Protección inteligente contra ataques avanzados

KASPERSKY lab

¿Te avisamos del próximo IT Digital Security?

Protección inteligente contra ataques avanzados

Los ataques dirigidos y las amenazas avanzadas, incluidas las APTs, son algunos de los riesgos más peligrosos para las empresas, y sin embargo pocas están preparadas para hacerles frente. Y es que a pesar de que las amenazas y las técnicas que utilizan los cibercriminales cambian, muchas empresas siguen basando su seguridad en enfoques tradicionales.

Las amenazas avanzadas y especialmente dirigidas pueden pasar desapercibidas durante semanas, meses e incluso años. Tiempo aprovechado por los ciberdelincuentes para adentrarse en los sistemas y causar un daño que a menudo es irreparable. El famoso Shadow IT, la incontrolada conectividad del IoT, confianza extrema en la digitalización, una visión demasiado optimista de la seguridad perimetral, falta de visibilidad, empleados poco concienciados con la seguridad, software desactualizado e incluso falta de profesionales son algunos de los factores que contribuyen al éxito de los ataques dirigidos

Podría parecer que, sabiendo cómo se producen los ataques, su detección pudiera ser más fácil. La realidad, por supuesto, es más complicada, y por

Anatomía de un ataque dirigido

Los ataques dirigidos son procesos a largo plazo que pueden comprometer la seguridad y dan acceso a los atacantes el control de los sistemas TI de la víctima. Aunque algunos ataques utilicen APTs –muy efectivas, pero costosas de implementar—, otros pueden usar técnicas mucho más sencillas como malware avanzado o exploits de día cero.

En teoría, la cadena de un ataque dirigido parece bastante sencilla: Reconocimiento & Testing, Penetración, Propagación, Ejecución y Resultado. Esto podría dar a entender que bloquear de forma automática las primeras fases de un ataque podría ser suficiente para neutralizarlo.

Pero, en realidad, los ataques dirigidos son muy sofisticados y no lineales, en términos de progresión y ejecución. Así, las funcionalidades de detección automática, monitorización continua y "threat hunting" deben ser parte de una estrategia en varias etapas.

Un ataque dirigido es un proceso lento que viola la seguridad y permite al cibercriminal evitar los procesos de autorización e interactuar con la infraestructura TI; es decir, "esquivando" las tradicionales medidas de detección.

En primer lugar, hay que ver estos ataques como proyectos en constante evolución más que como una acción maliciosa única. Según nuestra experiencia en la monitorización de ataques globales, este tipo de operaciones duran al menos 100 días e incluso años para agencias gubernamentales, grandes empresas e infraestructuras críticas.

En segundo lugar, el proceso de estos ataques suele centrarse en determinadas infraestructuras y está diseñado para acabar con ciertos mecanismos de seguridad e incluso pueden inicialmente dirigirse a determinados empleados a través del email o incluso de las redes sociales. En el caso de los ataques dirigidos, la metodología y las fases se construyen alrededor de una víctima específica.

En tercer lugar, la operación es gestionada por un grupo organizado o grupo de profesionales, a veces internacional, armados con las herramientas más sofisticadas. Sus actividades van más allá de un proceso y podrían definirse como una operación de combate.

eso las capacidades de detección, monitorización continua y caza de amenazas se han convertido en elementos imprescindibles en una estrategia de defensa.

Así, la seguridad perimetral es insufiente para hacer frente a un ataque dirigido y avanzado. Y también lo es el uso de soluciones independientes. Se requiere la detección de múltiples eventos que están ocurriendo en todos los niveles de la infraestructura empresarial, y que esa información sea procesada por un sistema capaz de analizar múltiples capas, e interpretada por una solución que aplique inteligencia de seguridad en tiempo real.

> Las grandes empresas están respondiendo a las amenazas avanzadas adoptando soluciones de gestión de seguridad de la información centralizadas

En otras palabras, la mejor inversión es un enfoque que integre lo mejor de muchas tecnologías. A lo que hay que sumar la necesidad de expertos, porque una estrategia de seguridad efectiva exige no sólo de una continua monitorización y capacidad

Protección inteligente contra ataques avanzados

Kaspersky Threat Management and Defense reúne y refuerza varias soluciones de la compañía para proteger a las empresas de las amenazas complejas

de detección, sino una respuesta rápida y cualificada, con un adecuado proceso forense.

