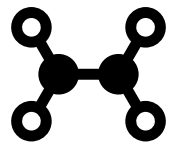


UNIDAD 2
AUDITORÍA DE INCIDENTES DE CIBERSEGURIDAD

Las amenazas más importantes relacionadas con el ciberespacio se pueden clasificar en dos grupos: amenazas contra la información, y amenazas contra la infraestructura. Las amenazas contra la información son aquellas que provocan una pérdida o un uso indebido de la información, el espionaje, el fraude, el robo de identidad, entre otras muchas. Por otro lado, las amenazas contra la infraestructura son aquellas que pueden provocar la interrupción parcial o total de los sistemas, como la infección de malware, ataques contra redes, sistemas, etc. En esta unidad vemos a realizar una taxonomía de estos incidentes, de como detectarlos, monitorizarlos y notificar a los responsables de responder a ellos.

TAXONOMÍA DE INCIDENTES DE CIBERSEGURIDAD.

La taxonomía que aquí se propone está tomada de la propuesta por la ENISA[1] la cual es básicamente la utilizada por el INCIBE[2] y que es necesario utilizar en la guía de nacional de gestión y notificación de ciberincidentes[3] A continuación se detallan los tipos de incidentes según su categoría:

Contenido abusivo

SPAM: correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.

Delito de odio: contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.

---

[1] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

[2] https://www.incibe-cert.es/taxonomia

[3]https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Pornografía infantil, contenido sexual o violento inadecuado: material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.

Contenido dañino:

Sistema infectado: sistema infectado con malware. Ejemplo: sistema, computadora o teléfono móvil infectado con un rootkit.

Servidor C&C (Mando y Control): conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.

Distribución de malware: recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.

Configuración de malware: recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de webinjects para troyano.

Malware dominio DGA: nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).

Obtención de información

Escaneo de redes (scanning): envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.

Análisis de paquetes (sniffing): observación y grabación del tráfico de redes.

Ingeniería social: recopilación de información personal sin el uso de la tecnología. Ejemplos: mentiras, trucos, sobornos, amenazas.

Intento de intrusión

Explotación de vulnerabilidades conocidas: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ejemplos: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).

Intento de acceso con vulneración de credenciales: múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.

Ataque desconocido: ataque empleando exploit desconocido.

Intrusión

Compromiso de cuenta con privilegios: compromiso de un sistema en el que el atacante ha adquirido privilegios.

Compromiso de cuenta sin privilegios: compromiso de un sistema empleando cuentas sin privilegios.

Compromiso de aplicaciones: compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.

Robo: intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.

Disponibilidad

DoS (Denegación de Servicio): ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.

DDoS (Denegación Distribuida de Servicio): ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

Sabotaje: sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.

Interrupciones: interrupciones por causas externas. Ejemplo: desastre natural.

Compromiso de la información

Acceso no autorizado a información: acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.

Modificación no autorizada de información: modificación no autorizada de información. Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.

Pérdida de datos: pérdida de información. Ejemplos: pérdida por fallo de disco duro o robo físico.

Fraude

Uso no autorizado de recursos: uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales.

Derechos de autor: ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplos: Warez.

Suplantación: tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

Phishing: suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

Vulnerable

Criptografía débil: servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.

Amplificador DDoS: servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist.

Servicios con acceso potencial no deseado: servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.

Revelación de información: acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos: SNMP o Redis.

Sistema vulnerable: sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Otros

Otros: todo aquel incidente que no tenga cabida en ninguna categoría anterior.

APT: ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Ciberterrorismo: uso de redes o sistemas de información con fines de carácter terrorista.

Daños informáticos PIC: borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas

graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Amenaza persistente avanzada

Una amenaza persistente avanzada, también conocida por sus siglas en inglés, APT (por Advanced Persistent Threat), es un conjunto de procesos informáticos sigilosos orquestados por un tercero (organización, grupo delictivo, una empresa, un estado,...) con la intención y la capacidad de atacar de forma avanzada (a través de múltiples vectores de ataque) y continuada en el tiempo, un objetivo determinado (empresa competidora, estado,...). Este malware es instalado usando exploits que aprovechan vulnerabilidades de la máquina objetivo. Para realizar la infección es habitual aprovechar vulnerabilidades de día cero.

Desde la terminología militar podría decir que las APT están basadas en capacidades SIGINT en las que la adquisición es activa mediante ataque al objetivo (capacidades CNA de CNO) para modificar el comportamiento y funcionalidad para que proporcione los datos que queremos adquirir. Por ejemplo podríamos instalar malware o elementos hardware (implantes).

Las APT se caracterizan por:

Ser orquestadas por grupos organizados con grandes recursos (capacidad avanzada de ataque) y con mucho interés en el objetivo del ataque y en su información. Ejemplos típicos de estas organizaciones son servicios de información, mafias organizadas, ejércitos, grupos terroristas o activistas. El uso en la denominación del término ‘amenaza’ indica la participación humana para orquestar el ataque.3. Por su propia naturaleza puede ser difícil distinguir que equipo concreto está detrás de cada APT. Se han identificado más de 150 grupos, donde cabe destacar la especial importancia de grupos procedentes de China, Rusia e Irán. Los grupos organizadores de APT más conocidos son los que, al menos de manera presunta, son apoyados directamente por los gobiernos más activos en el ámbito de la ciberserguridad

El atacante persigue mantener el control de la infraestructura de la víctima de forma continuada. Típicamente varios años. Para que no sea detectado durante tanto tiempo el software malicioso tiene que:

Estar instalado en varias máquinas para mantener la persistencia en caso de sustitución, formateo o rotura de la máquinas. Estas máquinas es bueno que no tengan reputación negativa o que tengan muchas vulnerabilidades de esta forma evitaremos que esté en listas negras. El número de máquinas no tiene que ser suficientemente bajo como para no llamar la atención o evitar ser descubierto de forma casual.

