• EFEMÉRIDES •

Google y VirusTotal: diez fructíferos años con Málaga en el corazón

El pasado mes de abril se cumplieron 10 años desde que Google adquiriera VirusTotal, incluyendo la apertura de una pequeña oficina de la multinacional en Málaga. La noticia desató una pregunta recurrente: ¿Por qué Google se interesa por un servicio como VirusTotal? Hoy, 10 años después, es el momento de desvelar algunos detalles de aquella operación y de echar la vista atrás para observar su evolución.

VirusTotal es una plataforma *crowdsourcing* de inteligencia de amenazas. Tras la apariencia de un *multiscanner online* gratuito, el servicio analiza, clasifica y correlaciona miles de millones de ficheros e infraestructuras en Internet para ofrecer una imagen de las amenazas que acechan en la Red. VirusTotal tiene la capacidad de un telescopio para ver cómo se relacionan entre sí una constelación de familias de *malware* o ataques dirigidos y, al mismo tiempo, permite hacer zoom en un punto concreto de esa red de puntos interconexos y analizar un espécimen a nivel microscópico. Si la misión de Google es organizar la información mundial para que sea universalmente accesible y útil, VirusTotal hace lo propio en materia de ciberseguridad.

¿Qué disparó el interés de Google en Virustotal? En 2010 enviaba un *e-mail* a un ingeniero de Google, a puerta fría, donde les ofrecía una cuenta con máximos privilegios para que pudieran explorar VirusTotal. Así empezó una relación que a los pocos meses fructificó en un primer acuerdo de intercambio de servicios: acceso a VirusTotal a cambio de poder hospedar nuestro servicio en Google Cloud. Por aquel entonces VirusTotal sufría el ataque constante de DDoS provenientes de *botnets* que querían tirar el servicio para evitar la detección de sus nuevos *bots*, además el volumen de ficheros que debíamos almacenar y la propia base de datos hacía cada vez más complicado el escalado de nuestra infraestructura. VirusTotal no volvería a sufrir una caída por ataques DDoS.

El servicio siguió creciendo, era el punto central de la industria para tener acceso a las últimas amenazas, a lo que sumamos desarrollos como YARA, otro estándar de facto para la creación de firmas de detección. En ese punto llegó un primer intento de adquisición por parte de una de las mayores compañías de ciberseguridad que incluía su motor en VirusTotal. ¿Ser juez y parte?, aquello podía desestabilizar el ecosistema. Fue en ese momento, en 2012, cuando Google y VirusTotal acordamos unirnos pensando en el largo plazo y en mantener la neutralidad de un servicio que tenía como misión mejorar la seguridad global. Diez años después puedo decir que hicimos lo correcto.

El resto es historia. En 2015 VirusTotal se convertía en el primer equipo de ciberseguridad de Google en pasar a X, sus laboratorios secretos donde incuban los proyectos más disruptivos. Allí desarrollamos Chronicle, la primera empresa de ciberseguridad de Alphabet en 2018 y que un año más tarde se uniría a Google Cloud. Para entonces el equipo de Málaga había crecido a más de 40 ingenieros, y en 2021 se anunciaba que Google elegía la ciudad para crear el nuevo Centro de Excelencia en Ciberseguridad con alcance internacional, que se inaugurará en 2023. Ahora comienza un nuevo capítulo donde lo mejor está por llegar.

Bernardo Quintero
Security Engineering Director
GOOGLE