METODOLOGÍA CTI – INVESTIGACIÓN RANSOMWARE

Índice

1. Objetivos

El principal objetivo de este trabajo es crear una estrategia efectiva para proteger a las organizaciones ante una amenaza tan creciente en el ciber mundo como es el ransomware. Para lograr este objetivo se debe crear una metodología muy precisa, pues esta técnica es utilizada frecuentemente por los hackers, especialmente para atacar los sectores industriales estratégicos de la economía de un país, ya que estas empresas suelen ser las poseedoras de la información más sensible, y por lo tanto la más valiosa.

Uno de los objetivos es conocer a fondo a nuestros enemigos y para ellos debemos plantearnos quiénes son los potenciales adversarios de nuestra empresa, qué tipo de amenazas utilizan, donde suelen atacar, cuando atacan, porque lo hacen y cómo operan.

Otro de los objetivos centrales es tratar de prevenir el ataque antes de que ocurra, y para ello debemos crear una red de seguridad empresarial.

Los hackers siempre quieren negociar, ya que los datos obtenidos no les suelen ser útiles, por lo que se deben conocer los procesos de negociación para poder obtener el mayor beneficio posible de la negociación.

Además, existen informes que aseguran que las empresas españolas son más vulnerables a un ataque de ransomware que la media mundial, demostrándose así la importancia de crear una metodología como esta.

Es importante también educar a los trabajadores para que sean conscientes de los peligros que existen en el mundo digital, y concienciar de que cualquiera de ellos puede ser la puerta de acceso utilizada por los hackers para ejecutar el ransomware, por lo que se deben dar cursos de ciberseguridad a todos los empleados.

2. Selección del threat actor a investigar

En cuanto a la victimología, para poder analizar que empresas similares a la nuestra han sido atacadas con ransomware y evaluar la vulnerabilidad, las fuentes más fiables son:

- https://ransomwatch.telemetry.ltd/
- https://ransomlook.io
- https://www.ransomware.live/#/.

En cuanto a localizar ataques a empresas de nuestra área geográfica, las fuentes que se pueden usar son las siguientes:

- https://cybermap.kaspersky.com/special/ransomware/es
- https://www.comparitech.com/blog/information-security/global-ransomware-attacks/
- https://threatmap.fortiguard.com/

Para conocer qué víctimas importantes han sufrido ransomware, incluyendo ejemplos, se pueden consultar las siguientes fuentes:

- https://www.welivesecurity.com/es/
- https://www.comparitech.com/es/antivirus/estadisticas-ransomware/
- https://www.sophos.com/es-es/whitepaper/state-of-ransomware

3. Obtención de reportes de fuentes públicas o privadas

A la hora de investigar un Threat Actor, es importante revisar qué análisis existen por partes de terceros, ya sean fuentes públicas o privadas.

Fuentes públicas

Cuando hay una tendencia muy clara y hay un incremento exponencial de ataques por parte de un grupo de ransomware, es posible que los principales diarios electrónicos relacionados con el mundo de la ciberseguridad estén haciendo eco. Por lo que pueden ser una buena fuente para coger contexto de la amenaza.

Los más destacables son:

- https://elhacker.net/
- https://www.bleepingcomputer.com/
- https://thehackernews.com/
- https://www.darkreading.com/
- https://www.securityweek.com/

Otras fuentes públicas interesantes suelen ser los blogs de *vendors*. Estos reportes suelen ser más completos y técnicos que los anteriores. Los más interesantes suelen ser:

- https://www.mandiant.es/
- https://www.trendmicro.com/
- https://www.kaspersky.es/
- https://www.group-ib.com/
- https://www.crowdstrike.com/es-es/
- https://unit42.paloaltonetworks.com/
- www.recordedfuture.com/
- https://socradar.io/

Fuentes privadas

Una gran parte de empresas, disponen de un SaaS de Threat Intelligence en los que pueden encontrar análisis hechos y actualizados por analistas de inteligencia del propio SaaS. Este tipo de reportes suelen ser más completos y más técnicos que los públicos, por lo que pueden ser una gran fuente de información. Estos reportes suelen contener perfil del actor, análisis de malware, reglas de detección, paquetes para threat hunting, análisis de los últimos ciberataques.

