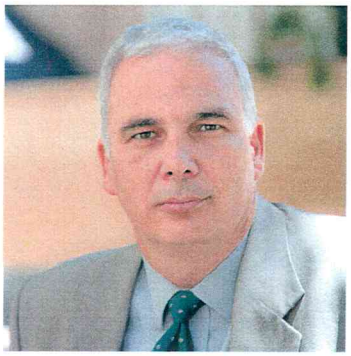
IOC: indicadores de COMPROMISO

José Ramón Monleón

CISO de Orange y director técnico del proyecto PAD-IOC de ISMS Forum



Francisco Lázaro

CISO de Renfe, director del Centro de Estudios en Movilidad e IoT y miembro de la Junta Directiva de ISMS Forum

Carles Solé

CISO de CaixaBank, miembro del comité del Cyber Security Centre y de la Junta Directiva de ISMS Forum

En el escenario actual, asistimos a una imparable escalada de ataques a la seguridad de los sistemas y redes informáticas por parte de agentes hostiles cada vez más numerosos y competentes, capaces de coordinarse entre ellos y reutilizar técnicas y herramientas. Estos ataques, además, afectan a cualquier empresa, independientemente de su tamaño o sector.

Para hacernos una idea, aunque sea parcialmente, del volumen de amenazas, basta indicar que un sólo fabricante asegura que sus sistemas recogen diariamente información sobre más de 157 millones de intentos de engaño a sus clientes para conectarse a URL peligrosas (a través del correo y la navegación), sobre la exposición de las redes de éstos a más de 353 millones de archivos infectados, así como que en esos mismos clientes intentaron instalarse o iniciarse más de 71 millones de programas no deseados.

La colaboración a la hora de compartir información sobre los ataques, los *modus operandi* y las técnicas y herramientas usados en los mismos se considera de vital importancia para la protección eficaz de las organizaciones objetivo; compartición en cualesquiera de las modalidades posibles entre las entidades privadas y los organismos públicos (pública-privada, pública-pública y privada-privada).

Esta información está muchas veces sólo en posesión de los proveedores que ofrecen herramientas y servicios de seguridad o sólo en posesión de una organización, no compartida entre todas las empresas potencialmente atacadas. Actualmente esa falta de comunicación entre potenciales "victimas" es una debilidad que permite que una amenaza pueda ir afectando empresa tras empresa, de forma masiva, con el consiguiente beneficio para los atacantes. Se necesita, por lo tanto, que las empresas cooperen de forma continua y en tiempo real en la construcción de una inteligencia colectiva sobre amenazas.

Cuando hablamos de inteligencia sobre amenazas, debemos comprender que el concepto va más allá de una lista de direcciones IP consideradas atacantes o de mala reputación o de *hashes* de archivos maliciosos sospechosos. La verdadera inteligencia proviene del conocimiento de una amenaza emergente (o existente) basado en pruebas, que puede utilizarse para sustentar decisiones sobre cómo responder a la misma. No sólo ofrece los *bits* específicos de la amenaza sino, lo que es más importante, el contexto en el que se lleva a cabo el ataque. Identifica los indicadores de ataque y de peligro. Los expertos y las tecnologías de seguridad pueden utilizar la inteligencia sobre ciberamenazas para ofrecer mejor protección frente a ellas o detectar su presencia en sus entornos de confianza.

Barreras al intercambio

Desde hace años, en España, diferentes grupos de empresas han compartido información sobre amenazas y ataques. También determinados organismos públicos han dado pasos decididos para proporcionar información en este sentido. Pero los mecanismos utilizados (avisos, correos, listas de distribución) si bien eficaces, tal y como lo muestran las encuestas de satisfacción, han sido poco eficientes y, sobre todo, nada escalables a los órdenes de magnitud en los que las ciberamenzas están creciendo.

Ante esta necesidad, durante los últimos años han aparecido una serie de mecanismos orientados a facilitar la compartición automatizada de información de seguridad sobre los ataques y atacantes. Estos sistemas han evolucionado a medida que más

organismos interesados se incorporaban a su definición.

