Scitum

NUEVAS TÉCNICAS DE PROTECCIÓN ANTE AMENAZAS AVANZADAS

TELMEX está contigo

NUEVAS TÉCNICAS DE PROTECCIÓN ANTE AMENAZAS AVANZADAS

PANORAMA ACTUAL

Los ataques recientemente sucedidos han aumentado la preocupación sobre temas de amenazas avanzadas, por mencionar algunos ocurridos últimamente:

- Millones de datos de tarjetas de crédito fueron robadas de las tiendas departamentales *Target*.
- La operación *DragonFly* comprometió sistemas de empresas de Estados Unidos, Francia, Italia y Alemania.
- El banco *JP Morgan* perdió gigabytes de información sensible de sus clientes durante un ciberataque.
- De forma muy similar a *Target*, la cadena de tiendas *Home Depot* reconoce el robo de información de 54 millones de tarjetas de crédito de sus clientes.

Nota: Para un mayor detalle sobre estos incidentes le recomendamos consultar nuestro *white paper* "¿Qué es la Ciberseguridad?".

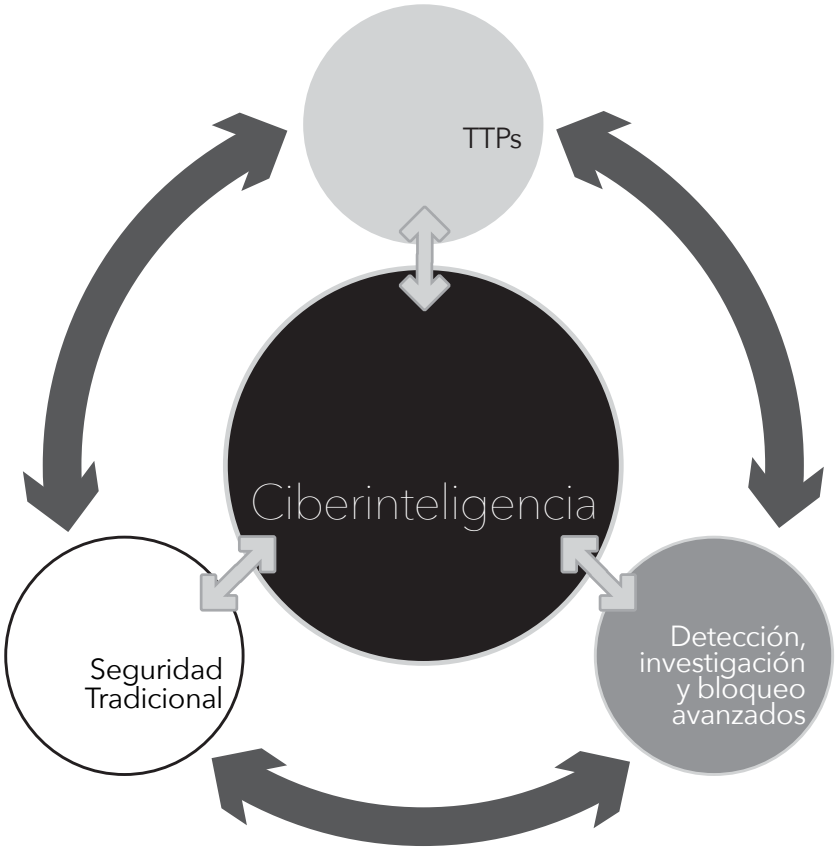
Hechos como los mencionados anteriormente nos ayudan a hacer conciencia de que las amenazas son cada día más complejas y avanzadas, detrás de ellas se encuentran actores que han creado un ecosistema completo que les permite contar con los recursos económicos y tecnológicos necesarios para moverse con libertad. Este panorama ha puesto a las organizaciones en desventaja ya que la mayoría tarda mucho tiempo en detectar cuando se ha materializado una brecha de seguridad, incluso pueden pasar meses antes de la detección. Sin importar el sector o giro de las organizaciones todas se encuentran en mayor o menor medida expuestas a estas ciberamenazas.

