WWW.CONECTRONICA.COM OCTUBRE 2021 Nº 245

conectrónica

tecnología y elementos de conexión y conectividad

ACTUALIDAD
Empresas, acuerdos, investigación y desarrollo. Informes...

EVENTOS
Se abre el registro de visitantes para ISE 2022

CIBERSEGURIDAD
Dualidad del malware inteligente avanzado (ofensivo y defensivo), puntos de actuación y operativa de expansión transparente

REDES DE ACCESO ABIERTO
Redes de Acceso Abierto - Economía colaborativa y telecomunicaciones

CASO DE ÉXITO
Switches de alto rendimiento para la red 10 Gigabit del Clúster de Química Computacional de la Universitat de Barcelona

CENTROS DE DATOS
Baterías para centros de datos sostenibles de Microsoft

PRODUCTOS

Tecnología y elementos de conexión y conectividad

Número 245
OCTUBRE 2021
Depósito Legal:
M-27337/96
ISSN 1136-7539

Redacción, Suscripciones y Publicidad:
C/ Poema Sinfónico, 25-27,
Escalera 2, 1°, 5B
28054 Madrid
Tel.: +34 91 706 56 69

e-mail:
redaccion@conectronica.com
www.conectronica.com

Edita:
GM2 Publicaciones Técnicas, S.L.

Dirección:
Carlos Martínez

Diseño:
Carlos Montoro

Precio del ejemplar:
10 euros + IVA
Suscripción:
60 euros + IVA

suscripciones@conectronica.com

síganos en

SUMARIO

conectrónica

ACTUALIDAD 4
Empresas, acuerdos, investigación y desarrollo. Informes...

EVENTOS 12
Se abre el registro de visitantes para ISE 2022

CIBERSEGURIDAD 16
Dualidad del malware inteligente avanzado (ofensivo y defensivo), puntos de actuación y operativa de expansión transparente

REDES DE ACCESO ABIERTO 28
Redes de Acceso Abierto - Economía colaborativa y telecomunicaciones

CASO DE ÉXITO 30
Switches de alto rendimiento para la red 10 Gigabit del Clúster de Química Computacional de la Universitat de Barcelona

CENTROS DE DATOS 34
Baterías para centros de datos sostenibles de Microsoft

PRODUCTOS 38

#245

EET lanza Lanview

Con la intención de expandir su negocio en el área de soluciones de red profesionales, EET España lanza su nueva marca Lanview. Lanview nace como una marca especializada en infraestructura de cable. En su catálogo se puede encontrar desde cableado estructurado, redes de fibra, gabinetes y armarios rack para servidores, hasta distribución de energía relacionada.

"Estamos entusiasmados con el lanzamiento de Lanview y esperamos ofrecer un valor mejorado a nuestros clientes. Para EET, este es un paso importante hacia el desarrollo y la ampliación de nuestro negocio, ya que Lanview une nuestras áreas de negocio y fortalece nuestra posición como el distribuidor IT de valor añadido líder en Europa". afirma Sonia Marcos, Managing Director de EET España.

Entre los productos más destacados, se puede encontrar el cableado estructurado. Lanview suministra soluciones de cableado de cobre desde Cat5e (ancho de banda de 100MHz) hasta Cat7a para anchos de banda de 1200MHz, tanto para aplicaciones interiores como exteriores. También cuenta con una amplia gama de soluciones de fibra óptica disponibles en todas las versiones estandarizadas de fibra (monomodo y multimodo), conectores y acopladores.

Lanview ofrece también una gama completa de racks y armarios murales, de alta calidad y diseñados para empresas, centros de datos, centros de control de seguridad y todo tipo de aplicaciones diarias de cableado. Y finalmente, la empresa tiene una amplia variedad de unidades de distribución de energía (PDU). Las PDU están disponibles para una gran variedad de tamaños y tipos de enchufe.

CoComm firma un acuerdo estratégico con la operadora mexicana EXiS

CoComm ha firmado una nueva colaboración en México junto a EXiS, un operador móvil virtual (OMV) que ofrece soluciones de conectividad flexibles. Esta alianza estratégica nace con el objetivo de derribar la brecha digital en zonas rurales y acelerar la digitalización empresarial en México, a través de un modelo de conectividad móvil, flexible y escalable.

En virtud del acuerdo, Exis Telecom comercializará en México los teléfonos de Cocomm, que se caracterizan por combinar prestaciones de la telefonía móvil y fija gracias a incorporar tarjeta SIM. De este modo, se proporciona conexión de voz y datos de alta calidad a través de la red de antenas de telefonía móvil, sin depender de instalaciones de fibra, y con dispositivos compatibles con 2G, 3G, y 4G.

La escalabilidad y flexibilidad de este modelo ayudará a las empresas mexicanas a mejorar su productividad y adaptarse a las nuevas necesidades de movilidad sin hacer grandes inversiones. Los teléfonos operan en entornos seguros y adaptados al teletrabajo, ya que permiten trasladar a cualquier lugar todas las funcionalidades de la oficina: videollamadas, acceso al software de la empresa, etc.

Además, los dispositivos de CoComm y la infraestructura de de EXiS Telecom conforman un proyecto que mejorará el acceso a voz y datos incluso en aquellas zonas rurales donde aún no hay despliegue de fibra. Casi 30 millones de personas en México no tienen acceso a Internet, según la encuesta del INEGI, Instituto Nacional de Estadística y Geografía de México.

Otro de los principales focos del acuerdo es dotar a las empresas de las herramientas necesarias para impulsar su digitalización empresarial como clave de competitividad para el país.

Exis Telecom opera bajo la red de Altan y utiliza la plataforma integral proporcionada por el Habilitador de Redes Móviles Virtuales (HRMV) mexicano VADSA (Valor Agregado Digital, S.A. de C.V.). Gracias a las infraestructuras del operador, la tecnología de CoComm garantizará la conectividad de empresas y empleados desde cualquier ubicación, sin costes de cableado, de forma flexible y escalable.

Previsiones de mercado de fibra óptica actualizadas para 2021-2026

En la Conferencia virtual FTTH 2021, el FTTH Council Europe ha dado a conocer dos informes: las últimas cifras de las Previsiones FTTH para 2021 y 2026 y una visión general de los despliegues de fibra en las zonas rurales.

Previsiones de FTTH para 2021 y 2026
Las previsiones de mercado abarcan 39 países y ofrecen un análisis individual de 15 países.

Las cifras son coherentes con las estimaciones anteriores y prevén unos 197 millones de hogares cableados a FTTH/B en 2026 en la UE27+Reino Unido, frente a los 118 millones de este año, siendo Alemania, Reino Unido, Países Bajos e Italia los que experimentarán un crecimiento más notable.

Según las previsiones, el número de abonados alcanzaría los 135 millones en 2026 en la UE27+K y los 197 millones en la UE39. Nuestras estimaciones también muestran que en 2026, la tasa de adopción de FTTH/B3 para EU27+UK será ligeramente superior (68,7%) a la de EU39 (65,3%), experimentando ambas una evolución constante a lo largo de los años.

Varios factores han contribuido a fomentar el despliegue de redes. La crisis de Covid provocó un aumento del tráfico de datos y de la demanda, lo que ha hecho que los inversores privados impulsen considerablemente sus proyectos de despliegue en favor de la FTTH/B para soportar el continuo aumento del tráfico. Además, la puesta en marcha de programas nacionales (infraestructuras y digitalización) y los nuevos objetivos digitales europeos para 2025 y 2030 conducirán a la aceleración de la conectividad de fibra completa en todos los países europeos.

"Esta tendencia se verá intensificada por los nuevos patrones de uso que están animando a los operadores a migrar a soluciones FTTH, capaces de ofrecer nuevos servicios al mismo tiempo que contribuyen al reto de la sostenibilidad", dijo Vincent Garnier, Director General del FTTH Council Europe.

"El informe muestra que todavía hay un enorme potencial de crecimiento en términos de conectividad en muchos países de la UE, pero el despliegue general está avanzando a un ritmo rápido. Sin embargo, incluso con la infraestructura instalada, el FTTH Council Europe considera que aún queda un largo camino por recorrer para alcanzar una sociedad totalmente digitalizada. Creemos firmemente que para abrazar la próxima década digital y dar forma a la transformación digital de Europa para 2030, la asimilación es el próximo reto, y pedimos a los responsables políticos que tomen las medidas necesarias para que los usuarios finales se beneficien del mundo de nuevas posibilidades que ofrece la conectividad de fibra completa."

Despliegues de fibra en zonas rurales
Por primera vez, el FTTH Council Europe también ha lanzado este año el primer informe oficial sobre la fibra total en las zonas rurales de Europa, que ofrece una visión general de los objetivos, las acciones y los resultados de los despliegues de FTTH en las zonas rurales en una selección de 10 países de la UE4. Mientras que más de dos tercios de los hogares rurales disponen actualmente de un acceso NGA5, la cobertura de FTTH/B sigue estando rezagada en las zonas no densas, con sólo un 22% de hogares cubiertos, frente al 45% de todos los territorios de la UE27+Reino Unido.

La FTTH/B se despliega progresivamente, pero a un ritmo muy diferente entre los países estudiados. Mientras que España encabeza la clasificación con un 60,5 % de cobertura rural de FTTH/B en 2020, a Alemania le queda un largo camino por recorrer, con sólo un 9,8 % de cobertura. Sin embargo, cabe destacar que esto representa una proporción mayor de hogares rurales que la media de la UE e indica un despliegue más equilibrado en las zonas rurales y urbanas de Alemania.

"El FTTH Council Europe cree que las zonas rurales deberían beneficiarse de los mismos servicios que las urbanas y, por tanto, los fondos públicos deberían ayudar a reducir esta brecha digital allí donde la financiación privada no es posible debido a la falta de argumentos comerciales. Sin embargo, para aprovechar al máximo el dinero público, sólo los proyectos de fibra completa deberían poder recibir financiación, ya que se trata de la infraestructura más segura para el futuro y más respetuosa con el medio ambiente", indicó Eric Festraets, Presidente del Consejo Europeo de FTTH.

Estefanía Valencia Artiga nombrada Responsable de Riesgo Tecnológico y Cumplimiento Regulatorio en Fujitsu

Estefanía Valencia ha sido nombrada por Fujitsu como responsable de Riesgo Tecnológico y Cumplimiento Regulatorio en el uso de las Tecnologías de Ciberseguridad para España. Su incorporación es clave para liderar el negocio de la seguridad de la multinacional nipona, y supondrá un impulso de esta área, clave en el mundo de la transformación digital en nuestro país.

Estefanía Valencia aporta una gran experiencia de más de 10 años, derivada de una larga trayectoria en el mercado de consultoría en seguridad a grandes clientes, así como a medianas y pequeñas empresas de todo tipo de sector de actividad, habiendo pertenecido y liderado equipos en EY, GMV, Áudea y Experis IT.

Es Máster en Derecho Empresarial por la Universidad Autónoma de Madrid. Y cuenta con las mejores certificaciones del mercado como CDPSE, CISM, Lead Auditor ISO 27001 e ITIL Foundations v.3. Asimismo, recientemente participó en la 1ª edición del Curso Superior en Dirección de Seguridad Digital y Gestión de Crisis Corporativa impartido por AESYC-Universidad de Alcalá de Henares.

Ha liderado múltiples proyectos a nivel nacional e internacional, entre los que se destaca el Proyecto de Adecuación al Reglamento Europeo de Protección de Datos en una Entidad del Sector Asegurador con matriz en España; el Servicio de Asesoramiento Técnico para la adecuación a la Normativa de Seguridad de la Información en la misma Entidad; la creación e implantación del Modelo de Gestión de Ciberriesgos en Entidades del Sector Financiero, así como el self-assessment del marco de control de Entidades Financieras (SCIIF,SWIFT, TARGET2, PCI-DSS, GDPR, ICT Risk EBA, NIST, ISO27001, etc.).

NFON se incorpora a ASOTEM

NFON Iberia, una entidad de NFON AG se ha incorporado a ASOTEM en España. ASOTEM es una asociación de operadores cuyo objetivo es promover los servicios de telecomunicaciones especializados en el mercado corporativo.

La asociación está formada en la actualidad por 16 operadores y busca promover objetivos comunes de los operadores de telecomunicaciones integrados en ASOTEM, como asuntos regulatorios y de competencia, la reducción de los costes operativos, la puesta en marcha de proyectos de innovación, así como el aumento de su presencia internacional, con el fin de obtener una mayor eficiencia y visibilidad.