Estos productos suelen ser interesantes también para analizar tendencias. Por ejemplo: qué ataques afectan más a nuestro sector y a nuestro país. Podremos ver qué vulnerabilidades se están explotando más, métodos de ataque más usados en un periodo de tiempo en concreto, atacantes más activos, sector al que se está atacando más, etc.

Aparte, este tipo de *vendors* te permiten monitorizar la red de manera más sencilla, rápida y eficaz que una herramienta de código abierto.

4. Obtención de muestras de las herramientas / malware usados por el threat actor para realizar un análisis estático / dinámico

Honeypots: sistema para atraer adversarios como señuelo para que realicen un ataque sobre el sistema. Dando lugar a la obtención de muestras de malware lanzadas en el servidor Honeypot.

VirusTotal: ofrece la opción de cargar archivos para examinarlos y obtener detalles sobre un hash, IP o URL, incluyendo su comportamiento, detecciones y conexiones con otras muestras a través de elementos como el proceso padre o los archivos que genera. También posibilita la creación de reglas para identificar nuevas muestras vinculadas a campañas de adversarios, así como la utilización de reglas Yara para detectar y analizar nuevas muestras.

Valhalla YARA Rules: plataforma con una enorme base de datos de reglas Yara y Sigma, donde filtrando por reglas yara de interés permite obtener hashes de muestras detectadas por estas.

MISP: plataforma de inteligencia para compartir amenazas.

MalwareBazaar: base de datos de muestras de malware, donde están catalogadas y permite buscar muestras.

ThreatFox: base de datos con IoCs, etiquetados los malwares, facilitando la búsqueda por familia.

Hybrid Analysis: permite obtención de muestras a través del uso de reglas Yara.

AlienVault: dispone de un repositorio enorme de muestras para búsqueda de estas y relacionar con otra.

5. Afiliación del TA con otros grupos (IABs, APTs, etc.)

Análisis general del adversario como las TTPs con el fin de detectar coincidencias que permitan potenciales atribuciones a otro grupo. Esto implica un análisis de objetivos de los aspectos compartidos, especialmente en el código de malware y las herramientas utilizadas, para determinar posibles afiliaciones.

MITRE ATT&CK: permite localizar grupos y sus posibles afiliaciones, como sus TTPs, herramientas empleadas, etc.

ThreatMiner: obtención de información de un adversario y obtención de información de reporte realizados por otras empresas, ayudando a obtener IoCs, herramientas, objetivos recientes y si se correlacionan con algún otro grupo

apt.etda.or[.]th: permite realizar búsquedas sobre adversarios, herramientas. Muestra información sobre afiliaciones de un adversario, motivaciones, herramientas empleadas, operaciones, sectores a los que se dirige. Además, buscando por herramienta permite ver qué grupos la emplean.

Crowdstrike: para obtener información de adversarios.

CISA: tiene una base de datos enorme para obtener información de adversarios

Socradar.io: permite buscar perfiles de amenazas muy completos

6. Negociación del rescate con el grupo: Precios que dan los threat actors, descuentos, técnicas negociación

La negociación de rescate con un grupo de ransomware es una cuestión comprometida ya que existen dos vertientes ante esta idea, la de negociar para recuperarse del ataque y la de muchas instituciones como por ejemplo, el FBI que aconseja a las víctimas que eviten negociar con los piratas informáticos, argumentando que pagar rescates incentiva el comportamiento criminal, además de no asegurar la liberación de los datos, la extorsión puede continuar, igualmente es posible que expongan los datos robados públicamente, etc.

Lejos de entrar en esta diversidad de opiniones, una posible negociación es importante para ambos bandos y tienen que estar preparados para ello.

Los grupos de ransomware disponen de personal encargado de investigar a la empresa objetivo para saber cómo pueden negociar, lo que pueden demandar e intentar cerrar un acuerdo con la organización víctima y así salir victoriosos del ataque.

