EL MUNDO (ED. CATALUNYA) INNOVADORES 08/01/13
BARCELONA
Prensa: Mensual
Tirada: 20.849 Ejemplares
Difusión: 12.910 Ejemplares
Cód: 65729270
Página: 10
Sección: OTROS Valor: 3.950,00 € Área (cm2): 794,4 Ocupación: 96,11 % Documento: 1/1 Autor: Núm. Lectores: 51640

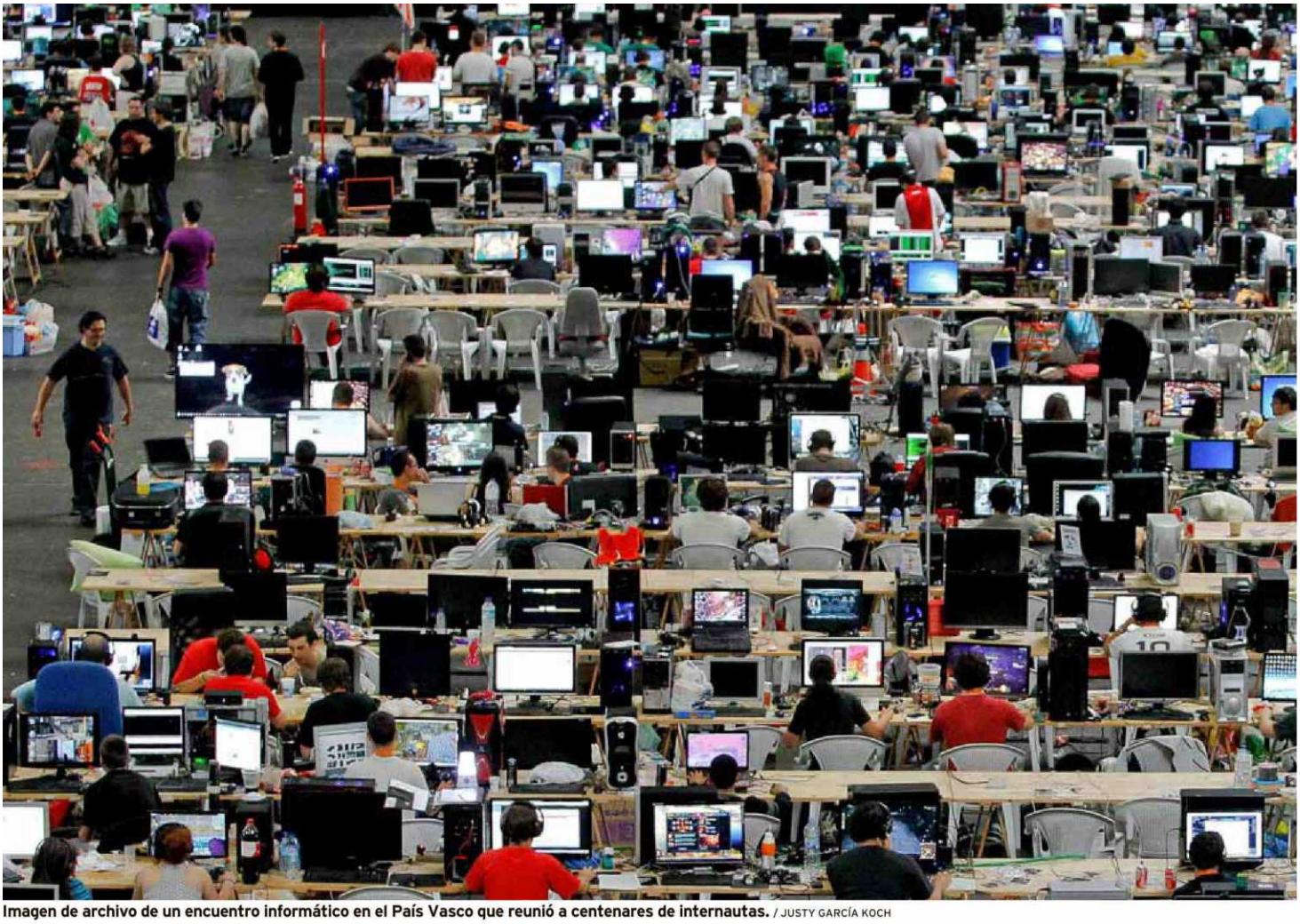

Imagen de archivo de un encuentro informático en el País Vasco que reunió a centenares de internautas. / JUSTY GARCÍA KOCH

Respuesta más rápida y visual al ciberataque

Investigadores de las universidades de Burgos, Salamanca y Politécnica de Valencia desarrollan una herramienta capaz de asegurar respuestas en un espacio determinado de tiempo ante un ataque informático. Por **M. A. Rodríguez**

A medida que avanzan las nuevas tecnologías, fundamentalmente las asociadas a la informática y a internet, también lo hacen los riesgos. Virus, ataques, violación de la intimidad o usurpación de datos desde otro dispositivo... y, en muchas ocasiones, los sistemas de seguridad no son todo lo rápidos que deberían ser para presentar batalla y vencer al atacante.

