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

- **¿Qué tipo de amenaza es?**

El tipo de amenaza es un backdoor. El virus Backdoor es un troyano que abre una puerta trasera en el sistema de tu computadora y permite que un hacker remoto tome el control de tu equipo sin que lo sepas.

- **¿Cómo comienza y cómo se propaga esta amenaza?**

Como vectores de infección inicial, el grupo ha estado aprovechando la explotación de dispositivos vulnerables expuestos a Internet, como servidores web e interfaces de gestión para equipos de red. 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?**

Se documentaron amenazas de muchos tipos, entre ellas las más importantes:
•EarthWorm, un simple túnel de red con servidor SOCKS v5 y funcionalidades de transferencia de puertos
•Mimikatz y varias versiones, incluido SafetyKatz
•Nbtscan, un escáner de NetBIOS de línea de comandos para Windows
•NetCat, una utilidad de red que lee y escribe datos a través de conexiones de red.
•PortQry, una herramienta para mostrar el estado de los puertos TCP y UDP en sistemas remotos
•SMBTouch, utilizado para determinar si un blanco de ataque es vulnerable a EternalBlue
•Varias de las herramientas filtradas de la NSA por ShadowBrokers.

- **¿Qué solución o medida recomendarían?**

Para mantenerse protegido de Backdoor, lo recomendable es:

Instalar un buen antivirus en la PC. Mantenerlo actualizado. Si el antivirus admite las actualizaciones automáticas, configurarlas para que funcionen siempre así.
Tener activada la protección permanente del antivirus en todo momento.

Además de contar con esta protección, por supuesto también está el uso del sentido común y la precaución a la hora de navegar por Internet y descargarnos archivos; si una página no es de confianza o te resulta sospechosa, no entrar en ella, si el antivirus nos avisa de algún peligro, no entrar en ella y, sobre todo, no descargar archivos de lugares poco confiables o de remitentes desconocidos, o archivos sospechosos de conocidos.