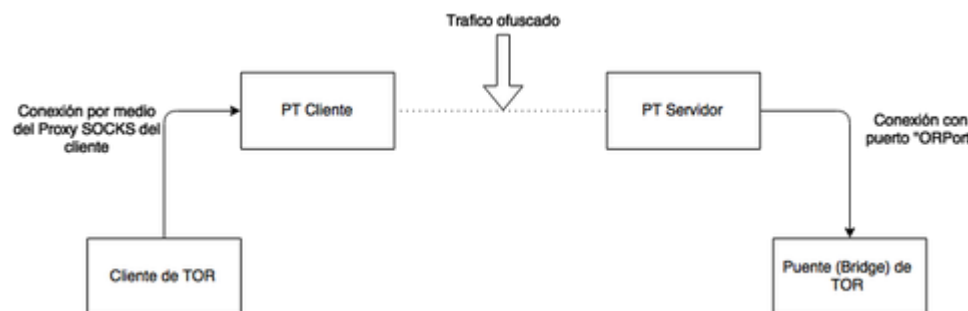


TORTazo nació en septiembre del año 2014 como una necesidad de auditar lo que se hacía en el deep web y que hasta el momento quedaba ajena a las posibilidades de análisis de quienes se dedican a la seguridad informática.

El prograador de la herramienta declaraba ésto en la famosa web "thehackerway" sobre su proyecto *"Hace un par de semanas he terminado de desarrollar la versión 1.1 de Tortazo y dado que he incluido varias cosas que me han parecido interesantes, en esta entrada hablaré un poco sobre los cambios y mejoras que se han incluido en esta primera versión estable (o eso espero) del proyecto. Para aquellos que no saben de que va todo esto, desde hace unos meses se me ocurrió desarrollar un framework de auditoría centrado exclusivamente en la web profunda de TOR (aunque tengo pensado extender sus funcionalidades a otras redes como I2P), la razón es muy simple, porque actualmente no hay, o al menos que yo conozca, herramientas que permitan ejecutar pruebas de penetración contra repetidores o servicios ocultos en TOR. Mi idea ha sido crear un framework que incluya varias funcionalidades y utilidades que puedan ser utilizadas por usuarios finales y por desarrolladores que quieran ejecutar rutinas de código contra repetidores maliciosos o servicios ocultos, algo así como Metasploit Framework, pero enfocado a la web profunda. Además de lo anterior, cuenta con una pequeña API que permite crear plugins que rápidamente se integran en Tortazo y permite reutilizar funciones para conectividad, acceso y pentesting en la web profunda. Aunque llevo algunos meses de desarrollo y estoy bastante satisfecho con los resultados, aun hay muchas cosas que me quedan por implementar, cosas que se pueden mejorar y seguramente, cosas que se deben corregir, pero tengo el animo y la motivación para hacerlas en la próxima versión."*

Debido a su cercano nacimiento TORTazo aun no esta completamente desarrollado, si bien reúne ya todas las virtudes que precisa cualquier analista de seguridad que se precie. Y por lo pronto ya permite analizar el tráfico que existe entre los distintos servidores de la red TOR, al situarse enmedio del tráfico y analizarlo desencapsulando el envío y la recepción de dichos paquetes de comunicaciones.



TORTazo, ajenamente a lo que se pudiera suponer como una injerencia por parte de los Gobiernos para analizar y espiar el tráfico de la red TOR es una iniciativa privada que parte de aquellos que se dedican al análisis forense y por pura necesidad innovan herramientas con las que desarrollar su labor. Los Gobiernos con total seguridad dispondrán desde hace mucho más tiempo de herramientas que hacen lo mismo que TORTazo, pero que para evitar su detección intentan ocultar de la opinión pública como pasó con PRISM.