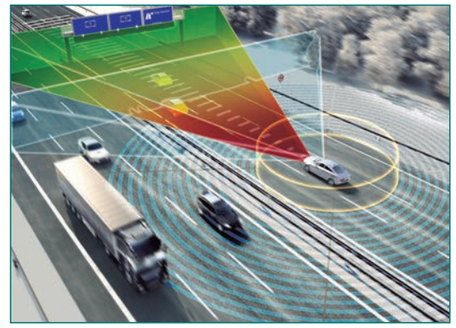
"A nivel de empresa, es muy emocionante unirse a ASOTEM. Creo que es muy necesario dar una vuelta a todo el marco regulatorio de las telecomunicaciones y adaptarlo, por ejemplo, a la aparición de nuevos servicios de comunicaciones desde la nube", explica David Tajuelo, director general de NFON Iberia.

HUBER+SUHNER se convierte en proveedor de antenas de radar

HUBER+SUHNER suministra antenas de radar de producción en serie a Continental, uno de los mayores proveedores de nivel 1 de la industria del automóvil. El alcance del suministro incluye antenas que aportan una contribución fundamental a las aplicaciones de radar de próxima generación.

La conducción automatizada se considera una de las formas de movilidad con mayor potencial para el futuro. HUBER+SUHNER iniciará la producción en serie de antenas de radar para Continental, uno de los principales fabricantes mundiales de sistemas de asistencia al conductor. Este paso representa un gran avance para la empresa en la implementación de sus objetivos estratégicos de crecimiento en el sector del automóvil, especialmente en el uso de la tecnología de antenas 3D y, por tanto, en el campo de la conducción automatizada.

Las actuales aplicaciones de radar en el vehículo sólo proporcionan información limitada, que ya no satisface los futuros requisitos de la conducción automatizada. Los sistemas de asistencia al conductor de la próxima generación deben ser capaces de manejar situaciones complejas. Para ello es necesario disponer de



información completa, como la ubicación de un objeto, su dirección, su altura y su velocidad. La tecnología de antenas de HUBER+SUHNER desempeña un papel fundamental a la hora de proporcionar una imagen más precisa de la situación del tráfico a una distancia de hasta 300 metros e incluso en condiciones meteorológicas y de visibilidad deficientes.

La cooperación acordada con la unidad de negocio de Sistemas Avanzados de Asistencia al Conductor, Continental, se extiende durante ocho años. El inicio de la producción en serie y la entrega de las antenas está previsto para este año. En consecuencia, desde el inicio del desarrollo en 2018, se han realizado considerables inversiones iniciales para crear capacidades de desarrollo y, con vistas al inicio de la producción en serie, se han realizado elevadas inversiones en equipos de producción.

Keysight se une a la Google Cloud Partner Initiative

Keysight Technologies, Inc ha anunciado que se ha unido a la Google Cloud's partner initiative para dar soporte a la orquestación ágil de servicios innovadores 5G en el extremo de la red.

Un número creciente de operadores móviles están aprovechando la computación en la nube y en el extremo de la red para ofrecer conectividad de alta velocidad, baja latencia, y segura en el extremo de la red a la vez que optimizan la eficiencia operativa. Keysight se ha unido a la iniciativa de colaboradores de Google Cloud para habilitar un ecosistema 5G centrado en la nube que conecta una infraestructura basada en software desde el extremo de la red de acceso radio (RAN) hasta el núcleo.

Los proveedores de telecomunicaciones están migrando sus operaciones de red y de aplicaciones hacia soluciones nativas en la nube basadas en contenedores. Los despliegues 5G en modo standalone (SA) utilizando hardware comercial disponible (COTS) con interfaces de estándar abierto están acelerando la virtualización de arquitecturas RAN y de tecnología de fraccionado de red (network slicing). Esta transformación digital está facilitando la innovación

en el extremo de la red con procesado de datos en tiempo real más cerca de donde los datos son recopilados y consumidos.

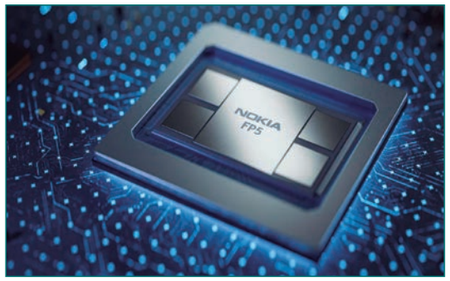
Keysight ofrece un amplio rango de soluciones para la validación temprana de diseños, de interoperabilidad de sistemas y de prestaciones, de seguridad de red y de punto de acceso, así como de cumplimiento con las especificaciones del 3GPP y de O-RAN. El porfolio de soluciones Keysight de extremo a extremo, construido con plataformas hardware y software comunes, facilita que un ecosistema centrado en la nube acelere el despliegue de tecnologías de computación multiacceso en el extremo de la red (MEC), de virtualización de funciones de red (NFV) y de inteligencia artificial (AI). Esto permite a los operadores móviles orquestar con confianza servicios innovadores de conectividad inalámbrica en el extremo de la red.

Nokia lanza el silicio de enrutamiento de quinta generación

Nokia ha anunciado el lanzamiento de FP5, su quinta generación de silicio de enrutamiento IP de alto rendimiento. Como nuevo eje de las plataformas de enrutamiento de servicios IP de Nokia, FP5 permitirá a los proveedores de servicios atender el imparable crecimiento de los requisitos para escalar la capacidad de redes, posibilitar nuevos servicios IP de velocidad superior y proporcionar una protección incomparable frente a las crecientes amenazas a la seguridad de las redes.

Partiendo de cuatro generaciones de procesadores de red líderes del sector, Nokia sube el listón al añadir compatibilidad con las interfaces de enrutamiento 800GE de alta densidad, una reducción del 75 % en el consumo energético y nuevas prestaciones de cifrado integradas a velocidad de línea basadas en flujo.

En un momento en el que las arquitecturas de nube, el 5G e Industria 4.0 continúan impulsando la transformación de las redes, los proveedores de servicios necesitan que las redes IP para tareas críticas sean cada vez más seguras, ágiles y sostenibles. Las redes IP deben garantizar el alto rendimiento y la integridad para responder al crecimiento de las amenazas procedentes de ataques a nivel de red y de infracciones de seguridad. También deben ser capaces de adaptarse a cambios imprevistos y de atender la evolución de servicios durante toda la vida útil de la red. Asimismo, el equipamiento de red IP debe tener un consumo cada vez más eficiente para minimizar su impacto ambiental.



Con la introducción del silicio de procesamiento de redes de quinta generación FP5, Nokia brinda una nueva gama de soluciones de enrutamiento IP que ayuda a los proveedores de servicios a atender estos requisitos nuevos y cambiantes mediante la transformación de las redes IP para tareas críticas.

Nokia lleva mucho tiempo a la vanguardia como proveedor de seguridad integrada para redes IP. Con FP4, la empresa transformó la defensa de DDoS volumétrica con detección y mitigación basada en routers. FP5 proporciona una capa adicional de protección de la red con la introducción de «ANYsec», una nueva capacidad de cifrado a velocidad de línea basada en flujo que se integra directamente en el chipset. ANYsec admite la prestación de servicios IP seguros, incluidos MPLS y enrutamiento de segmentos, bajo demanda y a escala, sin que se vean afectados el rendimiento o la eficiencia energética. Los proveedores de servicios pueden garantizar la integridad y la confidencialidad de todos los datos que fluyen a través de sus redes.

Con FP5, Nokia lleva al mercado un salto generacional en la capacidad de red de los enrutadores. Las plataformas de routers de servicios de Nokia son las primeras en admitir 800GE de alta densidad e interfaces de enrutamiento de canal libre de 1,6 Tb/s para diversas aplicaciones, como transporte móvil, núcleo IP, peering, BNG y edge de proveedor. Las nuevas tarjetas de línea basadas en FP5 admitirán 14,4 Tb/s (19,2 Tb/s con la capacidad de agregación inteligente de Nokia.) Una nueva serie de plataformas 7750 Service Router-1 con factor de forma fijo permite que las ventajas de FP5 también lleguen a ubicaciones de red pequeñas.

Los procesadores de red FP5 de Nokia reducen el consumo de energía por bit en un 75 %. Puesto que FP5 ofrece compatibilidad retroactiva con FP4 y está totalmente integrado en las versiones más recientes de Service Router Operating System (SR OS) de Nokia, todas las características existentes se admiten desde el primer día en el nuevo hardware. A través de esta estrategia de evolución alineada de hardware y software, Nokia proporciona a sus clientes una protección de la inversión incomparable y sostenible.

Como procesador de red plenamente programable, FP5 brinda la agilidad necesaria para actualizar la red conforme cambien los estándares y las aplicaciones. Su rendimiento determinista, combinado con conocimientos completos de telemetría, garantiza que los operadores de redes puedan ofrecer una red IP apta para mantenimiento y servicio tanto ahora como en el futuro. Las plataformas basadas en FP5 de Nokia estarán disponibles a partir de la primera mitad de 2022.

Phoenix Contact S.A.U. certificada por el TÜV SUD conforme a IEC 62443 2-4

La IEC 62443 es una serie de normas internacionales sobre ciberseguridad para sistemas de control industrial y redes informáticas en entornos de operación. La norma está dividida en diferentes secciones y describe tanto los aspectos técnicos como los relacionados con los procesos de la ciberseguridad industrial.

Divide a la industria en diferentes roles: el operador, los integradores (proveedores de servicios de integración y mantenimiento) y los fabricantes. Cada uno de estos roles sigue un enfoque basado en el riesgo para prevenir y gestionar los riesgos de seguridad en sus actividades.

Phoenix Contact está certificada en su rol de fabricante de equipos y, en algunas filiales, también en su rol de integrador.

Desde finales del pasado mes de junio, Phoenix Contact España está certificada según la IEC 62443-2-4, lo que permite ofrecer a nuestros clientes unos servicios de ciberseguridad de mayor garantía y calidad a los operadores durante la integración o el mantenimiento de las soluciones de automatización. La subsidiaria española de Phoenix Contact se convierte así en el único fabricante industrial de nuestro país con esta certificación a nivel local.

Nokia lanza el software Charging Configurator para permitir la monetización del 5G en tiempo real para los CSP

Nokia ha anunciado hoy un microservicio configurador de carga para su actual solución de monetización Nokia Converged Charging (NCC), que permite a los Proveedores de Servicios de Comunicaciones (CSP) crear nuevas lógicas de carga y ofertas de servicios y avanzar más rápido en el mercado al configurar nuevos e innovadores servicios 5G.

La solución de tarificación mejorada de Nokia, la primera de su clase, utiliza una interfaz de usuario empresarial intuitiva con funcionalidad de arrastrar y soltar y declaraciones en lenguaje natural para crear nuevas ofertas de precios y de mercado, sin necesidad de ninguna codificación.

Con reglas de tarificación preintegradas y flexibles, la solución NCC mejorada permite a los CSPs mantenerse al día con las necesidades cambiantes de los clientes para monetizar cualquier servicio que pueda ser medido, como las porciones de red y las ofertas de IoT para empresas y consumidores, lo que a su vez desbloquea nuevas fuentes de ingresos para los operadores.

Aprovechando los microservicios en contenedores nativos de la nube, NCC soporta la carga de ultra baja latencia y alta frecuencia. NCC es totalmente compatible con el 3GPP y aprovecha los estándares del sector, incluidas las API abiertas del TM Forum, para minimizar el tiempo necesario para incorporar nuevos clientes.

Las soluciones de carga de Nokia son compatibles con los principales CSP y con más de mil millones de abonados en todo el mundo. La solución de carga mejorada de Nokia se desplegará en octubre entre los clientes actuales de NCC, como Sunrise, Taiwan Star Telecom y varios CSP globales de primer nivel.

Alianza estratégica de Xilica y Sennheiser

Xilica® anuncia su alianza con Sennheiser para desarrollo de una solución plenamente integrada para sala de reuniones, que minimice el tiempo de instalación, mejore la calidad del sonido y optimice la colaboración entre los usuarios finales.

La nueva asociación aprovechará los productos de audio de ambas empresas, ofreciendo al usuario gran fluidez para desplegar sistemas de audioconferencia adaptables y fáciles de usar con las TI.

La solución completa, que combina el micrófono beamforming TeamConnect Ceiling 2 de Sennheiser con el ecosistema DSP, las interfaces de usuario y los puntos finales de red de Xilica, garantiza una excepcional nitidez en las conversaciones de participantes presenciales y remotos en espacios híbridos. Con ello, los usuarios finales pueden moverse con flexibilidad por el espacio y personalizar a su gusto sus presentaciones, asegurando al máximo la audibilidad. La perfecta integración del TeamConnect Ceiling 2 de Sennheiser con los procesadores Xilica Solaro y los puntos finales de red Xilica Gio beneficiará tanto a los integradores como a los usuarios finales, permitiendo una instalación fácil y sin códigos y con una compatibilidad validada con antelación.

