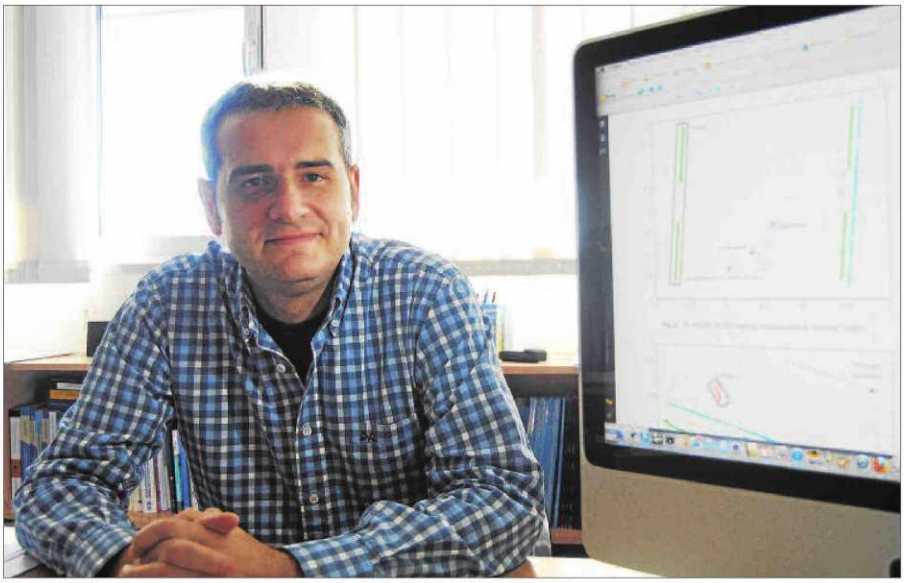
LEVANTE (EMV)
VALENCIA
09/12/12
Prensa: Otra
Tirada: 54.848 Ejemplares
Difusión: 40.035 Ejemplares
Cód: 64589161
Página: 8
Sección: EMPRESAS Valor: 4.418,00 € Área (cm2): 625,7 Ocupación: 62,36 % Documento: 1/1 Autor: Núm. Lectores: 266000

TEXTO
Alba Lúa

TECNOLOGÍA
Prevención
Investigadores valencianos colaboran en la creación de un programa que identifica amenazas en las redes informáticas y las presenta de forma sencilla al usuario y con tiempo necesario para responder al ataque.



Vicente Julián, investigador del grupo de tecnología informática de la UPV. EMV

Usuario prevenido vale por dos en la red

Investigadores de la Politécnica valenciana desarrollan un sistema que advierte de posibles ataques informáticos de forma sencilla y rápida

■ Mejor prevenir que curar. Así pensaron los investigadores de la Universidad Politécnica de Valencia (UPV) quienes, en colaboración con la Universidad de Burgos y la Universidad de Salamanca, han creado una herramienta que facilita a los administradores de las redes informáticas la detección de posibles amenazas, de una forma lo suficientemente rápida para que quede en anecdótico lo que podría haber acabado en ataque.

Hasta ahora, los piratas informáticos podían navegar por la red a sus anchas sin levantar sospechas, ya que su actividad pasaba completamente desapercibida por no saber reconocerla. La idea de los investigadores de estas tres universidades es simplificar esta labor y que sea el propio sistema el que advierta de que algo no va bien. Vicente Julián, investigador del grupo de tecnología informática de Inteligencia Artificial de la UPV, define este programa como «la antesala de un ataque cibernético». La herramienta, denominada RT-MOVICAB-IDS, fija su actividad en reconocer, basándose en experiencias pasadas y en el análisis del flujo de actividad de una determinada red, las anomalías en su uso que puedan resultar posibles amenazas. «Si se está intentando acceder a una información reservada para el administrador de la red, el programa se activa y se pone en alerta», explica Julián.

El método es muy sencillo y apto para los menos avezados en cuestiones informáticas. «El programa proporciona una representación en 2D, en la que aparecen líneas en dos colores», explica el investigador, «habrá un color para el flujo normal y las líneas que se salgan de esta tendencia tendrán diferente color y pendiente. Es muy visual y el usuario lo notará enseguida cuando un comportamiento se salga fuera de lo habitual».

La principal novedad de este proyecto consiste en la acotación del tiempo de análisis y detección de la amenaza. «Si se está produciendo el ataque, un ciberhacker puede hacer caer el sistema en 100 15 minutos», explica Julián. «Este programa presenta un umbral de entre dos y cinco minutos en la localización del problema, lo que da espacio al usuario para buscar formas de defenderse y contrarrestar el ataque». El grupo de investigadores está trabajando en el ajuste del tiempo de detección aunque, según expone Julián, «cuanto menor sea el tiempo de análisis de una posible amenaza, mayor es el margen de error».

Esta iniciativa ha surgido de la suma de las capacidades de dos grupos interdisciplinares. A los estudios en ciberseguridad de las universidades de Burgos y Salamanca, se ha añadido la investigación en inteligencia artificial del grupo de la politécnica valenciana. Los investigadores burgaleses ya habían desarrollado un proyecto similar, a partir del que plantearon la posibilidad de hacer este programa híbrido en cuanto a tecnologías. Los miles de usuarios que acceden a la red hacen imposible el rastreo particular de cada uno, por lo que la utilización de la inteligencia artificial para manejar los grandes volúmenes de información y para poder clasificarlos según patrones resulta un factor clave para el proyecto. «En principio esto es un prototipo totalmente funcional y debería adaptarse en concreto a las características de una determinada empresa», cuenta Julián y explica que, aunque el programa es el resultado de una investigación básica, podría llegar a trasladarse a la industria.

Tecnología

LEVANTE-EMV

NUEVAS VERSIONES CADA VEZ MÁS INDEPENDIENTES

▶ El proyecto RT-MOVICAB-IDS es la primera fase de la investigación para la identificación de amenazas y prevención de ataques en las redes informáticas. Actualmente, este modelo sólo advierte al administrador en el caso de que éste se encuentre monitorizando el sistema constantemente, por lo que no sería efectivo en el caso de que estuviera ausente en el momento de la detección de la amenaza. Por ese motivo, el grupo de investigadores está desarrollando una ampliación del programa que tome algunas decisiones de forma automática para la interrupción de los ataques que sean detectados y hacer que así, la presencia del administrador fuera prescindible.

«El programa presenta un gráfico con líneas de dos colores, unas para el flujo normal y otras para las anomalías, lo que permite detectarlas rápidamente»