Hack the Box — Sherlock UFO-1

Sherlock UFO-1

- **Perfil**: Blue Team - Cyber Threat Intelligence
- **Sección**: Threat Intelligence
- **Dificultad**: Muy fácil

En este laboratorio vamos a estar resolviendo un ejercicio correspondiente a la plataforma especializada en ejercicios de ciberseguridad y hacking, Hack the Box, dentro del apartado de sus sherlocks, que son labs de blue team.

Para este ejercicio utilizaremos la herramienta de MITRE ATT&CK para la inteligencia de amenazas.

Enunciado: *"Al pertenecer al sector ICS, su equipo de seguridad debe estar siempre al día y ser consciente de las amenazas que se ciernen sobre las organizaciones de su sector. Acabas de empezar como becario de inteligencia de amenazas, con un poco de experiencia en SOC. Tu jefe te ha dado una tarea para poner a prueba tus habilidades en la investigación y lo bien que puedes*

utilizar Mitre Att&ck en tu beneficio. Investigue sobre Sandworm Team, también conocido como BlackEnergy Group y APT44. Utilice Mitre ATT&CK para comprender cómo mapear el comportamiento y las tácticas de los adversarios de forma práctica. Supera la evaluación e impresiona a tu jefe porque la inteligencia de amenazas es tu pasión".

UFO-1 — SOLUCIÓN

Task 1:

> According to the sources cited by Mitre, in what year did the Sandworm Team begin operations?
>
> *2009*

A la hora de ingresar a MITRE ATT&CK, tenemos el apartado de CTI (*Cyber Threat Intelligence*), donde hallaremos en un costado los diferentes grupos de ataque con sus respectivas técnicas, tácticas y procedimientos.

Dentro de esta sección, ingresaremos al grupo que debemos investigar. En este caso, es Sandworm Team, un grupo de origen ruso, vinculados incluso con el ciberataque de NotPetya en 2017.

Allí también encontraremos la fecha en la que supuestamente iniciaron sus actividades según la fuente.

Task 2:

> Mitre notes two credential access techniques used by the BlackEnergy group to access several hosts in the compromised

> network during a 2016 campaign against the Ukrainian electric power grid. One is LSASS Memory access (T1003.001). What is the Attack ID for the other?
>
> *T1100*

Como vemos, se nos mencionado un ciberataque en cuestión que fue perpetrado por este grupo cibercriminal.

Vamos a ir en detalle con este ataque cibernético dentro del apartado de “Campañas” por parte de Sandworm Team

Dentro de este apartado, podemos observar las técnicas utilizadas por el grupo para poder realizar el ataque referidas al contexto de acceso por credenciales.

Se nos comenta que LSASS Memory access (una metodología reiterada para la extracción de credenciales), la cual tiene la Attack ID T1003.001, pero debemos encontrar la siguiente.

Clásico. Un ataque de fuerza bruta para poder autenticarse en varios hosts.

Allí podemos observar también la Attack ID, que es T1100.

Task 3:

> During the 2016 campaign, the adversary was observed using a VBS script during their operations. What is the name of the VBS file?
>
> *ufn.vbs*

Sin salirnos de esta sección del sitio, seguiremos observando las técnicas utilizadas en el ataque.

Bajando un poco encontraremos una técnica que llama la atención, relacionada con la aplicación de movimiento lateral por la red.

Rápidamente encontramos el script en VBS en cuestión, el cual fue utilizado como una herramienta para facilitar el accionar del movimiento lateral.

Task 4:

> The APT conducted a major campaign in 2022. The server application was abused to maintain persistence. What is the Mitre Att&ck ID for the persistence technique was used by the group to allow them remote access?
>
> *T1505.003*

Vamos a volver a la sección donde se listaba los ciberataques realizados por este grupo, donde abajo del ataque anterior, encontramos uno más reciente, concretamente en el año 2022.

Se nos solicita que respondamos con la Attack ID de una técnica de persistencia usada por el grupo para permitir el acceso remoto.

Hay un gran número de técnicas utilizadas, pero debemos centrarnos solo en esta característica.

Debajo en el listado, vamos a encontrar una técnica bastante común entre los atacantes que comprometen sitios web.

El despliegue en una “Reverse Shell” permite al atacante mantener una conexión directamente con la máquina de la víctima, ejecutando comandos allí.

De este modo, se abre una especie de túnel donde el atacante permanecerá conectado (generando persistencia) con el equipo a menos que sea detectado.

Task 5:

> What is the name of the malware / tool used in question 4?
>
> *Neo-REGEORG*

No hace falta irnos muy lejos, ya que, en el mismo párrafo donde se describe la técnica, podemos observar el nombre de la webshell desplegada.