En estos momentos existen dos estándares principales de intercambio de información sobre indicadores de compromiso (IOC) y ataques: STIX y OpenIOC. Pero siguen existiendo barreras al intercambio. En ocasiones la política de la empresa, el miedo a interferir en investigaciones o las implicaciones legales pueden frenar las iniciativas de compartición. Y las empresas que hasta el momento comparten de forma moderada esta información, lo hacen sólo a un círculo íntimo, pues existe una verdadera desconfianza a la pérdida de confidencialidad y sobre el riesgo reputacional al que se podrían someter.

Por otro lado, existe en algunas organizaciones un recelo casi atávico a compartir con el Estado este tipo de información y al uso que de la misma hará el organismo público. Por ejemplo, convirtiéndose en alguna forma de obligación o requisito legal.

Finalmente, los fabricantes de productos de seguridad que suministran servicios de inteligencia y reputación quieren preservar su conocimiento de las amenazas, lo que en ocasiones llaman "telemetría de amenazas" o "inteligencia sobre amenazas", como derechos de *copyright* frente a otras empresas que comercializan servicios similares.

PAD-IOC

ISMS Forum no ha sido ajeno a esta problemática y, dentro de su filosofía de colaboración e impulso de la seguridad de la información, ha puesto en marcha un proyecto que intenta dar solución a la necesidad de intercambio de IOC entre distintas organizaciones mediante canales seguros, confidenciales, legales e independientes entre sí.

Se trata del PAD-IOC, un proyecto de plataforma abierta de intercambio de indicadores de IOC de ISMS Forum, en el que participan conocidas empresas de diferentes sectores industriales (Banca, Telecomunicaciones, Transporte y Construcción, entre otras) conjuntamente con otras compañías de la industria de seguridad (*antimalware* de red y puesto final o ciberseguridad, entre otras).

Desde ISMS Forum se pretende establecer no sólo los mecanismos técnicos que permitan el intercambio, sino también las reglas de juego que hagan viable y mantenible el que las diferentes partes interesadas compartan información de ataques sin perder confidencialidad ni la propiedad del conocimiento. Se pretende que cada organización pueda aportar los IOC que considere convenientes, estableciendo para cada uno de ellos su estrategia de distribución hacia el resto de participantes, canalizándolo y almacenándolo en un entorno centralizado, que será el que dé acceso a esa información mediante el uso de perfiles de usuarios y grupos de acceso para cada organización.

Será necesario que cada entidad pueda determinar, para cada IOC, con qué otros participantes quiere que se comparta la información, pudiendo ser o bien pública y accesible por cualquiera o bien sólo compartida por un grupo cerrado de participantes.

Estándares

Para que todo intercambio de inteligencia sobre ciberamenazas funcione eficazmente, resulta fundamental disponer de estándares técnicos reconocidos para compartir información. Ha habido muchos esfuerzos para intentar consensuar un formato único para intercambiar inteligencia sobre ciberamenazas. En el año 2010, MITRE, con la financiación y supervisión del Departamento de Seguridad Nacional de EEUU (DHS), comenzó a desarrollar una arquitectura de información sobre amenazas cuyo objetivo era generar la representación de un indicador de ciberamenazas automatizable. Éste fue el primer esfuerzo para centrarse específicamente en la creación de una representación estructurada y automatizable del ciclo de vida de las ciberamenazas, el formato de mensajes relacionado y el protocolo de intercambio. Los trabajos se concretaron en tres especificaciones:

- TAXII™, *the Trusted Automated eXchange of Indicator Information*.
- STIX™, *the Structured Threat Information eXpression*.
- CybOX™, *the Cyber Observable eXpression.*

PAD-IOC de ISMS Forum soportará el intercambio de IOC con los estándares OpenIOC y STIX/Cybox, y la entrada y salida de información entre ambos estándares.

La organización confía enormemente en que, una vez integrada en la infraestructura y las operaciones de una empresa asociada, la inteligencia sobre ciberamenazas de PAD-IOC, así como la seguridad de redes y sistemas de sus asociados mejorará de manera importante.

La colaboración entre entidades es un factor clave que va a cambiar la balanza frente a las actuales amenazas, ya que hasta la fecha el aislamiento entre entidades y la falta de colaboración ha sido un factor aprovechado por los atacantes para que las consecuencias de sus acciones se extiendan.

PAD-IOC: juntos hacemos más. ■