Ser lo más sigiloso posible. Con la aparición de las Amenazas persistente avanzadas se ha dado un paso cualitativo en la complejidad de las técnicas de ocultación del software malicioso y de sus actividades. A esta nuevas técnicas avanzadas se las ha llamado Técnicas de evasión avanzadas o AET (del inglés Advanced Evasion Techniques)

Diseñado para evitar que sea localizado. Es habitual que el software disponga de capacidades automáticas que ante la más mínima duda de detección o intervención asociada a sus actividades se suelen borrándose rápidamente y volviéndose a reorganizar en servidores alternativos.

Diseñado de forma que si es localizado su análisis revele la mínima información sobre el ataque y el atacante. Es decir, se dificulte cualquier análisis TECHINT. Por ejemplo usar código cifrado u ofuscado, borrar la información comunicada, no usar comentarios, estar en idioma inglés, estilo de programación aséptico,que los identificadores no revelen ningún tipo de información.

El uso en la denominación del término ‘persistente’ indica que existe un control y monitorización externos para la extracción de datos de un objetivo específico de forma contínua.

El atacante usa varios vectores de ataque y persistencia para obtener y mantener el acceso a la red de la organización. El uso en la denominación del término 'avanzado' indica el uso de sofisticadas técnicas que utilizan software malicioso para explotar vulnerabilidades en los sistemas.

Una APT puede tener diferentes objetivos:

Robo de información (ciberespionaje) tanto de estado como industrial. La mayoría de APT tienen este tipo de objetivo. Ejemplos de APT centradas en este objetivo son Duqu (buscaba información sobre el programa nuclear iraní), Flame (buscaba robo de información general sobre Oriente Medio), Shady RAT (buscaba información en diferentes sectores, en especial gobierno y defensa estadounidense), Red October (buscaba información diplomática, en especial en Europa del Este, antiguas repúblicas soviéticas y Asia Central), Net Traveler (buscaba información mediante ataque de phising personalizado a personas relevantes),

Careto (buscaba información especialmente sobre Marruecos), Uroburos (buscaba información sensible de grandes empresas, estados y servicios de inteligencia de Europa y Estados Unidos) y Titan Rain (buscaba información de defensa de los Estados Unidos de América).

Provocación de daños o terror. Con esta motivación son típicos las campañas APT contra sistemas de control industrial (ICS) de industrias de distintos sectores. Ejemplos de este tipo de campañas son las realizadas con el (software malicioso Stuxnet (orientado al sabotaje del programa nuclear iraní), las campañas usando las distintas versiones de Shamoon (orientado a la destrucción de los datos del sector energético de países de Oriente Medio enemigos de Irán13) o las campañas de grupos vinculados a Rusia (Dragonfly, Dragonfly 2.0 y Sandworm) con objetivo la industria energética y con capacidad de controlar y provocar cortes de suministros en los sistemas de plantas eléctricas, de la red de energía y de algunos oleoductos.

Beneficio económico. El fin último de algunas APT es obtener un beneficio económico ya sea, por ejemplo, vendiendo la información obtenida, comprando acciones de empresas basándose en información privilegiada, comprando acciones de empresas que se van a beneficiar del sabotaje que se va a realizar a otras, o simplemente alquilando sus servicios con un determinado fin (espionaje, sabotaje,...). Se han detectado grupos APT, como Cozy Bear o Fancy Bear, que alquilan sus servicios.17 otros, como Desert Falcon, desarrollan operaciones mercenarias de ciberespionaje seleccionando sus víctimas cuidadosamente y buscando archivos con datos sobre ciertos temas.

Servidores externos involucrados: En una amenaza persistente avanzada es habitual que varios servidores externos a la red comprometida, colaboren para la consecuención del objetivo. Lo más frecuente es que estos servidores sean a su vez servidores comprometidos que la APT usa sin el conocimiento de sus propietarios. Ejemplos de servidores que es frecuente que intervenga a una APT son:1

Servidor externo para la descarga inicial del malware que compromete a la víctima. La descarga típicamente es introducida en la organización de la víctima a través de un correo eslectrónico, un phising personalizado o es descargado a través de un servidor web comprometido. A veces el software malicioso se descarga directamente, pero lo más frecuente es que se descargue primero un programa dropper que no contiene código dañino pero que se ejecuta con el objetivo de descargarse el malware.

Servidor de control y mando. Es el responsable de enviar órdenes a los equipos comprometidos y recibir informaciones indicando el estado o el resultado de la ejecución de una orden. Estos servidores permiten a atacante el control remoto del malware y alterar su comportamiento cambiando su configuración. Por ejemplo puede poner el malware en estado latente, indicarle que se autodestruya o que infecte otro dispositivo.

Servidor de exfiltración. Es el servidor que reciba la información robada para que el atacante pueda acceder a ella. Normalmente se transmite usando algún tipo de protección. Por ejemplo usando cifrado preferiblemente asimétrico (necesita clave privada para descifrar), usando esteganografía, usando fichero portadores (ejemplo imagen JPEG con datos ubicado después de la marca de fin imagen 0xFFD9) o transmitiendo la información a trozos

Para dificultar la localización del origen del ataque, los servidores se suelen establecer en cadenas de N saltos con un número N elevado. Por ejemplo, una cadena de servidores de exfiltración donde el primer servidor de la cadena obtiene la información desde el malware y se la pasa al segundo servidor de la cadena. El segundo de la cadena se la pasa al siguiente y así sucesivamente. A veces en lugar de usar una cadena se usa una botnets (redes de equipos zombis controlados por un atacante y que le permiten automáticamente transferir información robada por medio mundo hasta llegar a su destino real).