Como parte de la alianza, Xilica facilita la funcionalidad TruVoicelift en el TeamConnect Ceiling 2 (TCC2) de Sennheiser en toda su Serie Solaro de DSP, cuyo testeado y calibración automáticos de audio simplifican la instalación de múltiples micrófonos TCC2 de Sennheiser con el consiguiente ahorro de horas de trabajo durante el montaje del sistema. Además, con TruVoicelift se consigue reducir sonido, amplificar el altavoz y crear, en el caso de participantes que intervienen desde espacios concurridos, zonas focalizadas en ellos. Gracias a eso, y al sistema patentado de reducción de sonido de Xilica y los algoritmos de cancelación de eco HearClear, la nueva solución reduce considerablemente las distracciones en reuniones.

A todo ello hay que sumar que el TeamConnect

Ceiling 2 de Sennheiser y los procesadores Xilica Solaro ofrecen la sincronización de estado "mute" para Microsoft Teams, permitiendo realizar acciones mute basadas en software, como pulsar un botón de la aplicación Microsoft Teams, para que se refleje a lo largo de la cadena y de vuelta al indicador de estado LED del TCC2 de Sennheiser. Del mismo modo, el uso de las interfaces de usuario de Xilica permite que una acción mute se refleje en el TeamConnect Ceiling 2 de Sennheiser y de vuelta en la aplicación Microsoft Teams, garantizando una total visibilidad a los usuarios de la sala de reuniones.

Por otro lado, está previsto que el módulo de seguimiento de cámara follow-me esté ampliamente disponible para el TeamConnect Ceiling 2 de Sennheiser en el cuarto trimestre de 2021, lo que permitirá realizar PTZ automatizado usando la información de señal de posición del TeamConnect Ceiling 2, dando todavía más libertad a los usuarios de la sala de reuniones para hacer presentaciones en sus respectivos espacios sin tener que preocuparse de la infraestructura AV.

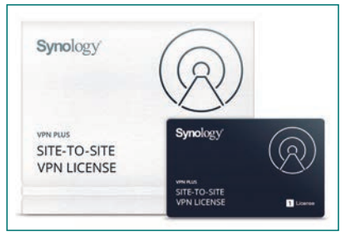
Las licencias de Synology VPN Plus mantendrán su formato gratuito para todos los usuarios

Synology ha anunciado que su solución VPN Plus para routers de la marca mantendrá su formato gratuito para siempre. La compañía decidió ofrecer su solución VPN de forma gratuita a raíz de la situación provocada por la pandemia de 2020, con el objetivo de mejorar la seguridad de las redes de sus usuarios y facilitar el teletrabajo.

Ahora, la Synology ha confirmado que seguirá ofreciendo un formato sin coste para su solución, en línea con su compromiso con la protección y seguridad de los usuarios.

"Lanzamos este programa para apoyar a las empresas de todo el mundo durante la fase inicial de la crisis de la COVID-19. Tras 18 meses, la tendencia es irreversible: el trabajo remoto se ha convertido en la nueva normalidad", afirma Rebecca Lin, directora de producto VPN Plus en Synology Inc.

"Creemos que nuestros usuarios deben seguir disfrutando de los beneficios de nuestra tecnología VPN sin preocuparse por los costes. Por esta razón hemos decidido ofrecer de forma gratuita y para siempre las licencias Synology VPN Plus".



El nuevo programa permite a los propietarios y usuarios de los routers Synology de las series RT1900ac, RT2600ac y MR2200ac activar las licencias de Acceso a VPN cliente y Site-to-Site VPN sin coste adicional, para siempre.

Acerca de VPN Plus
VPN Plus permite a los Routers Synology alojar un potente servidor VPN fácil de configurar y administrar. Es compatible con SSTP, OpenVPN, L2TP over IPSec, así como con el protocolo SSL VPN y el cliente de escritorio ligero propios de Synology. La VPN basada en portal web ofrece a los usuarios acceso directo a los espacios de la intranet de la empresa e incluso permite proporcionar a los empleados acceso remoto al escritorio basado en un explorador.

Vectra AI inicia sus operaciones comerciales en la península ibérica

Vectra AI anuncia el inicio de sus operaciones comerciales en la península ibérica y el nombramiento de Ricardo Hernández como Country Manager para España y Portugal. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid, Ricardo Hernández ha trabajado durante 25 años en el sector de la ciberseguridad, desarrollando su carrera en diferentes fabricantes, entre ellos, Kaspersky Lab, Check Point, Tufin o Forescout. En su nuevo puesto se encarga de la estrategia comercial y del desarrollo de la red de distribución de Vectra con el apoyo de Paolo Lauretti, Regional Partner Manager para la Región Europa del Sur que ayudará a la selección de los Partners en la península ibérica.

Asimismo, Vectra AI ha nombrado a Antonio Huertas como System Engineer para España y Portugal. Ingeniero informático por la Universidad Politécnica de Madrid, Antonio Huertas ha desarrollado su carrera profesional durante más de 20 años en el sector de la ciberseguridad en compañías como Check Point o Palo Alto Networks. Actualmente, en Vectra AI es responsable de preventa en la península ibérica.

Fundada en 2012 con sede central en San José, California, Vectra AI tiene oficinas en Austin, Texas, Boston, Mass., Irlanda, Suiza, Alemania, Reino Unido y Francia. Impulsados por la IA (Inteligencia Artificial), Vectra y su plataforma de detección y respuesta a amenazas buque insignia Cognito® permiten a las organizaciones más consecuentes del mundo detectar automáticamente y responder rápidamente a los ciberataques ocultos en la nube, el centro de datos y los entornos empresariales.

La plataforma Cognito está formada por Cognito Detect™ y sus homólogos de IA igualmente potentes, Cognito Recall™ y Cognito Stream™.

Cognito Detect automatiza la detección en tiempo real de atacantes ocultos, desde las cargas de trabajo de la nube y los centros de datos hasta los dispositivos de los usuarios y del Internet de las cosas (IoT).

Cognito Recall es un entorno de investigación en la nube que permite la búsqueda de amenazas asistida por IA y la investigación forense de incidentes, mediante los metadatos y detecciones proporcionados por Cognito Detect.

Cognito Stream ofrece metadatos de red a escala empresarial enriquecidos con información de seguridad en formato Zeek a aplicaciones de gestión de eventos e información de seguridad (SIEM - security information and event management) y lagos de datos (Data Lakes) sin la complejidad, el ajuste constante y la limitación de escala de Zeek de código abierto.

Estado del despliegue, retos de la industria y perspectivas del mercado 5G en 2022

El 5G está preparando el camino para un mundo totalmente digitalizado y conectado. En los últimos dos años se han realizado numerosas pruebas de campo y se ha acelerado el número de despliegues comerciales. Además, el 5G está empezando a adoptarse en una amplia gama de industrias, desde la fabricación hasta la atención sanitaria.

Con un alto rendimiento y una latencia ultrabaja, el 5G puede aprovechar muchas áreas de gran valor, como el control robótico en 3D, la monitorización de la realidad virtual y el control médico a distancia, que las tecnologías anteriores no podían abordar. El 5G está redefiniendo y acelerando sectores como el de la automoción, el entretenimiento, la informática y la fabricación, y en última instancia cambiará la forma de trabajar y vivir de las personas.

IDTechEx lleva muchos años investigando temas relacionados con el 5G y ha publicado su versión más reciente del informe de investigación de mercado sobre el 5G "Tecnología 5G, mercado y previsiones 2022-2032". Este informe de investigación de mercado e inteligencia empresarial investiga los principales aspectos técnicos, industriales y regionales que afectan al mercado del 5G, en rápida expansión.

¿Qué banda de frecuencias va en cabeza: sub-6 GHz o mmWave? ¿Cuál es la perspectiva de despliegue en 5 regiones clave?
El término 5G hace referencia a un conjunto de tecnologías de comunicación móvil mejoradas y actualizadas, así como a las nuevas características derivadas de las nuevas bandas de frecuencia: 3,5-7 GHz (también conocidas como sub-6 GHz) o > 24 GHz (también conocidas como mmWave), y mayores anchos de banda, por lo que puede hacer frente a múltiples retos en muchos sectores que las generaciones anteriores no podían. Según la investigación de IDTechEx, el 56% de los servicios comerciales de 5G en el mundo operan en el rango sub-6 GHz. Casi todas las estaciones base en el espectro sub-6 GHz están en las ciudades. La figura 1 representa la estrategia de despliegue de la red utilizada por los operadores de telecomunicaciones para construir su red 5G, mostrando que las bandas de frecuencia más altas se utilizarán en gran medida en las regiones densamente pobladas.

Cada país/región tiene su propio calendario de liberación de espectro. Aunque la mayoría de los países liberaron inicialmente el espectro sub-6 GHz, hay algunas excepciones. La agencia reguladora estadounidense, por ejemplo, emitió primero el espectro de ondas milimétricas y no liberó su banda sub-6 GHz hasta principios de 2021. En consecuencia, las previsiones de despliegue de la 5G y la estrategia de implantación de cada país serán diferentes. El informe "5G Technology, Market and Forecasts 2022-2032"

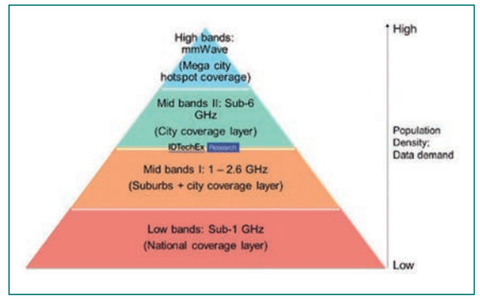


Figura 1: Estrategia de despliegue de la red 5G, extraída del informe "5G Technology, Market and Forecasts 2022-2032" de IDTechEx.

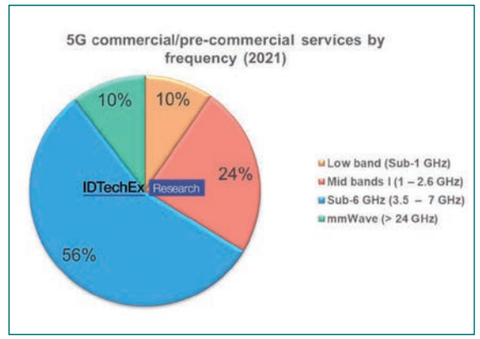


Figura 2: Servicios comerciales/ precomerciales de 5G por frecuencia (2021), del informe "5G Technology, Market and Forecasts 2022-2032" de IDTechEx.

de IDTechEx incluye un análisis regional detallado del estado de despliegue del 5G y la futura hoja de ruta de despliegue en cinco regiones clave: Estados Unidos, China, Japón, Corea del Sur y Europa, incluyendo la estrategia gubernamental, la financiación y el calendario y la hoja de ruta de despliegue del 5G de los principales operadores nacionales de telecomunicaciones, así como el análisis de los ingresos.

Dos tecnologías esenciales para el futuro desarrollo del 5G: mmWave y red de acceso radioeléctrico abierta (Open RAN)

Las ondas milimétricas, que hasta ahora se utilizaban exclusivamente para comunicaciones militares, satelitales y de radar para automóviles, se han introducido recientemente en el conjunto de frecuencias para las comunicaciones móviles, permitiendo un rendimiento máximo de datos de 20 Gbps con una latencia ultrabaja de 1 ms. Una frecuencia tan alta requiere el desarrollo de nuevos materiales y diseños de dispositivos. Por ejemplo, los dispositivos de ondas milimétricas necesitan materiales de baja pérdida con una constante dieléctrica y una pérdida de bronceado mínimas, así como soluciones de embalaje avanzadas, para evitar una pérdida de transmisión excesiva. Debido a la corta longitud de onda de las comunicaciones mmWave, el dispositivo es cada vez más compacto e integrado, lo que hace que la gestión energética y térmica sea aún más crítica. En este informe, IDTechEx evalúa los puntos débiles técnicos y explora las tendencias e innovaciones tanto para los materiales como para el diseño del 5G para superar estos cuellos de botella. Además, el informe también ofrece una visión general del sector de las ondas milimétricas 5G, una revisión de los principales actores, un análisis de la cadena de suministro y una mirada a las aplicaciones verticales que posibilita la tecnología de ondas milimétricas.

