La socialización de la lucha contra las ciberamenazas

La lucha contra el cibercrimen debe tomar una nueva dirección en la que modelos colaborativos 2.0 permitan socializar la lucha contra las ciberamenazas mediante una comunidad y/o grupos. De esta forma se suplirán las carencias actuales de falta de información fresca, global y de calidad. En este artículo se explica qué modelos colaborativos van a ayudar a acometer esta nueva cruzada contra los *chicos malos*.

Daniel Solís Agea

Actualmente, la cantidad de proveedores de ciberinteligencia o *threat intelligence* va en aumento. Esto denota que es un mercado en pleno auge y en el cuál se están posicionando diferentes actores ofreciendo sus distintas visiones y soluciones.

Aunque existe una gama interesante de fabricantes y MSSPs ofreciendo estos servicios, absolutamente ninguno de ellos puede garantizar que tenga el 100% de la información referente a las ciberamenazas que puedan o vayan a existir. Por estos motivos cada vez más los fabricantes se unen para poder dar una mayor oferta de valor, juntando piezas de información sobre los *chicos malos* y las amenazas que ocurren en internet.

Desafortunadamente, el diferencial aportado es escaso ya que la gran mayoría acceden a las mismas fuentes de información, carecen de infiltración en el cibercrimen o son meros redistribuidores de información pública.

Además, los ciberdelicuentes están cada vez más organizados o las nuevas y emergentes amenazas que crecen exponencialmente no permiten adaptarse al ritmo de recolección de información y detección.

¿Cómo se puede solucionar este problema?

La respuesta es sencilla, con modelos colaborativos de intercambio de información. Aunque más allá de la colaboración entre organismos y asociaciones, que son esenciales, se tiene que llegar a colaborar con los usuarios potenciales de ataques y que pueden ser los ojos de un objetivo común: la lucha contra el cibercrimen.

Ahora más que nunca ha llegado la hora de socializar el *threat intelligence* o la lucha contra las ciberamenazas.

Sistemas de intercambio no eficientes

¿Por qué no han funcionado tan eficientemente otros sistemas de intercambio de información? En general los sistemas de intercambio de información en otras disciplinas no han funcionado excesivamente, como es el caso del intercambio de indicadores de riesgos y salvaguardas. Desafortunadamente, no han sido todo lo pragmáticos y efectivos e incluso reales (que tocasen con los pies en el suelo) que deberían para ser operativos y aplicables en el sufrimiento del día a día de los departamentos de seguridad, CISOs y empresas.

Además, muchas veces los han abanderado organismos, empresas, organizaciones o incluso "profesionales" que, en vez de velar por el bien del conjunto y de todos los actores invitados a participar, se han dedicado a imponer las necesidades de su departamento o empresa. Todo ello sin tener en cuenta el intercambio global y colaborativo. Este hecho, junto a las claras carencias de estos sistemas, los ha llevado a la impracticabilidad o a su nula evolución. De igual modo, los sistemas de intercambio de información sobre ciberamenazas no deben caer en las mismas carencias, las cuales se enumeran en el siguiente apartado.

Carencias de los sistemas actuales y cómo se subsanarán

• **Carencia de círculos de confianza**. Todo el mundo se compromete a intercambiar pero nadie se fía de nadie. Existe una clara falta de confianza, por lo que los futuros sistemas deben facilitar el intercambio de datos a diferentes niveles de confianza.

