Por: Yureli Cacho Carranza,
Petroquimex.

La Conectividad Informática Representa un Factor de Riesgo para el Sector Industrial

Los ciber-ataques pueden poner en riesgo infraestructura crítica, ocasionar pérdida de producción y un quebranto económico considerable. De ahí la importancia de contrarrestarlos

Kaspersky Lab es una compañía global de origen ruso, dedicada a la ciberseguridad con más de 20 años de trayectoria a la que todavía algunos identifican como una firma antivirus solamente. Sin embargo, dado el constante avance tecnológico, hace tiempo que su co-fundador y director general Yevgueni Valentínovich Kasperski, más conocido como Eugene Kaspersky, decidió invertir en investigación y desarrollo de tecnología de vanguardia, a fin de ofrecer soluciones de seguridad y servicios muy especializados, capaces de combatir amenazas digitales avanzadas, las cuales además están en permanente evolución; proporcionando no sólo innovaciones técnicas, sino estrategias que protejan las terminales e infraestructura crítica o crucial de gobiernos y empresas.

El investigador senior de Seguridad Roberto Martínez, forma parte del equipo global de investigadores (GreAT por sus siglas en inglés) de Kaspersky Lab en Latinoamérica y, junto con otros colegas de Brasil, Colombia, Argentina y su director en Miami; analiza e investiga nuevas amenazas, dado que desde hace varios años existen ciber ataques muy enfocados al sector industrial y sobre todo a su infraestructura física.

Cómo empezó el problema

El gusano informático *Stuxnet* fue considerado la primera ciber arma de la era moderna, un código o programa malicioso —*malware*— que infectó sistemas industriales basados en la aplicación para la Supervisión, Control y Adquisición de Datos o Scada de Siemens Simatic WinCC/PCS 7, cuyo impacto en Medio Oriente fue bastante considerable al provocar daños en las centrifugadoras nucleares de Irán en 2010 y destruir más de mil máquinas. “Hasta entonces, nadie se había imaginado lo que podría pasar si algún virus o *malware* dañara sistemas industriales, y a partir de entonces comenzaron a propagarse una serie de incidentes, donde el blanco se dirigió, de las computadoras personales a complejos siste-

EXPO Oil&Gas México 2019

Onshore&Offshore Conference

1era Edición

26 - 28 Marzo 2019

Centro de Convenciones Tabasco 2000, Villahermosa Tabasco

Con un modelo diferente e innovador

MESAS DE NEGOCIOS

Adquiera conocimiento relevante sobre el sector de energía en México y sus nuevas áreas de oportunidad

Evento organizado por:

Oil & Gas ALLIANCE

VINCULACIONES QUE GENERAN NUEVOS NEGOCIOS

Medio oficial y coordinador

Petroleo & energia

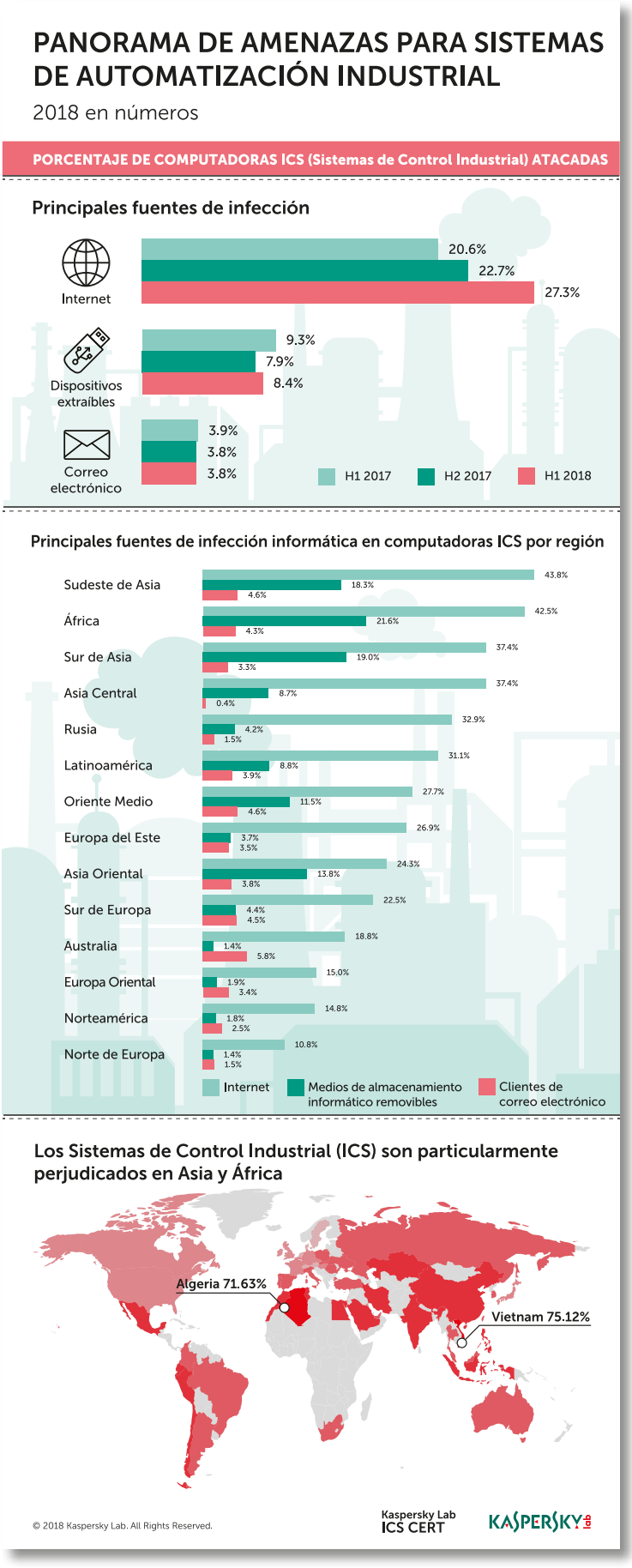
INFORMACIÓN:

