

Filtran datos de la empresa Gamma Group dedicada a la venta de tecnología de vigilancia – Enjambre Digital

Por Thalía Güido

El pasado miércoles 6 de agosto un hacker reivindicó la acción de haber desmantelado una red de la compañía Gamma International, que se dedica al desarrollo y comercialización de tecnología para la vigilancia y publicó vía twitter cerca de 40 GB de datos internos de la empresa. Entre ellos se encontraban código fuente, listas de precios y notas para ser publicadas. Gamma no ha emitido ninguna postura hasta el momento mientras investigadores de Malware y activistas de derechos humanos celebran la publicación de dichos datos.

En México según el reporte de CitizenLab y las investigaciones del colectivo ContingenteMX hay equipos de la firma Gamma Group operando bajo las redes de los proveedores de acceso a internet de lusacell y Telmex. Por ejemplo por FinFisher que es un equipo compuesto de software y hardware que permite mantener vigilancia de forma focalizada en el interior de una red informática, desde el monitoreo de llamadas de video y audio, registro de correo electrónico, hasta la posibilidad de controlar la cámara y el micrófono de los equipos de las víctimas.

Éste miércoles desde la cuenta de twitter @GammaGroupPR se han estado publicado los documentos internos del producto desarrollado por Gamma, FinFisher.

Los activistas hablan

El investigador Erick King, de Privacy International, organización que defiende y promueve el derecho a la privacidad alrededor del mundo, después de conocer esta noticia le dijo al sitio alemán de noticias netzpolitik.org :

En los últimos años se ha descubierto un foco que ha iluminado las prácticas secretas del hacking del gobierno. Esta área, completamente sin restricción, de inteligencia colectiva, se suma a una de las formas más intrusivas de vigilancia que cualquier gobierno puede llevar a cabo.

Gamma Group es una de las compañías más agresivas en tratar de facilitar la aplicación para los gobiernos del mundo con dichas herramientas pero >sin un debate público o leyes claras que autoricen su uso. >Esas técnicas no son lícitas”.

Privacy International y EFF ambos han presentado demandas en nombre de activistas que han sido fichados por el gobierno de Etiopía usando Fin Fisher. Muchos otros activistas han sido blanco de sus regímenes represores y las empresas de vigilancia como Fin Fisher deben de tomar responsabilidad por el papel que están jugando dentro de esta represión y dejar de hacer estar prácticas tan perjudiciales.

Jacob Appelbaum, investigador de seguridad de cómputo declaró a netzpolitik.org:

Este software explotador es muy comúnmente usado – en nuestro uso diario de teléfonos, computadores personales y en nuestra infraestructura- son problemas que deben de ser resueltos, y en lugar de resolverlos están siendo vulnerados para cualquier atacante sin importar su motivo.

La enorme publicación de los 40GB de información levanta preguntas muy interesantes – compañías que se hacen pasar por otras como RealPlayer, Adobe y otras han sido bien documentadas por terceros; ahora tenemos más evidencia de estos vectores de ataque, así como los gobiernos que han tomado partido en esta especie de fraude para su propio beneficio.

Aquí la traducción del post en Reddit del mismo usuario que se adjudicó la filtración a Gamma Group:

[...] hace un par de días cuando hackeé la cuenta de Gamma revelé 40 GB de datos de esta empresa. Tengo fuertes evidencias que indican que ellos sabían que han estado vendiendo su software para el ataque de los activistas Bahraini, junto a muchas cosas más dentro de esos 40GB.

Aquí hay un torrent de toda esa información. Por favor comparte. Aquí un feed de twitter donde estoy posteando algunas de las cosas más interesantes, empezando lento para irlo construyendo mejor que sólo publicar toda la peor mierda de una sola vez.

Los siguientes son algunos documentos que se filtraron por medio de la cuenta de twitter: