Grupo 6

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

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

* ¿Qué tipo de amenaza es?

Es un malware llamado “Backdoor”

* ¿Cómo comienza y cómo se propaga esta amenaza?  
  Identifica los puntos vulnerables de acceso en un dispositivo y le da control parcial o total a otras personas para que hagan lo que quieran con él.

Una vez dentro de un sistema, sus operadores utilizan herramientas de código abierto para escanear el entorno y realizar movimiento lateral. El acceso interactivo se logra de dos maneras: (1) a través de un backdoor personalizado que llamamos Turian que deriva del backdoor Quarian; y (2) en menos casos, cuando se requiere un acceso más directo e interactivo, se implementan ciertas herramientas de acceso remoto de código abierto.

* ¿Hay más de una amenaza aplicada?

Sí, no sólo es el backdoor, sino la recopilación de información y los ejecutables para robar información de unidades extraíbles flasUSB, por ejemplo: parte malisiosa de BalkanRAT, BalkanDoor,

* ¿Qué solución o medida recomendarían?

Lo más recomendable es seguir las reglas básicas de ciberseguridad: tener cuidado con los correos electrónicos y examinar tanto los archivos adjuntos como los enlaces que puedan venir en ellos; mantener actualizado sus equipos y utilizar una solución de seguridad confiable.

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.