Компания ЭлкомСофт обнаружила уязвимость в системе аутентификации снимков компании Nikon

Москва, Россия –28 апреля 2011 года – Компания «ЭлкомСофт» (ElcomSoft Co. Ltd.) исследовала систему проверки подлинности фотоснимков, созданную компанией Nikon, которая устанавливает наличие или отсутствие изменений в изображении с момента создания снимка, и обнаружила серьезную уязвимость в способе обработки ключа шифрования защищенного снимка. Это в свою очередь позволило компании извлечь оригинальный ключ подписи из цифровых зеркальных фотоаппаратов фирмы Nikon. Пользуясь данной уязвимостью, можно создавать измененные цифровые фотоснимки с действительным ключом аутентификации. Компания «ЭлкомСофт» подготовила несколько фальшивых изображений, которые успешно проходят проверку программы Image Authentication Software компании Nikon.

Компания «ЭлкомСофт» уведомила CERT и компанию Nikon о данной проблеме и подготовила ряд измененных цифровых фотоснимков, которые признаются как подлинные программой аутентификации изображений компании Nikon. Однако компания Nikon не предоставила никакого ответа и не проявила ни малейшего интереса к данной проблеме.

О программе Image Authentication компании Nikon

С помощью модулей цифровой подписи, имеющихся в топовых цифровых зеркальных фотокамерах Nikon, программа Image Authentication должна была позволить пользователям проверить подлинность фотоснимка. Согласно заявлению компании Nikon, данная система представляет доказательства аутентичности изображения для «правоохранительных органов, правительственных организаций, средств массовой информации, страховых компаний, а также при выполнении различных прикладных задач». Однако, компания «ЭлкомСофт» наглядно продемонстрировала, что заявления двух главных производителей цифровых фотокамер, Canon и Nikon, являются пустым «очковтирательством».

Предыстория

Достоверность фотографических улик может иметь огромное значение в ряде ситуаций. Суды, новостные агентства и страховые организации могут принять фотоснимки с цифровой подписью в качестве настоящего доказательства. Однако если подобное доказательство сфальсифицировано, последствия могут быть крайне тяжелыми. Самые нашумевшие случаи связаны с фальсификациями, организованными фотографами-любителями, фотожурналистами, редакторами, политическими партиями и даже армией США.

Чтобы справиться с этой проблемой, основные производители фотооборудования, а именно компании Canon и Nikon, разработали свои собственные корпоративные системы проверки подлинности фотоснимков. В 2010 году компания «ЭлкомСофт» уже произвела анализ защиты системы проверки подлинности цифровых изображений компании Canon, которая так же как и система компании Nikon, должна была доказывать подлинность изображений в глазах масс медиа, правоохранительных органов, правительственных организаций и бизнес структур. Однако компания «ЭлкомСофт» показала, что в программной проверке компании Canon существует серьезная уязвимость, которая так и не была решена до сегодняшнего дня.

Через полгода, компанией «ЭлкомСофт» была обнаружена похожая уязвимость в цифровых зеркальных фотокамерах Nikon. Найденная уязвимость показывает, что данные подтверждения подлинности снимков могут быть сфальсифицированы, поэтому всей системе проверки аутентичности снимков компании Nikon нельзя и не стоит доверять. Соответственно, успешно проведенная проверка подлинности с помощью программы Image Authentication не является настоящим доказательством.

Некоторые аспекты системы безопасности компании Nikon

При разработке цифровой системы безопасности важно тщательно и аккуратно использовать все составляющие системы. Безопасность всей системы зависит от самого слабого звена. В случае с системой проверки аутентичности фотоснимков компании Nikon, компания не доработала, по меньшей мере, одно: суть уязвимости заключается в способе обработки криптографического ключа подписи, который неправильно обрабатывается и поэтому его можно легко извлечь из фотокамеры, как уже показали разработчики «ЭлкомСофт». После получения ключа подписи, его можно использовать для подписи любой фотографии, вне зависимости от того была она изменена, отредактирована или вообще создана на компьютере. Подписанное изображение успешно пройдет проверку подлинности с помощью программы Nikon Image Authentication.

Настоящая уязвимость существует во всех современных фотокамерах Nikon, которые поддерживают программу Nikon Image Authentication, включая цифровые зеркальные фотоаппараты Nikon D3X, D3, D700, D300S, D300, D2Xs, D2X, D2Hs, и D200.

Компания «ЭлкомСофт» поделится некоторыми техническими данными на одной из предстоящих конференциях по безопасности, но полная информация не будет разглашаться. Производитель и координационный центр CERT были извещены о проблеме. Компания «ЭлкомСофт» связалась со многими отделениями Nikon, включая представительства Nikon в США, Европе и Японии, однако вразумительного ответа не последовало, и компания не выразила заинтересованности в данном вопросе.

ООО «ЭлкомСофт»

Компания «ЭлкомСофт» – российский разработчик программного обеспечения и поставщик услуг в области восстановления паролей и данных. Решения ElcomSoft используются корпорациями, входящими в список Fortune 500, а также правительственными организациями, правоохранительными органами и спецслужбами по всему миру. Компания ElcomSoft является членом Российской Криптологической Ассоциации, имеет статус сертифицированного партнера Microsoft (Microsoft Gold Certified Partner) и Intel (Intel Software Partner). Компания основана в 1990 году, головной офис ElcomSoft находятся в Москве. Более подробная информация доступна на сайте http://www.elcomsoft.ru

Компания «ЭлкомСофт» предлагает ряд отредактированных фотографий, которые легко проходят проверку подлинности с помощью комплекса Nikon Image Authentication Software на странице http://nikon.elcomsoft.com