Consideraciones sobre el ataque informático a Gamma Group

CNT - TELECOMUNICACIONES Y SERVICIOS INFORMÁTICOS :: 15/08/2014

Desde el 3 agosto se viene reivindicando desde Internet un ataque informático a la empresa Gamma Group, en el que han resultado robados 40GB de información. Gamma Group es una corporación internacional dedicada a fabricar programas para vigilancia y control de equipos e infraestructuras informáticas, cuyos clientes son cuerpos militares, agencias de espionaje y cuerpos de policía internacionales, que usan los productos de dicha empresa para vigilar individuos e incluso Estados enteros.

La reivindicación del ataque

El ataque ha sido reivindicado en Twitter y en Reddit, y el pasado 8 de agosto fué publicado un documento en el cual el hacker explica cómo actuó para robar la información de Gamma Group.

Además de la explicación propiamente técnica del ataque, el hacker deja unos comentarios del motivo que le ha llevado a ello:

"*You'll notice some of this sounds exactly like what Gamma is doing. Hacking is a tool. It's not selling hacking tools that makes Gamma evil. It's who their customers are targeting and with what purpose that makes them evil. That's not to say that tools are inherently neutral. Hacking is an offensive tool. In the same way that guerrilla warfare makes it harder to occupy a country, whenever it's cheaper to attack than to defend it's harder to maintain illegitimate authority and inequality. So I wrote this to try to make hacking easier and more accessible. And I wanted to show that the Gamma Group hack really was nothing fancy, just standard sqli, and that you do have the ability to go out and take similar action.*

Solidarity to everyone in Gaza, Israeli conscientious-objectors, Chelsea Manning, Jeremy Hammond, Peter Sunde, anakata, and all other imprisoned hackers, dissidents, and criminals!"

La información que ha salido a la luz

Toda la información que ha sido robada ha sido puesta a libre disposición en Internet a través de un torrent, y desde entonces muchas personas están dedicándose a analizarla.

Resumiendo la información, los productos que vende la empresas se pueden dividir en tres grupos principales:

- Productos de intrusión e infección, para ganar el acceso a un dispositivo (ordenador, móvil, tableta, servidor, red telemática) e instalarle el programa de vigilancia
- Productos de vigilancia remota, para vigilar desde remoto los usuarios que han sido infectado

- Productos de formación, para instruir quién compre el producto sobre su uso

Todos estos productos han sido comprados por estados a nivel mundial y, en particular, por aquellos que se definen como "democráticos" (cómo Estados Unidos, Alemania, Holanda, Francia, Japón,...).

Todavía hay mucho trabajo para completar el análisis de toda la información que se ha liberado, así como su verificación y publicación (con las debidas consideraciones). Por parte del Sindicato de Telecomunicaciones y Servicios Informáticos de CNT-AIT, empeñaremos las siguientes semanas en ello.

Consideraciones sobre lo ocurrido

El hecho de que existan empresas que fabrican programas de vigilancia y que lo estados estén interesados en ellos, no es ninguna novedad: para ganar sus guerras y para cumplir con sus fines de vigilar y reprimir, los estados necesitan todas las tecnologías disponibles. Desde que existen las tecnologías informáticas los Estados las han usado en el ámbito militar, aunque en los últimos diez años estamos viendo que estas tecnologías han llegado a las manos de las masas y, por ello, los cuerpos de represión de los Estados las están usando también en el ámbito civil.

La complicidad de las empresas

Debemos tener en cuenta que, además de Gamma Group, hay muchas otras empresas que se dedican a desarrollar software y hardware con el fin controlar y vigilar a la ciudadanía, y por esto desde nuestro sindicato les consideramos directamente responsables de los crímenes cometidos por los estados.

Un evidente ejemplo español es el SITEL, sistema de escuchas telefónicas del Ministerio de Interior utilizado por la Policía Nacional y la Guardia Civil que ha sido desarrollado por la empresa ETI A/S y que es gestionado por Fujitsu España Services.

El conjunto de las empresas que ayuda a las fuerzas militares y represivas no se limita solo a las que desarrollan las herramientas puesto que hay muchas otras que les ayudan en el rastreo, investigación e interceptación de sus propios clientes. Un claro ejemplo es Facebook, que implanta acuerdos con la policía para ofrecer acceso total a la información de los usuarios.

El desarrollo de los Estados

Además del uso de herramientas desarrolladas por empresas privadas, los estados dedican muchos esfuerzos y recursos en construir sus propias herramientas para las tareas más importantes. Uno de los ejemplos más famosos son las herramientas que la NSA (agencia de inteligencia del gobierno de los Estados Unidos) desarrolla y usa para vigilar el trafico en Internet.

¿Qué hacer?

Consideramos que las herramientas tecnológicas no son neutrales por si mismas, puesto que su mismo desarrollo y uso generan estructuras de poder. El desarrollo de una herramienta para vigilar a las masas es, en si, una herramienta para aumentar el poder de control de unas pocas personas sobre la demás.

Por esto consideramos que la lucha tecnológica es parte de la lucha de clases, donde nuestro papel como clase trabajadora es defendernos de los ataques represivos y construir nosotras mismas las herramientas que necesitamos.

Como ya venimos haciendo, seguiremos con la difusión de conocimientos informáticos con charlas y talleres, y al mismo tiempo intentaremos dar un paso más adelante con nuevas formas de lucha.

SI NO QUIERES QUEDARTE CON LOS BRAZOS CRUZADOS, ACTIVATE Y PASA A LA ACCIÓN...¡¡HAY MUCHO QUE HACER!!

SINDICATO DE TELECOMUNICACIONES Y SERVICIOS INFORMÁTICOS DE MADRID

CNT-AIT

[email] informatica.madrid@cnt.es

[web] informaticamadrid.cnt.es

[twitter] @cntmadridinform

---

https://www.lahaine.org/mm_ss_est_esp.php/consideraciones-sobre-el-ataque-informatico