Independencia en el Ciberespacio

Por Gunnar Wolf

Gunnar Wolf es administrador de sistemas para el Instituto de Investigaciones Económicas de la UNAM y desarrollador del proyecto Debian GNU/Linux.
http://gwolf.org

Es de sobra conocido que la comunicación sobre redes de datos TCP/IP es fácil de espiar — El diseño de Internet desde sus inicios está enfocado a la confiabilidad, no a la privacidad, hecho que se hace obvio en sus protocolos a todos niveles. Esta es una realidad a la cual los usuarios de Internet nos hemos acostumbrado desde siempre.

La respuesta clásica se centró en el cifrado de las comunicaciones (usar secure shell en lugar de telnet, emplear https en vez de http, etc.) Esto, sí, lleva a que el contenido de las comunicaciones cuyos protocolos pueden ser cifrados se vuelvan inintelegibles para un adversario. Esta respuesta, tristemente, ha demostrado ser insuficiente por la profundidad y seriedad de cómo se ha configurado el modelo de adversario.

La sospecha de que las redes de telecomunicaciones (sean analógicas o digitales) sean utilizadas para el espionaje no es nada nuevo. A inicios de la década de los noventa, era frecuente que los jóvenes que enviábamos mensajes a través de las redes de *BBSes (Bulletin Board Systems*, sistemas de boletín electrónico, y de cierto modo antecesores de Internet para las comunicaciones personales) agregáramos al final de todos nuestros mensajes, como parte de nuestras firmas, líneas autogeneradas con palabras clave alineadas para la idiosincrasia contraterrorista del momento, por el estilo de «Bomb Lybia Arafat Plane Washington Kill President». Hacíamos esto, argumentábamos, porque el gobierno estadounidense analizaba todas nuestras conversaciones, primero efectuando un filtrado *grueso* y posteriormente haciendo trabajo a detalle; si incluíamos estos mensajes en todas nuestras comunicaciones, obligaríamos al filtrado grueso a reportar muchos falsos positivos, sobrecargando sus (mucho más valiosos) sistemas de filtrado fino. Hubo varios *nombres clave* que tuvo este espionaje en los años que a mí me tocó ser parte de la vanguardia que luchaba por proteger a nuestro amado ciberespacio, ese entorno que apasionadamente defendió John Perry Barlow (músico, poeta, ensayista, y uno de los primeros pensadores sociales que se dedicaron a analizar el significado de la red para la sociedad) en su *Declaración de Independencia del Ciberespacio* [1] en 1996. Cito el inicio de esta declaración, en traducción propia:

> *Gobiernos del Mundo Industrial, viejos gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. A nombre del futuro, les pido que nos dejen en paz. No son bienvenidos entre nosotros. No gozan de soberanía donde nos reunimos.*
>
> *No tenemos un gobierno electo, y es poco probable que lleguemos a tenerlo, así que me dirijo a ustedes sin más autoridad que aquella con que siempre habla la libertad misma. Declaro que el espacio social global que estamos construyendo es naturalmente independiente de las tiranías que ustedes buscan imponernos. No tienen derecho moral de gobernarnos, ni poseen método alguno de coerción que tengamos alguna razón para temer.*
>
> *Los gobiernos obtienen sus justos poderes del consentimiento de los gobernados. Ustedes no han ni solicitado ni recibido el nuestro. No los invitamos. No nos conocen, ni conocen nuestro mundo. El ciberespacio no yace dentro de sus fronteras. No piensen que pueden construirlo, cual si fuera un proyecto de construcción pública. No pueden. Es un acto de la naturaleza, y se crece a sí mismo mediante nuestras acciones colectivas.*

Hace veinte años, este escrito resonó muy fuertemente con todos nosotros, quienes llevábamos cinco, diez, veinte años creando nuevos medios de comunicación con la tecnología y los recursos que teníamos a nuestra disposición; la variedad tecnológica en esa época era impresionante, y había espacio para la participación de todo tipo de perfiles... Siempre alineados a lo que con el tiempo dio en conocerse como la *ética hacker.*

Pero me estoy *yendo por las rama*s hacia un tema del cual se puede hablar mucho más, y del cual disfruto mucho rememorar y escribir. A los interesados en esta temática, puedo recomendarles el libro publicado el año pasado por la Universidad del Claustro

de Sor Juana, «Ética hacker, seguridad y vigilancia» [2], en el que tuve el honor de participar con un capítulo.

