**“Uso de la criptografía moderna”**

Isaac Vásquez

La criptografía es una práctica que en la modernidad es obligatoria o nosotros como usuarios debemos procurar que lo sea, entrando a la página de un banco vemos que hay comunicación encriptada por medio de SSL/HTTPS, como usuarios podemos elegir incluir una firma digital para cifrar aún más la comunicación y autenticar que somos nosotros quienes estamos realizando una acción en específico, otro ejemplo son las comunicaciones P2P que se transmiten a través de WhatsApp, las cuales presentan un grado de encriptación de chat a chat que es único, podemos ver que cuando entramos en Facebook entramos bajo el mismo protocolo SSL/HTTPS y si leemos las políticas de seguridad, nos damos cuenta que cierta información se encuentra guardad en la base de datos de manera encriptada para protegernos de ataques cibernéticos, como podemos ver la criptografía está presente en todas partes y en todo momento aunque no se pueda distinguir a simple vista.

Antes de elegir un punto para enfocarnos, podríamos realizar una síntesis de los consejos y medidas indicados en el Anexo del taller:

1. **Mensaje cifrado:** Observar si una aplicación de mensajería cifra los mensajes de extremo a extremo.
2. **Políticas de privacidad:** Leer siempre la política de privacidad de las aplicaciones y ser consciente de que no es necesario dar todos nuestros datos a una plataforma de servicios.
3. **Detectores:** Utilizar herramientas con apoyo criptográfico para detectar rápidamente si entra malware a través de una aplicación.
4. **Agregadores:** Utilizar agregadores con precaución, ya que pueden recopilar información sensible.
5. **Conexiones públicas:** Utilizar redes públicas puede suponer un peligro a la privacidad y a los datos.
6. **VPNS:** Instalación de Redes Privadas Virtuales en el celular.
7. **Anonimato:** Utilizar redes TOR, I2P, Freenet, para la conservación de la privacidad del usuario.
8. **Dominios seguros:** Percatarnos de que el dominio que estamos accediendo presente https, ya que presenta una capa de cifrado de datos.
9. **Certificado digital:** Instalar un certificado digital y utilizarlo para firmar documentos, de manera tal que podamos saber que el documento no ha sido modificado en el proceso.
10. **Respaldos:** Realizar copias de seguridad de los datos del teléfono.
11. **Educación del usuario:** Ser consciente de la información que se revela continuamente, como la localización, gustos de consumo o ideas políticas, ya que esto puede hacer que seamos más vulnerables como consumidores y ciudadanos.

Se selecciona el consejo “***Anonimato***” para ser abordado más a fondo:

El anonimato en internet es un tema que necesita un poco de investigación para poder acceder a ella, el artículo nos habla de TOR, I2P, Freenet. Todas ellas están en la misma familia “darknet” y pretenden dar anonimato por medio de encriptación y técnicas de ruteo. Mundialmente TOR es la herramienta de anonimato más conocida y por ende será el objetivo principal de esta investigación.

Vamos a abordar algunos principios de TOR:

* “Tor Browser aísla cada sitio web que visitas para que los rastreadores y anuncios de terceros no puedan seguirte. […]” (Torproject).
* “Tor Browser evita que alguien que esté viendo tu conexión sepa qué sitios web visitas” (Torproject).
* “Su tráfico se retransmite y cifra tres veces a medida que pasa por la red Tor” (Torproject).

Como se puede observar TOR vigila y protege la conexión, a través de la encriptación y cifrado de tramas, por medio de una red de servidores (miles de servidores) “administrados por voluntarios conocidos como repetidores Tor” (Torproject).

Si bien, TOR suena bastante bien, cuando se menciona TOR en conversaciones, viene acompañado de muchos temores e incertidumbres. Es por este motivo que se empezaron a crear herramientas externas que utilizan TOR, sin tener que navegar a través de él, dándole la misma seguridad al usuario del anonimato y cifrado de los datos.

Entre estas herramientas podemos encontrar a Proxychains, anonsurf, sshutle, torsocks, entre otras. Por temas de conocimiento personal abarcaremos a fondo proxychains.

Proxychains, aprovecha el servicio TOR para ejecutar comandos y que salgan a través de otra IP, bastante útil para esconder la nuestra, es una herramienta que viene instalada por defecto en Kali, solo hay que configurarla, para configurarla primero se debe instalar el servicio de TOR:

# Instalar TOR

sudo apt-get install tor

# Iniciamos el servicio

service tor start

# debemos configurar el proxychains

nano /etc/proxychains.conf

Para realizar una correcta configuración de proxychains, debemos asegurarnos de cumplir estos pasos:

1. En nano /etc/proxychains.conf debemos asegurarnos de establecer random\_chain o dynamic\_chain.
2. En chains\_len configuramos los saltos a nivel de proxy, si deseamos hacerlo.
3. Al final del archivo vamos a definir los Socks:
   1. socks5 127.0.0.1 9050
   2. socks5 127.0.0.1 9150
   3. El puerto 9050, corresponde al sock5 principal del servicio TOR.
   4. El puerto 9051, corresponde al sock5 secundario (no viene instalado por defecto) del servicio de TOR Browser.
4. Para activar el puerto 9150, habría que modificar el torrc ubicado en /etc/tor/torrc.

Con estos pasos ya podremos ejecutar comandos anónimamente para esconder y encriptar la comunicación a través de TOR. Ejemplo:

proxychains firefox google.com

Referencias

Torproject.org “Anonymity Online” (2023). Navegar en privado. Explora libremente. <https://www.torproject.org/>