CONTROLES, HERRAMIENTAS Y MECANISMOS DE MONITORIZACIÓN, IDENTIFICACIÓN, DETECCIÓN Y ALERTA DE INCIDENTES: TIPOS Y FUENTES

IDENTIFICACIÓN

No es fácil en todos los casos determinar con precisión si se ha producido o no un ciberincidente y, si es así, identificar su tipo y evaluar a priori su peligrosidad. Básicamente, los indicios de que nos encontramos ante un ciberincidente pueden provenir de dos tipos de fuentes: los precursores y los indicadores. Un precursor es un indicio de que puede ocurrir un incidente en el futuro. Un indicador es un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.

Algunos ejemplos de precursores podrían ser: Las entradas de log del servidor Web, con los resultados de un escáner de vulnerabilidades; El anuncio de un nuevo exploit, dirigido a una atacar una vulnerabilidad que podría estar presente en los sistemas de la organización;

Amenazas explícitas provenientes de grupos o entidades concretos, anunciadoataques a organizaciones objetivo.

Para identificar un incidente de seguridad, determinar su alcance y los sistemas afectados por el mismo, se pueden obtener indicios de múltiples maneras en función de la naturaleza y tipo de incidente. Uno de los principales mecanismos es el análisis de logs, registros y fuentes de información para detectar anomalías. Sin ánimo de exhaustividad, fuentes de información a considerar en este punto son:

- Consolas de antivirus.
- Sistemas de Detección / Prevención de Intrusión (IDS/IPS).
- Alertas de sistemas de correlación de eventos de seguridad o SIEM.
- Registros de auditoría para detectar intentos de acceso no autorizados.
- Registro de conexiones bloqueadas en los cortafuegos.
- Registro de conexiones realizadas a través de proxys corporativos.
- Registros en herramientas DLP (Data Loss Prevention).
- Bloqueo de cuentas de usuario u otras anomalías reportadas en masa al CAU o que impliquen algún riesgo como pérdidas de USBs o equipos portátiles.
- Consumos excesivos y repentinos de memoria o disco en servidores.
- Anomalías de tráfico como picos de consumo a horas no habituales.
- Volcados de red, mediante port mirroring por ejemplo, que permitan confirmar alguna sospecha de incidente.

La detección de este tipo de anomalías permite identificar un posible incidente de seguridad, así como la naturaleza o el alcance del mismo. En el caso de que alguno de estos registros presentase alguna anomalía, sería necesario su análisis detallado para determinar si realmente existe un incidente.

Este análisis se puede realizar, por ejemplo, mediante la detección de tráfico de red malicioso, identificando la infraestructura afectada, las direcciones de origen y destino, valores de puertos utilizados, TTL, protocolos, etc.

Estas acciones ayudarán a determinar si realmente hay un incidente de seguridad y su naturaleza.

A nivel de sistema, algunos ejemplos para conocer si está siendo afectado por un incidente son:

- Cuentas de usuario inusuales en el sistema o especialmente privilegiadas.
- Ficheros ocultos o con tamaños, nombres o ubicaciones sospechosas, pudiendo indicar los mismos algún tipo de fuga de información o registro por parte de algún malware.
- Ficheros con permisos inusuales, con SUID o GUID en rutas no habituales, ficheros huérfanos y que pudieran determinar algún tipo de intrusión o rootkit.
- Entradas sospechosas en el registro, principalmente en el caso de infecciones por malware en sistemas Windows, donde ésta es una de las principales técnicas que el malware utiliza para asegurar su persistencia en el sistema infectado.
- Procesos y servicios inusuales, no sólo servicios a la escucha, si no con conexiones establecidas a puertos o host extraños, poco habituales o incluidos en algún tipo de lista negra de servidores de Comando y Control (C&C) utilizados por las botnets.
- Cargas excesivas de disco o memoria pueden estar producidas por un incidente de seguridad como malware, denegaciones de servicio o intrusiones.
- Sesiones abiertas en la máquina desde otros equipos, anomalías en las tablas de la base de datos,carpetas compartidas inusuales, o un elevado número de conexiones con algún flag TCP activado de manera anómala y que pudiera evidenciar un ataque de denegación de servicio.
- En el caso de equipos de usuario o terminales móviles, pueden indicar algún tipo de infección en el sistema, entre otros: comportamiento anómalo de alguna aplicación, ventanas emergentes del navegador, conexiones muy lentas, reinicios o aplicaciones que se cierran sin motivo.
- Tareas programadas o actividad sospechosa en los registros de auditoría y logs que indique un funcionamiento anormal del sistema o intentos de intrusión en algún servicio mediante por ejemplo fuerza bruta.
- Reporte del antivirus corporativo o de alguna herramienta habitualmente instalada en el sistema de identificación de rootkits, de control de integridad de ficheros, firma de los

binarios, etc. No es recomendable instalar ad hoc estas herramientas en un sistema sospechoso ya que pueden alterar las fechas de acceso de los sistemas y suponer una pérdida de evidencias.

Aunque en la organización se contemplen todas estas medidas para identificar un incidente de seguridad y el equipo o equipos afectados, no es descartable que la identificación del incidente se produzca a través de una fuente de información externa, un reporte de un CERT o de otro organismo, de un usuario externo a la organización, etc.[4]

CLASIFICACIÓN, VALORACIÓN, DOCUMENTACIÓN, SEGUIMIENTO INICIAL DE INCIDENTES DE CIBERSEGURIDAD.