Julio César

Director Comercial
Oil & Gas Alliance
+52 1 (55) 6374 2292
j.cortes@oilandgasalliance.com

/oilandgasalliance

www.expoilandgasmx.com



mas industriales. Situación que se ha ido incrementando", según relata Roberto Martínez.

En ese sentido, esta compañía ha logrado identificar campañas de ataques muy dirigidos al sector industrial, que comprenden incidentes relacionados con ciber-espionaje y el acceso a la información de equipos o de personas clave en diferentes organizaciones, así como sabotajes a sistemas industriales, similares incluso al del ataque informático *BlackEnergy* que en diciembre de 2015 afectó los sistemas de energía eléctrica de Ucrania.

Medidas de Kaspersky Lab para hacer frente a este tipo de sucesos

Roberto Martínez señala que la empresa desarrolla herramientas como Kaspersky Industrial Cybersecurity para proveer de seguridad y protección a sistemas industriales; dado que las diferentes industrias, por ejemplo, la eléctrica o petrolera, tienen áreas en donde por un lado se maneja la parte operativa y por otro, la de producción. Por lo tanto, existen características muy particulares que requieren soluciones específicas para asegurar los sistemas y evitar la presencia de virus o de actividades sospechosas en su red.

Kaspersky Lab no ofrece solamente un programa informático como tal para que sólo se instale. En el caso de Kaspersky Industrial Cybersecurity se trata de un conjunto de tecnologías y servicios diseñados para proteger las capas y los elementos verdaderamente industriales de una organización que, acompañado de una estrategia de ciberseguridad, cualquier organización o empresa, sea privada o de gobierno, por ejemplo la Comisión Federal de Electricidad o Petróleos Mexicanos, logren estar protegidas ante posibles ataques; puesto que son infraestructuras críticas e importantes para el país y, por ende, susceptibles de ser atacadas. De manera que, se desarrollan diver-

La supervisión y las respuestas oportunas a incidentes en redes industriales, deben ser una prioridad esencial de las áreas de TI

sas estrategias y ello incluye el reconocimiento del tipo de amenazas, análisis sobre la forma en la que han sucedido los ataques, estudio de los factores que los atacantes aprovechan, es decir las vulnerabilidades que explotan y cómo es que logran tener acceso. Con base en esos y otros parámetros, se genera una solución para cada caso en particular, haciendo uso de las tecnologías desarrolladas por Kaspersky Lab; manifestó el entrevistado.

Resultados de algunos estudios desarrollados por Kaspersky Lab en 2018

Información proporcionada por la compañía refiere que, en organizaciones industriales como centrales eléctricas; la digitalización y la conectividad están propiciando que se recurra al internet de las cosas (IoT, por sus siglas en inglés) porque para mejor desempeño de las operaciones, los sistemas de control industrial (ICS, también por sus siglas en inglés) son una buena alternativa. No obstante, dicha tendencia también implica riesgos de ciberseguridad y 65 por ciento de las empresas considera que la afectación a sus sistemas de control es más probable si se utiliza el internet de las cosas. Mientras que más del 77 por ciento estima que su organización podría convertirse en blanco de un incidente de ciberseguridad y 48 por ciento admite carecer de medidas para detectar o vigilar ataques relacionados con sus redes de control industrial, los cuales podrían llevar a circunstancias catastróficas, así como ocasionar grave perjuicio a los productos, pérdida de producción y por ende de oportunidades comerciales.

La eficiencia de la automatización contra la preocupación por la ciberseguridad

Los administradores de las tecnologías de la información (TI) que trabajan en las empresas, pueden desconocer los incidentes que ocurren dentro de los sistemas de control industrial, debido a que no tienen un enfoque unificado con relación a la ciberseguridad general de la organización. En el transcurso de 12 meses, casi dos tercios, 64 por ciento, de las compañías encuestadas por Kaspersky Lab experimentó al menos un ataque convencional de *malware* o virus en sus ICS. Mientras que 30 por ciento sufrió un ataque de *ransomware*, un programa dañino que restringe el acceso a sistemas operativos.

