Uso de herramientas combinadas de análisis de malware y enriquecimiento de resultados

Abstract: a medida que aumenta la complejidad de los sistemas informáticos y crece la dependencia de estos por parte de empresas y organismos, aumentan también las amenazas a las que se ven expuestos. La superficie de exposición no deja de crecer y se hace necesario contar con medios igual de evolucionados para contrarrestar este crecimiento, de forma que se puedan tomar decisiones en tiempo real para proteger los activos que, además, estén fundamentadas en datos y tengan, por lo tanto, una base legítima.

Contenido:

1. CONTEXTO

Como se indicaba en el *Informe de Amenazas y Tendencias Edición 2020*[1], el uso de técnicas de ingeniería social sigue siendo uno de los principales vectores de ataque utilizados. Este tipo incidentes de seguridad está en auge: "Fraude al CEO", spear-phishing basados en información pública o robada sobre las víctimas, correos con falsas facturas o multas, correos que indicar al usuario que debe acceder a un enlace, etc.

El correo electrónico destaca con claridad como el canal más utilizado, a través del que se realizan campañas de phishing que, mediante la suplantación de servicios o personas, incitan al receptor del correo electrónico a descargar un fichero adjunto, pulsar en un enlace, facilitar determinada información o incluso a realizar una acción concreta; por ejemplo: una transferencia bancaria.

En este escenario se plantea la necesidad de contar con herramientas o plataformas que permitan cubrir la mayor parte de vectores de amenazas que afectan a una superficie de ataque creciente y que además permitan a los usuarios, que en muchos casos forman parte de la ejecutiva de empresas y organismos, tomar decisiones rápidas para poner a salvo sus activos basadas en datos reales, fidedignos y fáciles de comprender.

[1]Informe de Amenazas y Tendencias Edición 2020. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

De esta forma, y con el objetivo de evitar que el mayor número de amenazas que afectan a los activos de empresas y organismos se materialicen en incidentes de seguridad, es necesario disponer de tecnologías que analicen en tiempo real los activos expuestos (electrónica de red, sistemas operativos o servidores de aplicaciones entre otros) y procedan de la forma más automática posible. Esta rapidez se fundamenta en la necesidad tanto de optimización de recursos como de minimización del tiempo de respuesta.

2. ANÁLISIS DE AMENAZAS

Las tecnologías de seguridad implementan mecanismos de análisis que permiten detectar amenazas conocidas y no conocidas, clasificándose según su funcionamiento y amenazas potenciales en análisis estáticos y dinámicos.

2.1 Amenazas conocidas

Se denominan amenazas conocidas a aquellos elementos sospechosos o muestras de malware que han sido identificadas previamente mediante un proceso de análisis por parte de investigadores expertos reconocidos, y que han sido incorporadas a una base de datos pública o privada de un fabricante de soluciones antimalware o de un centro de respuesta a incidentes.

2.2 Amenazas no conocidas

Se denominan amenazas no conocidas a aquellos elementos sospechosos o muestras de malware que no han sido identificadas previamente por ningún fabricante u organismo, no formando parte de base de datos alguna de una solución de seguridad y siendo necesario por lo tanto detectarlas mediante métodos heurísticos o dinámicos de perfilado y comportamiento.

2.3 Análisis estático

Se denomina análisis estático al realizado sobre una muestra (fichero, URL o cualquier elemento sospechoso) sin detonar, es decir, sin acceder al mismo si se trata de un documento, sin ejecutarlo si se trata de un archivo ejecutable o sin acceder al recurso web si se trata de una dirección sospechosa.

Para ello, las herramientas de análisis estático como son las soluciones *endpoint* o el software antivirus, analizan constantemente la memoria del activo y recorren sus sistemas de ficheros en busca de posibles amenazas conocidas, comparando constantemente sus propiedades con una base de datos mantenida por el fabricante o por la comunidad de usuarios.