Mejorando los procesos de seguridad de las empresas

El departamento de seguridad es responsable de la protección de los procesos de negocio de la información críticos. Esto incluye, por ejemplo, la adopción de soluciones automatizadas y componentes de software y la transición a la gestión digital de documentos.

El crecimiento del número de amenazas avanzadas y de los ataques dirigidos ha generado también un aumento del número de soluciones disponibles. Con el fin de recopilar, almacenar y procesar los datos generados de forma desestructurada, los procesos actuales han de actualizarse y redefinirse. Esto incluye:

- Priorización manual de las amenazas y la evaluación de los factores que potencialmente pueden referirse a un ataque dirigido
- Recopilación de información acerca de ataques dirigidos y estadísticas de amenazas avanzadas
- Identificación de una respuesta ante incidentes
- Análisis de objetos sospechosos en el tráfico de red y archivos adjuntos en los emails
- Detección de actividad inusual dentro de la infraestructura protegida

Las grandes empresas están respondiendo a las amenazas avanzadas pasando a una gestión centralizada de la seguridad, una consolidación de los datos de diferentes soluciones de segu-

Protección inteligente contra ataques avanzados

Los ciberataques se han convertido en operaciones de gran alcance, programados por fases y en los que se tiene en cuenta tanto las infraestructuras como las personas

ridad a través de la recopilación automática de datos y la correlación de eventos –SIEM y unificando su presentación con centros de monitorización (SOC).

Pero, este enfoque, para ser efectivo contra ataques dirigidos y amenazas avanzadas, necesita de una comprensión de los problemas de seguridad y un profundo conocimiento y análisis de las ciberamenazas.

Un marco adaptativo de seguridad

Prevenir, Detectar, Responder y Predecir son las cuatro áreas clave del ciclo de actividades de Kaspersky Lab. Un ciclo que asume que los sistemas de prevención tradicionales funcionan en conexión con las tecnologías de detección, analítica de amenazas, capacidades de respuesta y técnicas de seguridad predictiva.

Esencialmente, supone que los sistemas de prevención tradicional han de funcionar en coordinación con tecnologías de detección, analíticas de amenazas, capacidades de respuesta y técnicas de seguridad predictivas. Esto ayuda a crear un sistema de seguridad que constantemente se adapta y responde a los retos emergentes de las empresas. Implementar un enfoque de seguridad adaptativo reduce de forma significativa el riesgo de ataques y, obviamente, los daños.

Modelo de seguridad adaptable

Protección inteligente contra ataque avanzados

Kaspersky Threat Management and Defense
Kaspersky Threat Management and Defense utiliza una combinación única de tecnologías y servicios basada en la implementación de una estrategia de seguridad adaptativa, que permite:

- Prevenir y reducir el número de amenazas avanzadas y ataques dirigidos
- Detectar e identificar las actividades sospechosas (ataques dirigidos)
- Responder, reducir las brechas de seguridad e investigar los ataques
- Predecir dónde y cómo se producirán los próximos ataques

Prevención – tecnologías para reducir el riesgo de ataques

Durante un ataque dirigido, las tecnologías de seguridad convencionales basadas en la prevención pueden detectar algunos incidentes, pero generalmente no pueden determinar si los incidentes individuales son parte de un ataque mucho más peligroso y complejo. Aún así, las tecnologías multicapa basadas en la prevención siguen siendo un elemento clave en el nuevo enfoque proactivo para protegerse contra los ataques dirigidos.

KASPERSKY ENTERPRISE CYBERSECURITY

CLICAR PARA VER EL VÍDEO

Y es esencial para las empresas continuar utilizando tecnologías de seguridad tradicional para automatizar el filtrado y bloqueo de eventos e incidentes, lo que ayuda a evitar distracciones innecesarias y centrarse en la búsqueda de incidentes relevantes. Además, refuerza la infraestructura contra técnicas fáciles de ejecutar, como pueden ser de ingeniería social o email con malware. De hecho, toda la inversión basada en seguridad perimetral y endpoint, junto con los controles implementados, ayuda a incrementar la cantidad de esfuerzo e inversión que tienen que llevar a cabo los ciberdelincuentes para penetrar en la red.

