Ejercicio individual 2

Estudio de un ejemplo de código malicioso

Normas.Tema

- Código malicioso asignado:

  nº_asignado = (id * cte) **mod** tam = **((**id **mod** tam**)* (**cte **mod** tam**)) mod** tam

  – id: DNI o pasaporte

  – cte: constante indicada en web de asignatura

  – tam: nº de elementos de lista

- Opciones:

  – Código malicioso asignado según web de asignatura (a)

    - O el inmediatamente anterior (b) o posterior (c)

  – Sobre código malicioso elegido por alumno (d)

    - No incluido en lista de web de asignatura
    - No elegido previamente por otro alumno

    } Incluidos todos los alias

- Indicar opción ((a), (b), (c), (d)) claramente en Introducción

Normas. Estructura y contenido

1. Portada
   - Título
   - Nombre y apellidos
   - NIF
   - nº de matrícula
   - Cálculo de número asignado
2. (Indice)
3. Introducción
   - Opciones elegidas:
     - Código malicioso
     - Tipo
     - Familia
4. Ficha resumen
5. Conclusiones
6. Referencias
7. (Anexo)

Normas. Estructura y contenido

1. Portada
2. (Indice)
3. Introducción
4. Ficha resumen
5. Conclusiones
6. Referencias
7. (Anexo)

- Denominación (nombre, alias, …)
- Origen / autor
- Destinatario
- Fecha de lanzamiento
- Fecha de descubrimiento
- Tipo de código malicioso
- Funcionamiento general
  - Modo de infección
  - Modo de replicación
  - Modo de propagación
  - Modo de ocultación
  - Ejecución de la carga
- Tipo de vulnerabilidad relacionada
- Modo de desinfección
- Ejemplo(s) de ataque(s) donde se ha empleado
- Medidas de seguridad tomadas tras su descubrimiento
- Resto de miembros de su familia
- Otra información relevante

Apartados separados y con título para cada punto

Normas. Aclaraciones

- OJO: Los nombres empleados en la lista pueden corresponder a:
  - Código malicioso (único o familia)
  - Botnet
  - Herramienta: paquete de explotación (*exploit kit*), de acceso remoto (*RAT*), …
  - Varios de los tipos anteriores
- En caso de familia
  - Elegir entre
    - Características comunes
      (En funcionamiento general se pueden explicar diferencias entre miembros)
    - Miembro cualquiera
- En caso de varios tipos
  - Elegir cualquiera

} Dejar bien claro en Introducción

- Necesario definir términos nuevos o que se utilicen con un sentido distinto al visto en clase

Normas. Aclaraciones (cont.)

- Tipo de código malicioso
  - Según independencia y autorreplicación
  - Añadir especialidad si corresponde
  - Si es necesario otro código para infectar, incluir también tipo de este último
- Funcionamiento general
  - Resumido y explicado
- Si algún tipo de dato no tiene sentido para el elemento descrito, señalarlo como No se aplica
- Si no se encuentra dato, señalarlo como Desconocido
  - Necesario incluir explicación de intentos para recabarlo
    - Búsquedas realizadas
    - Solicitudes de información (copia oculta a sbernardos@fi.upm.es) y respuestas
- Origen de información claro
  - Mención acortada en texto y datos completos en referencias

Normas. Aclaraciones (cont.)

- Formatos permitidos
  - pdf, doc(x), zip, rar
- Cuidado con ortografía
- Estilo uniforme
  - No cortar y pegar
- Precaución con traducciones automáticas
- Antes de entrega no se responderán consultas que impliquen una corrección del documento

Norma no cumplida → nota = 0