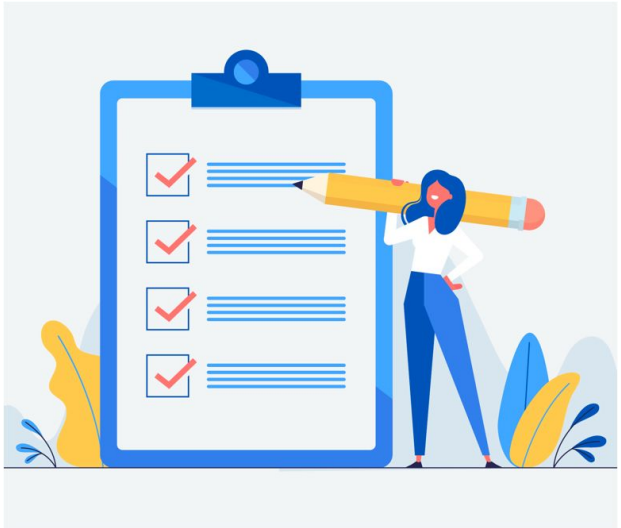
Actividad Tipos de Amenazas

Utilizando este documento de presentación, cada mesa deberá resolver y completar en cada hoja , que le corresponde según su número de mesa.



Mesa 2

Nota : https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizaciones-diplomaticas/

1. ¿Qué tipo de amenaza es?
    a. Es un spyware
2. ¿Cómo comienza y cómo se propaga esta amenaza?

Su metodología de ataque inicial consiste en explotar aplicaciones vulnerables expuestas a Internet en servidores web, con el fin de droppear y ejecutar un webshell. Después del compromiso, a través del webshell, BackdoorDiplomacy utiliza software de código abierto para el reconocimiento y la recopilación de información, y hace uso de la técnica DLL search order hijacking para instalar su backdoor: Turian. Finalmente, BackdoorDiplomacy emplea de manera separada un ejecutable para detectar medios extraíbles, probablemente unidades flash USB, y copiar su contenido en la papelera de reciclaje de la unidad principal.

Para su propagación utiliza mensajes por Wpp que apela a la necesidad de quienes precisan una ayuda e intenta dar la sensación de que se trata de un dominio real asociado a una campaña legítima.

Mesa 2

Nota :
https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizaciones-diplomaticas/

1. **¿Hay más de una amenaza aplicada ?**

Phishing dado que engañan a las personas para que descarguen el malware a partir de los mensajes de Wpp.

2. **¿Qué solución o medida recomendarían ?**

- Es importante tener siempre las últimas versiones instaladas. Con esto nos referimos a contar con actualizaciones de sistema, así como también de las aplicaciones que tengamos instaladas.
- Es vital por supuesto contar con programas y herramientas de seguridad.
- Hay que evitar también navegar por páginas inseguras o que inspiren confianza. Además mucha atención a las redes sociales, otro medio por el cual podrían promover amenazas de este tipo.