Certified Tech Developer
The Ultimate Degree

Deberán leer cada una de las noticias asignadas y responder en un documento de Google Presentations para todas las mesas, las siguientes consignas:

- Nota:

  https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/

- ¿Qué tipo de amenaza es?

Es un troyano que introduce una backdoor y un rootkit mediante la cual se puede controlar a la computadora comprometida sin que el usuario lo detecte.

- ¿Cómo comienza y cómo se propaga esta amenaza?

Se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

- ¿Hay más de una amenaza aplicada?

BalkanRAT es un troyano y BalkanDoor es un backdoor que viene adentro del troyano y rootkit es un malware que sirve para ocultar todo de la vista del usuario.

Todos se distribuyeron por malspam, son emails con archivos adjuntos que traen los malwares.

- ¿Qué solución o medida recomendarían?
- **Troyano: Eliminación**

Lo primero que tienes que hacer es instalar un software antivirus, si es que no lo tienes ya. Sigue siempre los consejos que te ofrece el fabricante para la protección del equipo.

Ejecuta el antivirus en modo seguro para que el programa empiece a realizar un completo análisis de tu equipo y detectar cualquier troyano o virus.

Una vez que el antivirus detecta el problema, será muy fácil eliminar troyanos. Deja que termine todo el análisis antes de pasar a la acción para librarte de ellos.

Terminado el análisis, el programa te mostrará varias opciones para resolver problemas de seguridad o virus que hayan aparecido. No marques la opción de restaurar sistema ya que eso puede hacer que los troyanos que elimines se restauren también.

Cuando haya terminado el proceso de eliminar troyanos y cualquier otro virus detectado en el análisis, reinicia el ordenador. Debes seleccionar que quieres iniciar el PC en modo seguro.

Ve al panel de control para eliminar cualquier programa al que el troyano le haya podido afectar. Esta información te la da el antivirus después de detectarlos.

Debes eliminar también las extensiones que tengas instaladas en el navegador que estén en riesgo. Si tienes dudas de cuáles son, quítalas todas y vuelve a instalarlas, salvo si alguna fue la que te metió el troyano en el equipo.

Cuando todo lo anterior no funciona y no encuentras remedio, quizás lo mejor sea formatear tu ordenador. Con esto te aseguras partir de cero y que no quede rastro de ningún troyano o virus. Haz una copia de seguridad antes de empezar y revisa bien los programas que vas a instalar para evitar que se cuelen los troyanos otra vez.

- **Backdoor: eliminación**

La eliminación manual de un backdoor no es fácil y, de hecho, lo mejor es recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, de manera que cuando encuentran un virus lo marcan para su posterior eliminación. Este proceso viene explicado paso a paso por el propio antivirus que estemos usando, por lo que generalmente es sencillo de hacer. También podemos recurrir a otros programas de limpieza, como Cleaner o

Malwarebytes Anty-malware, para usarlos tras realizar el análisis con el antivirus.