Informe técnico

Cómo hacer frente al proceso de ataque completo: antes, durante y después

Es hora de un nuevo modelo de seguridad

El panorama de amenazas de la actualidad no se asemeja para nada al de solo 10 años atrás. Los ataques poco sofisticados que provocaban daños controlables han dado paso a operaciones de crimen online modernas que presentan una mayor sofisticación, fondos suficientes y la capacidad de ocasionar una interrupción considerable en las organizaciones y las infraestructuras nacionales. No se trata solo de que estos ataques avanzados sean difíciles de detectar, sino que permanecen en las redes durante largos periodos y acumulan recursos de red para efectuar ataques en cualquier otro lugar.

Los sistemas de defensa tradicionales que basan la protección exclusivamente en la detección y el bloqueo ya no son adecuados. Es hora de un nuevo modelo de seguridad que haga frente al proceso de ataque completo: antes, durante y después.

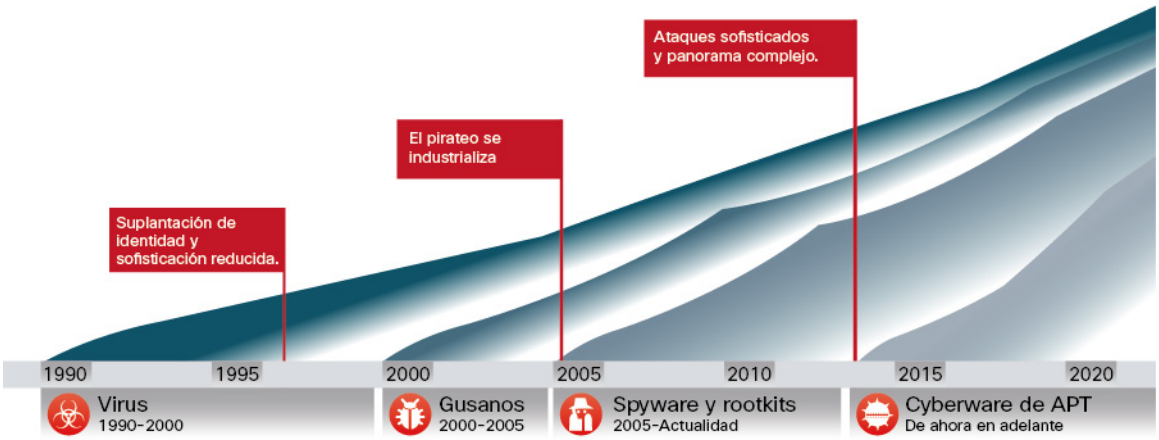
La industrialización del pirateo

Los primeros virus para PC aparecieron hace más de 25 años. Poco podíamos imaginarnos entonces que era solo el principio de lo que acabaría convirtiéndose en la "industrialización del pirateo".

Durante unos 10 años, los virus fueron el principal método de ataque, pero se mantuvieron a raya a lo largo del tiempo gracias a la gran capacidad de los sistemas de defensa para bloquearlos y protegerse de ellos. Alentados por la notoriedad y el conocimiento obtenido a partir del descubrimiento y la publicación de nuevas vulnerabilidades, los atacantes continuaron innovando. Como resultado, se generaron distintos ciclos de amenazas, una especie de “carrera armamentística”, por así decirlo. Aproximadamente, cada cinco años los atacantes lanzan nuevos tipos de amenazas: desde macrovirus hasta gusanos, pasando por spyware y rootkits. Por ello, los responsables de la seguridad deben innovar rápidamente para proteger las redes frente a estas amenazas.

No nos sorprende el hecho de que estos ciclos coincidan con los principales cambios tecnológicos que plantearon nuevos vectores de ataque (consulte la figura 1). Los primeros virus se centraban principalmente en el sistema operativo y se distribuían mediante ‘sneakernet’ (transferencia de información electrónica). Los virus de macro se aprovecharon de los usuarios que compartían archivos. Las amenazas de tipo gusano que se desplazaban de un equipo a otro hicieron uso de redes empresariales y del aumento de la actividad de Internet. El spyware y los rootkits llegaron con las nuevas aplicaciones, los nuevos dispositivos y las comunidades online. Actualmente, nos enfrentamos a malware avanzado, ataques selectivos y amenazas persistentes avanzadas (APT). Lo que separa esta época de las anteriores son las motivaciones y las herramientas que subyacen a los ataques, que los hacen especialmente difíciles de detectar, comprender y detener.