Una vez detectada la amenaza, estas soluciones eliminan la muestra que la originó o la colocan en cuarentena, avisando al usuario para que pueda tomar las medidas que

considere oportunas. Este planteamiento tiene una serie de ventajas y como contrapartida, algunas carencias básicas:

- Ventaja: este tipo de análisis es muy rápido, al realizarse en la mayoría de los casos una comparación del *hash* (cadena de caracteres identificativa del fichero que resulta de aplicar un algoritmo matemático unidireccional) con una base de datos de *hashes* existente, obteniendo el veredicto en milisegundos.
- Carencia: la efectividad de este proceso depende de que las muestras estén catalogadas en la base de datos del fabricante con anterioridad a la materialización de la amenaza, por lo que es posible que una muestra de malware de reciente creación no sea detectada.
- Ventaja: en muchos casos, las soluciones de software de análisis estático cuentan con la posibilidad de identificar algunos comportamientos de las muestras que se hayan saltado esa primera identificación, de forma que, si coinciden con los perfiles que el fabricante ha determinado, se pueda detener la amenaza y clasificarlos adecuadamente.
- Carencia: este proceso implica que la muestra se ha saltado ese paso previo y está actualmente en proceso de ejecución sobre el activo afectado, proceso que normalmente implica que este activo ya está comprometido y hace necesaria una valoración sobre la extensión del daño y las probabilidades de que comprometa el resto de la infraestructura.

2.4 Análisis dinámico

Se denomina análisis dinámico al realizado sobre la detonación de la muestra (la apertura del documento, la ejecución del archivo o el acceso real al recurso web) en un entorno controlado conocido como *sandbox*. Una *sandbox*, por lo tanto, es un entorno de análisis y detonación que, entre otras herramientas, cuenta con máquinas virtuales que simulan los activos de una empresa u organismo.

Mediante el análisis del proceso de detonación, las herramientas y plataformas de análisis dinámico son capaces de elaborar un perfil en base a las operaciones realizadas y los cambios registrados sobre el sistema operativo de estas máquinas virtuales. Este perfil se valora gracias a una métrica que asigna, a una muestra, una probabilidad de ser maliciosa en función de las amenazas que genera para estos sistemas.

La clave está en que, a diferencia de un análisis estático, cuyos resultados pueden estar avalados por un proceso de investigación que ha catalogado la muestra con anterioridad, en el análisis dinámico se hace necesaria de forma habitual la revisión por parte de un analista experto para determinar si el resultado asignado es el correcto o se trata de un falso positivo o negativo.

Por lo tanto, este tipo de análisis tiene una serie de ventajas frente al análisis estático y como contrapartida, una serie de carencias:

- Ventaja: este análisis no depende de una base de datos de amenazas de un fabricante, por lo que podría detectar potencialmente cualquier tipo de amenaza de forma independiente a la evolución o estado de mantenimiento de las soluciones de seguridad.
- Carencia: los resultados del análisis no han sido corroborados por un analista experto, por lo que es posible encontrarse ante un falso positivo (en caso de que la muestra o elemento sospechoso despliegue un comportamiento excesivamente agresivo) o ante un falso negativo (en caso de que la muestra o elemento sospechoso esté preparado para reducir su perfil de actividad si detecta que está siendo analizado o si no dispone de los elementos necesarios para su detonación).
- Ventaja: la detonación del elemento no se produce en ningún caso sobre los activos de la empresa u organización, por lo que es posible comprobar los efectos de este proceso en sistemas completamente aislados y ajenos a la misma.
- Carencia: en el caso de amenazas dirigidas y preparadas para atacar una tecnología en concreto los resultados de la detonación no serán del todo satisfactorios al no poder desarrollarse en su totalidad.
- Ventaja: es posible realizar plantillas de análisis usando como base los activos de la empresa u organización, simulando en casos más extremos la totalidad de su infraestructura.
- Carencia: estos sistemas de análisis requieren de potencia de computación y un uso extensivo de recursos, por lo que tradicionalmente no están al alcance de todas las empresas u organismos.