El despliegue de la infraestructura 5G es fundamental para permitir la adopción generalizada del 5G. Los proveedores de sistemas de telecomunicaciones heredados, como Huawei, Ericsson y Nokia, tienen una gran participación en el mercado de la infraestructura 5G, según IDTechEx, con Huawei dominando con el 36% en 2020, seguido de Ericsson con el 27%

Los operadores de telecomunicaciones están impulsando el desarrollo de la RAN abierta (es decir, redes basadas en componentes RAN desagregados con interoperabilidad estandarizada, incluido el uso de hardware de caja blanca no patentado, software de código abierto de diferentes proveedores e interfaces abiertas) para eliminar la naturaleza propietaria de los sistemas RAN, diversificar la cadena de suministro de los proveedores en la industria de las telecomunicaciones, aportar más innovación, reducir el coste del despliegue de la RAN (recuerde que el coste de despliegue de la 5G es más caro que el de la 4G) y reducir el coste de operación. Algunos de los principales operadores de telecomunicaciones ya han puesto en marcha redes Open RAN 5G a pequeña escala a mediados de 2021. Muchas más han trazado planes para desplegar redes 5G en el futuro utilizando la tecnología Open RAN. ¿Cómo podría la RAN abierta alterar el mercado de la infraestructura 5G e influir en la dinámica general de la cadena de suministro? ¿Quiénes son los actores en el campo de la Open RAN? ¿Cuál sería el posible modelo de negocio de la Open RAN? ¿Es la RAN abierta más barata que el sistema heredado? ¿Cuáles son las actitudes y estrategias de los proveedores de sistemas heredados en relación con la RAN abierta? ¿Cuáles son los retos pendientes de Open RAN? El informe de IDTechEx analiza en detalle todas estas cuestiones que ayudarán al lector a comprender la tendencia futura del mercado de la infraestructura 5G.

Perspectiva del mercado 5G:

El mercado 5G está a punto de despegar. Para finales de 2032, se prevé que los servicios móviles de consumo generen unos ingresos de 800.000 millones de dólares, y los mercados de macroinfraestructura 5G se expandirán siete veces más que en 2020, según IDTechEx. La previsión se basa en un extenso análisis de datos primarios y secundarios, combinado con una cuidadosa consideración de los impulsores del mercado, las limitaciones y las actividades de los actores clave. El informe proporciona una cifra de despliegue histórico (2019 - 2021) y una previsión a diez años (2022 - 2032) para diferentes segmentos, incluidos los ingresos de la telefonía móvil 5G, las suscripciones y la infraestructura basada en cinco regiones globales (EE.UU., China, Corea y Japón, Europa y otros), el envío de móviles globales 5G, los ingresos de acceso inalámbrico fijo global 5G y el envío de equipos prometidos por el cliente (CPE), y los componentes críticos 5G como los amplificadores de potencia.

Un 83% habrá desplegado Wi-Fi 6/6E en 2022

El 83% de los proveedores de servicios y fabricantes de equipos y empresas de todo el mundo habrán desplegado Wi-Fi 6/6E o tienen previsto hacerlo antes de que finalice el año 2022. Esta es una de las principales conclusiones de la última encuesta intersectorial realizada por la Wireless Broadband Alliance, el organismo mundial del sector dedicado a mejorar los estándares y servicios Wi-Fi.

Las conclusiones, publicadas por la WBA como parte del Informe Anual de la Industria 2022 de la WBA, destacan cómo el espectro de 6GHz permitirá que el Wi-Fi admita aún más usuarios y nuevos casos de uso, como las redes sensibles al tiempo (TSN) para las aplicaciones de la Industria 4.0. El 58% de los encuestados afirma que 6GHz es crítico o muy importante para su estrategia. Esta perspectiva refleja el rápido crecimiento tanto de la armonización global como de la selección de dispositivos:

- 41 países, que representan el 54% del PIB mundial, han autorizado el uso de 6GHz

- Más de 338 millones de dispositivos Wi-Fi 6E entrarán en el mercado este año

- Casi el 20% de todos los pedidos de dispositivos Wi-Fi 6 serán compatibles con 6GHz en 2022

El nuevo informe incluye actualizaciones sobre diversas tecnologías, modificaciones e iniciativas, como la convergencia 5G y Wi-Fi 7 (802.11be). También conocido como Extremely High Throughput (EHT), se prevé que Wi-Fi 7 admita un rendimiento de hasta 30 Gbps, unas tres veces más rápido que Wi-Fi 6. La WBA espera que los dispositivos Wi-Fi 7 hagan su debut en el mercado en 2025.

El informe también cuantifica el impulso global de WBA OpenRoamingTM, que permite a los usuarios conectarse de forma automática y segura a millones de redes Wi-Fi en todo el mundo, y sin necesidad de inicios de sesión, registros o contraseñas. Los encuestados dijeron que la itinerancia es la segunda capacidad Wi-Fi más importante para el éxito comercial, especialmente para los entornos de las ciudades inteligentes.

- El 40% de los encuestados ha implantado Passpoint/OpenRoaming, como los campus hospitalarios de Adventist Health en EE.UU., o tiene previsto hacerlo antes de finales de 2022

- El 70% de los encuestados que participan en una red Wi-Fi pública en toda la ciudad, o que planean hacerlo, apoyarán la itinerancia en toda la ciudad, uniéndose a varios municipios de toda Europa que lo han implementado

La versión 2 de OpenRoaming se anunció en junio y define nuevas e importantes funcionalidades, entre ellas la compatibilidad con los acuerdos de nivel de servicio (SLA) a través de un nivel de calidad de servicio que garantiza una experiencia de transmisión en alta definición de "nivel de plata" en las redes de OpenRoaming. El servicio Silver-tier ya está disponible en el 95% del ecosistema OpenRoaming.

Tiago Rodrigues, director general de la WBA, comenta: "Los proveedores de servicios, los fabricantes de equipos y las empresas de todo el mundo ven más valor que nunca en el Wi-Fi".

"A pesar de toda la incertidumbre debida a la pandemia, el 56% de los encuestados dijo tener más confianza en la inversión en Wi-Fi que hace un año. Esta confianza también se manifiesta en el número de miembros de la WBA que participan en diversos proyectos -un aumento del 15% respecto a 2020- y en el récord de 20 proyectos en desarrollo o ya en marcha. Un ejemplo es su gran interés en la convergencia de 5G y Wi-Fi 6, incluyendo cómo los operadores móviles pueden aprovechar Wi-Fi como parte de su estrategia de 5G en términos de maximizar la cobertura y la capacidad."

Se abre el registro de visitantes para ISE 2022

El registro de visitantes para ISE 2022 ya está abierto, ofreciendo a la comunidad internacional de AV e integración de sistemas una oportunidad esperada para "Levantarse. Reconectar. Encender el futuro' en su nueva sede en la Fira de Barcelona Gran Vía.

ISE 2022 reunirá de forma segura a la industria AV y ofrecerá a los asistentes la oportunidad de interactuar y experimentar en persona y de primera mano tecnologías y soluciones líderes en el mundo. Una de las novedades de 2022 es el registro de los visitantes sin necesidad de papel en forma de credenciales digitales emitidas a través de la nueva aplicación ISE. La aplicación también será una rica fuente de información y contenidos adicionales.

Mike Blackman, director general de Integrated Systems Events, declaró: "Como evento presencial, estamos en una posición única para reunir todos los elementos de la industria bajo un mismo techo. En los preparativos para nuestro regreso a Barcelona, junto con nuestros copropietarios AVIXA y CEDIA, hemos trabajado duro para asegurar que ISE 2022 ofrezca a la industria una experiencia que realmente valga la pena: mostrar la innovación, inspirarse con algunos de los más brillantes en el negocio, y lo más importante, reunirse después de tantos meses difíciles de separación".

Distribuido en cinco pabellones de la Fira Gran Vía, el recinto ferial se ha organizado en cinco Zonas Tecnológicas para ofrecer una experiencia mucho mejor a los visitantes. Hasta ahora, más de 700 empresas se han comprometido a exponer. Con amplios pasillos, un diseño de fácil navegación y marcas líderes en la industria mostrando innovaciones tecnológicas y más, ISE 2022 proporcionará tanto al canal AV como a los usuarios finales mucha inspiración y soluciones para transformar sus negocios.

Las cinco zonas tecnológicas son

- **Audio (Pabellón 7)**
- **Señalización digital y DooH (pabellón 6)**
- **NUEVO: Iluminación y puesta en escena (pabellón 7) - con una zona especial de demostración de iluminación**
- **NOVEDAD: Residencial y edificios inteligentes (pabellón 2) - zonas recien combinadas**
- **NUEVO: Comunicaciones Unificadas y Tecnología Educativa (Pabellón 2) - zonas recien combinadas**

Nuevo en ISE

Una innovación para 2022 es la Sound Xperience de ISE. Situado a pocos metros de la Fira Gran Vía, este complejo de cines dedicado ofrece doce salas de escucha de configuración única para mostrar el audio con profundidad, precisión y claridad milimétrica. Esta iniciativa, en colaboración con el complejo de Eventos Filmax Cinema Gran Vía, es el escenario definitivo para probar el sonido característico de las principales marcas de audio del mundo.

El ISE también ha ampliado sus áreas de demostración de

tecnología. Habrá tres nuevas áreas de demostración que cubren la iluminación y la puesta en escena (dentro de la Zona de Iluminación y Puesta en Escena), el audio y la señalización digital (ambas al aire libre). Aprovechando las amplias instalaciones del recinto, estas nuevas áreas permitirán a los visitantes experimentar estas importantes soluciones multitecnológicas en montajes "reales".

Programa de conferencias y contenidos inspiradores

Reconocido como destino de contenidos inspiradores, ISE 2022 ofrecerá numerosas oportunidades de desarrollo profesional a través de su programa de contenidos multilingües de cinco días de duración.

Combinando una mezcla de sesiones de pago y gratuitas, el programa de liderazgo intelectual de 2022 abarca una amplia variedad de temas del sector. El programa, que comenzará el lunes con dos conferencias de un día de duración, se desarrollará en tres escenarios específicos dentro del pabellón 1. El Foro, de acceso gratuito, comenzará con sesiones magistrales diarias y será presentado por la futurista Amelia Kallman. También habrá contenido español en la Zona de Experiencia AV, producida con AVIXA, mientras que el Pabellón Catalán, en asociación con ACCIO, promete una gran experiencia para los visitantes de la región local.

"Estamos encantados de reunir a la comunidad AV en la nueva sede de ISE en Barcelona, una ciudad vibrante conocida por su creatividad e innovación", dijo Sarah Joyce, Chief Global Officer de AVIXA. "Habrá muchas oportunidades de formación para que los asistentes exploren, incluyendo nuestros talleres de medio día de CTS (Especialista en Tecnología Certificada) en varios idiomas, junto con eventos para los miembros como el desayuno de CTS alemán, el desayuno de los miembros italianos, y los eventos del Consejo de Mujeres de AVIXA y del Consejo de Diversidad de AVIXA. La Zona de Experiencia AV vuelve con una conferencia de dos días presentada en español que explorará el AV en los mercados minorista, de hostelería y corporativo. No podemos esperar a ver a todos en la feria en 2022".

Con ponentes expertos, presentaciones y paneles de discusión, el programa de la Conferencia ISE comprende:

- **Conferencia sobre edificios inteligentes (lunes 31 de enero)**
- **Cumbre sobre señalización digital (lunes 31 de enero)**
- **Cumbre sobre salas de control (martes 1 de febrero)**
- **NUEVO: Cumbre sobre lugares de trabajo inteligentes (martes 1 de febrero, por la tarde)**
- **Cumbre sobre el aprendizaje digital (miércoles 2 de febrero, por la tarde)**
- **NOVEDAD: Cumbre sobre eventos en directo (jueves 3 de febrero - p.m.)**
- **NOVEDAD: Conferencia sobre tecnología para superyates (viernes 4 de febrero - mañana)**

Giles Sutton, Co-CEO interino de CEDIA comentó: "Junto con toda la comunidad de profesionales de la integración doméstica, CEDIA espera con gran interés la celebración de ISE 2022 en Barcelona. El evento del próximo año marca el comienzo de una nueva y emocionante era para nuestra industria, ya que miramos más allá de los desafíos de los últimos dieciocho meses hacia un futuro más brillante para todos nosotros.

CEDIA llevará a cabo un extenso programa de desarrollo profesional en la feria, proporcionando una amplia gama de oportunidades para que los asistentes aprendan nuevas habilidades, aumenten sus conocimientos y construyan una carrera vibrante y satisfactoria en la industria. No podemos esperar a volver a conectar con visitantes de todo el mundo en la Fira Gran Vía en febrero de 2022."

