ElcomSoft descubre vulnerabilidad en el Sistema de Autenticación de Imagenes de Nikon

Moscow, Russia – April 28, 2011 – ElcomSoft Co. Ltd. analizó el sistema de Autenticación de imágenes de Nikon, un suite seguro que verifica si la imagen ha sido alterada después de la toma y descubrió una mayor vulnerabilidad en el manejo de la clave de inscripción que protege la imagen. Esto permitió a la empresa extraer la clave de inscripción original de la cámara Nikon. Al explotar esta vulnerabilidad se hace posible fabricar las imágenes alteradas con una firma de autenticación absolutamente válida. ElcomSoft logró extraer la clave de inscripción de imagen original y producir una serie de imágenes falsificadas que fueron validadas por Nikon Image Authentication Software

ElcomSoft ha notificado a CERT y Nikon sobre este asunto y preparó una serie de imágenes digitales alteradas que fueron validadas como imágenes auténticas por el software de autenticación de Nikon. Hasta el momento Nikon no ha respondido ni ha mostrado interés por el asunto.

Acerca de Nikon Image Authentication System

Junto con los módulos de firma incluidos en SLRs de primera calidad elaborados por Nikon, el objetivo de Nikon Image Authentication Software era permitir a los usuarios determinar si la imagen fue alterada después de la toma. Según Nikon, el sistema sirve para asegurar la autenticidad de imágenes para agencias de orden público, agencias gubernamentales, compañías de seguro, negocios y agencias de noticias. Como demostró ElcomSoft, las promesas hechas por dos productores de cámaras digitales más grandes, Canon y Nikon, no eran del todo ciertas.

Antecedentes

Credibilidad de la evidencia fotográfica puede ser sumamente importante en una variedad de situaciones. Los tribunales, noticieros, compañías de seguro pueden aceptar fotos digitales firmadas como una evidencia válida. Si estas pruebas han sido falsificadas, las consecuencias pueden ser muy graves. Existen muchos casos de fraude cometido por fotógrafos entusiastas, periodistas, editores, partidos políticos, y hasta el Ejército de los Estados Unidos

Para resolver el problema, los fabricantes del equipo fotográfico más grandes, entre ellos Canon y Nikon desarrollaron sus propias versiones del sistema de autenticación de imágenes. En 2010, ElcomSoft analizó el sistema de autenticación de imágenes propia de Canon. Igual al sistema de Nikon, el de Canon tendría que probar la autenticidad de imágenes para los medios de comunicación, agencias de orden público, agencias gubernamentales y de negocios. ElcomSoft demostró que el sistema de Canon tenía unas fallas que todavía no han sido arregladas, casi medio año después del descubrimiento.

Seis meses después, ElcomSoft descubrió que una vulnerabilidad similar existía en cámaras digitales SLR fabricadas por Nikon. La existencia de esta vulnerabilidad significa que los datos de autenticación de imágenes pueden ser falsificados, el hecho que hace imposible confiar en Nikon Image Authentication System. Como consecuencia, no se puede usar las imágenes validadas por Nikon Image Authentication Software como pruebas de autenticidad.

El caso de Nikon's Security System

Al diseñar el sistema digital de seguridad es muy importante implementar todas partes del sistema igual y apropiadamente. El sistema entero es tan seguro como su elemento más débil. En el caso de Image Authentication System de Nikon, la empresa no logró terminar todo el proceso exitosamente. La vulnerabilidad está en el manejo de la clave de inscripción. Como la clave criptográfica de inscripción no se usa correctamente, esta puede ser extraída, lo que fue comprobado por los investigadores de ElcomSoft. Al obtener la clave, se puede usar para firmar cualquier imagen, no importa si esta ha sido alterada, editada o hasta generada por computadora previamente. Después la imagen pasará por autentica y validada por Image Authentication Software de Nikon

La vulnerabilidad existe en todas cámaras de Nikon que soportan Nikon Image Authentication, incluyendo Nikon D3X, D3, D700, D300S, D300, D2Xs, D2X, D2Hs, y D200 digital SLRs.

ElcomSoft compartirá algunos detalles técnicos en una de las conferencias de seguridad en un futuro próximo. Aunque todos los detalles no serán revelados en los intereses de responsabilidad pública. El vendedor y CERT Coordination Center han sido informados sobre el asunto. ElcomSoft ha contactado a todas las sucursales de Nikon, incluyendo Nikon EUA, Nikon Europa y Nikon Japón, sin embargo la empresa no ha hecho ningún comentario ni ha mostrado interés alguno sobre el hallazgo.

ElcomSoft ha extraído la clave de inscripción y para probar el concepto ha preparado una serie de imágenes falsificadas que fueron validadas por Nikon Image Authentication Software como originales. Para ver estas imágenes pulse aquí http://nikon.elcomsoft.com

Acerca de ElcomSoft

Establecido en 1990 ElcomSoft Co. Ltd desarrolla las herramientas de computadoras forenses de última generación, ofrece un entrenamiento en informática forense y consultas sobre evidencia digital. Desde 1997 ElcomSoft ha estado apoyando a empresas, agencias de orden público, agencias militares y de inteligencia. Los productos de ElcomSoft se utilizan por muchos corporaciones de Fortune 500, agencias militares alrededor del mundo, gobiernos extranjeros y la mayoría de las empresas de contabilidad. ElcomSoft y sus empleados son miembros de la Asociación Rusa de Criptología (RCA). ElcomSoft es un Microsoft Gold Certified Partner e Intel Software Partner. Para más información visite http://www.elcomsoft.es

Para ver las imagenes alteradas que fueron validadas por Nikon Image Authentication Software pulse aquí http://nikon.elcomsoft.com