Fuente:
TIC Beat
ESET ha publicado el análisis de sus pronósticos sobre los próximos ciberataques que sufriremos en 2017, año en el que el temible ransomware vendrá estrechamente ligado al Internet de las Cosas y la proliferación de dispositivos conectados.

No solo es una de las amenazas preferidas de los hackers, uno de los tipos de malware más usados y el dolor de cabeza que no deja dormir a las pymes, sino que además, su peligro será exponencialmente más peligroso conforme el Internet de las Cosas se asiente en nuestras vidas y el número de dispositivos conectados se multiplique.

Según ha destacado ESET en su informe Tendencias 2017: “La Seguridad como rehén”, preparado por los expertos de su laboratorio de investigación, el ransomware seguirá siendo uno de los protagonistas más relevantes el próximo año. Este se trata de un software malicioso capaz de bloquear un ordenador desde una ubicación remota y encriptar todos los archivos que este contenga.

Así, la compañía destaca en su informe que verá la luz el denominado “Ransomware de las Cosas”, también bautizado como RoT, que exigirá una gran preparación por parte de las empresas para blindar su protección y El objetivo principal del estudio es que tanto empresas como usuarios estén mejor preparados para afrontar los próximos desafíos y así puedan mantenerse protegidos.

El informe sugiere que durante el próximo año 2017 el ransomware seguirá teniendo un papel protagonista, y nacerá el bautizado como Ransomware de las Cosas o RoT, que ofrece a los ciberdelincuentes la posibilidad de secuestrar dispositivos para exigir a posteriori el pago de un rescate a cambio de devolver el control para al usuario. Según sugiere Stephen Cobb, 2017 podría ser el año del jackware, vocablo que alude al traslado del ransomware más allá de ordenadores y dispositivos móviles -véase los gadgets del hogar conectado o el coche conectado-.

Las personas, el eslabón más débil de la ciberseguridad

Los dispositivos inteligentes no serán el único objetivo viable, sino que los hackers también se centrarán en atacar las infraestructuras críticas, de las cuáles depende la seguridad física, económica o pública de un país. En suma, vitales para el desarrollo cotidiano de una sociedad.

La industria de la salud -con dispositivos médicos y centrados en la monitorización de la actividad física-, también sufrirán estos ataques, junto al sector de los videojuegos, que también dejan la puerta abierta a la explotación de vulnerabilidades o la instalación de malware, con el propósito de acceder a todo tipo de

información financiera, personal y de partidas de los gamers. Otra tendencia a destacar es el aumento del malware móvil, cada vez más insistente y complejo.

Desde Eset subrayan que el denominador que atraviesa todos los ejes abordados es la importancia de la formación y la educación para usuarios, empresas y fabricantes a fin de que comprendan los riesgos actuales y futuros y tomen dimensión de que la era de la conectividad y la llegada del Internet de las Cosas implica un profundo cambio de mentalidad.

Estar preparados es muy importante para no permanecer en un escenario con tecnología de última generación pero gestionada con conceptos de seguridad de hace más de una década. Además del usuario final, es importante que los gobiernos adopten marcos legislativos que prioricen la ciberseguridad, las empresas apuesten por las soluciones punteras y la contratación de profesionales, y que los desarrolladores no posterguen la seguridad de sus productos en detrimento de la usabilidad.

Disponible en: http://www.ticbeat.com/seguridad/ransomware-de-las-cosas-2017-informe-eset/ [1]

Links
[1] http://www.ticbeat.com/seguridad/ransomware-de-las-cosas-2017-informe-eset/