Por otro lado, la empresa que sufre el ataque tiene que valorar si llevar a cabo la negociación, esto dependerá de qué haya sido comprometido, hasta dónde puede llegar la extorsión, y saber si hay backups para recuperarse del cometido de los cibercriminales. Para esta búsqueda, se pueden usar herramientas como **Malpedia** o **Ransomlook**.

Antes de comenzar la negociación, los expertos en la materia como pueden ser **GroupSense** o **Coveware** recomiendan asegurarse que la organización ha sido aislada del ataque y los ciberdelincuentes han sido expulsados de la red de la víctima. Tras ello, también habrá un equipo que, como en el grupo de ransomware, se encargue de recopilar toda la información del ataque, perfil del atacante, hechos anteriores, etc.

Si finalmente se decide iniciar la negociación los expertos recomiendan:

- Empezar a restaurar algunos de sus sistemas mediante backups, y junto con ello, alargar la negociación ya que puede suponer una ventaja para la empresa.
- Tratar la situación como una transacción comercial habitual.
- Ser persuasivos, siendo amables, incluso alabando su trabajo. Es importante no ser agresivos ya que se podría truncar la negociación.
- Generalmente, los cibercriminales suelen pedir el 20% de las ganancias en forma de rescate, pero siempre están dispuestos a negociar. Por ejemplo, un gran descuento que se podría obtener es por “pronto pago”.

7. Posible solapamiento del TA con otros grupos (código, herramientas, infraestructura, etc)

Tras evaluar el comportamiento y movimientos de diferentes grupos de ransomware, desde Kaspersky llegaron a la conclusión de que la mayoría seguía un mismo patrón. Como muchos desarrolladores, los cibercriminales no dejan de lado la posibilidad de la reutilización de código y de herramientas open source. Esto hace que se puedan trazar unos esquemas o modelos para saber qué harán y cómo funcionan en cada fase del ataque y así, poder estar prevenidos.

Esta información está recogida y catalogada en **MITRE ATT&CK**: (https://attack.mitre.org/groups/ y https://attack.mitre.org/software/)

También, resulta útil revisar informes de *vendors* como **Kaspersky** en el que analizan estas secuencias.

8. Búsqueda de infraestructura del threat actor

Para realizar una búsqueda de la infraestructura del threat actor podemos utilizar diferentes servicios y herramientas:

Existen diferentes servicios online que contienen información sobre grupos de ransomware, como por ejemplo **Ransomwatch**, **Ransomlook**, **Ransomwarelive**.

También se puede realizar una búsqueda sobre el actor en **Malpedia** y de esta forma obtener información relacionada sobre este e incluso reglas yara de detección.

Como hemos comentado anteriormente, es de gran utilidad obtener diferentes informes de empresas del sector sobre el actor en cuestión. Algunas de ellas pueden ser: **Mandiant**, **Unit42**, **Kaspersky**, **Crowdstrike**, **Group Ib**, **Recorded Future**, **Socradar**.

Finalmente podemos utilizar diferentes **Google Dorks** para la búsqueda que estamos llevando a cabo:

Ej; buscar informes de diferentes empresas sobre el actor, en este caso del equipo de **unit42**.

site:unit42.paloaltonetworks.com "nombre actor"

Ej; buscar alguna información sobre el actor en cuestión que contenga “mitre” o “mitre att&ck”

“nombre actor” mitre

“nombre actor” mitre att&ck

“nombre actor” “mitre att&ck”

De esta forma, obteniendo siempre información relacionada de mitre sobre el actor podemos obtener en muchas ocasiones información relevante de la infraestructura de este.

9. Reglas de detección

Para obtener diferentes reglas de detección dedicadas al actor en cuestión, podemos revisar también algunos informes en los cuales suelen añadir reglas tipo **Yara** o **Sigma**.

En servicios como **Malware Bazar** o **Alien Vault** se pueden encontrar, además de diferentes muestras utilizadas por el actor, algunas reglas Yara.