Características y eventos

El Día de la Carrera Audiovisual vuelve a ISE 2022, este año tendrá lugar el jueves 2 de febrero. Con el apoyo de AVIXA, CEDIA e ISE, esta iniciativa está diseñada para mostrar las oportunidades de carrera en toda la industria AV y asegurar que la próxima generación de profesionales AV tenga las habilidades para hacer frente a los desafíos del futuro. Un grupo selecto de estudiantes de tecnología de universidades y escuelas técnicas de toda Europa disfrutará de una visita organizada.

El ISE también colabora estrechamente con la ciudad de Barcelona, la Generalitat de Cataluña y las autoridades españolas. Habrá eventos sociales muy agradables y características diseñadas para mostrar el nuevo hogar del ISE en Barcelona. Más adelante se darán más detalles.

Los premios Inavation Awards, producidos por el IML, se estrenan en Barcelona. Asociados desde hace tiempo a la ISE, estos premios celebran los proyectos y las tecnologías desplegadas por los integradores de sistemas, los consultores y los directores de tecnología. Los Premios Inavation tendrán lugar el martes 1 de febrero y prometen ser una gran noche. Los premios al diseño de stands, que celebran y reconocen los esfuerzos de los expositores de la ISE por crear stands de exposición impactantes y eficaces, también tendrán lugar durante la feria.

Un entorno seguro

Las medidas de seguridad de Covid se mantendrán en constante revisión para garantizar los planes más apropiados para la situación en febrero de 2022, ya que ISE sigue trabajando estrechamente con el recinto, la ciudad de Barcelona y las autoridades sanitarias locales y nacionales. Las posibles medidas podrían incluir el uso de máscaras faciales, el distanciamiento social y la provisión de medidas de saneamiento reforzadas en todo el recinto. Para acceder al recinto se exigirá una prueba negativa, una prueba de vacunación o una prueba de recuperación.

Pronto se anunciarán más detalles sobre estas medidas, pero mientras tanto, la inscripción ya está abierta, puedes reservar aquí tu entrada: https://iseurope.org/register.php

Integrated Systems Europe, ISE 2022, tendrá lugar en la Fira de Barcelona Gran Vía del 1 al 4 de febrero de 2022. El programa de la Conferencia ISE se desarrollará desde el lunes 31 de enero hasta el viernes 4 de febrero.■

Dualidad del malware inteligente avanzado (ofensivo y defensivo), puntos de actuación y operativa de expansión transparente

En el presente artículo se exponen las dos facetas del malware inteligente avanzado (ofensivo o convencional y defensivo antagónico al malware ofensivo), se recorren los itinerarios no determinísticos de dichos malware, se identifican formas de defensa y estructura del malware, se exploran sus efectos tanto nocivos como de defensa y protección, se tipifican los puntos de actuación y por último se indagan las formas de expansión.

Prof. Dr. Javier Areitio Bertolín
Director del Grupo de Investigación Redes y Sistemas

Hoy en día se pueden observar dos facetas en el malware inteligente avanzado, la más común es el malware ofensivo (o dañino), pero también existe una faceta menos conocida y disruptiva denominada malware defensivo (es antagónico al malware ofensivo y opera al mismo nivel de detalle del malware ofensivo) diseñado para neutralizar, inactivar, paralizar, inhabilitar, revertir, inactivar, bloquear, esterilizar, con capacidades y habilidades retrospectivas, para anular, cazar, eliminar, parar e invertir procesos de (cambios, eliminaciones, bloqueos, espionajes, datos robados, DoS, etc.), es capaz de reparar modificaciones-creaciones, etc. al malware ofensivo.

El malware inteligente puede considerarse como una ciberarma tanto ofensiva (por defecto) como defensiva (faceta menos conocida). Esta dualidad del malware inteligente genera dos comportamientos o formas de actuar: una negativa, malware ofensivo (es la que estamos acostumbrados por defecto donde se hace el mal, se llevan a cabo sabotajes, se espía, se roba, se secuestran dispositivos, se suplantan identidades, se perjudica, se daña, se mata, se contamina, etc.

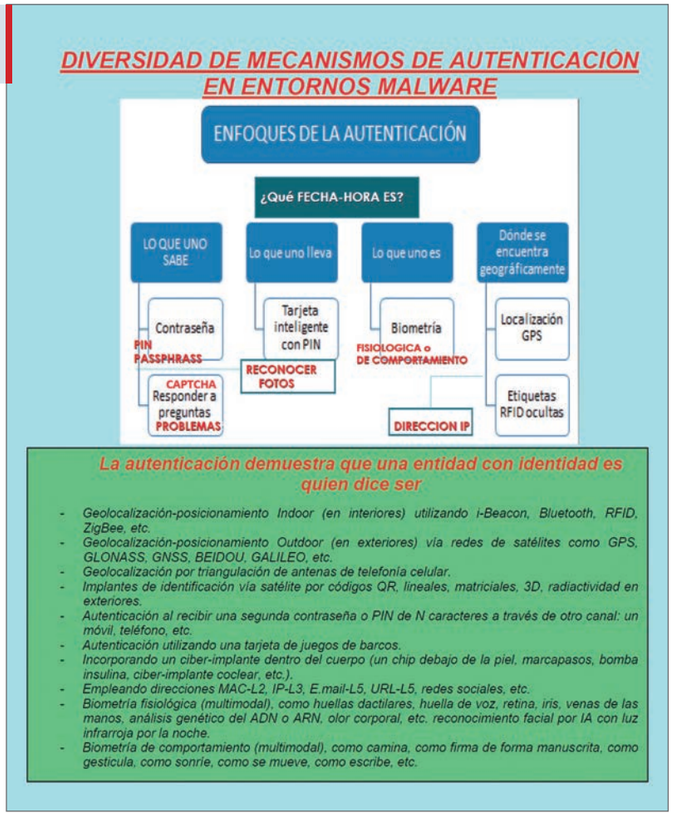
Algunos ejemplos de malware ofensivo son: RigEK, Dridex, Ryuk, Wiper-Meteor, Obot, Remcos (tipo RAT), Ursnif (tipo troyano), KPOT, CTB-Locker, Hawkeye, BitPaymer, XAgent, TeslaCrypt, Zeus (tipo troyano), WannaMiner (tipo cryptomining), DarkGate, Ragnar-Locker, Octubre-Rojo, MyloBot, Glupteba (tipo backdoor), Phorpiex, NRSMminer, Ramnit, Maze, Necro, CryptoLocker, Predator-the-Thief, LokiBot, Hiddad, Shamoon, Danabot, Emotet, Cerberus, Trickbot, Energetic-Bear-Dragonfly, Valak (tipo infostealer), CryptoWall, Zloader, RubyMiner, NanoCore, Lotoor, xHelper, Icefog, Mirai, Clop (tipo ransomware), DoppelPaymer, RCS, Grupo ByC, Pykspa, Duqu, Vidar, Sodinokibi, Hangover, Snake-Uroburos, Stuxnet (para sabotajes), IcedID, Formbook, APT1, XMRig, Lucifer, Flame, PreAMO, NetTraveler, Guerrilla, Coinhive, JSECoin, Careto/The Mask, Equation Group, BlackEnergy, etc.).

El malware ofensivo lo infecta todo (lo aislado y mucho más lo conectado a Internet). La otra forma de actuar es la positiva, malware defensivo (más moderna, diseñada para inactivar, bloquear, anular, esterilizar malware ofensivo y proteger equipos, personas, infraestructuras, APPs, APIs, etc.). Se trata de transformar las funcionalidades conocidas de los malware ofensivos, en positivo, mejorándolas y dar capacidades de protección para crear malware defensivo (por ejemplo, incluyendo funcionalidades en positivo de las ya conocidas como rootkit, backdoor, worm, troyano, virus, etc.).

El término malware (integra las cuatro palabras malicious software-firmware-hardware). Puede tener tres naturalezas (software, firmware y hardware) y puede actuar, situarse, operar, etc. sobre software (directamente como códigos/programas o en forma de explotación de vulnerabilidades en dicho software), firmware (directamente como microcódigos/microprogramas o en forma de explotación de vulnerabilidades en dicho firmware) y hardware (caso de troyanos hardware maliciosos o de defensa o en forma de explotación de vulnerabilidades en dicho hardware).

El malware es tanto una ciberarma (tanto ofensiva como defensiva) como una herramienta sofisticada de ciber-ataque (tanto para realizar acciones perversas como defensivas contra el malware ofensivo para proteger) y también es una ci-

FIGURA 1 ▪ DIVERSIDAD DE MECANISMOS DE AUTENTICACIÓN EN ENTORNOS MALWARE



ber-amenaza (tanto para realizar operaciones maliciosas como defensivas contra el malware ofensivo). Todo en nuestro mundo presentan un doble uso, es decir es dual y puede ser utilizado tanto para el bien como para el mal. El malware inteligente puede tener su actuación siniestra (es lo que caracteriza al malware ofensivo de toda la vida) pero también puede comportarse de forma positiva (malware defensivo antagonista al malware ofensivo cuya finalidad es de protección, diseñado para inactivar, inhabilitar, esterilizar, paralizar, anular, revertir, etc. al malware ofensivo).

Todas las estrategias, tácticas, técnicas, procedimientos, formas de actuar conocidas e inferidas del malware ofensivo (formas de infectar, moverse, pivotar, contagiar, activar sus cargas útiles, ocultarse, propagarse, comunicarse, saltar de una a otra entidad, realizar movimientos multidireccionales, actualizarse, obtener ganancia de funciones, no ser detectado, evitar trazabilidad, etc.) se transforman en positivo de forma realzada para crear, y diseñar e implementar malware inteligente defensivo (o malware de protección). Esto significa que todo lo aprendido del malware ofensivo (en sentido positivo) está trasladándose de forma mejorada al malware defensivo o malware bueno. Actualmente se observa un mayor número de organizaciones infectadas sin saberlo con infinidad de categorías y variantes de malware inteligente no detectado, asintomático.

El malware inteligente de hoy en día es cada vez más persistente, no descubrible, ciber-resiliente y supone un ciber-riesgo extremo debido a sus capacidades actuales de transmisión oculta, nivel de infectabilidad, guiado-direccionabilidad muy precisa, cambio de forma-morfismo y de localización, creación de nuevas funcionalidades, grado de supervivencia, localización precisa de objetivos, ganancia de funciones, invisibilidad (basado en ciber-mimetización, esteganografía, canales subliminares, rootkits avanzados, etc.), no detectabilidad, etc.

Hoy en día, dentro de los malware inteligentes (ofensivo y defensivos) (basados en inteligencia artificial, modulares, superpersistentes, con auto-control, distribuidos, ciber-resilientes, multifuncionales, deslocalizados, de múltiple carga útil, que cambian de forma, con capacidad para actualizaciones y recargas locales y remotas, resistentes a la ciber-forensia, no detectables, con capacidades para interaccionar con la Deep-Web y con la Dark-Web, etc.) se esconde todo un ejército y arsenal de funcionalidades actualizables lo que les permite realizar infinidad de tareas a diferentes víctimas o conjunto de objetivos muy diversas de forma muy sigilosa, no detectable, cubriendo sus rastros y trazas, identificando a las víctimas e infectando con múltiples mecanismos (tanto maliciosos como de protección) y utilizando múltiples tácticas, técnicas y estrategias como “spay-and-pray” (propagación-distribución masiva y global), “guiado estricto-específico” (propagación-distribución concreta a objetivos puntales), liberación de (contramedidas, señuelos, trastaferros de engaño, deception y desinformación), ocultación anti-ciberforense, ocultación subliminar, ciber-mimetización, ocultación esteganográfica-criptográfica post-cuántica multinivel totalmente homomórfica, etc.