Detección – detectar la amenaza antes de que ocurra

Cuanto antes se detecte un ataque, menores serán las pérdidas financieras y el tiempo de interrupción

Prevenir, Detectar, Responder y Predecir son las cuatro áreas clave del ciclo de actividades de Kaspersky Lab

del negocio. De ahí la importancia de una adecuada tecnología de detección. Ya que los ataques dirigidos son complejos y compuestos, su detección exige un profundo conocimiento práctico sobre cómo funcionan estos ataques. Se necesitan tecnologías de detección capaces de acceder a los datos de inteligencia de amenazas en tiempo real, capaces de realizar análisis detallados de comportamientos sospechosos que pueden estar ocurriendo en diferentes niveles de la red.

Así, la habilidad para detectar ataques dirigidos pasa por soluciones y servicios conectados capaces de ofrecer:

- ***Formación***
- ***Experiencia en el descubrimiento de ataques dirigidos:*** *auditoría única de la infraestructura con el fin de encontrar rastros de compromiso.*
- ***Solución especializada,*** *como es la suma de la plataforma Kaspersky Anti Targeted Attack y Kaspersky Endpoint Detection and Response*
- ***Datos para el intercambio de información*** *sobre amenazas en tiempo real y actualizaciones sobre amenazas*
- ***Informes personalizados*** *para comprender mejor las fuentes y los métodos utilizados.*
- ***Threat Hunting***
- ***Servicios 24/7***

Respuesta – cómo recuperarse de un ataque

Como es lógico de poco vale la detección de una amenaza si no estamos en condiciones de responder a ella de manera ágil y al final consigue dañar la organización. Después de detectar un ataque es importante contar con expertos de seguridad con habilidades y experiencia que ayuden a evaluar y rectificar el daño, que sean capaces de recuperar rápidamente sus operaciones, recibir información inteligente de la acción a llevar a cabo después del proceso de investigación de incidentes, y que además sean capaces de planificar acciones que impidan que el ataque vuelva a repetirse.

Para evitar el mayor número de sorpresas desagradables en un incidente de ciberseguridad, es necesario desarrollar con antelación un proceso de respuesta ante ataques dirigidos y complejos. Y una de las herramientas que puede reforzar esta estrategia es un sistema de respuesta y detección endpoint (EDR) que aporta niveles adicionales de protección, tales como:

- ***Visibilidad y control.*** Las soluciones EDR permiten a los responsables de seguridad recopilar grandes cantidades de datos para un análisis detallado de todos los endpoints, pudiendo analizar de forma remota cualquier anomalía, eliminar o bloquear la amenaza y lanzar los procesos de recuperación. De este modo, disponen de un conocimiento de los incidentes que les permite priorizar y tomar de forma rápida cualquier respuesta.
- ***Normativa.*** Con la creciente dependencia del cloud y unas normativas cada vez más exigentes (GDPR, PCI DSS, etc.), las soluciones EDR pueden jugar un papel muy importante ya que permiten una monitorización constante y un registro de los incidentes de toda la red.
- ***Caza de amenazas.*** Una solución EDR efectiva

busca de forma proactiva evidencias de intrusiones –como indicadores de compromiso- en cualquier endpoint de la red en tiempo real. Con la automatización de las tareas clave de detección y respuesta, las soluciones EDR ayudan en el análisis y la gestión de incidentes.

- ***Procesan millones de alertas.*** Con el número de incidentes registrados por las soluciones de seguridad aumentando constantemente, las empresas necesitan encontrar un modo de verificar y analizar de forma más rápida y eficiente cualquier evento del que sus soluciones de seguridad les alerten. EDR ayuda a las empresas a validar y priorizar las alertas de seguridad más importantes y a adquirir mayor conocimiento de los métodos de ataque.
- ***Reducción de costes.*** Si la empresa puede detectar y remediar una intrusión antes de que el intruso cause algún daño o disrupción, es posible evitar cuantiosas pérdidas. La solución EDR ayuda a detectar y responder de forma rápida, limpiando los sistemas atacados y reduciendo el

