Un hacker español en China: crónica de la participación en DEFCON

Entre los días 11 y 13 del pasado mayo tuvo lugar en Beijing una nueva edición del afamado congreso de hacking DEFCON. En esta ocasión dos representantes de la compañía española Internet Security Auditors –Gonzalo Sánchez y el argentino Fabián Cuchietti– tuvieron ocasión de presentar –correspondiéndoles a ellos inaugurar la sucesión de charlas en el evento– una interesante ponencia centrada en el despliegue de malware con Google. En las siguientes líneas el especialista español explica la enriquecedora experiencia de acudir a este congreso de referencia, al tiempo que ambos expertos exponen las líneas maestras de la conferencia presentada.

Gonzalo Sánchez

EL CONGRESO

DEFCON es diferente a cualquier congreso que hayamos conocido y esto es algo que se percibe desde el primer momento. Esto es así por el equipo de la organización, pasando por el resto de ponentes del congreso y por supuesto por todos los asistentes, que lo convierten en algo impresionante desde el principio. DEFCON era para nosotros el escalafón de mayor nivel en el planeta en lo que a congresos de hacking se refiere.

El evento tuvo lugar en el hotel KunTai de Beijing. Ubicado a las afueras de la ciudad y en una zona de grandes edificios de oficinas, tenía un corto desplazamiento al aeropuerto. Al menos, dentro de lo que son los tiempos de transporte en coche en Beijing, que por momentos se vuelven muy complicados. Las comodidades y servicios del hotel eran de primer nivel y sin duda nos resultó una estancia muy confortable.

DEFCON organizó un *planning* de ponencias para los tres días de primer nivel; pero en paralelo existía una gran variedad de actividades que resultaron ser, en nuestro caso particular, la parte más interesante del congreso. Afortunadamente, al ser la nuestra la primera conferencia, tuvimos a su término tiempo libre para disfrutar de las actividades del mismo.

Por un lado estaban los DEFCON villages; se trataba de pequeños talleres temáticos, eminentemente prácticos, donde se podía practicar desde la apertura de candados de diferentes complejidades, pasando por hardware hacking de múltiples dispositivos, aplicabilidad de inteligencia artificial o el ya tradicional en estos congresos, de hacking de vehículos.

Figura 1. Acceso al congreso

Y por otro lado los DEFCON Workshops; igualmente en formato taller con una programación de días y horas concretas, eminentemente prácticos y que para nosotros resultaron ser lo más interesante de estos días. Cada uno asistimos a los que nos apetecían más.

En mi caso particular, el más interesante resultó ser el *workshop* de análisis de *malware*, donde en formato CTF el organizador planteó una serie de desafíos de análisis de varios tipos de caballos de Troya, *keyloggers* y diferentes tipos de *malware*, que había que ir resolviendo mediante el estudio del comportamiento del mismo y a contrarreloj para conseguir la mejor puntuación.

Como es habitual, DEFCON China también contó con su apartado *Capture The Flag*, reconocido en el sector como uno de los eventos CTF de mayor nivel técnico en el mundo, donde los diferentes equipos que habían conseguido clasificarse para la fase final del congreso, lucharon por la victoria. Fue una competición muy apretada desde el principio, muy intensa, y que podía seguirse en línea a través de los videomonitores gigantes que Baidu colocó en la sala. Acabó ganando el equipo *Nu1l*.

Es importante destacar aquí el papel de Baidu, principal *sponsor* del congreso, con una presencia dominante en el mismo, organizador del mismo CTF, y que durante todos los días ocupó un stand principal para mostrar sus últimos adelantos en realidad virtual y su traductor portátil (con un sorprendente y brillante desempeño), y cuyo personal nos dio la oportunidad de conocer más acerca de este gigante chino que pelea de igual a igual en muchos sectores con otras empresas de la talla de Google o Amazon.

En total, tres días repletos de actividades y charlas a cada cual de mayor interés, en los que fue imposible asistir a todo, pero que cumplió sobradamente con lo que esperábamos.

SPREADING MALWARE WITH GOOGLE (NICE QUILOMBO)

El material

Los productos de Google gozan de una buena reputación en el mercado, puesto que suelen ser sinónimo de niveles de seguridad razonablemente altos. Además, debido a la popularidad de todos los servicios de la compañía de Mountain View, los ratios de usuarios utilizando sus aplicaciones son muy elevados. Los dos factores representan un gran punto de apoyo para un escenario donde se pretende conseguir una efectiva dispersión de *malware*.

Además, Google sin duda representa un gran desafío para cualquier investigador de vulnerabilidades.

En este caso, el producto sobre el cual centramos el descubrimiento es Google Earth. La aplicación, de sobra conocida, permite la localización y visualización car-

tográfica de gran parte del globo terráqueo junto con la aplicación de capas de fotografía digital desde satélite.

Nuestro vector de infección serían los ficheros de tipo KML (y su versión comprimida KMZ), que almacenan en su interior información geográfica en formato muy similar al XML. Es muy común encontrar en Internet este formato de fichero, ya que se utiliza para compartir ubicaciones geográficas. Las temáticas son múltiples: se comparten en páginas oficiales de cartografía con temáticas como desastres naturales o incendios forestales, rutas de aficionados al deporte en la naturaleza, o con temáticas más desenfadadas, como ubicaciones de los últimos PokemonGo.