Figura 1. La industrialización del pirateo



La industrialización del pirateo está dando lugar a una economía criminal más rápida, efectiva y eficiente que se aprovecha de los ataques a nuestra infraestructura de TI. El intercambio organizado de vulnerabilidades es un negocio floreciente y lucrativo, donde el mercado abierto propicia el paso de la vulneración al robo, a la obstrucción y a la destrucción. Y, como los ciberdelincuentes se han dado cuenta de que pueden ganar bastante dinero con esto, su trabajo se ha convertido en un proceso más estandarizado, mecanizado y dirigido. Los atacantes conocen el carácter estático de las tecnologías de seguridad clásicas y sus implementaciones dispares, por lo que pueden explotar las lagunas de seguridad y las vulnerabilidades que generan. Incluso es habitual que los grupos de hackers sigan los procesos de desarrollo de software, por ejemplo, las pruebas de calidad y garantía o las pruebas de laboratorio a las que se someten las tecnologías de seguridad antes de su lanzamiento, para asegurarse de que podrán seguir esquivando todas las protecciones habituales.

Ahora también hay incentivos financieros significativos para actuar con sigilo, por lo que muchos grupos de “hackers activistas” optan por lanzar ataques que darán como resultado ganancias económicas o políticas con pocas posibilidades de que se impongan penas o se formulen acusaciones. Los nuevos métodos (como las aplicaciones que saltan entre puertos y protocolos, la tunelación cifrada, los troyanos "droppers", las amenazas de diversa índole y las técnicas que usan la ingeniería social y los ataques de día cero) han hecho que sea más fácil, rápido y barato para los hackers acceder a las redes, y que sea más difícil para los responsables de la seguridad detectarlos y evitar sus acciones. Con un carácter muy esquivo, los ataques pueden cambiar rápidamente a medida que avanzan por la empresa buscando una posición persistente y datos críticos de los que apoderarse.

Reto "cualquiera a cualquiera"

Las redes modernas ampliadas y sus componentes evolucionan constantemente, a la vez que generan nuevos vectores de ataque. Entre ellos, se incluyen los dispositivos móviles, las aplicaciones móviles y habilitadas para Web, los hipervisores, las redes sociales, los navegadores web y los equipos integrados, así como una proliferación de dispositivos y servicios que apenas atisbamos a intuir como consecuencia de la tendencia "Internet of Everything". Las personas están dentro y fuera de la red, usan cualquier dispositivo, acceden a cualquier aplicación y usan nubes muy diferentes. Esta ubicuidad es lo que denominamos “reto cualquiera a cualquiera”. Aunque estas dinámicas han mejorado nuestras comunicaciones, también han supuesto un aumento de los puntos de entrada y de los métodos que los hackers usan para acceder. Por desgracia, la forma que tienen muchas organizaciones de concebir la seguridad no ha evolucionado al mismo ritmo.

La mayoría de las organizaciones asegura que amplía las redes usando tecnologías dispares que no funcionan juntas. También es posible que recurran en exceso a los proveedores de servicios buscando seguridad en la nube y a las empresas de alojamiento para proteger la infraestructura de Internet. En esta nueva realidad, los administradores de seguridad suelen tener poca visibilidad y escaso control sobre los dispositivos y las aplicaciones que acceden a la red corporativa. Además, su capacidad es limitada a la hora de estar a la altura de las nuevas amenazas.