• **Múltiples e insufribles formas de *reporting***. Los formatos de *reporting* han sido, hasta la fecha, complicados. Además, cada actor ha querido imponer el suyo, lo que ha llevado a crear inoperatividad y una carencia enorme de agilidad, por lo que ha sido tan improductivo que han quedado prácticamente obsoletos. En el caso de las ciberamenazas, la industria lleva trabajando en estándares y formas de *reporting* como IOCs, STIX, Cybox, etc., que subsanarán este problema. Además, se centran en indicadores o información que es cuantitativa, no únicamente cualitativa (por no decir subjetiva y sin criterio alguno). Dichos nuevos estándares y "lenguajes de *reporting*" van a ayudar a actuar de una forma mucho más ágil, concreta y pragmática (*hash* de *malware*, IPs de C&Cs, *yara rules*, etc.). La información compartida es legible por las máquinas (MRTI – *Machine Readable Threat Intelligence*), por lo que los elementos de seguridad tales como cortafuegos, IPS, SIEMs, etc. saben cómo procesar dicha información.

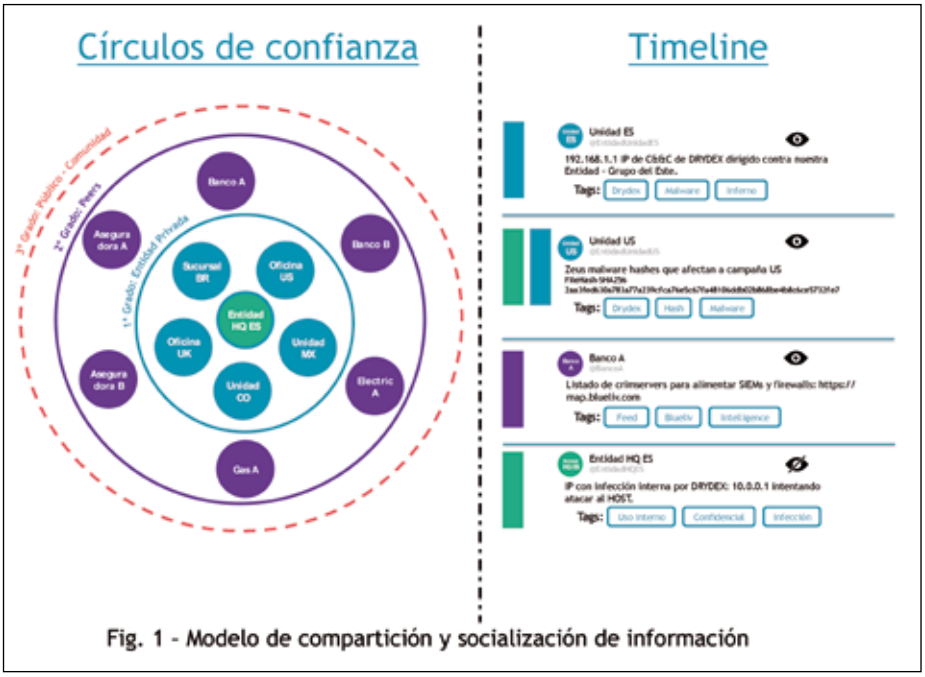

Fig. 1 - Modelo de compartición y socialización de información

• **Limitación de fuentes de información**. Tener múltiples fuentes es tan crítico como saber dónde ir a buscar la información (sitios *underground*, fuentes cerradas y fuente privadas) y, más importante, saber analizarla y correlacionarla. Por ello, la socialización de las ciberamenazas debe facilitar el intercambio de información de fuentes globales y concretas, sobre todo la *crowdsourced* con múltiples colaboradores, que es lo que puede llegar a obtener mejores volúmenes de información con la cantidad y calidad (frescura), muy valiosas para combatir el cibercrimen.

• **Falta de empoderamiento en la capacidad de análisis**. Para un único sector o tecnología o para varios sectores. La información compartida puede ser única y específicamente para un sector o grupo (financiero, industrial, infraestructuras

críticas…) aunque debe tener en cuenta a todos los actores de diferentes industrias y la capacidad de ofrecer análisis para aprender de la experiencia. Por ejemplo, hacer un seguimiento de un *malware* focalizado en un único sector debe permitir compartir conclusiones y mitigaciones de forma rápida y localizable de modo sencillo. Algo tan fácil de solventar mediante el uso de etiquetas de información, vinculado con los indicadores o IOCs.

