Un 'troyano' muy sofisticado

L. R. - Barcelona - 28/09/2010

Se llama Stuxnet y es un *programa* malicioso del tipo *troyano* muy avanzado, que aprovecha la vulnerabilidad MS10-046 de los sistemas operativos Windows CC, empleados en los sistemas SCADA**.**

Supervisory Control and Data Acquisition (SCADA, por sus siglas en inglés) son programas de producción industrial que se utilizan en las grandes infraestructuras críticas, como las plantas de tratamientos de agua, de control eléctrico o de tráfico, oleoductos y centrales nucleares, entre otras. Su principal fabricante es la compañía alemana Siemens.

"Stuxnet es muy sofisticado porque utiliza técnicas de *rootkit* para instalarse en el sistema operativo. El *troyano,* además, queda camuflado y latente en el equipo infectado hasta que su autor decide activarlo", explica Emilio Castellote, jefe de producto de la empresa de seguridad informática española Panda Software.

Al haber sido detectado en infraestructuras críticas, donde la conexión a Internet suele ser nula o muy restringida, "se cree que el contagio ha sido realizado a través de dispositivos extraíbles, como un lápiz de memoria USB, un disquete o un CD".

Stuxnet -del que todavía no está confirmada su autoría- se detectó por primera vez el pasado mes de junio por VirusBlokAda, empresa de seguridad bielorrusa. A finales de agosto se descubrió la última variación del patógeno informático, de la que ahora ha habido un rebrote.

Este tipo de *troyanos* no van destinados a la infección masiva de ordenadores domésticos. Su objetivo es muy concreto y "personalizado". Castellote no solo considera que es "un claro caso de ciberterrorismo, porque ataca a infraestructuras críticas y es muy sofisticado. También podría ser sabotaje industrial porque el autor del *troyano* puede controlar o modificar de forma remota cualquier parámetro que el programa automatizado controla. Por ejemplo, aumentar o disminuir el caudal de un oleoducto".

Microsoft aseguró en agosto que Stuxnet había infectado a más de 45.000 ordenadores en el mundo. Según la firma de seguridad informática estadounidense Symantec el 60% de las máquinas están alojadas en Irán, el 18% en Indonesia y el 8% en India.