3. ADA - ANÁLISIS COMBINADO AUTOMATIZADO

El CCN-CERT ha puesto a disposición de las organizaciones dos (2) soluciones que cubren estos tipos de análisis: MARÍA, una plataforma de análisis estático para detectar amenazas conocidas; y MARTA, una plataforma de análisis dinámico para detectar amenazas no conocidas.

La evolución de las amenazas y el incremento constante de la superficie de exposición de empresas y organismos hace necesario impulsar una evolución paralela de estas soluciones, en donde:

- MARTA y MARÍA interactúen entre sí, compartiendo resultados y ayudándose mutuamente a detectar tanto las amenazas conocidas como las no conocidas.

- La reutilización de la información y resultados de un análisis mejore la capacidad de análisis y detección general, detectando campañas de malware mediante la correlación de los mismos.
- Se aporten datos a la organización que ayuden a justificar su decisión de aislar o destruir la muestra analizada.
- La presentación de resultados pueda ser interpretada por diferentes perfiles sin necesidad de ser personal investigador.

Del proceso natural de la evolución tecnológica, y con el objetivo de dar respuesta a las necesidades planteadas anteriormente, el CCN-CERT pone a disposición de su comunidad la solución ADA, una nueva plataforma de análisis avanzado de malware capaz de conseguir un análisis en profundidad, similar al resultante de un proceso de investigación en detalle.

Con ella, el CCN-CERT ofrece una solución integral con una interfaz simple, sencilla y con resultados interpretables dentro de un proceso complejo de investigación. ADA es la evolución natural de las capacidades de análisis dinámico (MARTA) y las capacidades de análisis estático (MARÍA), de forma que desde el interfaz de ADA y de forma unificada, el usuario puede acceder a todas las características que ya ofrecían por separado ambas soluciones y a las nuevas que resultan de su uso combinado.

ADA ofrece entre otras las siguientes ventajas:

- **Interfaz unificado**: ADA permite acceder a las capacidades de análisis de MARTA y MARÍA desde un solo interfaz, de manera que los usuarios solo tienen que aprender a usar e interpretar los resultados de una única herramienta.
- **Interacción completa con el proceso de análisis**: ADA muestra en tiempo real los resultados de proceso de análisis en las máquinas virtuales de análisis empleadas, permitiendo a los usuarios analistas autorizados incluso la interacción directa con el mismo.
- **Perfil ejecutivo**: ADA surge de la necesidad de acercar la complejidad de los resultados obtenidos a un público que puede no tener los conocimientos requeridos para interpretar sus resultados pero que tiene que consumirlos para tomar decisiones estratégicas.

  Para ello, ADA interpreta y simplifica los resultados obtenidos, dando acceso también al personal que lo requiera a aquellos que pueden ser utilizados en procesos de investigación compleja.
- **Entorno de análisis aislado:** la información que es analizada por ADA solo puede ser consultada por los propios usuarios, por lo que su privacidad está asegurada. Además, ADA no utiliza plataforma alguna de terceros para el análisis de las muestras, todas las consultas se realizan en base a elementos que forman parte de la plataforma.

- **Estadística e información actuable:** ADA utiliza el cómputo total de los análisis del usuario para generar estadísticas que permiten saber el nivel de amenaza medio al que se enfrentan los activos de una organización, así como determinar cuál es la tendencia y patrones de ataque que siguen las muestras que han sido analizadas.
- **Generación de informes automáticos:** tras finalizar un análisis, ADA genera un informe ejecutivo que es enviado por correo al usuario, para que pueda adjuntarlo como evidencia al proceso de detección de la amenaza.
- **Capacidades de investigación avanzadas:** ADA incluye la posibilidad de generar un informe de investigación completo. Además, los investigadores pueden revalorar el resultado del análisis de forma que los procesos de correlación y la base de datos de amenazas interna se beneficien de ello.
- **Potencia de análisis:** ADA incorpora en una sola plataforma gran cantidad de herramientas de análisis estático y dinámico cuyo acceso comercial supondría un gran coste para sus usuarios, cerrando en este caso la brecha tecnológica que se produce por la asimetría entre los recursos utilizados por los atacantes y las víctimas.