También, al realizar una búsqueda sobre el actor en **Malpedia** se pueden obtener diferentes reglas Yara. Otro servicio bastante completo para encontrar este tipo de reglas es **YARAify**. Finalmente se puede realizar el siguiente dork para encontrar reglas sobre el actor: “nombre actor” yara rule

Para el caso de las reglas Sigma, un servicio esencial de referencia es **SOCprime**. También se podrían realizar búsquedas para el actor en cuestión en el **repositorio oficial** de reglas Sigma. Y finalmente se podría también realizar un dork parecido al anterior para encontrar reglas: “nombre actor” yara rule

Existe también el servicio online **Valhalla** que contiene tanto reglas Yara como Sigma.

10. Recomendaciones para prevenir el ataque del TA.

Las recomendaciones para prevenir un ataque de un TA pueden fluctuar dependiendo de la amenaza, los puntos de acceso que utilicen, etc.

En primer lugar, se deben tener los básicos:

- Que los empleados dispongan de un gestor de contraseñas como 1Password es muy importante. Tener credenciales robustas y distintas en cada plataforma que usemos puede prevenir el acceso o movimiento lateral de un Threat Actor.
- 2FA. El segundo factor de autenticación es fundamental para el acceso a software.
- EDR actualizado. Disponer de un EDR actualizado puede ayudar a la detección de actividad sospechosa en la red de la empresa.

En el caso que se esté explotando una vulnerabilidad, es imprescindible tener un procedimiento de patch/vulnerability management eficiente y rápido. En este procedimiento impera:

a. La inventarización, saber qué usuarios y máquinas disponen de este software vulnerable.
b. En el caso que haya un parche disponible, forzar la actualización.
c. En el caso que se trate de un 0day y no haya un parche oficial disponible, se deberán aumentar los esfuerzos de detección en el caso de explotación por parte de un actor.
   Es imprescindible una buena monitorización de Exploits o PoCs de Exploit en markets, foros, canales de telegram, etc. De esta manera, se podrán analizar y crear reglas de detección más precisas.

En el caso que un proveedor o cliente de nuestra empresa haya sido víctima de un ransomware, se deberá realizar una investigación interna de lo siguiente:

- Recopilar toda la información posible sobre el threat actor, para crear reglas de detección y monitorización de la red de la empresa.

- Analizar los canales de comunicación y conexión que tenemos con la otra empresa. Por ejemplo: los últimos correos intercambiados, por si pudieran contener archivos maliciosos o phishing de otro tipo.
- Por parte del departamento de GRC se deberá realizar un análisis de impacto en cuanto a los datos comprometidos de nuestra empresa. Ya que es posible que se hayan expuesto contratos, emails de contacto, etc.

Finalmente, tener una política de DEFCON predefinida, bien estructurada y clara con los posibles escenarios, nos puede ayudar a agilizar y prevenir un ciberataque. En el ámbito de la ciberseguridad, DEFCON representa los niveles de amenaza y preparación para enfrentar ataques cibernéticos. Estos niveles pueden variar según la organización que los implemente, pero típicamente van desde DEFCON 5 (menor amenaza) hasta DEFCON 1 (amenaza máxima).

11. Sumario ejecutivo del Threat Actor.

En este apartado, se resumirá la información más importante que se ha ido recabando a lo largo de la investigación. Tendrá que tener las siguientes características:

- Tiene que ser lo más descriptiva posible, pero a la vez lo más concisa, ya que se recogerán los puntos más destacables.
- Ser visual: incluir una infografía, como puede ser el Modelo Diamante. Para realizarlo, podemos utilizar herramientas como **XMIND**.

12. Anexos

Anexo I – TTP

Para la identificación de TTPs el analista seguirá el siguiente procedimiento:

1. Investigar como el adversario interactúa con plataformas y aplicaciones para tratar de detectar actividad sospechosa. Tratar de identificar como realiza el acceso inicial y las actividades post-compromiso.

2. Investigar los comportamientos del adversario

a. Analizar reportes sobre como el comportamiento del adversario se manifiesta en las intrusiones. Como fuentes adicionales para esta tarea se pueden utilizar reportes de otros vendors o investigadores, CERTS, organizaciones gubernamentales, etc.
b. Buscar términos clave en la plataforma ATT&CK de MITRE puede ser de gran ayuda para identificar comportamientos. Ejemplo: “creación de una *scheduled task*”, “ejecución de powershell” etc.

