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

Robert Lougy, *Fiscal General Interino*

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

División de Leyes
Michelle Miller, *Directora Interina*

Para publicación inmediata:
Día 10 de Mayo del 2016

Para más información contacte:
Lisa Coryell, 973-504-6327

Alerta al Consumidor: Amenaza de incremento de "Ransomware" que toma la información de su computadora como rehén

NEWARK – La Office of the Attorney General y la New Jersey Division of Consumer Affairs hoy alertan a los consumidores acerca del aumento de la amenaza de "ransomware," una clase de programas maliciosos que codifican o cierran, valiosos archivos digitales y los tienen de rehén por dinero.

Estos ataques de viruses, los cuales crecieron mucho el año pasado, se esperan que se sucedan con más frecuencia en el 2016, según la New Jersey Cybersecurity and Communications Integration Cell ("NJCCIC"), que rastrea las amenazas en línea por todo el estado. Individuos, negocios, agencias del gobierno, e instituciones privadas son vulnerables a este virus paralizador que por lo general se transmite a través de un email infectado.

"Ransomware se está convirtiendo en una gran amenaza a la ciber-seguridad, ya que hackers (piratas) muy sofisticados obtienen ganancias enormes 'secuestrando' y manteniendo rehenes los archivos privados de información sensitiva que pertenecen a organizaciones globales engañando a los individuos miembros para que le den acceso," dijo el Acting Attorney General Robert Lougy.

Los empleados de grandes instituciones como las agencias del gobierno, burós de implementación de leyes, corporaciones, y organizaciones de salud, son bombardeadas con emails infectados con estos viruses disfrazados como mensajes de sus supervisores o de otros personajes de autoridad. Incluso el más sofisticado usador de webs con frecuencia no piensa dos veces acerca de pulsar en un enlace desconocido cuando la directiva viene de sus supervisores.

Los individuos usando su computadora personal en sus casas tampoco están inmunes a los ataques. Los criminales de cibernética se están enfocando en servidores de la red de organizaciones con gran cantidad de miembros, como alumnos de asociaciones y grupos religiosos para mandar falsos emails a los miembros, con la esperanza de

infectar las computadoras.

Una vez que han obtenido acceso a la computadora de un individuo, los programas maliciosos (malware) empiezan a codificar los archivos y carpetas en discos locales, en cualquier disco adjunto, discos de reserva, y posiblemente otras computadoras de la red a las que la víctima está conectada. Las víctimas con frecuencia no saben que están infectadas hasta se dan cuenta de que no pueden acceder a su información o empiezan a recibir demandas de dinero, usualmente en la forma de Bitcoin u otra forma de dinero virtual que no se puede rastrear.

Los hospitales ansiosos de recuperar los archivos electrónicos de los pacientes, padres preocupados de mantener los números de seguro social de sus hijos de las manos de los ladrones de robo de identidad y abuelas desesperadas de recobrar las fotos de la familia se enfrentan con el dilema: pagar o arriesgar perder los valiosos archivos para siempre.

“Estamos alertando a los consumidores para que tomen precauciones contra el incremento de amenaza de ransomware para que se protejan y a sus empleados de estos viruses maliciosos,” dijo Steve Lee, Acting Director of the New Jersey Division of Consumer Affairs. “Los criminales de cibernética son cada día más sofisticados con sus ataques, por lo tanto los consumidores tienen que estar más vigilante para prevenirlos.”

Sugerencias para evitar Ransomware:

- Tenga cuidado con juegos gratis, toolbars y otras software. Antes de descargar software, asegúrese que el software es de una fuente fiable.
- Nunca pulse en sospechosos enlaces en emails o anuncios pop up. Incluso cuando la fuente es legítima – como un email de su banco – juegue seguro yendo al sitio web de su banco.
- No se fíe en particular de emails con adjuntos que parecen que vienen de marcas conocidas cuando aparecen de repente.
- Tenga la misma precaución con sus teléfonos inteligentes así como con su computadora personal y de oficina.
- Regularmente preserve sus archivos importantes, incluyendo esas fotos valiosas de familia, y preserve la información fuera de línea para custodiarla.
- Asegúrese que las computadoras de su casa tienen anti-virus, anti-spyware, y anti-malware software.
- Como la ransomware también puede atacar desde un sitio web, asegúrese que vulnerables plugins como Flash y Java requieran su permiso para funcionar.
- Use extensiones de bloqueo en browsers para prevenir “drive-by” infecciones de anuncios que contienen códigos maliciosos.
- Use protección para bloquear el acceso a su web y emails de maliciosas redes y escanee todos sus emails, adjuntos, y descargue y configure los emails servers para anticipar bloquear emails conteniendo sospechosos adjuntos como .exe, .vbs, and .scr.
- Considere utilizar una herramienta gratis o comercial disponible de anti-ransomware de cualquiera de los vendedores líderes de software de seguridad de computadoras.

Por desgracia, la proliferación y sofisticación de los ataques de ransomware hace muy difícil que incluso el más cuidadoso usuario de la web pueda mantenerse seguro. Y una vez que ha sido victimizado, no hay mucho que la víctima pueda hacer para encontrar a los criminales que han hecho los ataques porque los lanzan de anónimos internet enrutadores que son muy difíciles o imposible de rastrear. Pero hay pasos que puede tomar para prevenir pagar por el rescate.

Si sospecha que es una víctima de ramsonware:

- Desconéctese de las redes inmediatamente si sospecha una infección y no se reconecte hasta que la computadora o dispositivo ha sido completamente inspeccionado y limpiado.
- Alerte a la apropiada seguridad de contacto dentro de su organización si nota actividad rara en sus redes, computadoras, o aparatos móviles.
- Depende de la variedad de ransomware que lo ha invadido, una herramienta gratis de decodificación puede ser disponible. Para determinar qué clase de variante ha infectado su sistema pulse en NJCCIC Ransomware website.

Si su organización es la víctima de la infección de ransomware, o le gustaría aprender más acerca de la compartición de información de ciber seguridad, análisis de amenazas, y reportes de incidentes, vaya a NJCCIC website, o póngase en contacto con Cyber Liaison Officer en njccic@cyber.nj.gov.

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 (http://www.facebook.com/pages/NJ-Division-of-Consumer-Affairs/112957465445651) y chequee nuestro calendario en línea de eventos venideros en Consumer Outreach (http://www.njconsumeraffairs.gov/ocp/Pages/Consumer-Oureach.aspx).

###