Más de 600 apasionados de la Seguridad, en Rooted CON 2012

La tercera edición de la cita más innovadora, despierta y atrevida de la Seguridad TIC sacia el hambre de nuevas experiencias y certifica un nuevo éxito de la organización.

En la imagen superior, el comité organizador de Rooted CON durante la keynote. A la izquierda, el aforo repleto en el salón de actos de la sede de Mutua Madrileña.

Tx: AGN.
Ft: Rooted CON.

UN AUDITORIO REPLETO de jóvenes (y no tan jóvenes) con ganas de devorar las líneas de código que manaban de las presentaciones de los expertos encendió la mecha de Rooted CON 2012. La 'vitola' inconfundible de este encuentro es un público entregado, como el de un partido de fútbol o un concierto de rock, con la salvedad de que este colectivo está deseoso de incorporar a su 'disco duro' conocimiento sobre *hacking* y Seguridad.

La sede de Mutua Madrileña acogió a un total de 660 registrados -que agotaron las entradas en pocos días- del 1 al 3 de marzo, en unas jornadas intensas de conferencias, *networking* y compadreo *techie*.

Román Ramírez, impulsor y cara visible de esta iniciativa, tuvo palabras de agradecimiento para los patrocinadores: AlienVault, CCN-CERT, Deloitte, HexRays, Immunity, IOActive y Telefónica. "Ellos contribuyen a que se celebre este congreso, donde demostramos que no todo se hace fuera –reivindicó-. Todos los ponentes son hispanoparlantes, que ponen en valor que (en España) también hacemos las cosas bien". En Rooted se esfuerzan cada año por escoger las ponencias en función de su originalidad y valor técnico, según explicó Ramírez, criterios que determinan la calidad de su agenda.

En el mundo de la seguridad no todo es blanco o negro, tal y como sucede con la reputación *online*. Una dirección IP puede ser fiable en determinados escenarios y en otros no tanto, pero lo complicado es averiguarlo y separar el trigo de la paja. Con el propósito de compartir esta experiencia se presentaron Guillermo Grande y Alberto Ortega, empleados de AlienVault Labs. "El problema que abordamos es analizar una enorme cantidad de tráfico y ver si es malicioso o no -argumentó Grande-. La reputación es un valor basado en el comportamiento previo de las IP que hemos analizado, pero en AlienVault vamos más allá de si es buena o mala, tratamos de ver si sirven para hacer determinadas conexiones".

Reputación IP

El experto explicó que para lograrlo es necesario contar con información muy actualizada, un método definido y disponer de un elevado rango de detección. En la web del fabricante de Open Source Security Information Management (OSSIM) se pueden consultar las características de las últimas IP incorporadas y su ubicación geográfica. ¿Cómo trabaja AlienVault para incorporar a su base de datos de reputación solamente las IP limpias? Como recordó Alberto Ortega, gigantes como Google o Akamai manejan rangos de IP enormes, donde es normal que se escapen algunas direcciones con *malware*: "Si llega contenido maligno, desestimamos esa dirección, gracias a un prefiltro entre nuestro servidor y la base de datos", añadió.

Fraude e ingeniería social

En un ejercicio eminentemente práctico, Luis Delgado, estudiante de Telecomunicaciones y colaborador del *blog* Security by Default, demostró que la mensajería instantánea se halla lejos de ofrecer garantías de protección de la información. Paso a paso, Delgado fue capaz de obtener el nombre de usuario y contraseña correspondiente a una cuenta que él mismo había creado en Google Talk, a través de una cadena de conexión vulnerable y con un simple ataque *Man in the middle*.

Por su parte, Mikel Gastesi, analista de la unidad de eCrime de S21sec, puso el acento en la ingeniería social como método de fraude financiero. Aunque resulte sorprendente, existen clientes de banca *online* que acceden a dar todos los números de su tarjeta de coordenadas en un falso panel que adopta la apariencia de portal bancario. Gastesi reveló cómo los ciberdelincuentes vulneran el segundo factor de autenticación, como puede ser el móvil: "Ni siquiera PayPal o pasarelas de pago seguro están libres. En el mercado *underground* se puede conseguir una inyección para una entidad concreta por 60 dólares y un paquete completo con una *botnet* asociada, por 400". El reto de la industria es combatir estos ataques fomentando la concienciación: "Estamos intentando dar soluciones técnicas a un problema que no lo es, que depende del conocimiento y de la información", matizó. ■