Socialización de la lucha contra amenazas 2.0.

La socialización de la lucha contra las ciberamenazas debe facilitar información de primera mano y subsanar las carencias citadas anteriormente. Pero aún resulta más importante que, al ser una necesidad social o 2.0, deba vincularse a una causa (sin ánimo de lucro y con un claro modelo social) que permita involucrar a expertos, fabricantes, organizaciones y usuarios. Debe ser un vehículo que dé pie a reportar información por el bien común.

Existen algunas iniciativas en la red social Twitter, como #malwaremustdie!, dónde la comunidad del *reversing* o expertos en *malware* han iniciado una cruzada para acabar con dicho problema en Internet. La iniciativa es buena, con un toque romántico que le da un carácter de persistencia y fuerza luchadora. Pero más allá de un *hashtag* en Twitter y un blog, no es un sistema como tal. Por otro lado, FS-ISAC tiene diferentes iniciativas, que acaban limitándose mayoritariamente al sector financiero y que acaban controlándose por una única compañía vinculada a esta organización, contrariando a los participantes que comparten su información de forma colaborativa, para lucro de otros. Y es que se debe entender que **lo que es de la comunidad, se hace para la comunidad**; si se pierde este espíritu, adiós a la socialización de la lucha contra las ciberamenazas.

Definición del sistema de socialización

El sistema ha de ser muy ágil y facilitar la colaboración entre todos los actores. Este sistema debe ser visualmente atractivo, vinculado a una comunidad y que permita la interacción y la generación de información sobre ciberamenazas de forma sencilla e inteligible para cualquier usuario. Además ha de permitir su personalización con diferentes objetivos:

- Permitir recolectar a un usuario de la comunidad la información que sea únicamente y específicamente de su interés.
- Clasificar y buscar la información de forma sencilla, mediante etiquetas.
- Poder interactuar e intercambiar información directamente con iguales o *peers* que sean del mismo ámbito de interés o poder dar acceso restringido a los círculos de confianza creados por el usuario. Estos círculos de confianza (ver **Figura 1**) deben tener un mínimo de tres grados de clasificación:

– **1er grado**. Ámbito profesional y restringido de una empresa (ya sean usuarios, unidades de negocio o países en el caso de grupos multinacionales), facilitando el intercambio en concreto de una amenaza que afecte a una unidad de negocio o país y que pueda reproducirse en otros ámbitos geográficos. Por ejemplo, un ataque de *phishing* perpetrado por una banda que actúe en Europa y pueda dirigirse a Latinoamérica.

– **2º grado**. Iguales (*peers*) o de su mismo sector, permitiendo compartir amenazas identificadas. Por ejemplo, el caballo de Troya bancario Dyre, que ataca al sector financiero.

– **3er grado**. Público, para todos los usuarios de la comunidad. Información que no revele nada competitivo ni de negocio y que permita la lucha activa, conjunta y colaborativa contra amenazas. Por ejemplo la organización de un DDoS por parte de Anonymous.

- Otorgar distintivos y reconocimientos a las empresas y usuarios más activos, mejorando su reputación como expertos en seguridad y reconociendo su tarea en la lucha conjunta.
- Generar un *feed*, a medida de las necesidades de información y de forma automática. Evidentemente, debe ser legible en formatos STIX, OpenIOC, etc. Además, este *feed* debe contener información generada por los usuarios que sigan dentro de la comunidad (al más puro estilo de red social) o según las etiquetas de las ciberamenazas que puedan interesar/afectar y que puedan ser directamente integradas/inyectadas en los elementos de seguridad clásicos (cortafuegos, SIEMs, IDS, etc.).