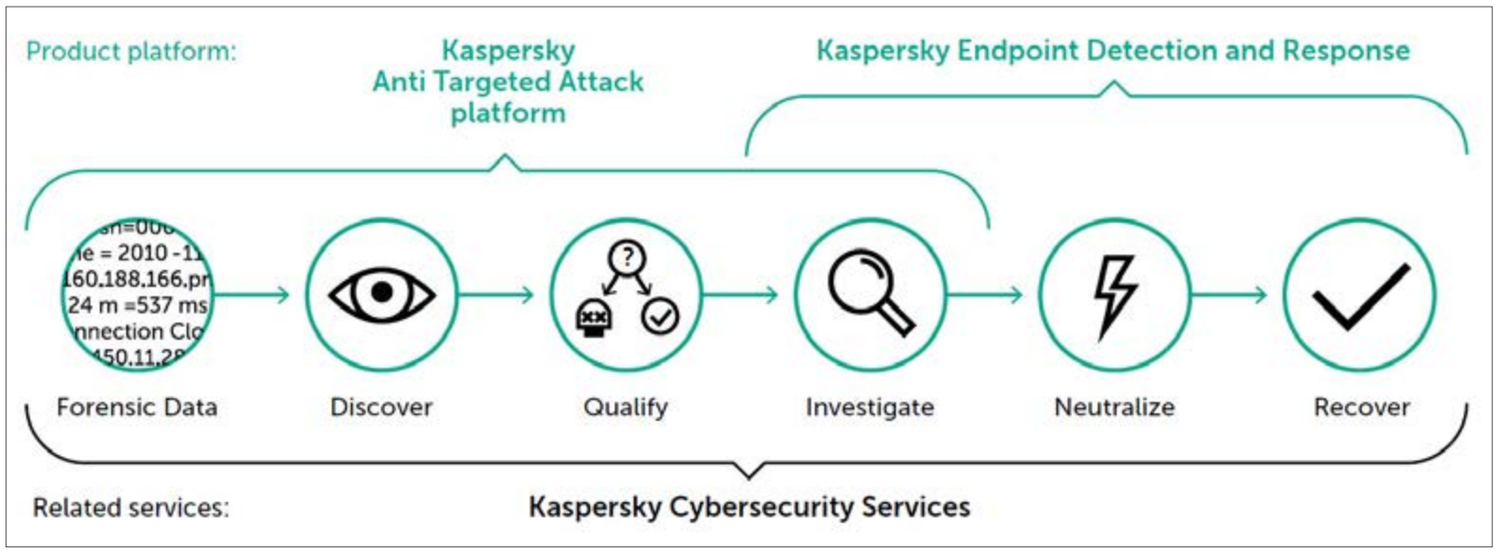
Kaspersky Endpoint Detection and Response

Contar con altos ratios de detección es solo una parte del proceso. La mejor tecnología de detección no sirve de mucho si no se cuenta con las herramientas y la experiencia necesaria para responder de forma rápida a las amenazas que están intentando penetrar en una empresa.

Kaspersky Endpoint Detection and Response proporciona:

- DETECCIÓN AVANZADA – que incluye aprendizaje automático, analizador de ataques dirigidos (Targeted Attack Analyzer -TAA-) y referencias del comportamiento de los endpoints. Todo ello, permite crear un histórico que puede utilizarse para descubrir cómo se producen las brechas.
- DETECCIÓN DE AMENAZAS PROACTIVA. Gracias a una base de datos centralizada – y a los Indicadores de Compromiso- es posible "cazar"y buscar proactivamente amenazas. Los endpoints son escaneados de forma proactiva para localizar cualquier anomalía y las brechas de seguridad.
- RESPUESTA ADAPTATIVA ANTE AMENAZAS que incluye una amplia gama de respuestas automáticas que ayudan a las empresas a evitar los procesos tradicionales de remediación –como la eliminación y "reimagine", que pueden resultar en costoso periodos de inactividad y pérdida de productividad.

