Cyber Defenders — IcedID

IcedID

- **Perfil**: Blue Team - Cyber Threat Intelligence
- **Sección**: Threat Intelligence
- **Dificultad**: Fácil

En este laboratorio vamos a estar resolviendo un ejercicio correspondiente a la plataforma especializada en actividades de práctica en ciberseguridad, CyberDefenders.

Para este ejercicio utilizaremos principalmente la herramienta de **MITRE ATT&CK** y la plataforma **VirusTotal** para la inteligencia de amenazas.

Enunciado: *"Se identificó a un grupo de ciberamenazas por iniciar campañas de phishing generalizadas para distribuir más payloads maliciosos. Los payloads más frecuentes eran IcedID. Se le ha proporcionado un hash de una muestra de IcedID para que analice y supervise las actividades de este grupo de amenazas persistentes avanzadas (APT)".*

Los indicadores de compromiso que se nos deja son los siguientes:

1. 191eda0c539d284b29efe556abb05cd75a9077a0

ICEDID — SOLUCIÓN

Task 1:

> What is the name of the file associated with the given hash?
>
> ***document-1982481273.xlsm***

En primer lugar, se nos solicita el **nombre del archivo** asociado con el hash que se nos otorgó.

Esta respuesta es sencilla de hallar. Simplemente alcanza con colocar el indicador de compromiso en la plataforma de VirusTotal y obtendremos en detalle más información, incluyendo el documento al que está vinculado este hash.

Una vez lo hayamos puesto, debemos dirigirnos al apartado de "*Details*", y bajando un poco veremos los nombres asociados al hash.

Task 2:

> Can you identify the filename of the GIF file that was deployed?
>
> ***3003.gif***

Siguiendo dentro de la plataforma de VirusTotal, pero dentro de la sección de "*Relations*", encontraremos en la primera parte las URL a las que se contacta este archivo.

Al parecer, varios de los enlaces a los que se comunica incluyen un **archivo GIF**, el cual es el que se nos solicita colocar.

Task 3:

> How many domains does the malware look to download the additional payload file in Q2?
>
> ***5***

Como se observa en la imagen anterior, son cinco los **dominios** a los que el malware se contacta para descargar ese archivo adicional.

Task 4:

> From the domains mentioned in Q3, a DNS registrar was predominantly used by the threat actor to host their harmful content, enabling the malware's functionality. Can you specify the Registrar INC?
>
> ***NameCheap***

Se está preguntando cuál fue el **Registrar** (empresa registradora de dominios) usado por el grupo atacante para registrar los dominios maliciosos mencionados en la pregunta anterior.

Justo por debajo de las URL a las que se contacta el malware, vamos a hallar los dominios a los que se contacta, con su respectivo Registrar.

En esta imagen, vamos a filtrar primero por los dominios considerados maliciosos.

Después de ello, lo esencial a tener en cuenta es en cuál de ellos se vincula el dominio con la URL donde está alojado el GIF malicioso.

Vemos que únicamente figura el Registrar de dos enlaces, la de Launchpad y NameCheap.

Sin embargo, la primera nos arroja un clásico error 404, por lo cual, y habiendo descartado esa opción, nos queda únicamente la segunda, que resulta ser la opción correcta.

Task 5:

> Could you specify the threat actor linked to the sample provided?

Gold Cabin

Para esta pregunta, nos moveremos hacia la plataforma de MITRE ATT&CK, donde podremos observar a qué **grupo cibercriminal** se vincula este software malicioso.

Debemos irnos al apartado de CTI → Software → IcedID.

Una vez estemos aquí, bajaremos hasta que encontremos los grupos que utilizaron este virus informático alguna vez y que se encuentren en la base de datos de este framework.

Como dato curioso, IcedID fue utilizado y aplicado en la famosa campaña de Emotet, uno de los malware más complejos de la historia.

Ingresamos al primer grupo, llamado TA551, donde también veremos los grupos asociados.

Task 6:

> In the Execution phase, what function does the malware employ to fetch extra payloads onto the system?
>
> ***URLDownloadToFileA***

Para resolver esta pregunta, debemos investigar otros informes de diversas plataformas, como es el caso de Fortinet.

En 2022, esta empresa de seguridad elaboró un análisis del malware IcedID, destacando diversas **operaciones** que este software malicioso realiza una vez infecta el equipo.

Podemos encontrar la respuesta en el análisis de su comportamiento.

¡Ejercicio completado!