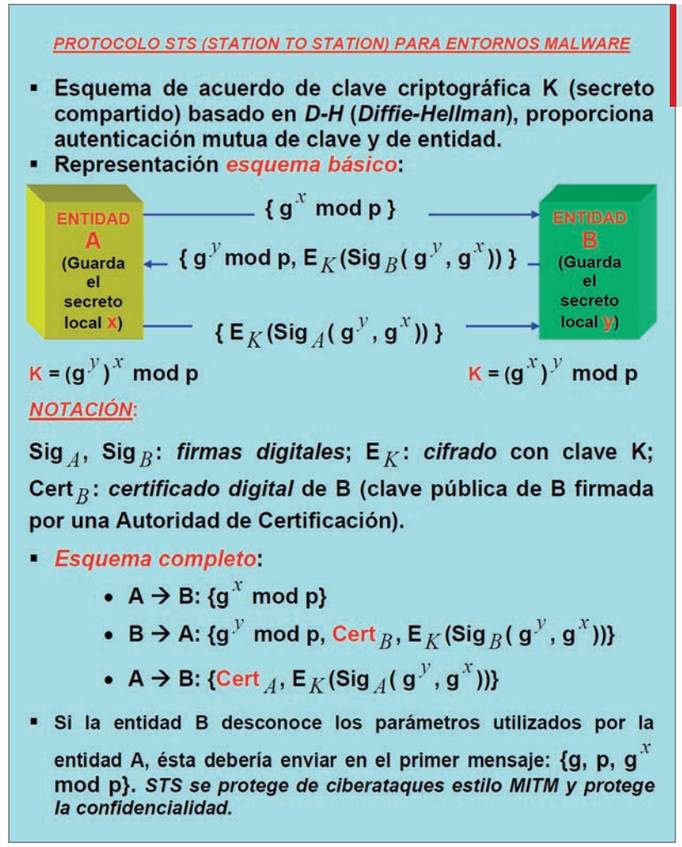
Algunos mecanismos criptográficos (para ocultar el significado de la información) post-cuánticos útiles en ecosistemas malware son:

(i) Criptosistemas basados en retículos-lattice como NTRU, GGH. (ii) Criptosistemas basados en código como los criptosistemas McEliece con códigos Goppa, códigos Gabidulin, etc. y los criptosistemas Bike-2. (iii) Criptosistemas CFPKM basados en polinomios no lineales con ruido. (iv) Criptosistemas basados en isogeny como SIKE. (v) Mecanismos de firma digital basados en retículos, basados en hash, basados en zero-knowledge y en multivariables con sistemas de ecuaciones. (vi) Mecanismos QRNGs (Quantum Random Number Generators).

ITINERARIOS NO DETERMINÍSTICOS DEL MALWARE INTELIGENTE.

El malware inteligente (tanto ofensivo como defensivo), esta presente, circula y opera en programas-software (aplicaciones, redes, APPs, browsers, sistemas operativos, hiperviso-

FIGURA 2 ▪ ESPECIFICACIÓN DEL PROTOCOLO STS (STATION-TO-STATION) CONTRA MITM (MAN-IN-THE-MIDDLE) ENTORNOS MALWARE



res, paquetes como Office de MS, etc.), microprogramas-firmware (como BIOS, TXE, EFI, etc.) y electrónica-hardware (CPUs, DSPs, GPUs, objetos IoT, motores de IA, etc.) y puede considerarse una ciber-amenaza (ofensiva o defensiva), una ciber-arma (ofensiva o defensiva) y una herramienta sofisticada de ciber-ataque (ofensiva o defensiva).

Actualmente el malware inteligente (autónomo, persistente, modular, dinámico, inteligente, no detectable, con capacidades de guiado y actualización, etc.) ya posee capacidades de supervivencia/vida latente con generación de variantes de escape inmunes frente a vacunas, técnicas anti-ciberforenses, retro-malware de defensa y anti-malware.

Esta, claro, el malware inteligente actual tiene un potencial de funcionalidades nunca imaginable y puede comportarse tanto para el mal (malware ofensivo) como para el bien (malware defensivo, antagónico al ofensivo). Integra inteligencia artificial y todas sus derivadas (como: machine-learning, sistemas expertos, deep-learning, filtrado colaborativo, redes neuronales profundas y convolucionales, procesamiento de lenguaje natural (NLP), análisis de pistas de audio basado en espectrogramas, synthetic-media, aprendizaje automático, ganancia de función sin firma, deep-fake, swaping-datos-biométricos cambiando datos reales por ficticios, etc.) y lógicamente es invisible para que no se deje interceptar, descubrir e identificar.

Los malware inteligentes se ubican y esconden en lugares insospechados como memorias RAM, PROM, ficheros, carpetas, unidades pen-drives, DVDs, memorias SSD, UFS (Universal Flash Storage), SIM de móviles, kernel del sistema operativo, CDROM, flash-3D, aplicaciones, routers, particiones de discos duros (incluso ocultas, transparentes y virtuales), periféricos, las nubes (cloud-computing, edge-computing y fog-computing), dispositivos de red, impresoras, objetos IoT/IIoT/IoMT, etc.

Los malware inteligentes se ocultan en:

(1) Software: programas compuestos por instrucciones, ficheros, carpetas, aplicaciones, drivers, dlls, APIs (Application Programming Interfaces), APPs, clientes, srtsp, servidores, peers P2P, etc. Infecta y ciber-ataca a protocolos inseguros y con vulnerabilidades como SNMPv1, GSM, NTP, DNS, SMTP, Erthernet (CSMA/CD), WiFi (CSMA/CA con WPA3), MQTT (Message Queue Server Telemetry Transport), IoT (Zigbee-IEEE802.15.4, Sigfox, LoRaWan, BLE (Bluetooth-Low-Energy), 6LowPan, tecnología celular 3G, 4G, 5G, 6G, etc.).

(2) Firmware: microprogramas compuestos por microinstrucciones, pueden operar en microprocesadores, microcontroladores, GPU (Graphical Processor Unit), DSP (Digital Signal Processor), ASIC, ASSP (Application Specific Standard Product), FPGA, CPUs (como Intel Core i9, AMD (Advanced Micro Devices) Ryzen-9, chip Apple A14, chip U1 con tecnología UWB/Ultra Wide Band (basada en el estándar IEEE 802.15.4.z) para los iPhone con sistema operativo iOS14 que dificultan el rooteado, etc.), dispositivos USB, BIOS, etc.

(3) Hardware: circuitos electrónicos que integren chips y componentes patológicos, troyanos hardware, etc. activos o en vida latente esperando un trigger.

Los malware inteligentes pueden utilizar contenido activo en páginas HTML, pueden estar residentes en memoria RAM (estilo malware sin ficheros), pueden ser persistentes al arrancar, pueden saltarse mecanismos CAPTCHA/re-CAPTCHA, son auto-replicantes, poli-meta-oligo-mórficos, algunos necesitan un fichero/programa de hospedaje para replicarse, otros la red y se ocultan evadiendo la detección y camuflando sus funcionalidades, otros persuaden al usuario (para que les ayude con ingeniería social como descarga y ejecuta, pulsa un link malicioso, aprieta un botón infectado de me gusta, etc.), otros mediante generación de sabotajes atacan directamente a la salud de las personas (crean accidentes en vehículos, desatan crisis epilépticas, crean desastres ecológicos y al medio ambiente, crean suicidios, etc.), etc.

Los malware inteligentes operan, actúan y se comportan

FIGURA 3 ▪ CRIPTOGRAFÍA HOMOMÓRFICA ADITIVA PARA ECOSISTEMAS MALWARE

CRIPTOSISTEMA ASIMÉTRICO PROBABILÍSTICO PAILLIER HOMOMORFICO ADITIVO

- ***GENERACIÓN DE CLAVES***:
  - **Dados dos números primos grandes secretos p y q. Se calcula *n = p.q*. Sea λ la *función de Carmichael de n*: $\lambda(n) = mcm(p-1, q-1)$. Se selecciona de forma aleatoria g perteneciente a Z_{n^2} de modo que mcd ($L(g^{\lambda} \bmod n^2), n) = 1$, donde la *función* $L(u) = \frac{u-1}{n}$.**
  - **La *clave pública* es (*g, n*), la *clave privada* es (*p, q*). El valor de λ es privado.**
- ***PROCESO DE CIFRADO***:
  - **Se desea cifrar un *texto en claro* M perteneciente a Z_n. Se elige de forma aleatoria un *nonce* r perteneciente a Z_n. El *texto cifrado o criptograma* es: $C(M, r) = g^M \cdot r^n \bmod n^2$**
  - **El cifrado posee la propiedad homomórfica aditiva C(M1) . C(M2) = C(M1 + M2) con r = r1.r2.**
- ***PROCESO DE DESCIFRADO***:
  - **Se recupera *el texto en claro* M = $\frac{L(C^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$. Dado un valor entero x, su bit menos significativo *LSB* de su representación binaria es *LSB (x) = x mod 2*. Así mismo *not(x) = (1 + x) mod 2; and(x, y) = x.y mod 2; or(x, y) = (1+x)(1+y)+1 mod 2*.**

CASO - 1: **Sea p = 3, q = 5 → n = 3.5 = 15; $n^2 = 225$; λ = mcm(p-1, q-1) = 4. Sea g = 13, M = 4, r = 2 → $C(M, r) = 13^4 \cdot 2^{15} \bmod n^2 = 30173 = 23$; $L(23^4 \bmod n^2) = (166 - 1)/15 = 11$; $L(13^4 \bmod n^2) = (211 - 1)/15 = 14$; M = 11 / 14 mod 15 = 11.14 = 4.**

CASO - 2: **Sea p = 13, q = 11 → n = 13.11 = 143; $n^2 = 20449$; λ = mcm(p-1, q-1) = 5.4.3 = 60. Sea g = 179, M = 2, r = 2 → $C(M, r) = 179^2 \cdot 2^{143} \bmod n^2 = 3339$; $L(3339^{60} \bmod n^2) = (6436 - 1)/143 = 45$; $L(179^{60} \bmod n^2) = (13443 - 1)/143 = 94$; M = 45 / 94 mod 143 = 45.35 = 2.**

CASO - 3: **Dadas *seis entidades autorizadas*: *A, B, C, D, E y F*. Existen *tres entidades elegibles* que se presentan a las elecciones. Los votantes que votan generan los valores secretos *M1 = 1, M2 = 4, M3 = 4, M4 = 1, M5 = 16, M6 = 1*. Si se eligen respectivamente como valores aleatorios/nonces r1 = 4, r2 = 17, r3 = 26, r4 = 12, r5 = 11, r6 = 32. Se desea sumar los votos de cada candidato, pero cada votante lo entregará cifrado al sistema de votación para que no se vea su valor. Como *Paillier es homomorfico aditivo* se recogerán los valores cifrados, se multiplicarán entre sí todos y se descifrará el resultado obteniendo la suma SUM de votos deseada. Sea p = 5, q = 7 → n = 5.7 = 35; $n^2 = 1225$; λ = mcm(p-1, q-1) = 12. Sea g = 141. Los cifrados de cada voto de cada votante son: *C(M1) = 359, C(M2) = 173, C(M3) = 486, C(M4) = 1088, C(M5) = 541, C(M6) = 163*. El *producto de todos los valores cifrados* es: C(SUM) = C(M1).C(M2).C(M3).C(M4).C(M5).C(M6) = (359 . 173 . 486 . 1088 . 541 . 163) mod 1225 = 983.**

Se descifra este criptograma: $L(983^{12} \bmod n^2) = (36 - 1)/35 = 1$; $L(g^{12} \bmod n^2) = (456 - 1)/35 = 13$. El descifrado SUM = 1 / 13 mod 35 = 27. Este resultado coincide con la suma de los valores *votos secretos* que cada entidad guardaba, es decir: SUM = M1 + M2 + M3 + M4 + M5 + M6 = 1 + 4 + 4 + 1 + 16 + 1 = 27. Si cada entidad codifica en cada valor secreto una fila de una tabla es posible hacer la suma de filas:

ENTIDADES	CANDIDATO-1	CANDIDATO-2	CANDIDATO-3		
A			X	00 00 01 = 1 = M1	C(M1) = 359
B		X		00 01 00 = 4 = M2	C(M2) = 173
C		X		00 01 00 = 4 = M3	C(M3) = 486
D			X	00 00 01 = 1 = M4	C(M4) = 1088
E	X			01 00 00 = 16 = M5	C(M5) = 541
F			X	00 00 01 = 1 = M6	C(M6) = 163
	01 = 1	10 = 2	11 = 3	SUMA ESTRUCTURADA DE VOTOS = 27 = 01 10 11	

como todo un "ejército de entidades bien ofensivas como defensivas".

Los malware inteligentes pueden realizar todo tipo de acciones no deseadas como infección de servicios financieros, ciber-atacar a la privacidad/intimidad, ciber-espiar (y luego sacar dinero de lo observado y controlar a la víctima/entidad en base a la información monitorizada e inferida, crear perfiles perversos, ciber-espiar con falsa bandera para crear confusión, monitorizar plataformas de pago, entidades bancarias, sitios Web, comercios, motores de búsqueda (como Google, Yahoo, etc.), proveedores de servicios y de telecomunicaciones, etc.), robar, secuestrar datos, denegación de servicios DDoS/DoS (a redes, a sistemas de IA, a dispositivos de computación, aplicaciones, nubes, proveedores de servicios, etc. utilizando inundación de syn, botnets, etc.