Task 6:

> Which SCADA application binary was abused by the group to achieve code execution on SCADA Systems in the same

> campaign in 2022?
>
> *scilc.exe*

Hay muchas técnicas relacionadas con abuso de binarios de aplicaciones en sistemas SCADA.

Sin embargo, hay una técnica en concreto que menciona un binario en cuestión usada para la ejecución de comandos en la plataforma de MicroSCADA.

Task 7:

> Identify the full command line associated with the execution of the tool from question 6 to perform actions against substations

> in the SCADA environment.
>
> *C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt*

Lo que se nos pregunta ahora es el path completo en la línea de comandos donde se asocia con la ejecución de la herramienta anterior para ejercer las acciones contra sistemas SCADA.

Vamos a salirnos del framework de MITRE y nos dirigiremos a una investigación relacionada con el ataque y realizada por Google.

Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology | Google...Written by: Ken Proska, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker...

En sí, es la principal referencia usada por MITRE para elaborar su investigación de técnicas usadas por el grupo ciberdelincuente, por lo que es de confiar.

Una forma en la cual vamos a ahorrarnos mucho tiempo es usando el buscador para observar elementos relacionados a *scilc.exe,* que es lo que nos importa en este caso.

Aquí se habla de la explotación de este software de SCADA usando este binario.

Justo por encima, encontraremos lo que se colocó en la línea de comandos.

Task 8:

> What malware/tool was used to carry out data destruction in a compromised environment during the same campaign?

CaddyWiper

En este caso, se nos solicita el malware utilizado para la destrucción de los datos en el sistema comprometido, refiriéndose a la misma campaña

Regresamos al MITRE ATT&CK para ver las técnicas usadas, donde encontraremos una referida a la destrucción de la información.

Allí también encontraremos la herramienta mencionada para perpetrar ese accionar.

Task 9:

> The malware/tool identified in question 8 also had additional capabilities. What is the Mitre Att&ck ID of the specific

> technique it could perform in Execution tactic?
>
> *T1106*

Vamos a ingresar a los detalles de este malware para visualizar las técnicas que posee.

Hay diferentes técnicas empleadas por CaddyWiper. Sin embargo, se nos pregunta por una técnica en específico relacionada con la ejecución.

Esta es la técnica correcta debido a que permite que el malware interactúe directamente con las funciones centrales del sistema operativo a un nivel bajo,

evitando abstracciones de mayor nivel que podrían estar monitoreadas o restringidas.

Task 10:

> The Sandworm Team is known to use different tools in their campaigns. They are associated with an auto-spreading malware that acted as a ransomware while having worm-like features. What is the name of this malware?
>
> *NotPetya*

Parece que este grupo ruso usa un ransomware con características de un gusano, y debemos descubrir el nombre del mismo.

Regresamos a la descripción del Sandworm Team para ver cuál es el virus informático en cuestión que están utilizando y esparciendo.

Bajaremos hasta el apartado de “Software”, donde nos encontraremos con un viejo conocido.

Un poco de nostalgia.

Task 11:

> What was the Microsoft security bulletin ID for the vulnerability that the malware from question 10 used to spread around the world?
>
> *MS17–010*

Si conoces la historia de Petya o WannaCry, sabrás que ambos explotaban mucho el servicio SMB para poder moverse lateralmente por la organización que infectaban.

Pues bien, recordemos que Microsoft lanzó, el 14 de marzo de 2017, sus respectivas actualizaciones de seguridad mensuales, donde se incluyó un parche para esta vulnerabilidad de Microsoft Windows SMB Server

Task 12:

> What is the name of the malware/tool used by the group to target modems?

> *AcidRain*

Pregunta sencilla. Un malware diseñado para vulnerar módems.

Volvemos al listado de software utilizados por el grupo para, leyendo su descripción, ver cuál es el nombre de dicho software malicioso.

Task 13:

> Threat Actors also use non-standard ports across their infrastructure for Operational-Security purposes. On which

> port did the Sandworm team reportedly establish their SSH server for listening?
>
> *6789*

Se nos pregunta qué número de puerto fue utilizado por el grupo para establecer conexión con su servidor SSH en escucha.

Lo podemos observar dentro del apartado de técnicas del grupo.

Task 14:

> The Sandworm Team has been assisted by another APT group on various operations. Which specific group is known to have

> collaborated with them?
>
> *APT*

Parece que este grupo ha sido asistido por otro APT en diversas operaciones.

En la descripción del Sandworm Team encontraremos la respuesta.

¡Ejercicio completado!