Por ello, investigadores de tres universidades españolas (Burgos, Salamanca y Politécnica de Valencia) se han unido para desarrollar una herramienta, denominada RT-MOVICAB-IDS, definida como «de ayuda a la detección precoz de ataques informáticos», cuya principal ventaja es «la acotación temporal del proceso de detección de intrusiones mediante la visualización gráfica del tráfico en una red de ordenadores», explican fuentes de las universidades.

Según comenta Álvaro Herrero, responsable del grupo de investigación Gicap de la UBU, la seguridad habitual suele funcionar con un sistema de alarmas que dan el aviso al administrador, las comprueba y clasifica los ataques. «Para facilitar esa labor, desarrollamos este sistema basado en la visualización. En menos tiempo permite una monitorización», apunta.

Con otros sistemas se dan situaciones normales que se pueden clasificar como ataques y a la inversa, por lo que esas formas de detección se basan en reconocer las estrategias. «Todo lo que encuentran similar con cierto grado definido, consiguen pararlo», comenta el investigador de la UBU. Aunque, añade, «hoy día no es posible», ya que uno de los principales problemas es, precisamente, la facilidad para cambiar estas estrategias.

Muestra visualmente los ataques para que el administrador pueda reconocerlos

La herramienta se basa en técnicas de inteligencia artificial para poder generar «un informe visual que permite al administrador de red detectar sencilla y rápidamente un posible ataque». Una vez conocido esto, comenzaría el protocolo de protección del servidor.

El origen de este trabajo conjunto entre las tres universidades están precisamente en la UBU, donde se desarrolló una fase previa entre 2004 y 2009, pero sin una pata fundamental de la nueva herramienta: esa acotación temporal del proceso de detección del virus, ya que permite ofrecer una respuesta dentro de un tiempo máximo.

Los protagonistas del proyecto dicen que «el objetivo de este trabajo de investigación era implementar un sistema que permitiera hacer un análisis de un gran conjunto de información en el menor tiempo posible y ofrecer sus conclusiones de forma gráfica y muy fácilmente comprensible por el personal menos experimentado».

Ataques comunes son, según Álvaro Herrero, un barrido de direcciones o de la base de información para la gestión de la red. «A través de técnicas inteligentes analizamos el tráfico que se produce para prevenir el ataque», pues la prevención es otra de las características del sistema.

Además, la herramienta llega en un momento en el que los ataques informáticos no paran de crecer.

El origen del proyecto está en la UBU, donde se desarrolló una parte entre 2004 y 2009

Según Vicente Julián, investigador del grupo de Tecnología Informática de la Universidad Politécnica de Valencia, «en EEUU, por ejemplo, estos ciberataques se han duplicado desde 2010 y el gasto incurrido por las empresas en respuesta a estos ataques se ha disparado un 40%».

Otra novedad de la herramienta, explica Emilio Corchado, investigador del Departamento de Informática y Automática de la Universidad de Salamanca, es «la posibilidad de orientarla hacia un amplio abanico de aplicaciones, como por ejemplo el análisis de información que fluye en las redes sociales, con gran potencial para predecir situaciones complejas o que conllevan algún tipo de riesgo como aquellas derivadas de revueltas sociales, manifestaciones o aglomeraciones no controladas».

Rizar el rizo sería, ya, que este sistema de detección de datos prácticamente en tiempo real y que monitoriza los ataques y asegura una respuesta rápida, pudiese responder por sí solo a los citados ciberataques. Y en ello están trabajando: en la «ejecución de mecanismos automáticos para la interrupción de los ataques una vez detectados», explica Vicente Julián, de la UPV. «Lo difícil es cómo compararte con otros. Al respecto, lo que hemos conseguido es ver que aun acotando temporalmente el tiempo de respuesta, los resultados son óptimos y podemos prevenir el ataque», sentencia.