La documentación de un incidente de Ciberseguridad depende de varias factores:

- Tipo de amenaza: código dañino, intrusiones, fraude
- Origen de la amenaza: interna o externa
- Categoría de seguridad o criticidad de los sistemas afectados
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en consecuencia, sus privilegios de acceso a la información sensible o confidencial.
- El número y tipología de los sistemas afectados.

Las características del incidente, tipo de recursos afectados y criticidad de los mismos determinará el impacto potencial sobre el negocio de la empresa, además del orden de prioridad en el tratamiento, en caso de detectarse más de un incidente de forma simultánea.

Además de tipificar los ciberincidentes dentro de un determinado grupo o tipo, la gestión de los mismos (asignación de prioridades y recursos, etc.) exige determinar la peligrosidad potencial que el ciberincidente posee. Para ello, es necesario fijar ciertos Criterios de Determinación de la Peligrosidad con los que comparar las evidencias que se disponen del ciberincidente, en sus estadios iniciales.

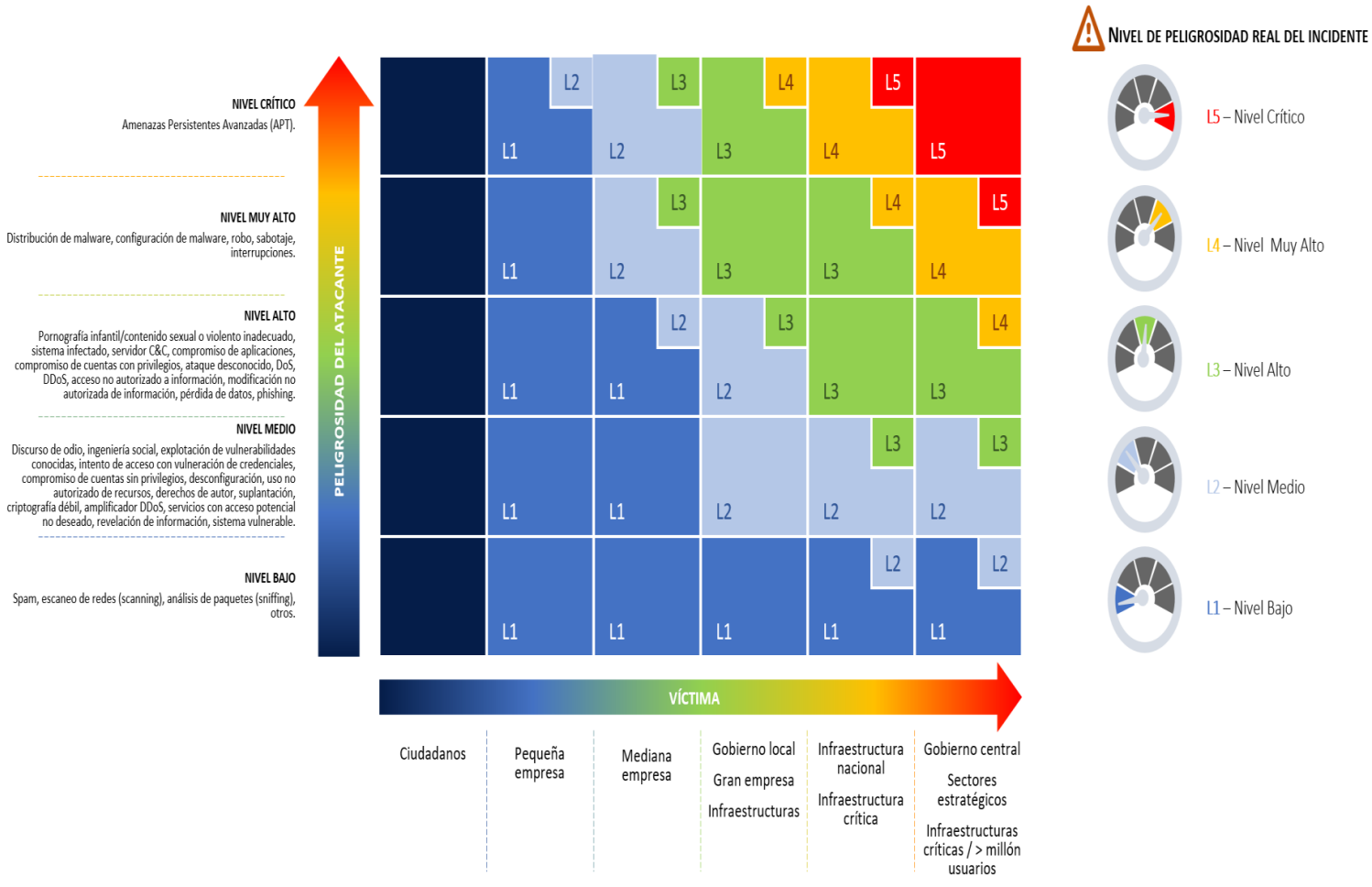
---

[4] Por ejemplo https://www.incibe.es/protege-tu-empresa/avisos-seguridad

El ENS señala que el impacto de un ciberincidente en un organismo público se determina evaluando las consecuencias que tal ciberincidente ha tenido en las funciones de la organización, en sus activos o en los individuos afectados.

El cuadro siguiente muestra cómo debe determinar el organismo afectado el Nivel de Impacto Potencial de los Ciberincidentes en la organización.

