Publicado en 28006 el 05/06/2013

Kaspersky Lab destapa la 'Operación NetTraveler', una nueva campaña de ciberespionaje global

Ya ha infectado a unas 350 víctimas de alto perfil, incluyendo instituciones gubernamentales, embajadas, industria del petróleo y gas, centros de investigación, contratistas militares y activistas políticos

La finalidad del ataque es el robo de datos y la cibervigilancia. Los datos robados extraídos del servidor C & C supera los 22 gigabytes

España está entre los diez países con más víctimas detectadas según KSN, junto con Mongolia, Rusia, India, Kazajstán, Kirguistán, China, Tayikistán, Corea del S

Madrid, 4 de junio de 2013 – El equipo de expertos de Kaspersky Lab ha publicado un informe de investigación sobre NetTraveler, una familia de programas maliciosos utilizados por APT (Advanced Persistent Threat) que ha comprometido a más de 350 víctimas de alto perfil en 40 países distintos. El grupo NetTraveler ha infectado a las víctimas tanto en el sector público como en el privado, incluyendo instituciones gubernamentales, embajadas, la industria del petróleo y gas, centros de investigación, contratistas militares y activistas políticos.

Según el informe de Kaspersky Lab, la amenaza ha estado activa desde 2004; sin embargo, el mayor volumen de actividad se ha dado entre 2010-2013. Recientemente, los principales dominios del grupo NetTraveler mostraron interés por el ciberespionaje, incluyendo la exploración del espacio, la nanotecnología, la producción de energía, la energía nuclear, el láser, la medicina y las comunicaciones.

Los métodos de infección:

• Los ciberdelincuentes infectan a las víctimas mediante el envío de correos electrónicos phishing con adjuntos maliciosos de Microsoft Office que contienen dos vulnerabilidades altamente explotadas (CVE-2012-0158 y CVE-2010-3333). A pesar de que Microsoft ya publicó parches para estas vulnerabilidades están siendo muy utilizados para ataques dirigidos y han demostrado ser eficaces.

• Los títulos de los archivos maliciosos adjuntos en los correos electrónicos de phishing demuestran el esfuerzo del grupo NetTraveler al personalizar sus ataques con el fin de infectar objetivos de alto perfil. Los títulos de los documentos maliciosos incluyen:

Army Cyber Security Policy 2013.doc
Report - Asia Defense Spending Boom.doc
Activity Details.doc
His Holiness the Dalai Lama’s visit to Switzerland day 4

Freedom of Speech.doc

Robo y extracción de datos:

• Durante el análisis, los expertos de Kaspersky Lab obtuvieron registros de infección de varios de los servidores de comando y control (C&C) de NetTraveler. Los servidores C&C se utilizan para instalar otros programas maliciosos en los equipos infectados y extraer datos robados. Kaspersky Lab calcula que la cantidad de datos robados almacenados en los servidores C&C de NetTraveler supera los 22 gigabytes.

• Los datos extraídos de las máquinas infectadas suelen incluir listas de archivos de sistema, keyloggs, y varios tipos de archivos, incluyendo PDFs, hojas de Excel y documentos de texto. Además, el toolkit de NetTraveler pudo instalar malware para robar información adicional con un backdoor que puede personalizarse para robar otro tipo de datos sensibles, como los de configuración de una aplicación o archivos de diseño asistido por ordenador.

Estadísticas de infecciones globales:

• En base al análisis de los datos del C&C de NetTraveler realizado por Kaspersky Lab, se han detectado un total de 350 víctimas en 40 países de todo el mundo, incluyendo los Estados Unidos, Canadá, Reino Unido, Rusia, Chile, Marruecos, Grecia, Bélgica, Austria, Ucrania, Lituania, Bielorrusia, Australia, Hong Kong, Japón, China, Mongolia, Irán, Turquía, India, Pakistán, Corea del Sur, Tailandia, Qatar, Kazajstán y Jordania.

• En relación con el análisis de datos de C&C, los expertos de Kaspersky Lab han utilizado Kaspersky Security Network (KSN) para identificar las estadísticas de infección adicionales. Los diez países con más víctimas detectadas por KSN son Mongolia seguidos por Rusia, India, Kazajstán, Kirguistán, China, Tayikistán, Corea del Sur, España y Alemania.

Hallazgos adicionales

• Durante el análisis de NetTraveler, los expertos identificaron seis víctimas que habían sido infectadas por tanto NetTraveler como por Octubre Rojo, que fue otra operación de ciberespionaje analizado por Kaspersky Lab en enero de 2013. Aunque no se observaron relaciones directas entre ambos

ciberdelincuentes, el hecho de que víctimas concretas fueran infectadas por estas dos campañas indica que las víctimas de alto perfil son el blanco de múltiples actores porque su información es un bien muy valioso.

Los productos de Kaspersky Lab detectan y neutralizan los programas maliciosos y sus variantes utilizadas por el Toolkit NetTraveler, como Trojan-Spy.Win32.TravNet y Downloader.Win32.NetTraveler. Los productos de Kaspersky Lab también detectan los exploits de Microsoft Office utilizados en los ataques de phishing, incluyendo Exploit.MSWord.CVE-2010-333, Exploit.Win32.CVE-2012-0158.

Para leer el análisis completo de la investigación de Kaspersky Lab y los detalles de NetTraveler y sus componentes maliciosos, por favor visite Securelist.

Datos de contacto:
Everythink PR

Nota de prensa publicada en: 28006

Categorías: Ciberseguridad