Cada seis meses, alrededor de 40% de las computadoras con sistemas de control industrial (ICS) enfrentan ataques, aumentando riesgos significativos en las organizaciones

Los ataques dirigidos representaron 16 por ciento en 2018, pero en 2017 fueron del 36 por ciento. Se infiere que las compañías que dependen de sistemas de control industrial son víctimas, sobre todo de amenazas convencionales como *malware*, *ransomware* y ataques dirigidos.

Por lo anterior, el desafío de la ciberseguridad resulta primordial para mantener los sistemas críticos en funcionamiento y a las empresas operando. Es preciso que las industrias mejoren sus políticas de seguridad cibernética e incluyan medidas que salvaguarden sus redes de control como la actualización de programas de respuesta a incidentes. Ante ello, sólo 15 por ciento de las organizaciones industriales usan soluciones en la nube computacional (la cual almacena y administra datos) para los sistemas de control Scada y la gestión de la infraestructura crítica.

El sector industrial no debe soslayar, el que las medidas de ciberseguridad tienen que ir de la mano con la adopción de nuevas tecnologías, cualquiera que éstas sean, con el propósito de que las recompensas o beneficios de la digitalización superen sus riesgos y se eviten daños operacionales graves, financieros y hasta de reputación. Para ello es preciso recurrir a soluciones experimentadas en ciberseguridad capaces de administrar la complejidad de los ecosistemas industriales conectados y distribuidos.

Escasez de personal, falta de inversiones y errores humanos; factores que ponen en riesgo la seguridad industrial

Cada seis meses, alrededor de 40 por ciento de las computadoras con Sistemas de Control Industrial (ICS) enfrenta ataques y esta brecha de ciberseguridad en una infraestructura

crítica puede aumentar los riesgos para las organizaciones, de manera significativa.

Conforme a la encuesta *Estado de la Ciberseguridad Industrial 2018*[1] realizada por Kaspersky Lab, empresas industriales y de energía tienen distintas opiniones sobre los efectos negativos que los ataques cibernéticos ocasionan en sus redes industriales. Sin embargo, cuando se trata de los problemas que afectan su capacidad para mantener las redes seguras, empresas de diferentes giros comparten tres preocupaciones: falta de personal, de inversiones, así como del factor humano.

1 Informe original: *The State of Industrial Cybersecurity 2018*: https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/

Mayor información sobre el Panorama de amenazas para la automatización industrial en sistemas H2 2017: https://ics-cert.kaspersky.com/media/KL_ICS_REPORT_H2-2017_FINAL_EN_22032018.pdf
https://ics-cert.kaspersky.com/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/

Un 73 por ciento de las empresas de energía afirmó que la mayor preocupación es comprometer la calidad de la producción por causa de un ciberataque. Empero, sólo 52 por ciento cuenta con medidas de respuesta específicas para lidiar con incidentes de esta índole, a pesar de la frecuencia y del impacto que generan los ataques a la red de sistemas de control industrial. Las organizaciones industriales, especialmente aquellas que tienen procesos tecnológicos complejos, necesitan trabajadores altamente especializados y calificados para poder cerrar esta brecha. En el sector de la energía, donde la infraestructura crítica nacional se maneja con la ayuda de sistemas de control industrial, el principal desafío en la administración de seguridad es contratar personal que cuente con las habilidades pertinentes, ya que la tarea de proteger las redes industriales, a menudo recae en los responsables de la seguridad de la información corporativa.

Una forma de prevenir o de disminuir el efecto de un ataque cibernético es la implementación de medidas y de procedimientos de seguridad sólidos para las redes de Sistemas de Control Industrial. La supervisión y las respuestas oportunas a los incidentes en las redes industriales deben convertirse en prioridades esenciales de seguridad para las áreas o departamentos de Tecnologías de la Información, al igual que la capacitación al personal de manera paralela. Esto minimizará el potencial conflicto que pudieran tener los negocios.

Ataques dirigidos como los *Triton* e *Industroyer* explotan la vulnerabilidad y pueden provocar desde filtraciones de datos, hasta la falla o una interrupción completa de los procesos de producción. Para evitarlo se requiere una combinación de medidas técnicas y administrativas, que incluye la implementación de sistemas especializados de defensa cibernética para todos los niveles de la infraestructura industrial.

SVF
MÉXICO

SOLUCIONES INTEGRALES

Somos una empresa con proyección y estructura a nivel latinoamericano y el Caribe. Nuestro objetivo es representar y distribuir marcas de prestigio internacional, generando soluciones integrales a nuestros clientes en diversos sectores como: Oli & Gas, industrial, construcción, marino, generación eléctrica y maquinaria. Es por esto que contamos con talleres especializados y un equipo humano altamente calificado, apasionado por el trabajo.

mtu Chicago Pneumatic DETROIT DIESEL CORPORATION SCANIA LIEBHERR WACKER NEUSON

Nos encontramos en Coatzacoalcos, Ver. Villahermosa,Tab. Mérida, Yuc. CDMX y Cancún, Qroo. Tel: +52 1 921 214 05 00
Lada sin costo: 01 800 000 27 28 Email: info@gruposvf.com Web: www.svfmexico.com