Habiendo garantizado la preservación de evidencias y reportado el incidente, hay que



proceder a la recuperación de los sistemas afectados.

En caso de incidentes de seguridad provocados por una intrusión o malware en sistema que no resultan críticos, una vez detectado el vector de infección o de intrusión en el sistema y establecidas las medidas correctivas oportunas para evitar que el incidente se reproduzca nuevamente, se puede proceder a restaurar el sistema afectado por el incidente mediante un backup que haya sido realizado anteriormente a la infección.

En sistemas críticos sobre los que no exista alta disponibilidad, habrá que valorar añadir al plan de continuidad del negocio la realización de copias periódicas de todo el sistema, no sólo de los datos. Esto puede permitir recuperar la actividad normal en caso de incidentes como los ocasionados por un malware o una intrusión, teniendo en cuenta que se debe evitar o bloquear el vector de ataque o de infección que afectó al sistema original.

En cualquier caso, en sistemas críticos siempre se deben seguir las instrucciones del fabricante del producto para su restauración o reinstalación, programando los mantenimientos correctivos y paradas de sistemas necesarias para llevar a cabo la recuperación del incidente.

De igual manera, en incidentes relacionados con vulnerabilidades siempre habrán de seguirse las recomendaciones del fabricante para mitigar o solucionar la vulnerabilidad, aplicando los parches oficiales liberados por el desarrollador

En la gestión de incidentes de seguridad resulta de gran importancia documentar todo lo aprendido en incidentes anteriores. Esas lecciones aprendidas pueden resultar vitales para evitar futuros incidentes de seguridad o solucionar nuevos incidentes con similares características.

Esto sirve para conocer con exactitud la naturaleza y tipo de incidente, las características del mismo y los vectores de infección con malware o intrusión para parametrizar los sistemas de seguridad de manera adecuada. Pero también para iniciar campañas de sensibilización adaptadas a la organización, conocer sus puntos más débiles y saber cómo protegerlos.

Es importante que esta documentación resulte muy detallada, permitiendo conocer qué herramientas se utilizaron y cómo, las investigaciones realizadas y sus resultados, las colaboraciones que se necesitaron, la documentación utilizada para resolver el incidente, la línea temporal de las acciones seguidas, etc.

También permite conocer a los atacantes, sus estrategias y sus patrones en las denegaciones de servicio. Las nuevas vulnerabilidades que afectan los sistemas más críticos de la organización también ayudarán en gran medida a prevenir y solucionar los posibles incidentes de seguridad.

Todas estas acciones técnicas y procedimentales de la organización deben tener siempre en cuenta las consideraciones legales que apliquen a la organización por su sector o ámbito, pero también otras como los principios del secreto de las comunicaciones y privacidad de las personas, el código penal, etc. y que requieran ser tenidas en cuenta durante el proceso de

resolución de un incidente, en especial en la toma y adquisición de evidencias que se deriven en un caso de análisis forense.

CONTROLES, HERRAMIENTAS Y MECANISMOS DE DETECCIÓN E IDENTIFICACIÓN DE INCIDENTES DE SEGURIDAD FÍSICA.

La herramienta LUCIA[5] (Listado Unificado de Coordinación de Incidentes y Amenazas), a disposición de los organismos del ámbito de aplicación del ENS, utiliza un sistema de seguimiento de tickets que puede usarse para documentar el desarrollo del ciberincidente y las acciones que se han llevado a cabo en cada momento, correspondientes a las fases de detección, contención, erradicación y recuperación.

Una vez notificado el incidente al organismo afectado por parte del Sistema de Alerta Temprana de Red SARA (SAT-SARA), de Internet (SAT-INET) o para los Sistemas de Control Industrial (SAT-ICS) del CCN-CERT, se realizará un seguimiento del mismo, asignándole un determinado Estado.

CONTROLES, HERRAMIENTAS Y MECANISMOS DE MONITORIZACIÓN, IDENTIFICACIÓN, DETECCIÓN Y ALERTA DE INCIDENTES A TRAVÉS DE LA INVESTIGACIÓN EN FUENTES ABIERTAS (OSINT).

Antes de analizar las fuentes y aplicaciones comunes de la inteligencia de código abierto, es importante comprender qué es realmente. La inteligencia de código abierto:

- Se produce a partir de información disponible públicamente.
- Se recopila, analiza y difunde de manera oportuna a un público apropiado
- Aborda un requisito de inteligencia específico

La frase importante en la que centrarse aquí es «disponible públicamente».

El término «código abierto» se refiere específicamente a la información disponible para el consumo público. Si se requieren habilidades, herramientas o técnicas especializadas para acceder a una información, no puede considerarse razonablemente de código abierto.

---

[5] https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html

Fundamentalmente, la información de código abierto no se limita a lo que puede encontrarse utilizando los principales motores de búsqueda. Las páginas web y otros recursos que se pueden encontrar usando Google ciertamente constituyen fuentes masivas de información de código abierto, pero están lejos de ser las únicas fuentes.

Para empezar, una gran proporción de Internet no se puede encontrar utilizando los principales motores de búsqueda. Esta llamada «web profunda» es una masa de sitios web, bases de datos, archivos y más que no pueden ser indexados por Google, Bing, Yahoo o cualquier otro motor de búsqueda. A pesar de esto, gran parte del contenido de la web profunda puede considerarse de código abierto porque está fácilmente disponible para el público.

Además, hay mucha información de acceso gratuito en línea que se puede encontrar utilizando herramientas en línea que no sean los motores de búsqueda tradicionales. Veremos esto más adelante, pero como un ejemplo simple, herramientas como Shodan y Censys se pueden usar para encontrar direcciones IP, redes, puertos abiertos, cámaras web, impresoras y prácticamente cualquier otra cosa que esté conectada a Internet.

