News
New Jersey
Office of the Attorney General
NEW JERSEY DEPARTMENT OF LAW & PUBLIC SAFETY

John J. Hoffman, *Fiscal General Interino*

División de Asuntos del Consumidor
Steve C. Lee, *Director Interino*

División de Leyes
Jeffrey S. Jacobson, *Director*

Para publicación inmediata:
Día 29 de Junio del 2015

Para más información contacte:
Jeff Lamm o Neal Buccino
973-504-6327

La División de Asuntos del Consumidor de New Jersey, la Comisión Federal de Comercio, llegan a un acuerdo con el desarrollador de una móvil app del que se alega pirateó los teléfonos inteligentes de New Jersey con nociva malware

---

NEWARK –En otra victoria para la seguridad de las computadoras y aplicaciones móviles de los residentes de New Jersey, la New Jersey Division of Consumer Affairs se ha unido a la Federal Trade Commission o FTC en un acuerdo con los fabricantes de "Prized," una aplicación móvil que se alega pirateó los teléfonos inteligentes Android y las tabletas con nociva malware.

Específicamente, el Estado y la FTC alegan que los consumidores que descargaron Prized en sus aparatos también sin quererlo descargaron software maliciosa que infectó los aparatos y causó que "minaran" por dinero virtual como Litecoin, Dogecoin, y Quarkcoin.

Pero el proceso de "minar" – que es muy extenuante en las computadoras y todavía más en los teléfonos inteligentes y en las tabletas – se alega dañaron los aparatos infectados de los dueños, y tenían la capacidad de dejar a los aparatos con casi ninguna habilidad de funcionamiento. Los dueños de los teléfonos inteligentes y de las tabletas se enfrentaron con la posibilidad de incrementos de costos de electricidad y de uso de data; acortar la vida de los aparatos; y dinero, tiempo, y el esfuerzo de remover el malware.

Los acusados en este asunto, el desarrollador de la aplicación, basado en Ohio, Equiliv Investments y Ryan Ramminger, ofrecieron el app Prized a través de sitios webs como Google Play y tiendas de app de Amazon.

El Acting Attorney General John J. Hoffman dijo, "Los consumidores, descargaron este

app pensando que -en la peor situación- no iba a ser tan útil o entretenida como estaban anunciando. En vez, la app se alega terminó siendo un caballo de Troya, para malware intrusiva, invasiva que tenía la capacidad de dañar los caros teléfonos inteligentes y otros aparatos móviles."

La División y la FTC hoy obtuvieron un acuerdo con Equiliv Investments y Ramminger en el U.S. District Court, District of New Jersey, en el que se les prohíbe a los acusados por mercadear o vender productos que funcionan como malware, y por engañar en la venta o anuncio de productos de software.

Además, los acusados deben, en los próximos 20 años, regularmente proveer a la División y a la FTC con documentos financieros, de personal, y otros documentos con la intención de ayudar a asegurar su completo cumplimiento con los términos del acuerdo así como con el Federal Trade Act y el Consumer Fraud Act. Los acusados también tienen que pagar $5,200 para reembolsar al State of New Jersey por costos legales y de investigación. Unos $44,800 de pago adicional serán suspendidos o perdonados dentro de tres años, proveyendo que los acusados cumplan con los términos completos del acuerdo de la Order.

Los acusados removieron la Prized app de Google Play y Amazon App en línea en las tiendas, del sitio web de Equiliv, y de las terceras partes de tiendas de app. La app no está disponible más para descargo.

El Director Interino de la Division of Consumer Affairs Steve Lee dijo, "Este no es el primer caso que hemos visto en el que el desarrollador de la software pensó aventajarse de los aparatos de dueños privados, sin el consentimiento de estos, para minar dinero virtual. Pero en este caso los teléfonos inteligentes, y no las computadoras están envueltos. Esto crea una posibilidad de un daño grande, ya que los aparatos móviles tienen un proceso más limitado de energía y con frecuencia vienen con un plan de data más caro."