Hay botnets para DDoS como Mirai, Black-Energy. Hay botnet de banca como Zeus cuyo objetivo es robar contraseñas. Hay malware capaz de robar cookies de navegadores Web, descifrar y realizar sniffer de sesiones SSL/TLS, modificar y corromper información-datos, por ejemplo, ficheros, causar daños físicos a personas, causar accidentes a vehículos conectados/autónomos incluso que cumplen revisiones con estándares como ISO 21434 y UNECE WP.29, dañar-corromper sistemas de control industrial (ICS/OT), sabotajes a sistemas ciber-físicos (CPS), permitir trastornar los controles del tráfico aéreo y los planes de vuelo de aviones, perturbar semáforos, motores de inferencia de IA, sistemas financieros (trampear la sincronización, relojes y velocidad de las operaciones para obtener beneficios), ciber-atacar a la sanidad, telecomunicaciones, teletrabajo (trabajo en remoto), videoconferencias, teleeducación (educación no presencial), es capaz de perturbar el vuelo de drones (por ejemplo, impulsados por pilas de combustible de hidrógeno de alta densidad de elevada autonomía de vuelo), trampear los resultados de votaciones electrónicas, provocar desastres en infraestructuras críticas, medio ambiente, satélites (en base a vulnerabilidades software y/o utilización de antenas ilegales perturbar la trayectoria por señales de posicionamiento de vehículos para que se pierdan, accidenten, etc.), trenes, buques, aviones, infectar las CPUs de dispositivos "soc (system-on-chip)" de vehículos conectados/autónomos (es el caso del malware Mirai Okiru), etc.

DEFENSAS CONTRA EL MALWARE INTELIGENTE.

Algunas estrategias de defensa y contramedidas vectoriales contra los malware inteligentes ofensivos (a todos los niveles predicción, prevención, detección, respuesta, correcciones, recuperación, etc.) son además de utilizar malware defensivo (que anulan, inactivan, bloquean, etc. al malware ofensivo):

(i) Desde el punto de vista de los dispositivos finales, plataformas, endpoints, objetos, sistemas de computación: mantener las actualizaciones y parches de ciberseguridad, mantener el software antimalware actualizado (tanto del producto, motores antimalware como de mecanismos de protección firmas, listas de reputación, configuraciones, whitelist, etc.), el implantar un sistema de firewalls en combinación con un cluster de IDSs/IPSs, no dejar la sesión abierta a pesar de que muchos servicios nos fuerzan por defecto a dejarla abierta (por ejemplo es el caso de algunos correos electrónicos vía Web), dar a los usuarios los mínimos privilegios necesarios para que puedan realizar sus trabajos (no más), generar comunicaciones VPN cifradas y con cadenas de proxies para el anonimato, establecer políticas y procedimientos de escaneo antimalware (automatizado y manualmente) suprimir plug-ins/scripts/macros/dlls maliciosos, implantar la gestión de vulnerabilidades y la actualización de herramientas malware, de qué aplicaciones son permisibles, de que sitios Web tienen reputación, implantar sistemas IAM de gestión de la identidad, autenticación multi-factor eficiente, etc.

(ii) Desde la perspectiva de las aplicaciones/APPs, controlar el uso de las aplicaciones, sus APIs, mantener las actualizaciones de ciberseguridad de las aplicaciones, sistemas operativos, browsers, proteger los valores de configuración de las aplicaciones, someter a las aplicaciones/APPs a una auditoría de código estática y dinámica efectiva, controlar vulnerabilidades en todo tipo de asistentes virtuales personales no sólo Alexa, Siri, Cortana, etc.

(iii) Desde el punto de vista de los datos, implantar ciberseguridad en los datos/metadatos, implantar las políticas de almacenamiento de datos con cifrado totalmente-homomórfico, post-cuántico y multicapa, hacer cumplir las regulaciones y certificaciones-normas como la regulación de protección de datos de la EU (o GDPR), la norma ISO/IEC 27701 sobre privacidad, las normas ISO/IEC 27001 e ISO / IEC 27002 de gestión de seguridad de la información, etc.), gestionar los backups y restores de forma remota y redundante, etc.

(iv) Desde el punto de vista de las redes, aplicar micro-segmentación para el control de redes, ejecutar una política de protección de red inalámbrica, cableada y vía satélite generalizada (WPAN-Bluetooth, WLAN-WiFi6-IEEE802.11ax/WPA3, LPWAN (Low-Power Wide Area Network), LoRaWan/Sigfox para IoT, ZigBee, RFID, NFC, redes celulares WWAN 2G, 3G, 4G, 5G, 6G bajo la banda D, comunicaciones por satélite y posicionamiento GPS, Glonass, GNSS, Galileo, proyecto de red de satélites star-link, etc.), establecer conexiones de red protegidas por VPN (con cifrado y anonimato por cadena de proxies), gestionar el acceso de visitantes, auditores, etc., detección anticipada de ciber-ataques/ciber-incidentes, monitorización de redes, control de cambios, aplicar la inteligencia de ciber-amenazas con todo tipo de fuentes como MalwareDomainList.com, realizar test de penetración, etc.

(v) Desde la perspectiva de la gestión de vulnerabilidades. Las vulnerabilidades son todo tipo de defectos, debilidades, errores, incapacidades, fallos, bugs, flaws, torpezas, etc. en (software, firmware, hardware, personas, organización, etc.). APPs y APIs defectuosas y APIs reprogramadas con fallos.

Problemas reiterativos de vulnerabilidad en el software como, por ejemplo, en Blockchain (en todo tipo de entornos como contratos inteligentes, en NFTs (Non-Fungible-Tokens, que son activos digitales únicos, indivisibles, transferibles, que permiten dar la propiedad del activo a alguien a través de Blockchain como Ethereum, por ejemplo, ficheros que se crearon una vez y se han podido diferenciar de sus copias, por tanto, pueden tener mucho valor en subastas, caso de fotos, dibujos, videojuegos, canciones, etc.), criptodivisas-criptomonedas, gestión descentralizada de identidades digitales, en sistemas financieros, en mecanismos de ciberseguridad, etc.).

Las vulnerabilidades de validación del recorrido del directorio, agujeros de ciberseguridad no previstos, confianza sin verificación, imprudencias, distorsión-deficiencias-atajos cognitivos, cobardías, miedos, malas configuraciones, canal de actualizaciones corrupto, deficiencias en implementaciones, diseños, despliegues, etc.

Se debe tener en cuenta que debe existir una política de actualizaciones de ciberseguridad que valore el entorno a ser actualizado, aplicar las nuevas actualizaciones (de protección y productos), evaluar y planificar el despliegue de actualizaciones y parches (reales y virtuales), desplegar políticas claras de formación (con técnicas pedagógicas avanzadas con prácticas que dejen huellas), adiestramiento y concienciación con prácticas que impliquen de verdad a toda persona implicada, etc. Actualmente es esencial detectar y prevenir todo tipo de malware para evitar ciber-riesgos.

Los malware inteligentes se replican. Por ejemplo, los malware con funcionalidad de virus necesitan un fichero huésped para difundirse mientras que los malware con funcionalidad de worm se difunden por la red aprovechándose del creciente número de vulnerabilidades.

Para evitar posibles situaciones de emergencia ciber-epidemiológicas es clave contar con entornos completos de protección distribuidos antimalware capaces de eliminar todo tipo de cadena de transmisión subliminar y sigilosa de malware incluso vía esteganográfica, con cifrado y compresión.

(vi) Desde el punto de vista de la caza de ciber-amenazas. Emplear un conjunto de técnicas como machine-learning, deep-learning, sistemas expertos, redes neuronales (profundas y convolucionales), análisis estático y dinámico del código, detección de incrementos extraños de los IOPs para algunas instancias en la nube, crecimiento anómalo del tráfico entre máquinas virtuales, bloqueo de exploits white-list, blacklist, IoCs (Indicators of Compromise/Cyberattack), VPN con cifrado y anonimato con proxies, IPS, ng-FW, AV, DLP, ng-IAM, NCS, SIEM, Helpdesk, ng-NAC, etc.

Es prioritario actuar automáticamente, adecuadamente y profesionalmente ya que, queramos o no, la situación va en aumento.

IDENTIFICACIÓN DE LA ESTRUCTURA DEL MALWARE INTELIGENTE.

La composición del malware inteligente puede ser código/microcódigo, contenido o hardware perverso.

El malware inteligente puede infectar y ciber-atacar a: (1) Software (a APIs, APPs, sistemas operativos, browsers, hipervisores, etc.).

(2) Firmware (a motores de inferencia de IA, routers, dispositivos de computación, etc. Las actualizaciones de firmware para chips de geolocalización mediante FOTA (Firmware-Over-The-Air) permiten que chips en general y receptores de GPS, Glonass, Beidou, etc. en particular se reprogramen, así mismo evitan desajustes semanales "week-rollover" en GPS. Si las actualizaciones se infectan, los resultados pueden ser nefastos).

(3) Hardware (a microprocesadores, microcontroladores, CPUs, GPUs, sistemas integrados completos SIP (System-In-Package), DSPs, FPGAs, ASIC, ASSP (Application-Specific-Standard-Products), RAM, ROM, PROM, discos, almacenamientos flash, etc.).

FIGURA 4 ▪ MECANISMO DE OCULTACIÓN DE INFORMACIÓN PARA ENTORNOS MALWARE

MECANISMO DE OCULTACIÓN ESTEGANOGRÁFICA DE INFORMACIÓN PARA MALWARE

- Este *mecanismo* parte del *esquema de compartición de secretos de Shamir* donde un secreto S se divide en fragmentos o puntos y para reconstruirlo se precisa conocer al menos un número mínimo K de *fragmentos o puntos* generados por un polinomio de grado (K – 1) de *interpolación de Lagrange*.
- El *mecanismo* recursivo aquí descrito permite ocultar información adicional (*nuevos secretos*, hasta un total de *(K – 2)* dentro de los fragmentos del *esquema de Shamir*. Este mecanismo puede actuar como un *canal esteganográfico* para transmitir información oculta o para *autenticación y verificación* del secreto S, por ejemplo, permite transportar *firmas digitales* o *funciones hash* de S, la identidad del propietario de S, una marca de tiempo, un localizador GPS, etc. Entre sus aplicaciones está el *almacenamiento/repositorio distribuido, seguro* y *fiable* de información en *Web*, las *redes de sensores*, los esquemas de *dispersión de información malware/C&C* y todo *entorno malware*.

CASO PRÁCTICO: Se desea ocultar el secreto *S = 65* de modo que con *K = 5* fragmentos de pueda recuperar el secreto. Además, se precisa ocultar *W = (K – 2)* secretos adicionales s_1, s_2 y s_3 dentro de los fragmentos anteriores. Sean estos tres secretos adicionales: $s_1 = 46$, $s_2 = 69$ y $s_3 = 72$.

ALGORITMO: (1) FASE DE GENERACIÓN FRAGMENTOS:

- Se elige un número primo p > max (S, s_i); por ejemplo p = 131, se operará en aritmética GF(131).
- Se elige de forma aleatoria y uniforme *un valor* y_{11} dentro de GF(p) y se hace corresponder con el punto (1, y_{11}). Por ejemplo: $y_{11} = 102$ → El punto será: (1, y_{11}) = (1, 102).
- *Se repite desde i = 1 a (K – 2)*:
  1) Se interpola (por *Lagrange*) los puntos (0, s_i) y (j, y_{ij}) desde j = 1 a i para generar i polinomios de *grado-i* $p_i(x)$.
  2) De $p_i(x)$ se calculan (i + 1) puntos: $y_{(i+1)j} = p_i(j + i)$ de j = 1 a (i + 1).
  3) Se generan (i + 1) puntos (j, $y_{(i+1)j}$) para j desde valor 1 a valor (i + 1).

