de la detección será la optimización de la capacidad de respuesta. Kaspersky Lab aborda estas cuestiones tanto en el nivel tecnológico como en el nivel de servicios:

Supervisor del sistema: el monitor exclusivo y proactivo de Kaspersky Lab es capaz de reaccionar a eventos del sistema complejos, como la instalación de controladores y la detección de comportamientos sospechosos.

Servicios de investigación: resuelva los incidentes de seguridad en vivo con ayuda de Kaspersky Lab. Desde análisis de malware hasta análisis forense digital, informes y respuesta ante incidentes, los clientes pueden aprender de los incidentes y, a la vez, mitigar el impacto de un ataque y restablecer los sistemas dañados.

SEGURIDAD EMPRESARIAL PROACTIVA, REACTIVA E IMPULSADA POR LA INTELIGENCIA

Decir que el malware se ha expandido parece un eufemismo: las amenazas avanzadas eluden las técnicas de bloqueo tradicionales, se puede comprar kits de malware listos para usar online por muy poco dinero y las herramientas capaces de crear automáticamente diversas variantes personalizadas a partir de una sola pieza de malware son solo la punta de un enorme iceberg de malware.

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 centradas en las empresas.

La incomparable trayectoria de Kaspersky Lab a la hora de descubrir las amenazas más sofisticadas e importantes, junto con sus tecnologías y servicios líderes del sector colocan a la empresa en una posición única para ofrecer la seguridad completa y adaptable que necesitan las empresas. Mientras que Kaspersky Security Network se alimenta de la inteligencia en tiempo real generada por más de 60 millones de nodos en todo el mundo, nuestro equipo de análisis e investigación global de élite aporta un conjunto único de habilidades y experiencia a nuestra investigación sobre amenazas, y desarrolla soluciones capaces de combatir amenazas cada vez más complejas y sofisticadas.

PARTNER DE CONFIANZA DE EMPRESAS, GOBIERNOS Y ORGANISMOS REGULADORES

Como es una empresa privada, Kaspersky Lab tiene absoluta libertad para realizar importantes inversiones en investigación y desarrollo lejos de las restricciones del mercado a corto plazo. Casi la mitad de nuestros 3000 empleados a nivel mundial trabajan en nuestros laboratorios de investigación y desarrollo, y se centran en el desarrollo de tecnologías innovadoras, la investigación de ciberguerras, ciberespionaje y todos los tipos de amenazas y técnicas.

Este enfoque de I+D interno de alta calidad ha llevado a que Kaspersky Lab se reconozca como un líder en el sector en lo que se refiere a tecnologías de seguridad de IT. Esta es solo una de las razones por las que más de 100 grandes OEM, incluidos Microsoft, Cisco Meraki, IBM, Juniper Networks y Alcatel Lucent, confían en Kaspersky Lab para proporcionar la seguridad que incluyen en sus propios productos.

Por esa razón también somos partner de confianza de gobiernos, cuerpos de seguridad y grandes empresas de todo el mundo. Respetadas organizaciones internacionales, incluidos la INTERPOL, Europol y numerosos CERTS, han invitado a Kaspersky Lab a mantener una colaboración y un asesoramiento con ellos de forma regular; además de realizar cursos de formación periódicos para la INTERPOL, prestamos asistencia en el lanzamiento del Laboratorio de ciencia forense digital de la INTERPOL.


Twitter.com/
kasperskyes


Facebook.com/
kasperskyes


Youtube.com/
Kasperskyespana

Kaspersky Lab, Moscú, Rusia
www.kaspersky.es

Todo sobre la seguridad en Internet:
www.viruslist.com/sp

Encuentra un partner próximo:
www.kaspersky.com/buyoffline

KASPERSKY lab