TAREA PARA EVALUAR EL MÓDULO ANÁLISIS Y DETECCIÓN DE MALWARE

Descripción

Realizar investigación de un Tipo de Malware con la finalidad de conocer de manera amplia y detallada su funcionalidad. Para lograr lo anterior, además del tipo, se usarán las familias y las variantes del malware. Como resultado de la investigación se creará un documento que contenga la información el cual deberá tener al menos lo siguiente:

1. Nombre
    a. El nombre será el más común utilizado por varias empresas de ciberseguridad.
    b. Lista de sinónimos.
2. Fecha de la 1ª aparición o detección.
3. Lugar del ataque
    a. El inicial y las subsiguientes zonas más afectadas del mundo.
4. Origen de la muestra
    a. Quien o en qué lugar se creó.
5. Descripción no técnica del comportamiento del malware.
6. Mecanismos de infección.
7. Comportamiento detallado
    a. Se otorgarán puntos extra si se usa el *framework* MITRE ATT&CK.
8. Referencias
    a. Libros, sitios web (blogs, fichas descriptivas de empresas de ciberseguridad, etc.), artículos científicos, etc.
    b. Trate de poner las referencias más serias.
9. Variantes
    a. Nombres asignados.
    b. Descripción de los nuevos comportamientos.
10. Línea del tiempo
    a. De la evolución del malware y sus variantes.
11. Lista de las muestras de malware
    a. Ubicación en internet, o
    b. Referencias al repositorio MAREA.
    c. Debe incluir los valores hash (MD5, SHA1, SHA256).

Asignación

El tipo y familia de malware a utilizar se asigna con base en la siguiente lista. Se tomará el numero de la lista del grupo para conocer el tipo y si hay más de 14 alumnos se reinicia la lista, es decir, al alumno 15 le toca el número uno.

No	Tipo	Ejemplos de Familias y variantes
1	Virus o Gusano	Stuxnet, NGVCK, Slammer
2	Adware, PUP	Superfish, Ask Toolbar, Fireball
3	Rootkit	Knark, Lrk
4	Adware	Fireball, Appearch
5	Keylogger	FinFisher, Project Sauron, Ghost keylogger, KeyGrabber
6	Backdoor	
7	Phishing	PayPal Scam, Dropbox Scam, Advanced-fee scam, etc.Tesis
8	Dropper o Downloader	Emotet, Httpdropper, MailDropper, VBDropper
9	Spyware	CoolWebSearch, Gator
10	Ransomware	Ryuk, DarkSide, Petya, Locky
11	Botnet	Andromeda, Mirai
12	Trojan	ZeusS, Zbot, ZeusX
13	Bomba lógica o Malware sin archivos	Frodo, Number of the Beast y The Dark Avenge

Entrega

Se anexa plantilla con el estilo del documento y un borrador de la estructura. Al terminar la investigación se deberá entregar el documento en formato Word a más tardar el 6 de diciembre del 2024 a las 23:59 hrs.