Aterricemos: Hace veinte años, lo que sabíamos al respecto eran meras suposiciones. Claro está, las telecomunicaciones internacionales estaban a un nivel incomparable de donde están ahora; las llamadas telefónicas internacionales eran carísimas, y las comunicaciones digitales estaban al alcance de un porcentaje risible de la población. Si en esa época dedicáramos nuestro tiempo real de trabajo, o espacio en una revista como Software Gurú, a hablar de la vigilancia generalizada... Se nos tacharía indudablemente de "conspiranóicos".

Este tema no es del todo nuevo en nuestra revista: En esta misma columna, escribí ya al respecto en los números 32 (mayo de 2011) y 42 (noviembre de 2013).

Desde las primeras revelaciones de *Wikileaks*, parte muy importante de las filtraciones de alto nivel que se han presentado son relativas a la profundidad del espionaje que se realiza de forma indiscriminada. Vemos por un lado acuerdos entre agencias de seguridad de diferentes gobiernos y conjuntos de puertas traseras en software de uso generalizado que se mantienen por años ocultamente escondidos por las mismas, y por el otro la proliferación de técnicas analíticas a profundidad, sustentadas en el indefinible Big Data, en manos de particulares.

Cabe mencionar, los marcos regulatorios que norman el funcionamiento de las citadas agencias de seguridad nacional se mantienen firme y convenientemente anclados en su anticuado lugar, hace cuando menos veinte años. Por ejemplo, ante la restricción de que el gobierno estadounidense no debe espiar la comunicación entre sus ciudadanos, analizar conexiones de red que se mantengan dentro de sus fronteras se vuelve complicado. Bueno, recientemente salió a la luz que la NSA efectúa ataques de ruteo BGP (*Border Gateway Protocol*, empleado para el ruteo a gran escala, entre los llamados Sistemas Autónomos) — "Empuja" las rutas de algunos paquetes para pasar por conexiones fuera de los Estados Unidos, facilitando el marco regulatorio dentro del cual pueden operar. Esto, volviendo al punto mencionado al inicio de esta columna, es posible porque BGP está diseñado para confiar; cualquier *sistema autónomo* puede indicar que es mejor o peor candidato que sus vecinos para determinadas rutas.

Hasta cierto punto, la respuesta de la sociedad ha cambiado. ¿Para bien? No me atrevo a afirmarlo ni rechazarlo categóricamente: Ya no se burlan de quienes hablamos de un espionaje a gran escala etiquetándonos como conspiranóicos con sombreros de papel aluminio... Pero, bajo el credo de que "la privacidad ha muerto, ya supérenlo", se le resta importancia y se relega a segundo término. Después de todo, ¿por qué habríamos de escondernos de empresas que mediante la analítica de Big Data nos entregan la información que nos importa, así sea publicidad enfocada o noticias que encajan con nuestra ideología, buscando mantenernos como fieles seguidores de sus sitios? Y... ¿los gobiernos? Bueno, si no tengo nada que esconder, ¿qué tengo que temer?

Afortunadamente, existen muchas herramientas cuyo uso puede llevarnos a dejar un rastro mucho menos seguible en la red; la más popular de ellas tal vez sea la Red Tor, una serie de nodos provistos por voluntarios en todo el mundo que proveen una malla de anonimización mediante ocultamiento criptográfico. El funcionamiento de Tor es verdaderamente sencillo, y espero abordarlo en una posterior entrega, y parte importante del esfuerzo del proyecto que la sustenta se ha enfocado en llevar a la Red Tor a quien la necesite, desarrollando herramientas para su usabilidad sin requerir de avanzados conocimientos técnicos.

Sé que dejo esta columna aparentemente inconclusa. Estoy iniciando con un proyecto que me llevará a trabajar el tema a mayor profundidad; retomaré esta temática en la próxima edición, profundizando en Tor y en cómo los usuarios de distintos niveles técnicos pueden aprovecharlo.

No quiero cerrar esta entrega sin mencionar el caso de Dmitry Bogatov, un jóven maestro universitario de matemáticas, activista y desarrollador de software libre, participante al igual que yo del proyecto Debian. Dmitry fue acusado de publicar material subversivo extremista en Internet, aunque está demostrado que no pudo haberlo hecho; es muy creíble que su acusación esté más bien relacionada con que operaba un nodo de salida de Tor. Dmitry fue encarcelado el pasado diez de abril, y hasta el momento de entrega de mi columna, no ha habido avance real en su proceso. Desde esta modesta trinchera, y con la poca influencia que una publicación tecnológica en México pueda tener, los invito a visitar el sitio Web https://freebogatov.org/en/ para enterarse de más detalles del caso y, en caso de que lo juzguen correcto, apoyar al caso.

Referencias y notas

[1] https://www.eff.org/cyberspace-independence

[2] http://elclaustro.edu.mx/pdf/EticaHackerSeguridadVigilancia.pdf