Nuevas dinámicas de seguridad

A la hora de enfrentarse con la combinación de ataques avanzados y la infraestructura "cualquiera a cualquiera", los profesionales de la seguridad se plantean a sí mismos estas tres importantes cuestiones:

1. *Con los nuevos modelos de negocio y los nuevos vectores de ataque, ¿cómo podemos mantener la seguridad y garantizar el cumplimiento normativo al mismo tiempo que nuestro entorno de TI continúa cambiando?* Las organizaciones que efectúan su transición a la nube, la virtualización o los dispositivos móviles para disfrutar de la productividad, la agilidad y la eficiencia que ofrecen estas tecnologías deben implementar una infraestructura de seguridad acorde con estos deseos.
2. *En un entorno con amenazas en constante evolución, ¿cómo podemos mejorar nuestra capacidad para protegernos continuamente frente a nuevos vectores de ataque y a amenazas cada vez más sofisticadas?* Los atacantes no discriminan: su objetivo es buscar el eslabón más débil de la cadena, sea cual sea. Inexorablemente dirigen sus ataques al objetivo. Con frecuencia, utilizan herramientas que se han desarrollado específicamente para evadir la infraestructura de seguridad del objetivo elegido. Hacen todo lo posible por pasar desapercibidos usando tecnologías y métodos que generan unos indicios prácticamente imperceptibles para no verse comprometidos.
3. *¿Cómo podemos resolver las dos primeras preguntas y, a la vez, reducir la complejidad y la fragmentación de las soluciones de seguridad?* Las organizaciones no pueden permitirse que haya lagunas en la protección que los sofisticados atacantes de hoy en día puedan aprovechar. Al mismo tiempo, el hecho de añadir complejidad con soluciones de seguridad dispares que no están integradas no generará los niveles de protección que exigen las amenazas avanzadas.

> *"El 100% de las empresas tienen conexiones con dominios que son sitios conocidos de amenazas de malware".*
>
> -Informe anual de seguridad de Cisco para 2014

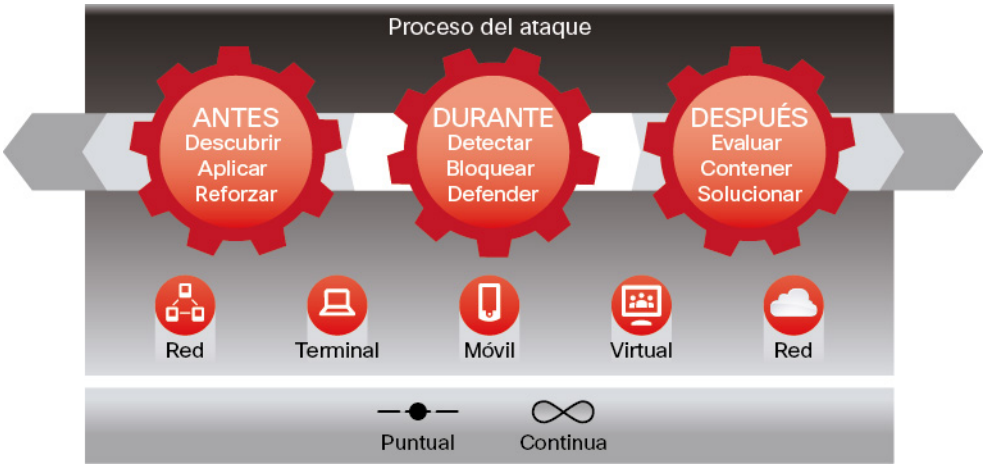
La combinación de estas dinámicas (que han cambiado los modelos de negocio, han generado un entorno de amenazas cambiantes y han provocado un aumento de la fragmentación y la complejidad de la seguridad) ha dado lugar a lagunas de seguridad, ha roto el ciclo de vida de la seguridad, ha reducido la visibilidad y ha planteado nuevos retos para administrar la seguridad. Para proteger realmente las organizaciones frente a estas dinámicas, es necesario cambiar el planteamiento que tenemos en torno a la seguridad. Ha llegado el momento de crear un nuevo modelo de seguridad basado en las amenazas.

Cómo hacer frente al proceso de ataque completo: antes, durante y después

Casi todas las herramientas de seguridad actuales se centran en proporcionar visibilidad en la red y bloquear el malware en el punto de entrada. Analizan los archivos una vez en un punto temporal inicial para determinar si son malintencionados. Pero los ataques avanzados no se producen en un único punto temporal, sino que van evolucionando y requieren una supervisión continua. Los piratas informáticos ahora emplean tácticas como el salto de puertos, el encapsulamiento, los ataques de día cero, la evasión y detección de las actividades de comando y control (C&C), las técnicas de suspensión, el movimiento lateral, el tráfico cifrado, las amenazas combinadas y la evasión en sandbox para eludir la detección inicial. Si el archivo no se detecta (o si evoluciona y se convierte en malintencionado después de entrar en el entorno), las tecnologías de detección de punto temporal dejan de ser útiles para identificar las actividades del atacante que se van desarrollando poco a poco.