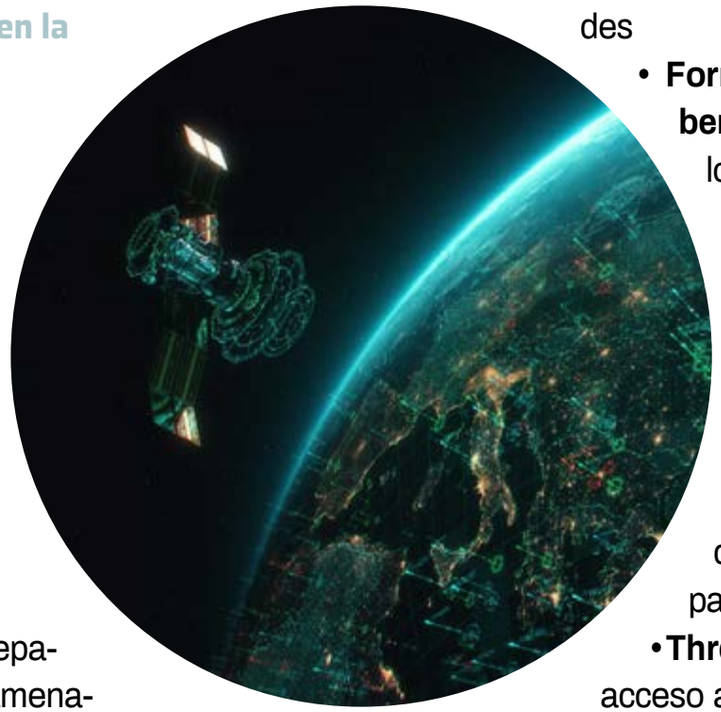
Una visibilidad completa y una detección precisa son solo una parte de esta "lucha". La propia naturaleza de los ataques dirigidos significa que los atacantes disponen siempre de nuevas técnicas y herramientas. Si ocurre una emergencia, el equipo de ciberseguridad necesita contar con un partner de confianza con la experiencia y habilidades necesarias.



Protección inteligente contra ataques avanzados

coste de gestión de un incidente y el tiempo de inactividad.

Predicción – un paso más en la protección del futuro



La constante evolución de los ataques obliga a una constante revisión de la estrategia de seguridad que tenga en cuenta las últimas amenazas. Tener acceso a expertos que estén al tanto de lo que corre, que sean capaces de probar los sistemas y las defensas, es vital para que las empresas estén preparadas frente a las nuevas amenazas.

Desde hace años, el equipo de expertos de Kaspersky Lab ha acumulado una experiencia y amplios conocimientos acerca de los ataques avanzados y dirigidos y de cómo funcionan. De hecho, están analizando constantemente nuevas técnicas de ataque. Esta enorme y valiosa experiencia "sitúa" a Kaspersky Lab en una posición privilegiada para predecir nuevos métodos de ataque y ayudar a las empresas a prepararse para combatirlas. Además, la compañía, ofrece servicios especializados para "robustecer" su infraestructura TI.

Entre estos servicios de Kaspersky Lab, se incluyen:

- **Test de penetración** para evaluar la eficacia de su actual seguridad
- **Application Security Assessment Services** – para ayudar en la búsqueda de vulnerabilidades
- **Formación avanzada en Ciberseguridad** para formar a los expertos de la compañía y ayudarles a implementar su propio SOC (Security Operation Center)
- **Informes de Inteligencia e Informes personalizados de Amenazas** para mantenerse al tanto y de forma constante acerca del panorama de amenazas.
- **Threat Lookup Portal,** con acceso a la base de datos global de inteligencia de Kaspersky Lab.

Con el actual panorama de amenazas, la estrategia de seguridad ha de evolucionar constantemente para responder a los nuevos retos. No ha de considerarse un estado, sino un proceso en continua evolución y desarrollo para evaluar las últimas amenazas y la efectividad de la seguridad de una empresa

Y todo ello, con el fin de poder adaptarse a los nuevos riesgos y demandas.

Enlaces de interés...

W Kaspersky Endpoint Detection and Response

W Guía de soluciones de detección y respuesta en endpoints para empresas 2018

Kaspersky Threat Management and Defense supone:

1.- Adoptar un modelo proactivo basado en la gestión del riesgo, monitorización continua, respuestas más eficaces y capacidades de detección de amenazas (threat hunting)

2. La infraestructura operacional optimiza los procesos diarios de seguridad y acelera la eficacia a través de un modelo multicapa que previene y detecta amenazas avanzadas en cada estadio del ataque.

3. Una plataforma integrada permite reducir las alertas de seguridad -que en muchas ocasiones sobrecargan al equipo -, proporcionando un contexto basado en inteligencia y una priorización de alertas que mejoran las tácticas de respuesta.

4. Visibilidad unificada de todos los estadios del ataque, permitiendo a los equipos de seguridad llevar a cabo análisis de amenazas más concretos y una investigación más fiable de los ataques, tanto conocidos como desconocidos, antes de lleguen a impactar en la empresa.

5. Acceso a la Inteligencia de Kaspersky Lab (Global Threat Intelligence), a través de diferentes portales. Este acceso aporta una visión única y proactiva de los motivos e intenciones de los atacantes, de forma que es posible priorizar y planificar las políticas e inversiones de seguridad.