Durante nuestra intervención presentamos dos vulnerabilidades en Google Earth: primero, mediante una vulnerabilidad de tipo *null pointer* se consigue una ejecución remota de código, que permite lanzar comandos en el equipo de la víctima y el acceso a ficheros locales en el mismo. La segunda vulnerabilidad es una inyección de código javascript que en nuestra charla aprovechamos para minar la criptomoneda Monero como caso de uso.

A continuación podemos mostrar el escenario del ataque:

La víctima con Google Earth instalado en su equipo, importa un fichero KML malicioso que ha conseguido por cualquier vía de ingeniería social. En este momento, se comunica con un servidor intermedio que a su vez conecta con la máquina real del atacante para descargar el *payload* real, que a continuación sirve al equipo víctima para su ejecución. En el momento que la víctima ejecuta el *payload* se explota la vulnerabilidad *null pointer* que permite evadir la *sandbox* de Google Earth y ganar acceso al sistema de ficheros y a poder ejecutar comandos de manera remota mediante una conexión directa con el atacante.

La charla

Teníamos el honor de abrir el congreso, éramos la primera ponencia tras la apertura de bienvenida por parte de la organización, y eso es algo que siempre recordaremos. Sin duda tenía un gran punto positivo y es que al ser los primeros, luego podíamos disfrutar del resto de congreso. Pero también era una responsabilidad enorme, ya que fue un momento de máxima asistencia. Y el camino hasta ese día no fue fácil.

Todo aquel que haya viajado a China habrá comprobado (o mejor dicho sufrido) un interminable sinfín de problemas de co-

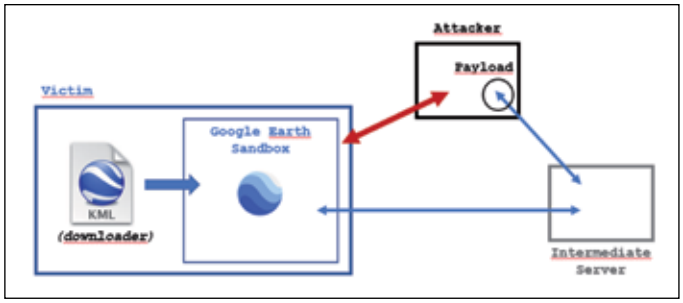

Figura 2. Escenario de ataque

nectividad con servicios de empresas que no pertenecen al país. En concreto, la gran mayoría de servicios de Google están bloqueados para acceder desde allí, y como ya es muy conocido, la utilización de redes

Figura 3. Intervención de los ponentes de Internet Security Auditors

VPN resulta imprescindible. Lo cierto es que durante la semana del congreso tuvimos enormes dificultades para conseguir llevar a cabo una demostración en directo de todo nuestro material. Las conexiones eran muy pobres, todas ellas muy restringidas y limitadas. Y condicionaban las demos en vivo de nuestra ponencia.

La charla arrancó con la habitual presentación personal y una introducción de todo el material. A continuación hicimos un *live show* con tres bloques, los tres casos de uso para mostrar los posibles impactos de las vulnerabilidades que llevábamos para presentar.

En el arranque realizamos las correspondientes presentaciones y pasamos a definir y presentar las vulnerabilidades, el escenario del ataque y los vectores de entrada. Mostramos múltiples ejemplos de páginas en internet con ficheros kml y kmz públicos para descargar y, por último, pudimos enumerar las versiones donde se consiguió evidenciar la existencia de la vulnerabilidad (en las últimas versiones de Windows y Linux).

A continuación arrancamos la demostración en vivo con el primer caso de uso de las vulnerabilidades: la ejecución remota de código. En esta fase pudimos enseñar cómo conseguíamos acceso a los ficheros locales de la máquina de la víctima y cómo podíamos editar y descargar ficheros de su equipo, al nuestro como atacantes.

En el segundo bloque de la demo, teníamos como objetivo inyectar código javascript que permitiera minar la criptomoneda Monero; pero en este caso, fue imposible poder tener una conexión a internet que nos permitiera enseñarlo. Sin embargo pudimos enseñar dónde se ubica el javascript dentro del fichero kml, qué conexiones realiza y cómo se explotaría la vulnerabilidad.

En el tercer bloque de la demo, y último, pudimos enseñar cómo tomar el control de la sesión de Google de la víctima mediante un robo de *cookies*. En este bloque final, enseñamos cómo se descargaba el fichero de *cookies* del navegador Mozilla Firefox de la víctima, nos lo importábamos en el equipo atacante para poder abrir sesión en el navegador del atacante con las credenciales de la víctima.

Y después… aplausos. Sin duda todos los problemas que sufrimos durante los días previos, y la presión y la ansiedad de impartir nuestra primera charla en DEFCON, desaparecieron al escuchar al auditorio aplaudir el resultado de la demostración. Mereció la pena. ■

Gonzalo Sánchez
Responsable de Auditoría
CEH, OCSP, CISSP, PCI ASV
INTERNET SECURITY AUDITORS