Este escenario cambia las reglas de la seguridad de la información, en el pasado se mencionaba que se deberían tener redes impenetrables, lo cual hoy se sabe que no es posible, los expertos coinciden en que tarde a temprano toda organización va a ser comprometida y el objetivo debe ser la detección temprana con la correcta respuesta para con esto lograr minimizar el impacto.

NUEVOS MODELOS PARA LA DETECCIÓN, INVESTIGACIÓN Y BLOQUEO

Los avances tecnológicos actuales han logrado que algunas de las técnicas de detección sean más robustas y den pie a nuevos modelos de detección y protección contra amenazas avanzadas.

En el siguiente diagrama "Capas de protección", se muestran diversos componentes que deben interactuar y soportar unos a otros con el propósito de ayudar a proteger a las organizaciones. Cada una de las capas debe alimentar a la otra de una manera bidireccional.



Capas de protección.

CAPAS DE PROTECCIÓN

A continuación describimos los nuevos esquemas más importantes.

1) Inteligencia

La capa de inteligencia pretende entender el contexto en el que se encuentra la organización respecto lo que está sucediendo en su entorno sea global o solamente regional, contemplo, entre otras, las siguientes disciplinas:

» **OSINT**: Es el acrónimo de "*Open Source Intelligence*", y se refiere a una de las técnicas para adquirir información con fines de inteligencia, -entendiendo por inteligencia a la identificación de campañas con fines negativos / dañinos, nuevos métodos de ataque y *malware*, así como nuevos actores -; Toda esta información se recopila a través de un monitoreo distribuido y análisis de contenido encontrado en fuentes públicas accesibles, una de las capas utilizadas es mejor conocida como WebInt (*Web Intelligence*) la cual está enfocada a la búsqueda de información en la *World Wide Web* y en ocasiones va más allá de las fuentes abiertas, dentro de su cobertura están la *Deep Web* y *Dark Web*.

» **SIGINT**: Es el acrónimo de "*Signal Intelligence*", y se refiere a obtener información a través del monitoreo distribuido y análisis de señales. Comunmente se colocan sensores en diversas localidades a nivel global que pueden identificar el comportamiento de amenazas conocidas y en muchos casos amenazas nuevas. Regularmente algunos de los componentes de seguridad tradicional como son *firewalls* e IPS's permiten compartir con el fabricante información estadística o metadatos del tráfico que fluye a través de los dispositivos, en este caso podemos decir que estos componentes forman parte de la red SIGINT del fabricante como un sensor adicional, lo que le brinda una mayor capa de visibilidad y cobertura. Los sensores a su vez pueden utilizar técnicas de detección avanzadas.

La información obtenida a través de las técnicas descritas previamente, es utilizada a su vez para robustecer las siguientes fuentes de información:

- **Base de datos de reputación**: Con base en la información obtenida se genera una base de datos de reputación, ésta contiene al menos los siguientes objetos: direcciones IP, URL y dominios. Permite relacionar los objetos con su comportamiento malicioso. Este comportamiento puede ser:
  - Comunicación Control & Comando
  - *Malware*
  - Actividades criminales
  - Explotación de vulnerabilidades

- ***White-list y Black-list***: La información de artefactos detectados puede generar un repositorio de información de *hashes* de archivos como son documentos, ejecutables para diversas plataformas, exploits, etc. Esta información permite la detección temprana de un archivo malicioso.
- ***Threat Intelligence***: Se refiere al repositorio de información que se ha construido gracias a la información de evidencia, los contextos, mecanismos, consecuencias e indicadores sobre las amenazas, dicha información debe estar estructurada para entender el funcionamiento técnico, social y político de las amenazas.

