

Publicado el 28/10/2014 15:45:35

InnoTec System colabora con el Centro Criptológico Nacional en la contención de ciberataques

El ciberespionaje y el robo de propiedad intelectual principales amenazas



 Me gusta 26  1      2

Valoración

InnoTec System, división de ciberseguridad del Grupo Entelgy, colabora activamente con el CCN-CERT, del Centro Criptológico Nacional (adscrito al Centro Nacional de Inteligencia, CNI) en la detección proactiva, protección y contención de las ciberamenazas sufridas por las **Administraciones Públicas y empresas de interés estratégico para el país** (energéticas, financieras, de seguridad y defensa, telecomunicaciones, farmacéuticas, químicas, etc.). Así, en los nueve primeros meses del año, se ha trabajado sobre más de 10.000 incidentes (frente a los 6.000 detectados en el mismo período del año anterior), de los cuales cerca de 1.200 fueron catalogados con una criticidad de entre muy alto y crítico.

El **Ciberespionaje y el robo de propiedad intelectual** constituyen sin duda una de las principales amenazas detectadas, que buscan particularmente información relevante y/o sensible, con alto valor estratégico, económico o político con fines de lucro o mejora competitiva para el atacante. De hecho, se observa un incremento de la complejidad en los métodos de ataque y desarrollo de malware avanzados, con técnicas de ofuscación que impiden su descubrimiento (gusanos, troyanos o virus personalizados destinados a eludir las medidas de seguridad de una organización y de los antivirus) y dirigidos contra objetivos cada vez más sofisticadamente seleccionados.

La gestión de estos ataques por parte del CCN-CERT se realiza a través de numerosos servicios. La colaboración de InnoTec con el **CERT Gubernamental Nacional** se centra principalmente en el **Servicio de Alerta Temprana (SAT) de internet**, destinado a la detección rápida de incidentes y anomalías con el fin de realizar acciones preventivas, correctivas y de contención. Su principal función, por tanto, es actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance.

Adicionalmente, InnoTec está desarrollando para el CCN-CERT una herramienta ad-hoc denominada **MARTA** (Motor de Análisis Remoto de Troyanos Avanzados) cuya función principal es el análisis automático de malware con el que hacer frente a las nuevas variantes de ataques, así como a las novedosas formas de infección que sufren las organizaciones.

Reducir el tiempo entre la infección y el análisis del código con el fin de evitar su propagación o facilitar más información en investigaciones forenses, son algunas de las ventajas que aportará esta nueva herramienta.