La información también puede considerarse de código abierto si es:

- Publicada o transmitida para una audiencia pública (por ejemplo, contenido de medios de noticias)
- Disponible al público por solicitud (por ejemplo, datos del censo)
- Disponible para el público por suscripción o compra (por ejemplo, revistas de la industria)
- Puede ser visto o escuchado por cualquier observador casual
- Accesible en una reunión abierta al público.
- Obtenido visitando cualquier lugar o asistiendo a cualquier evento que esté abierto al público

Estamos hablando de una cantidad de información verdaderamente inimaginable que está creciendo a un ritmo mucho más alto de lo que cualquiera podría esperar. Incluso si reducimos el campo a una sola fuente de información, Twitter por ejemplo, nos vemos obligados a hacer frente a cientos de millones de nuevos puntos de datos todos los días.

Esto, como probablemente has deducido, es la compensación inherente de la inteligencia de código abierto.

Como analista, tener una cantidad tan grande de información disponible es una bendición y una maldición. Por un lado, tienes acceso a casi todo lo que puedas necesitar, pero por otro lado, debes poder encontrarlo en un torrente de datos que nunca termina.

TIPOS

OSINT se puede clasificar, según el lugar donde se encuentran los datos públicos, en las siguientes categorías:

Internet es el lugar principal donde se encuentran los recursos OSINT, de hecho, muchos investigadores diferencian entre los recursos OSINT en línea y los fuera de línea utilizando el término «Cyber OSINT» para referirse exclusivamente a los recursos de Internet. Los recursos de Internet incluyen lo siguiente: blogs, sitios web de redes sociales, archivos digitales (fotos, vídeos, sonido) y sus metadatos, huellas técnicas de sitios web, cámaras web, web profunda (registros gubernamentales, registros meteorológicos, registros vitales, registros de delincuentes, impuestos y registros de propiedad), recursos de darknet, sitios web de fuga de datos, direcciones IP y cualquier cosa publicada en línea públicamente.

- Canales de medios tradicionales como TV, radio, periódicos y revistas.
- Publicaciones académicas como disertaciones, trabajos de investigación, revistas especializadas y libros.
- Documentos corporativos tales como perfiles de empresas, actas de congresos, informes anuales, noticias de empresas, perfiles de empleados y currículums.
- Información geoespacial como mapas en línea, imágenes de satélite comerciales, información de ubicación geográfica asociada a publicaciones en redes sociales, seguimiento de transporte (aéreo, marítimo, de vehículos y ferroviario).

Ahora que hemos cubierto los conceptos básicos de la inteligencia de código abierto, podemos ver cómo se usa comúnmente para la ciberseguridad.

Hay dos casos de uso comunes: hacking ético e identificación de amenazas.

Hacking ético y pruebas de penetración: Los profesionales de seguridad usan inteligencia de código abierto para identificar posibles debilidades en redes amigables para que puedan ser remediados antes de que sean explotados por actores de amenazas.

Las debilidades encontradas comúnmente incluyen:

- Fugas accidentales de información confidencial, como a través de las redes sociales.
- Puertos abiertos o dispositivos no seguros conectados a Internet
- Software sin parches, como sitios web que ejecutan versiones antiguas de productos CMS comunes
- Activos filtrados o expuestos, como código propietario en pastebins

Identificación de amenazas externas: Internet es una excelente fuente de información sobre las amenazas más apremiantes de una organización.

Desde la identificación de las nuevas vulnerabilidades que se explotan activamente hasta la interceptación de la «charla» del actor de amenazas sobre un próximo ataque, la inteligencia de código abierto permite a los profesionales de seguridad priorizar su tiempo y recursos para abordar las amenazas actuales más importantes.

En la mayoría de los casos, este tipo de trabajo requiere que un analista identifique y correlacione múltiples puntos de datos para validar una amenaza antes de tomar medidas. Por ejemplo, si bien un solo tweet amenazante puede no ser motivo de preocupación, ese mismo tweet se vería de una manera diferente si estuviera vinculado a un grupo de amenazas que se sabe que está activo en una industria específica.

Una de las cosas mas importantes que hay que tener en cuenta sobre la inteligencia de código abierto es que a menudo se usa en combinación con otros subtipos de inteligencia.

La inteligencia de fuentes cerradas, como la telemetría interna, las comunidades cerradas de web oscura y las comunidades externas de intercambio de inteligencia, se usa regularmente para filtrar y verificar la inteligencia de código abierto.

Hay una variedad de herramientas disponibles para ayudar a los analistas a realizar estas funciones, que veremos más adelante.

El lado oscuro de la inteligencia de código abierto

En este punto, es hora de abordar el segundo problema importante con la inteligencia de código abierto: si hay algo disponible para los analistas de inteligencia, también está disponible para los actores de amenazas.

Los actores de amenazas utilizan herramientas y técnicas de inteligencia de código abierto para identificar objetivos potenciales y explotar las debilidades en las redes objetivo. Una vez que se identifica una vulnerabilidad, a menudo es un proceso extremadamente rápido y simple explotarla y lograr una variedad de objetivos maliciosos.

Este proceso es la razón principal por la cual tantas pequeñas y medianas empresas son pirateadas cada año. No se debe a que los grupos de amenazas se interesen específicamente en ellos, sino a que se encuentran vulnerabilidades en la arquitectura de su red o sitio web utilizando técnicas simples de inteligencia de código abierto. En resumen, son objetivos fáciles.