Toda la información obtenida en esta capa es dinámica y es cambiante en el tiempo, la cual a su vez debe alimentar a las otras capas relacionadas con las funciones de detección o protección para poder generar algún tipo de acción. Esta capa no es nueva, sin embargo la obtención de la información dependía mucho del fabricante y/o de la organización que la ofrecía, por el contrario en la actualidad se están creando alianzas entre diversos fabricantes y organizaciones con el fin de obtener una mayor cobertura de visibilidad; permitiendo así que la información fluya de manera más rápida y eficaz, con lo anterior podemos concluir que la tendencia es la creación de ecosistemas de inteligencia.

2) Componentes de seguridad tradicional

Los componentes tradicionales de seguridad tales como *firewalls*, IPS, Antivirus, DLP; permiten proteger a la organización de amenazas conocidas. Cuando a estos componentes se les suma la capa de Inteligencia llegan a ser muy robustos; sin embargo no llegan a cubrir la detección de ataques dirigidos mediante herramientas avanzadas o nuevas, por tal razón es necesario adicionar la capa de detección y protección avanzada.

Contar con estos componentes es básico, ya que cubren las necesidades de detección de amenazas conocidas. Sin embargo, su visibilidad es limitada a amenazas estáticas conocidas; por esta razón cuando algo es nuevo o avanzado, dichos componentes no tienen la posibilidad de proteger.
Es importante mencionar que muchos de los componentes de seguridad tradicional han comenzado a evolucionar y algunos ya incluyen técnicas de protección avanzada.

3) Detección, investigación y bloqueo avanzados

Cuando se habla de detección, investigación y bloqueo avanzados nos referimos a técnicas que permiten ayudar en la detección de amenazas avanzadas, algunas de ellas las identifican de manera temprana, sin embargo otras están diseñadas más para el análisis a detalle o el hunting (investigación).

A continuación se hace una descripción de ellas:

» **IOC** (*Indicator of compromise*), es un artefacto forense o un remanente de una intrusión, el cual puede visualizarse o encontrarse tanto a nivel de *host* o en el tráfico de red. Un IOC puede resumirse como los metadatos de eventos que pueden ser observables durante una intrusión, estos pueden ser la creación de un archivo, la lectura de una llave de registro en *Windows*, la presencia de cierto artefacto en memoria, la suma de estos permiten crear el *footprint* (huella) de una intrusión y no sólo eso, se puede asociar a cierta familia de *malware*, técnica o grupo. Los IOC se están convirtiendo en un estándar en la industria en la actualidad, mediante ellos es posible el análisis de eventos de manera muy puntual y por lo tanto la detección de intrusiones tiene mayor nivel de certeza.

» ***Yara Rules***, es una herramienta que permite la identificación y clasificación de *malware*, mediante ella se pueden crear descripciones de familias de *malware* basadas en patrones, la descripción de estos patrones son llamadas reglas y consisten en cadenas o expresiones booleanas que permiten determinar la lógica de la regla. Estas reglas pueden aplicarse a archivos o procesos en ejecución con el propósito de determinar si una familia de *malware* está detrás de dicho archivo o proceso. La suma de IOC con *YARA rules*, puede ser una técnica muy poderosa para la caza de amenazas.

» ***Sink Holes***, son herramientas que operan a nivel de red, funcionan de manera equivalente a un *honeypot*, comúnmente conocidos como DNS *sinkhole*, permiten la falsificación de los servidores autoritativos de DNS para dominios y *host* maliciosos, con esto es posible negar la comunicación a estos dominios, o incluso redirigir el tráfico a un red de análisis y permite la detección de intento de contactar dominios o hosts relacionados con actividades de amenazas avanzadas. Esta técnica en muchas ocasiones también es utilizada para controlar el acceso a dominios que no cumplen con la política de seguridad de la organización.