3. Identificar las tácticas

El analista buscará a lo largo de los reportes sobre el adversario, enfocándose en ***qué*** es lo que estaba tratando de obtener y el ***porqué.*** Para la identificación de las tácticas:

a. Revisar las definiciones de ATT&CK para mapear los comportamientos detectados a tácticas. Ejemplo: “El adversario obtiene persistencia en el sistema creando una *scheduled task”* → Táctica: Persistencia [TA0003]
b. Identificar todas las tácticas usadas, ya que comprender el flujo del ataque nos ayudará más adelante a identificar las técnicas y sub-técnicas utilizadas.

4. Identificar las técnicas

El analista investigará los detalles técnicos para determinar ***cómo*** el adversario ha tratado de alcanzar sus objetivos. Para ello debe comparar el comportamiento con la descripción de las técnicas ATT&CK identificadas. Si se alinea con la descripción de la técnica, ya se puede mapear.

5. Identificar las sub-técnicas:

Como en el caso de las técnicas, se debe comparar el comportamiento con la descripción de las sub-técnicas ATT&CK identificadas. En este proceso, el analista debe:

a. Leer y comprender detalladamente las descripciones de las sub-técnicas para entender las diferencias entre ellas, que en determinados casos pueden ser sutiles.

b. En el caso de que la información contenida en los reportes analizados no permita diferenciar la sub-técnica utilizada, es preferible mantener la técnica que cubra todas las posibles sub-técnicas utilizadas.

Tabla de TTP:

Ejemplo:

Táctica	Técnica	Sub-Técnica	Nombre
TA0002	T1204	.001	User Execution: Malicious Link
		.002	**User Execution: Malicious File**

- Se deberán remarcar en negrita los TTPs que sean únicos para el adversario.
- Para los hipervínculos, se usarán los permalinks de ATT&CK
- Se procurará un enlace con las tácticas, técnicas y sub-técnicas en **ATT&CK navigator**.

Anexo II – IOCs

Para la identificación de IOCs el analista seguirá el siguiente procedimiento:

Se revisarán los reportes sobre el adversario sus intrusiones y se identificarán los siguientes tipos de indicadores:

Básados en Host	Basados en Red
Clave de registro	Dirección IPv4
Nombre de fichero	Dirección IPv6
Cadena de Texto	Hash de Certificado
Mutex	Dominio
Hash de fichero	Protocolo de comunicación
Directorio	URL

Tabla de IOCs:

Ejemplo de Tabla de indicadores:

Táctica	Técnica	Descripción	Tipo	Indicador
C2	T1218.007	URL del C2	URL	hXxp://3h[.]WF:8080/ZgMaAJK3xTC/

- Siempre que sea posible, se anexará la lista de indicadores en formato .json (STIX 2)*
  Para la conversión de indicadores podemos utilizar herramientas como **stix-tools:*

Para la elaboración de ambas tablas, el analista podrá usar las diversas fuentes mencionadas a lo largo de la metodología.

Bibliografía

Metodología práctica sobre Cyber Threat Intelligence (CTI): https://www.ginseg.com/recursos-para-el-analista/metodologia-practica-sobre-hunting/

La inteligencia de amenazas o Cyber Threat Intelligence : https://www.campusciberseguridad.com/blog/item/150-la-inteligencia-de-amenazas-o-cyber-threat-intelligence

Tesis “Metodología para la detección y reducción de ransomware” https://repositorio.unp.edu.pe/server/api/core/bitstreams/950ffec8-3a5a-4645-a9b8-f815a588ea86/content

Diamond Model of Intrusion Analysis: What, Why, and How to Learn: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/diamond-model-intrusion-analysis/

Cómo escribir informes de incidentes de seguridad: https://www.securityartwork.es/2019/03/18/como-escribir-informes-de-incidentes-de-seguridad/

What the Conti Ransomware Group Data Leak Tells Us: https://www.darkreading.com/cyberattacks-data-breaches/what-the-conti-ransomware-group-data-leak-tells-us

How to Negotiate with Ransomware Hackers: https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers