ESET: FriedEx es el trabajo de los desarrolladores de Dridex

ESET Latinoamérica, compañía especializada en detección proactiva de amenazas, ha descubierto que los autores del troyano bancario **Dridex** están también detrás de otra familia de malware de alto perfil, un ransomware sofisticado denominado **FriedEx**, también conocido como **BitPaymer**.

El troyano bancario Dridex apareció por primera vez en 2014 como un **bot** (programa informático cuya función es realizar tareas automatizadas a través de Internet) que rápidamente fue **convertido en uno de los troyanos bancarios más sofisticados del mercado**. El desarrollo parece ser estable, con nuevas versiones del bot lanzándose cada semana, e incluyendo pequeñas correcciones y actualizaciones.

La última gran actualización de la versión 3 a la versión 4, lanzada a comienzos de 2017, **ganó atención al adoptar la nuevas técnicas de propagación buscando evadir soluciones de seguridad más adelante ese mismo año al introducir un nuevo exploit zero-day** en la suite de ofimática de Microsoft , que ayudó a difundir el troyano entre millones de víctimas, como explica un comunicado de prensa.

ESET el año pasado lanzó una **herramienta que permite identificar procesos maliciosos que pudieran estar asociados a la amenazas y ligados a buscadores web**. La herramienta está diseñada para ayudar a los afectados por un incidente a descubrir potenciales infecciones de troyanos bancarios, incluyendo Dridex.

A su vez, **el ransomware inicialmente denominado BitPaymer, fue descubierto a comienzos de julio de 2017 por Michael Gillespie**. En agosto volvió a ser centro de atención y ocupó los titulares tras infectar hospitales del Servicio Nacional de Salud (NHS, por sus siglas en inglés) en Escocia. FriedEx se enfoca en objetivos y compañías de alto perfil más que en usuarios finales. El ransomware cifra cada archivo con una clave, que luego también es cifrada y guardada en el .readme_txt file correspondiente.

ESET asegura que **FriedEx** es el trabajo de los desarrolladores de Dridex. “Este descubrimiento nos da una imagen más clara de las actividades del grupo – podemos ver que el grupo continúa activo y no sólo actualiza constantemente su troyano bancario para mantener su soporte de inyecciones web para las últimas versiones de Chrome y para introducir nuevas funcionalidades como Atom Bombing para buscar evadir soluciones de seguridad, pero que también sigue las últimas “tendencias” del malware, creando su propio ransomware”, concluyó Camilo Gutierrez, jefe del Laboratorio de Investigación de ESET Latinoamérica.

.