Historial de la "Prized" App:

Una Queja puesta en la U.S. District Court por la Division y la FTC, anotaron que entre otras cosas:

Para tentar a los consumidores a que descargaran Prized y su malware, la app pretendía que los consumidores ganarían puntos que se podrían redimir por premios como ropa, accesorios, y tarjetas de regalo.

La descripción y términos de uso de la app no decían nada acerca de la posibilidad de que Prized podría piratear los aparatos de los usuarios. De hecho, los términos de uso de Equiliv específicamente representaron a los consumidores que Prized y su software "estaban libres y estarían libres de malware, spyware, time bombas, y virus"

A pesar de estas descripciones, Prized contenía malware que tomó control de los teléfonos inteligentes y de las tabletas de los usuarios e hizo que estos minaran por dinero virtual o "cryptocurrencies" conocidos como Dogecoin, Litecoin y Quarkcoin.

Cryptocurrencies, como dinero regular, se pueden usar para comprar mercancías y

servicios de mercaderes que deciden aceptarlos como pagos. Dogecoin, Litecoin, y Quarkcoin son generados o “minados” a través de resolver muy complicados algoritmos, un proceso que requiere una gran cantidad de proceso de la computadora.

Cuando una computadora se usa para minar dinero virtual, su energía de proceso se limita. Este proceso puede acortar la vida de la computadora y crear un costo alto de electricidad. Los efectos pueden ser todavía más nocivos para teléfonos inteligentes y otros aparatos móviles, los cuales tienen un proceso de energía menos que las computadoras, con frecuencia usan un plan de data más caro, y se pueden recalentar si les fuerza a preformar las funciones complicadas de computación requerida para minar cryptocurrency por un prolongado periodo de tiempo.

Además del uso de malware, Equiliv también en muchos instantes no proveyó a los consumidores con los puntos de redención que la app prometía.

La División y la FTC alegan que las acciones de Equiliv y Ramminger constituyeron violaciones del Federal Trade Commission Act y del New Jersey’s Consumer Fraud Act.

“Piratear los aparatos móviles de los consumidores con malware para minar dinero virtual no es solamente deplorable; es también ilegal,” dijo Jessica Rich, Director del FTC’s Bureau of Consumer Protection. “Estos estafadores están ahora prohibidos por intentar tal esquema otra vez.”

Los Deputy Attorneys General Glenn T. Graham y Elliott M. Siebers representaron al Estado de New Jersey en este asunto.

El Investigador Brian Morgenstern, asignado a la Division of Consumer Affairs’ Cyber Fraud Unit, condujo la investigación.

Este caso es parte del trabajo en curso de la FTC para proteger a los consumidores de tomar ventaja de la nueva emergente tecnología financiera, también conocida como FinTech. El avance de la tecnología expande las maneras en las que los consumidores pueden guardar, compartir, y gastar dinero. La FTC está trabajando para proteger a los consumidores mientras está animando innovaciones para el beneficio de estos.

La Division of Consumer Affairs implementa el New Jersey Consumer Fraud Act, el New Jersey Computer-Related Offenses Act, y otras leyes que protegen a los residentes de New Jersey en contra del robo de identidad, invasiones ilegales de privacidad, y otras violaciones relacionadas con las computadoras.

El "Manual de Seguridad en Cibernética" de la División (http://www.njconsumeraffairs.gov/News/Brochures/SpanishPages/Cyber-Security-Handbook-Spanish.pdf) incluye importante información para la protección de los consumidores en "Básica Protección en el Mundo Cibernético," "Previniendo el Robo de Identidad," y "Controlando su Privacidad."

Los consumidores que creen han sido abusados o engañados por un negocio, o sospechan de cualquier otra clase de abuso al consumidor, pueden poner una queja en línea (http://www.njconsumeraffairs.gov/ComplaintsForms/spanish/General-Complaint-

Form-Spanish.pdf) con la State Division of Consumer Affairs o pueden llamar a 1-800-242-5846 (gratis si llama desde New Jersey) o al 973-504-6200.

Siga a la Division of Consumer Affairs en Facebook, y chequee nuestro calendario en línea de eventos de abordo a la comunidad en Consumer Outreach.

###