Jerarquía e intercambio automatizado de información (TAXII, STIX)

Hasta ahora se ha argumentado cómo debería ser esta comunidad o red social que permitiera la socialización de la lucha contra las ciberamenazas. Ahora bien, dicho portal no debería ser el único elemento de intercambio de información y habría de alimentar a otros sistemas mediante el protocolo TAXII, en un sistema jerarquizado (ver **Figura 2**).

Este intercambio de información comprendería diferentes servidores TAXII, que intercambiasen información mediante STIX. El intercambio de información debería hacerse de la siguiente forma:

- **Servidores TAXII públicos**, abiertos y globales, controlados por CERTS u organizaciones sin ánimo de lucro. Una jerarquía similar a los *root servers* del protocolo DNS. A los que se conectarían las empresas para compartir de forma automatizada IOCs u otra información vital, para la lucha colaborativa en contra del cibercrimen. A su vez, la comunidad generaría contenido, que sería volcado automáticamente a dichos servidores TAXII, siempre y cuando dicha información hubiese sido clasificada como pública y publicable.
- **Servidores privados TAXII intra-grupo**, para compartir indicadores que no deban ser públicos, más bien indicadores que, por ejemplo, deban ser compartidos dentro de un grupo multinacional y que rápidamente alimenten a todos las soluciones de seguridad tradicionales para evitar expansiones de ciberataques de una localización geográfica a otra. Estos servidores, lógicamente, también estarían alimentados por los servidores TAXII públicos para estar al día de nuevos indicadores.
- **Servidores públicos TAXII extra-grupo**, dónde se hablarían con *peers* u organizaciones del mismo sector o similares y pudiesen intercambiar información específica de la industria. Por ejemplo, indicadores que solo afecten a un sector, tipo de tecnología y que puedan ayudar a la rápida contención de ciberamenazas. ■

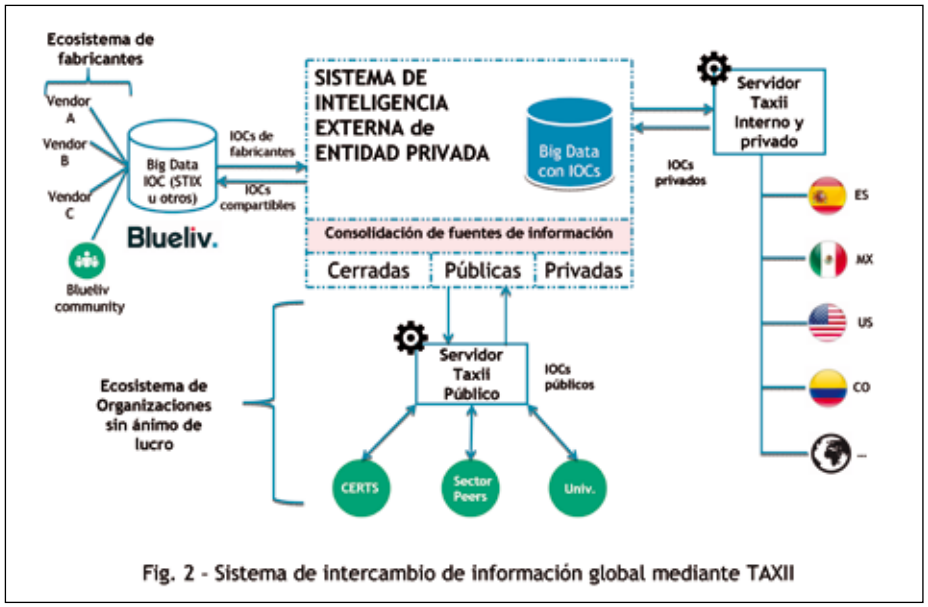

Fig. 2 - Sistema de intercambio de información global mediante TAXII

Daniel Solís Agea
CEO
BLUELIV

REFERENCIAS

[1] STIX, stix.mitre.org
[2] TAXII, taxii.mitre.org
[3] FS-ISAC, www.fsisac.com
[4] comunidad blueliv, https://map.blueliv.com