» ***Security Analytics***, uno de los problemas en la detección de amenazas tiene que ver con la gran cantidad de información que se puede recolectar en una organización, información y datos como son bitácoras generados por sistemas de TI, eventos generados por productos de seguridad como son firewalls, IPS, sistemas de administración de vulnerabilidades, información generada por capas de inteligencia, al intentar relacionar toda esta información con sistemas SIEM casi siempre se convierte en un problema cuando se requiere que los análisis estén en tiempo real; cuando se habla de *Security Analytics* se refiera a la capacidad de realizar análisis en tiempo real y de manera asimétrica entre los diferentes componentes, con el propósito de conocer el estado actual de la organización (*Situational awarness*), esto sin importar que la información esté resguardada en formato de bitácoras, alertas o tráfico de red. Con esto se pretende sumar la experiencia de la industria para generar conocimiento y aprendizaje de seguridad para la organización.
El tipo de tecnología utilizada está basada en *big data* y análisis no estructurado de datos.

» ***Behavior and Anomaly Analysis***, la detección de anomalías regularmente se da a nivel de tráfico de red y trata de entender los flujos de comunicación, protocolos y contexto en que se dan las comunicaciones dentro de la organización. Este tipo de análisis intenta detectar primeramente si el comportamiento presentado es parecido al que generaría una persona o pareciera algo más automatizado, también identifica el contexto en que se dan las comunicaciones, por ejemplo si la organización no tiene una relación comercial con algún país de Asia y se detecta que a las 2 de la mañana se da una comunicación a una dirección IP que está en Japón; eso puede disparar alguna alerta. El comportamiento y las anomalías van más allá de identificar que existe un canal de comunicación a una URL que cuenta con mala reputación, pretende entender el contexto en que se dan comunicaciones y detectar cualquier irregularidad.

Este tipo de técnica permite la detección de equipos comprometidos cuando intentan o establecen alguna comunicación con algún C&C o movimientos laterales cuando se presentan.
Cuando la anomalía se busca a nivel de host regularmente se realiza un análisis de *malware* y tiene como objetivo la ejecución del artefacto en un ambiente monitoreado con el propósito de entender su comportamiento. Este tipo de detección permite de manera muy rápida la identificación de acciones realizadas por el *malware*, las cuales pueden ser, creación de archivos, inyección en algún proceso en tiempo de ejecución, entre otras. Es importante recalcar que algunas plataformas de protección usan los *endpoints* en producción como el ambiente monitoreado y detectan cualquier comportamiento sospechoso, como la invocación de un *heap spray, hooking, process injector*, etc.; los cuales regularmente no son comportamientos comunes de los programas de sistemas operativos.

» ***Dynamic Analysis***, cuando se realiza un estudio de muestras de malware, el análisis dinámico representa el entendimiento del comportamiento en ambientes controlados, el tipo de información que se pretende identificar son llamadas a funciones, modificación o creación de archivos, desempaquetado de funcionalidades cifradas, detectar cambios o mutaciones en tiempo de ejecución.

» ***SandBoxing***, se refiere a una técnica o mecanismo de seguridad que restringe la ejecución de un programa, cuando es usado para la detección de amenazas avanzadas, es parte de un análisis dinámico y de comportamiento de las muestras de *malware*, dicho análisis regularmente se realiza en entornos virtuales como hiper visores propietarios, comerciales o libres, la muestra de *malware* se ejecuta en diversos sistemas operativos con diversas configuraciones de seguridad y aplicaciones instaladas, mediante esta ejecución se detectan las características con las cuales es posible la identificación de nuevas amenazas, así como la creación de IOC y *YARA rules*.

» ***SandNet,*** representa una técnica que realiza un análisis dinámico y comportamiento de las muestras de *malware* respecto al tráfico de red que generan, todo esto estudiado desde una red aislada que pretende emular o ser una red completa con diferentes componentes, el objetivo es detectar las funcionalidades, protocolos, conexiones que la muestra genera.

Este tipo de técnicas permite la identificación completa del comportamiento de una amenaza avanzada en su interacción con servicios de red, esto permite la creación de los IOC y Yara rules para el monitoreo constante de seguridad.