Los métodos de seguridad no pueden centrarse solo en la detección, sino que deben incluir la capacidad de reducir el impacto una vez que el atacante ha entrado. Las organizaciones deben concebir su modelo de seguridad de forma holística, además de tener visibilidad y control sobre la red extendida y el proceso de ataque completo: antes de que se produzca un ataque, durante el tiempo que está en curso e incluso después de que comience a dañar el sistema o a robar la información (consulte la figura 2).

Figura 2. El nuevo modelo de seguridad



- **Antes:** los responsables de la seguridad necesitan una visibilidad y una visión global de lo que hay en la red ampliada con objeto de implementar políticas y controles para defenderla.
- **Durante:** la capacidad para detectar y bloquear de forma continua el malware es fundamental.
- **Después:** los responsables de la seguridad necesitan seguridad retrospectiva para marginalizar el impacto de un ataque. Deben identificar el punto de entrada, determinar el ámbito, contener la amenaza, eliminar el riesgo de que se vuelva a repetir la infección y solucionar la interrupción.

Antes de que se produzca un ataque

Para hacer frente a los atacantes con identificación del contexto, se requiere una seguridad con identificación del entorno. Las organizaciones luchan contra atacantes que tienen más información sobre la infraestructura que los propios responsables de la seguridad que tratan de protegerla. Para poder organizar la defensa antes de que se produzca un ataque, las organizaciones necesitan una visibilidad total del entorno, incluidos, aunque sin limitarse a ellos, los hosts virtuales y físicos, los sistemas operativos, las aplicaciones, los servicios, los protocolos, los usuarios, el contenido y el comportamiento de la red, con la esperanza de conseguir una superioridad informativa sobre los atacantes. Los responsables de la seguridad deben comprender los riesgos de su infraestructura en función de su valor como objetivo, la legitimidad de un ataque y su historial. Si no conocen aquello que están intentando proteger, no estarán suficientemente preparados para configurar las tecnologías de seguridad que los defenderán. La visibilidad debe expandirse por toda la red, desde los terminales, el correo electrónico, los gateways web y los entornos virtuales hasta los dispositivos móviles, pasando por el Data Center. Una vez conseguida esta visibilidad, se deben generar alertas que permitan efectuar acciones, de forma que los responsables de la seguridad puedan tomar decisiones bien fundamentadas.

Durante un ataque

Los implacables ataques no se producen en un único punto en el tiempo, sino que se trata de una actividad continua que exige una seguridad continua. Las tecnologías de seguridad tradicionales solo pueden detectar un ataque en un punto temporal basándose en un único punto de datos del propio ataque. Este enfoque no resulta adecuado para los ataques avanzados. En su lugar, se necesita una infraestructura de seguridad basada en el concepto de la detección; uno que pueda agregar y relacionar datos procedentes de la red extendida con patrones históricos e inteligencia de ataques globales para ofrecer contexto y poder distinguir ataques activos, fuga de datos y reconocimiento del simple ruido de fondo. De esta manera, la seguridad deja de ser un ejercicio en un punto temporal y se convierte en un análisis continuo y un proceso de toma de decisiones. Si un archivo que se consideraba seguro consigue acceder y luego se demuestra que tiene un comportamiento malintencionado, las organizaciones pueden actuar al respecto. Con esta perspectiva en tiempo real, los profesionales de la seguridad pueden emplear la automatización inteligente para aplicar políticas de seguridad sin intervención manual.

Después de un ataque

Para hacer frente al proceso de ataque completo, las organizaciones necesitan seguridad retrospectiva. La seguridad retrospectiva plantea un reto de Big Data y unas exigencias que no todo el mundo es capaz de ofrecer. Con una infraestructura que puede recopilar y analizar los datos de forma continua para crear inteligencia de seguridad, los equipos responsables de la seguridad pueden identificar por medio de la automatización las indicaciones de riesgo, detectar malware suficientemente sofisticado como para alterar su comportamiento para evitar la detección y, finalmente, solucionar el problema. Los riesgos que pueden haber pasado desapercibidos hace semanas o meses se pueden identificar, evaluar, contener y solucionar.