Y la inteligencia de código abierto no solo permite ataques técnicos a los sistemas y redes de TI. Los actores de amenazas también buscan información sobre individuos y organizaciones que puedan usarse para informar campañas sofisticadas de ingeniería social mediante phishing (correo electrónico), vishing (teléfono o correo de voz) y SMiShing (SMS).

A menudo, la información aparentemente inocua que se comparte a través de redes sociales y blogs se puede utilizar para desarrollar campañas de ingeniería social muy convincentes, que a su vez se utilizan para engañar a los usuarios bien intencionados para que comprometan la red o los activos de la organización.

Esta es la razón por la que es tan importante utilizar la inteligencia de código abierto con fines de seguridad: te ofrece la oportunidad de encontrar y corregir las debilidades en la red de tu organización y eliminar información confidencial antes de que un actor de amenazas use las mismas herramientas y técnicas para explotarlas.

Técnicas de inteligencia de código abierto

Ahora que hemos cubierto los usos de la inteligencia de código abierto (tanto buenos como malos), es hora de ver algunas de las técnicas que se pueden utilizar para recopilar y procesar información de código abierto.

Primero, hay que tener una estrategia y un marco claros para adquirir y utilizar la inteligencia de código abierto. No se recomienda abordar la inteligencia de código abierto desde la perspectiva de encontrar cualquier cosa y todo lo que pueda ser interesante o útil. Como ya indicamos, el gran volumen de información disponible a través de fuentes abiertas simplemente es abrumador.

En su lugar, se debe saber exactamente lo que estás tratando de lograr, por ejemplo, para identificar y remediar las debilidades en tu red, y concentrar tus energías específicamente en el logro de esos objetivos.

En segundo lugar, debes identificar un conjunto de herramientas y técnicas para recopilar y procesar información de código abierto. Una vez más, el volumen de información disponible es demasiado grande para que los procesos manuales sean incluso ligeramente efectivos.

En términos generales, la recopilación de inteligencia de código abierto se divide en dos categorías: recopilación pasiva y recopilación activa.

Recopilación pasiva

La recopilación pasiva a menudo implica el uso de plataformas de inteligencia de amenazas (TIP) para combinar una variedad de fuentes de amenazas en una única ubicación de fácil acceso.

Si bien este es un paso importante desde la recolección manual de inteligencia, el riesgo de sobrecarga de información sigue siendo significativo.

Las soluciones de inteligencia de amenazas más avanzadas como Recorded Future resuelven este problema mediante el uso de inteligencia artificial, aprendizaje automático y procesamiento del lenguaje natural para automatizar el proceso de priorizar y descartar alertas basadas en las necesidades específicas de una organización.

De manera similar, los grupos organizados de amenazas a menudo usan botnets para recopilar información valiosa utilizando técnicas como el rastreo de tráfico y el registro de teclas.

Recopilación activa

Por otro lado, la recopilación activa es el uso de una variedad de técnicas para buscar información o conocimientos específicos.

Para los profesionales de seguridad, este tipo de trabajo de recolección generalmente se realiza por una de dos razones:

Una alerta recopilada pasivamente ha puesto de manifiesto una amenaza potencial y se requiere una mayor comprensión.

El enfoque de un ejercicio de recopilación de inteligencia es muy específico, como un ejercicio de prueba de penetración.

Herramientas OSINT

Para cerrar las cosas, veremos algunas de las herramientas más utilizadas para recopilar y procesar inteligencia de código abierto.

Si bien hay muchas herramientas gratuitas y útiles disponibles para profesionales de la seguridad y actores de amenazas por igual, algunas de las herramientas de inteligencia de código abierto más utilizadas son motores de búsqueda como Google, pero no como la mayoría de nosotros los conocemos.

Como ya hemos explicado, uno de los mayores problemas que enfrentan los profesionales de la seguridad es la regularidad con la que los usuarios normales y bien intencionados dejan accidentalmente activos e información sensibles expuestos a Internet. Hay una serie de funciones de búsqueda avanzada que se pueden utilizar para identificar la información y los activos que exponen.

Más allá de los motores de búsqueda, hay literalmente cientos de herramientas que se pueden usar para identificar las debilidades de la red o los activos expuestos.

Dando un paso más allá, podrías usar una solución de inteligencia de amenazas más avanzada como Recorded Future para determinar si una vulnerabilidad se está explotando activamente o si está incluida en algún kit de explotación activo.

Por supuesto, los ejemplos dados aquí son solo una pequeña fracción de lo que es posible usando herramientas de inteligencia de código abierto.

Hay una gran cantidad de herramientas gratuitas y premium que se pueden utilizar para buscar y analizar información de código abierto, con funcionalidades comunes que incluyen:

- Búsqueda de metadatos
- Búsqueda de código
- Investigación de personas e identidad.
- Número de teléfono de investigación
- Búsqueda y verificación de correo electrónico
- Vinculación de cuentas de redes sociales
- Análisis de imagen
- Investigación geoespacial y mapeo
- Detección de redes inalámbricas y análisis de paquetes.

Vamos a analizar las herramientas más importantes:

Maltego

Maltego es desarrollado por Paterva y es utilizado por profesionales de seguridad e investigadores forenses para recopilar y analizar inteligencia de código abierto. Puede recopilar fácilmente información de varias fuentes y usar varias transformaciones para generar resultados gráficos.

Las transformaciones están incorporadas y también se pueden personalizar según el requisito. Maltego está escrito en Java y viene preempaquetado en Kali Linux.

Para usar Maltego, se requiere el registro del usuario, que es gratuito. Una vez que los usuarios registrados pueden usar esta herramienta para crear la huella digital del objetivo en Internet.