» ***Network Forensics***, técnica que pretender realizar el monitoreo y análisis del tráfico de red de una organización; este análisis regularmente se hace en dos vertientes, la primera es un análisis en tiempo real al integrarlos con una capa de *Security Analytics*, la segunda es más al estilo "*post mortem*" donde se hace la caza de las amenazas o incluso el entendimiento de lo sucedido en un evento de seguridad.

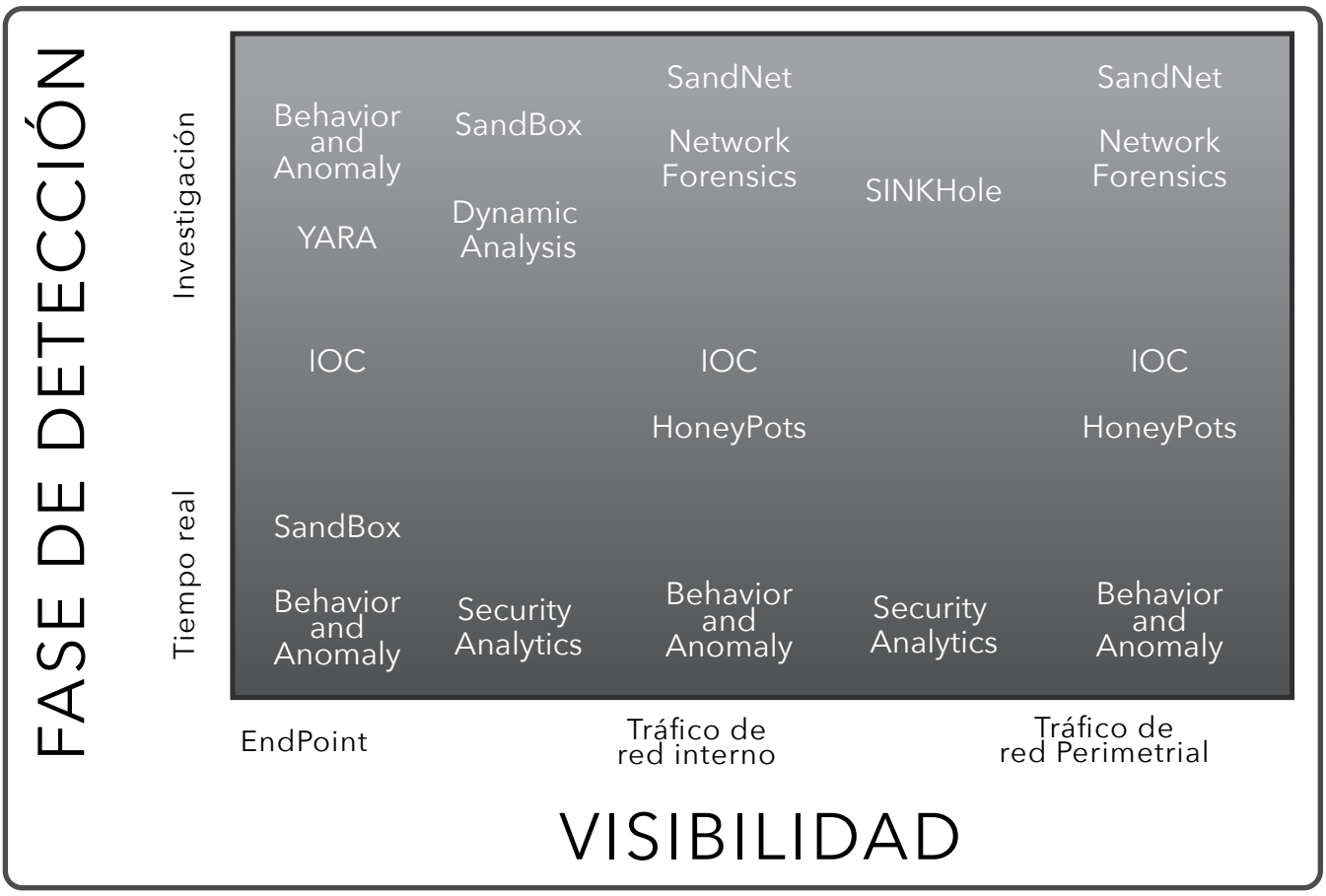
Este tipo de técnicas permiten la identificación y entendimiento de movimientos laterales, comunicaciones con C&C, extracción de información, reconstrucción de un ataque o actividad sospechosa, extracción de artefactos que están viajando por la red, análisis de seguridad posteriores sobre el tráfico con nuevos patrones de ataques.