Este modelo de seguridad centrado en las amenazas permite a las organizaciones hacer frente al proceso de ataque completo, a través de todos los vectores de ataque y responder en cualquier momento, a todas horas y en tiempo real.

Activación del nuevo modelo de seguridad

Para poder usar el nuevo modelo de seguridad, Cisco considera que las tecnologías de seguridad modernas deben cumplir estos tres imperativos estratégicos: deben tener la visibilidad como una de sus prioridades, deben centrarse en las amenazas y deben ser específicas para cada plataforma.

Basadas en la visibilidad: los administradores de la seguridad deben poder ver con precisión todo lo que sucede. Esta capacidad requiere una combinación de dimensión y profundidad (véase la figura 3). "Dimensión" hace referencia a tener la capacidad de ver y recopilar datos procedentes de todos los vectores de ataques potenciales en el fabric de red, los terminales, el correo electrónico, los gateways web, los dispositivos móviles, los entornos virtuales y la nube para obtener conocimientos sobre los entornos y las amenazas. "Profundidad" hace referencia a la capacidad de relacionar esta información, aplicar inteligencia para comprender el contexto, tomar decisiones mejor fundamentadas y realizar acciones manuales o automáticas.

Figura 3. Dimensión y profundidad

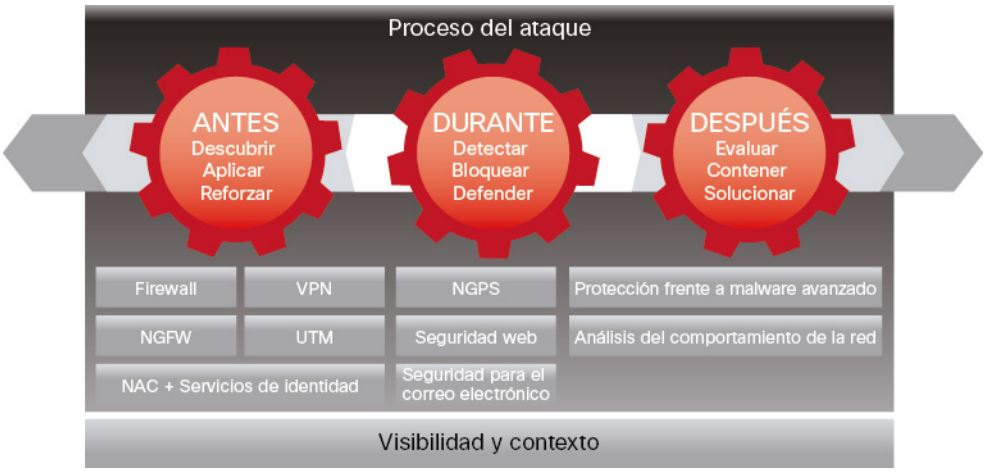
Centradas en las amenazas: las redes actuales se amplían hasta el lugar en que se encuentren los empleados, donde estén los datos y hasta el lugar desde el que se acceda a ellos. A pesar de los esfuerzos, mantenerse al día con esos vectores de ataque en constante cambio es un reto para los profesionales de la seguridad y una oportunidad para los atacantes. Las políticas y los controles son esenciales para reducir la superficie del área de ataque, pero las amenazas persisten. Como resultado, las tecnologías deben centrarse también en detectar, comprender y detener las amenazas. El hecho de centrarse en las amenazas significa ponerse en el lugar del atacante, aplicar visibilidad y contexto con objeto de comprender los cambios y adaptarse a ellos en el entorno y, a continuación, desarrollar protecciones y tomar medidas para detener las amenazas. El malware avanzado y los ataques de día cero exigen un proceso en curso que requiere análisis continuos e inteligencia de seguridad prestada en tiempo real desde la nube, la cual se debe compartir para mejorar la eficacia.