Shodan

Google es el motor de búsqueda para todos, pero Shodan es el motor de búsqueda para los piratas informáticos. En lugar de presentar el resultado como otros motores de búsqueda, mostrará el resultado que tendrá más sentido para un profesional de la seguridad.

Como profesional certificado en seguridad de la información, una de las entidades importantes es la red y los activos digitales. Shodan proporciona mucha información sobre los activos que se han conectado a la red.

Los dispositivos pueden variar de ordenadores, portátiles, cámaras web, señales de tráfico y varios dispositivos IOT. Esto puede ayudar a los analistas de seguridad a identificar el objetivo y probarlo para detectar varias vulnerabilidades, configuraciones predeterminadas o contraseñas, puertos disponibles, pancartas y servicios, etc.

Google Dorks

Google es uno de los motores de búsqueda más utilizados cuando se trata de encontrar cosas en Internet. Para una sola búsqueda, los resultados pueden ser de varios cientos de páginas ordenadas por orden de relevancia.

Los resultados varían de anuncios, sitios web, publicaciones en redes sociales, imágenes, etc. Google Dorks puede ayudar a un usuario a orientar la búsqueda o indexar los resultados de una manera mejor y más eficiente.

Digamos que el usuario quiere buscar la palabra nombres de usuario pero solo requiere los resultados con archivos PDF y no con sitios web. Esto se hace de la siguiente manera: <Tipo de archivo: busca una cadena particular en un archivo pdf>

Algunas de las otras opciones de indexación son:

Inurl: busca una cadena en la URL de la página.

Intitle: para buscar el título de una palabra clave.

Ext: para buscar una extensión particular.

Intext: busca un texto en particular en una página.

A veces también se conoce como pirateo de Google.

Harvester

Harvester es una excelente herramienta para obtener información relacionada con el correo electrónico y el dominio. Este está incluido previamente en Kali y puede ser muy útil para obtener información.

Metagoofil

Metagoofil está escrito por Christian Martorella y es una herramienta de línea de comandos que se utiliza para recopilar metadatos de documentos públicos. La herramienta viene incluida en Kali Linux y tiene muchas características que buscan el tipo de documento en el destino, descarga local, extracción de metadatos e informes de resultados.

Por ejemplo: los usuarios pueden escanear en busca de un tipo particular de documentos en un dominio particular. Metagoofil –d nmap.org –t pdf.

Recon-ng

Recon-ng es una gran herramienta para la recopilación de información de destino. Esto también se incluye en Kali. El poder de esta herramienta radica en el enfoque modular.

Para aquellos que han usado Metasploit, conocerán el poder de las herramientas modulares. Se pueden usar diferentes módulos en el destino para extraer información según las necesidades. Simplemente agrega los dominios en el espacio de trabajo y usa los módulos.

Check user names

Los sitios web de redes sociales contienen mucha información, pero será muy aburrido y tomará tiempo si necesitas verificar si un nombre de usuario en particular está presente en algún sitio web de redes sociales.

Para obtener dicha información, hay un sitio web www.checkusernames.com. Buscará la presencia de un nombre de usuario en particular en más de 150 sitios web. Los usuarios pueden verificar la presencia de un objetivo en un sitio web en particular para hacer que el ataque sea más específico.

Una versión más avanzada del sitio web es https://knowem.com que tiene una base de datos más amplia de más de 500 sitios web junto con algunos servicios más.

Tineye

Tineye se utiliza para realizar una búsqueda relacionada con la imagen en la web. Tiene varios productos como el sistema de alerta de tineye, API de búsqueda de color, motor móvil, etc. Puede buscar si una imagen ha estado disponible en línea y dónde ha aparecido esa imagen.

Tineye utiliza redes neuronales, aprendizaje automático y reconocimiento de patrones para obtener los resultados. Utiliza la coincidencia de imágenes, la identificación de marcas de agua, la coincidencia de firmas y varios otros parámetros para hacer coincidir la imagen en lugar de la coincidencia de palabras clave.

El sitio web ofrece extensiones de API y extensiones de navegador también. Simplemente puede visitar la imagen y hacer clic derecho sobre ella para seleccionar buscar en tineye.

Search code

Buscar texto es fácil en comparación con buscar un fragmento de código. Intenta buscar un ejemplo de código en Google y solicita que no te dé resultados irrelevantes.

El código de búsqueda te ofrece una función para buscar una línea de código que podría haber estado presente en varios sitios web para compartir códigos como Github, etc. Los usuarios pueden buscar funciones o métodos, variables, operaciones, fallos de seguridad y cualquier cosa que pueda constituir un segmento de código.

Los usuarios pueden buscar cadenas tan simples como «a ++» métodos demasiado complejos. Los resultados de búsqueda se pueden filtrar aún más en función de un repositorio o idioma en particular.

Cualesquiera que sean sus objetivos, la inteligencia de código abierto puede ser tremendamente valiosa para todas las disciplinas de seguridad.

En última instancia, sin embargo, encontrar la combinación correcta de herramientas y técnicas para tus necesidades específicas llevará tiempo, así como un grado de prueba y error. Las herramientas y técnicas que necesitas para identificar activos inseguros no son las

mismas que te ayudarían a realizar un seguimiento de una alerta de amenaza o conectar puntos de datos a través de una variedad de fuentes.

El factor más importante para el éxito de cualquier iniciativa de inteligencia de código abierto es la presencia de una estrategia clara: una vez que sepas lo que estás tratando de lograr y hayas establecido los objetivos en consecuencia, identificar las herramientas y técnicas más útiles será mucho más realizable.