» ***Static Analysis***, el análisis estático se refiere a realizar tareas de identificación en muestras de *malware* sin necesidad de ejecutar el programa, el propósito es la identificación de información que permita determinar su comportamiento, el tipo de información que se busca es el tipo de archivo, si es un archivo ejecutable de Windows (PE) la cantidad de secciones que tiene, si el archivo esta empaquetado, si el archivo está firmado digitalmente y si esta firma es válida, también se busca identificar las librerías y funciones de las cuales hará uso, por ejemplo si hace una llamada a la función de Windows "*IsDebuggerPresent*" muy probablemente incluye una protección para no permitir la depuración del programa.

Este tipo de técnicas permite la identificación pronta de artefactos que podrían ser considerados maliciosos y por lo tanto ser una amenaza.

» ***HoneyPots***, es una técnica que pretende el uso de trampas para la captura de amenazas o *malware*, estos honeypots pretenden ser parte de la infraestructura de una red y emular sistemas operativos o servicios de red con los cuales atraen hacia ellos los movimientos laterales de las amenazas; el propósito es la identificación y entendimiento de las amenazas.

El siguiente diagrama "Puntos de visibilidad" muestra el momento en que cada técnica es utilizada.



Puntos de visibilidad

TTP's

Cuando se habla de TTP's (*Tactics, Techiques and Procedures*) representa el cómo actúa un actor o adversario desde la fase de reconocimiento hasta la extracción de datos. El objetivo de una organización debería ser realizar su operación de seguridad a este nivel con lo cuál se está enfrentando al actor en potencia y no solo a las herramientas que está usando, con esto es posible lograr un modelo de seguridad adaptable y dinámica de protección.

CONCLUSIONES

Cada una de las técnicas descritas sirven para la detección y por lo tanto la protección contra amenaza avanzadas, cada una de ellas pueden ser utilizadas en diferentes fases del *Kill Chain* de una amenaza, sin embargo no son infalibles, por tal razón una arquitectura robusta de seguridad debería contemplar al menos protección a nivel perímetro, protección a nivel endpoint y captura de tráfico saliente a internet y en segmentos de red críticos.

Una consideración importante es que aun sumando la visibilidad y protección que brinda la seguridad tradicional, más la seguridad de detección avanzada soportado por la capa de inteligencia siempre existirá una pequeña brecha o punto donde alguna amenaza puede traspasar nuestros controles de seguridad, esta pequeña brecha debe ser compensada con una arquitectura robusta, procesos, procedimientos y personal capacitad, entrenado y certificado en temas de detección avanzada, con los cuales se puede aumentar el nivel de capacidad para buscar aquellas ciberamenazas que no han sido detectadas aún.

Patricio Sánchez
Scitum

Graduado como Licenciado en Sistemas Informáticos, ostenta certificaciones tales como : CISSP,CISM,GCIH,GWAPT,C|EH.

Ciudad de México
Plaza Inbursa / Torre Telmex
Av. Insurgentes Sur No. 3500 Piso 2, Col. Peña Pobre
C.P. 14060 Del. Tlalpan, México, D.F.
Conm.: +52 (55) 9150.7400
Fax: +52 (55) 9150.7478

E-mail: **ventas@scitum.com.mx**

www.scitum.com.mx