Específicas para cada plataforma: la seguridad no es ahora solo un problema de la red; sino que requiere un sistema integrado de plataformas abiertas y ágiles que proteja la red, los dispositivos y la nube. Estas plataformas deben ser extensibles, estar diseñadas para la escalabilidad y administrarse de manera centralizada para conseguir una política unificada y unos controles coherentes. En resumen, deben tener el mismo carácter ubicuo que los ataques a los que combaten. Esto supone dejar de implementar dispositivos de seguridad de punto único y pasar a integrar una verdadera plataforma de servicios y aplicaciones escalables y fáciles de implementar. Un enfoque basado en la plataforma no solo aumenta la efectividad de la seguridad y pone fin a los silos y las lagunas de seguridad que estos crean, sino que también acelera el tiempo de detección y optimiza la aplicación.

Cómo hacer frente al proceso de ataque completo

Para hacer frente a los retos de seguridad actuales y lograr una mejor protección, las organizaciones necesitan soluciones que abarquen el proceso de ataque completo y que estén diseñadas siguiendo principios como basarse en la visibilidad y estar centradas en las amenazas y la plataforma. Cisco ofrece una amplia cartera de soluciones de ciberseguridad basadas en las amenazas que abarcan todo el proceso de ataque.

Figura 4. Cómo hacer frente a todo el proceso de ataque



Estas soluciones específicas basadas en la plataforma ofrecen el conjunto más amplio de opciones de corrección y aplicación del sector en los vectores de ataque donde se manifiestan las amenazas. Estas soluciones funcionan juntas para ofrecer protección durante el proceso de ataque completo. Además, se pueden integrar en soluciones complementarias para conseguir un sistema de seguridad general.

- Antes de un ataque, las soluciones que incluyen firewalls, firewalls de última generación, control de acceso a la red y servicios de identidad, por nombrar algunos, ofrecen a los profesionales de la seguridad las herramientas que necesitan para descubrir las amenazas, además de aplicar y reforzar las políticas.
- Durante el ataque, las soluciones de seguridad web y del correo electrónico, junto con los sistemas de prevención de intrusiones de última generación, ofrecen la posibilidad de detectar y bloquear los ataques y defenderse de aquellos que hayan accedido a la red y ya estén en curso.
- Después de un ataque, las organizaciones pueden utilizar la protección frente a malware avanzada de Cisco y los análisis de comportamiento de red para evaluar de forma rápida y efectiva el alcance del ataque, contenerlo y solucionarlo para minimizar los daños.

Escalables como para usarlas en las organizaciones globales más grandes, estas soluciones están disponibles en la forma y en el momento en que las organizaciones las necesiten, como dispositivo virtual o físico o como servicios basados en la nube. Estas soluciones también se integran para ofrecer visibilidad continua y controles en toda la red ampliada y todos los vectores de ataque.

Conclusión

La industrialización del pirateo combinada con los "retos cualquiera a cualquiera" está cambiando profundamente la forma en que debemos proteger los sistemas, lo que nos lleva a plantearnos un nuevo enfoque de la seguridad cibernética. Las estrategias de seguridad que se centran en técnicas preventivas y defensas perimetrales dejarán libertad a los atacantes para que hagan todo lo que deseen una vez que estén dentro de la red.

El cambio de los modelos de negocio, el entorno de amenazas cambiantes y el aumento de la fragmentación y la complejidad de la seguridad han dado lugar a lagunas de seguridad, han roto el ciclo de vida de la seguridad, han reducido la visibilidad y han planteado nuevos retos para administrar la seguridad. Es hora de un nuevo modelo de seguridad basado en las amenazas que ofrezca a las organizaciones la visibilidad y el control que necesitan en la red ampliada y durante el proceso de ataque completo.

Cisco cuenta con una capacidad exclusiva para ofrecer un enfoque de seguridad centrado en las amenazas que reduzca la complejidad a la vez que proporciona una excelente visibilidad, un control continuo y una protección avanzada frente a las amenazas durante el proceso de ataque completo. Con este nuevo modelo de seguridad, las organizaciones pueden actuar de forma más rápida e inteligente antes de un ataque, durante su desarrollo y después de él.

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Amsterdam,
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax se encuentran en la Web de Cisco en **www.cisco.com/go/offices**.

Impreso en EE. UU. C11-731741-01 06/14