EN ESTE CASO:

- Se interpola (0, s_1) = (0, 46) y el punto x = 1 anterior (1, 102) y se obtiene el polinomio: $p_1(x) = (56.x + 46) \bmod p$.
- A partir de $p_1(x)$ se obtienen dos puntos para x = 2, 3 → y $y_{21} = p_1(2) = 27$, y $y_{22} = p_1(3) = 83$. Es decir (1, y_{21}) = (1, 27), (2, y_{22}) = (2, 83).
- Se interpola (0, s_2) = (0, 69) y los puntos anteriores (1,27) y (2,83) y se genera $p_2(x) = (49.x^2 + 40.x + 69) \bmod p$.
- A partir de p_2 se generan tres puntos para x = 3, 4, 5: $y_{31} = p_2(3) = 27$, $y_{32} = p_2(4) = 96$, $y_{33} = p_2(5) = 53$. Es decir: (1, y_{31}) = (1, 106), (2, y_{32}) = (2, 96), (3, y_{33}) = (2, 53).
- Se interpola (0, s_3) = (0, 72) y los puntos anteriores (1, 106), (2, 96), (2, 53) y se genera $p_3(x) = (111.x^3 + 38.x^2 + 16.x + 72) \bmod p$.
- A partir de p_3 se generan cuatro puntos para x = 4, 5, 6, 7: $y_{41} = p_3(4) = 119$, $y_{42} = p_3(5) = 43$, $y_{43} = p_3(6) = 98$, $y_{44} = p_3(7) = 33$. Es decir: (1, y_{41}) = (1, 119), (2, y_{42}) = (2, 43), (3, y_{43}) = (3, 98), (4, y_{44}) = (4, 33).
- Se interpolan los puntos (0, S) y ((j, $y_{(K-1)j}$) para j desde 1 a (K – 1) y se obtiene un polinomio de grado (K – 1). En este caso: Se interpola (0, S) = (0, 65) y los puntos anteriores (1, 119), (2, 43), (3, 98), (4, 33) y se genera $p_4(x) = (66.x^4 + 106.x^3 + 72.x^2 + 72.x + 65) \bmod p$.
- A partir del polinomio anterior $p_{(K-1)}$ se obtienen (K+W-1) puntos o fragmentos: [i, $p_{(K-1)}$ (i)] para i desde K hasta (K+W-1), del secreto S que además ocultan los secretos s_i. En este caso: A partir de $p_4(x)$ se generan 7 puntos, por ejemplo *N = 7* en x = 5, 6, 7, 8, 9, 10, 11: {(5,2), (6,40), (7,63), (8,130), (9, 50), (10, 37), (11, 55)}

(2) FASE DE RECONSTRUCCIÓN DE LOS SECRETOS (S, s_1, s_2, s_3):

- A partir de K = 5 fragmentos se obtiene $p_4(x)$ y con $p_4(0) = S$. Los valores/ordenadas de $p_4(x)$ en x = 1,2,3,4 se hacen corresponder a las abscisas x = 4,5,6,7, se interpolan estos 4 puntos y se obtiene $p_3(x)$, cuyo $p_3(0) = s_3$. Los valores de las ordenadas de $p_3(x)$ para x = 1,2,3 se hacen corresponder con las abscisas x = 3,4,5, se interpolan estos 3 puntos y se obtiene $p_2(x)$, cuyo $p_2(0) = s_2$. Los valores de las ordenadas de $p_2(x)$ para x = 1,2 (valores 27, 83) se hacen corresponder con las abscisas x = 2,3, se interpola, estos dos puntos (2,27), (3,83) y se obtiene $p_1(x)$, cuyo $p_1(0) = s_1$.

El malware inteligente puede construirse de diferentes formas:

(a) Conjunto de instrucciones software o programa basados en código (ofensivo o defensivo) (aquí se engloban los virus informáticos, el código antagonista o defensivo ante el código ofensivo, los gusanos, el adware, los troyanos software, las puertas traseras como swordfish, los rootkits, los infostealer, etc., algunos ejemplos de malware son: "nimda", "sql-slammer", "blaster", "sasser", "adylkuzz", "fireball", el malware "adylkuzz" se mete en un equipo sin que lo sepa su propietario para realizar cripto-minería no autorizada (crear y robar criptomonedas), etc.).

(b) Conjunto de microinstrucciones, microcódigo o microprograma firmware (ofensivo, es decir, insidioso-letal o de protección antagonista) compuesto por microinstrucciones (es el caso del firmware malicioso o de protección en smartphones, en routers WiFi, en drones, etc. que puede estar infectados en la cadena de suministro, BIOS contaminado, etc.).

(c) Circuitos electrónicos-chips maliciosos (o de defensa) con patologías activables (caso de los troyanos hardware y entre sus aplicaciones la obsolescencia programada, la clonación, modificación-sustitución de dispositivos físicos como, por ejemplo, cámaras de video vigilancia, chips de cifrado hardware o de firma digital que inexplicablemente dejan de cifrar o firmar correctamente, chips PRNGs (Pseudo-Random-Number-Generators) hardware que no generan números pseudoaleatorios operando de manera que desea el malware, etc.).

Es posible identificar los siguientes mecanismos-elementos en la composición del malware inteligente:

(i) Mecanismos de inserción. Permiten inyectar e instalar cada módulo, fragmento, semilla o carga útil del malware en los sistemas objetivos (ficheros, memoria RAM (volátil y no volátil), firmware, kernel, buffer, dispositivos de red, sistema operativo, hipervisor, navegador Web, etc.).

(ii) Mecanismos de evitación y ciber-resiliencia. Permiten evitar la detección del malware. Utiliza múltiples estrategias, tácticas, técnicas, procedimientos (uso de canales subliminares, esteganografía, side-channel, movimientos laterales, desplazamientos multi-direccionales, multi-dominio y multi-dimensionales, ciber-mimetización, mostrar partes sin valor para que se detecten y ocultar lo más importante, etc.).

(iii) Mecanismos de erradicación. Permiten eliminar el malware después de que la carga útil (funcionalidades maliciosas o de protección) se haya ejecutado después de haber sembrado semillas futuras.

(iv) Mecanismos de replicación y propagación. Permite crear copias del propio malware y propagarse a otras particiones, máquinas virtuales, nubes, dispositivos, por ejemplo, el malware con funcionalidad de worm/gusano.

(v) Mecanismos de disparo. Posibilita que uno o varios eventos de disparo (o trigger internos y externos) inicien ciertas cargas útiles o módulos del malware, por ejemplo, un instante de tiempo o fecha, un clic del ratón, un estado del sistema, etc.

(vi) Mecanismos de carga útil. Permiten transportar sus funcionalidades maliciosas (o de protección), por ejemplo, inyectar, posicionar o instalar otras cargas útiles como puertas traseras, explotar vulnerabilidades, formatear-borrar a bajo nivel discos duros, cambiar perversamente datos, configuraciones y programas, etc.

(vii) Mecanismos de ocultación. El malware se esconde en todo tipo de lugares (RAM, flash 3D, etc.) y contenidos (imágenes, videos, textos, etc.): (a) Pasivos. La aplicación que lo gestiona define el comportamiento que resulta cuando se abre el contenido. (b) Activos seguro. Los datos definen el comportamiento. (c) Activos no seguros. Por ejemplo, contenido Flash. (d) Explosivos. Pueden ejecutarse al explotar una o varias vulnerabilidades 0-day o n-day.

FIGURA 5 ▪ FIRMA DIGITAL ESTILO RABIN MODIFICADO PARA ENTORNOS MALWARE.

MECAMISMO DE FIRMA DIGITAL ESTILO RABIN MODIFICADO PARA ENTORNOS MALWARE

- **GENERACIÓN DE CLAVES PÚBLICA-PRIVADA EN LA ENTIDAD QUE FIRMA B:**
  - La entidad B selecciona dos números primos grandes: p = 3 mod 8, q = 7 mod 8. Calcula su producto n = p . q. La *clave pública* de B es: n y su *clave privada* es: d = (n – p – q + 5) / 8.
  - Sean por ejemplo p = 19, q = 23, entonces: n = 437 y d = (437 – 19 – 23 + 5) / 8 = 50.
- **PROCESO DE FIRMA DIGITAL-ELECTRÓNICA EN LA ENTIDAD QUE FIRMA B DEL MENSAJE M:**
  - El *espacio U de mensajes en texto en claro* son los números enteros positivos menores o igual a k = (Parte-entera-de [(n – 6) / 16]). En este caso: k = (Parte-entera-de [(437 – 6) / 16]) = 26.
  - Dado el mensaje M, la entidad B calcula: M1 = (16 . M + 6). Sea por ejemplo M = 5, entonces: M1 = (16 . 5 + 6) = 86.
  - La entidad B calcula el *símbolo de Jacobi* J como producto de *símbolos de Legendre*: $J = \left(\frac{M1}{n}\right) = \left(\frac{M1}{p}\right).\left(\frac{M1}{q}\right) = (M1^{(p-1)/2} \bmod p).(M1^{(q-1)/2} \bmod q)$. Se compara si: J = 1 → entonces se calcula la firma digital es: $S = M1^d \bmod n$; Si el valor de J = – 1 entonces se calcula la firma digital es: $S = (M1 / 2)^d \bmod n$.
  - En este caso: $J = \left(\frac{86}{437}\right) = \left(\frac{86}{19}\right).\left(\frac{86}{23}\right) = (86^9 \bmod 19).(86^{11} \bmod 23) = 18 . 22 = (– 1) . (– 1) =$ 1, entonces $S = 86^{50} \bmod 437 = 35$.
- **PROCESO DE VERIFICACIÓN DE LA FIRMA EN UNA ENTIDAD GENÉRICA A:**
  - La entidad A conoce la clave pública de B que es n.
  - La entidad A calcula M2 = $S^2 \bmod n$. Como se observa no se necesita el mensaje original M. Si M2 = 6 mod 8 entonces M3 = M2. Si M2 = 3 mod 8 entonces M3 = (2 . M2). Si M2 = 7 mod 8 entonces M3 = (n – M2). Si M2 = 2 mod 8 entonces M3 = (2 . [n – M2]).
  - *Verificar* que M3 pertenece al conjunto Q de mensajes { Z(m) tales que Z(m) = 16 . m + 6 para todo m del conjunto U que va desde cero a (Parte-entera-de [(n – 6) / 16]) }, en caso contrario rechazar la firma digital.
  - El conjunto Q es: {6, 22, 54, 70, 86, 102, 118, 134, 150, 166, 182, 198, 214, 230, 246, 262, 278, 294, 326, 358, 374, 390, 406, 422, 438, 454, 470, 486, 502, 518, 534, 550, 566, 582, 598, 614, 630, 646, ... }
  - Se recupera el mensaje M calculando: M = (M3 – 6) / 16.
  - En este caso: M2 = $35^2 \bmod 437 = 1225 = 351$. Como M2 es 7 módulo 8 entonces: M3 = (n – M2) = (437 – 351) = 86. Vemos que M3 pertenece a Q. Por tanto: M = (M3 – 6) / 16 = (86 – 6) / 16 = 5 Luego la firma digital es válida.

CASO PRÁCTICO:

La entidad B selecciona dos números primos grandes: p = 19, q = 31. Calcula n = p . q = 589, d = (n – p – q + 5) / 8 = 68. La clave pública es n = 589 y la privada d = 68. Para formar el mensaje M = 12, se calcula M1 = (16 . 12 + 6) = 198; $J = \left(\frac{M1}{n}\right) = +1$, luego $S = 198^{68} \bmod 589 = 102$ es la firma digital. *El proceso de verificación*: $M2 = 103^2 \bmod 589 = 391$ que vale 7 módulo 8 luego M3 = (n – M2) = 589 – 391 = 198. El valor 198 pertenece a Q. La entidad A recupera M = M = (M3 – 6) / 16 = 12 luego la firma se acepta. En este caso, los *símbolos de Jacobi* para los elementos del espacio U son: {6 (-1), 22 (1), 54 (-1), 70 (-1), 86 (1), 102 (1), 118 (1), 134 (1), 150 (-1), 166 (1), 182 (-1), 198 (1), 214 (1), 230 (1), 246 (1), 262 (-1), 278 (1), 294 (-1), 326 (-1), 358 (-1), 374 (-1), 390 (-1), 406 (-1), 422 (1), 438 (1), 454 (1), 470 (-1), 486 (-1), 502 (1), 518 (-1), 534 (-1), 550 (1), 566 (-1), 582 (1) }.

El número de malware inteligente crece cada día con diversidad de funcionalidades como: adialer.c y dialplatform.b de tipo dialer, agent.fyi y rustock.b de tipo backdoor, allaple.a y vb.at de tipo worm, c2lop.p y skintrim.n de tipo troyano software, lolyda.at y lolyda.aa2 de tipo PWS (PassWord Stealer; es un tipo de troyano que roba contraseñas, espía y roba datos), fakerean de tipo rogue, obfuscator.ad y wintrim.bx de tipo trojan downloader, etc.

El malware inteligente ciber-ataca aprovechándose de todo tipo de vulnerabilidades a cualquier tipo de interfaz: objeto (IoT/IIoT, IoMT) a objeto, persona a objeto, máquina a máquina o M2M, persona a máquina (según la compañía Skybox-Security muchos de los interfaces HMI que supervisan las redes OT están obsoletos, carecen de un parcheado adecuado, e incluso son incompatibles con los sistemas Windows sin realizar cambio alguno sobre la configuración original), persona a persona, GUI, CLI, TUI, API (Application Programming Interface).

El crear y modificar una API suele generar vulnerabilidades que aprovecha el malware para realizar sus actividades-operaciones, por ejemplo, saltarse la protección perimétrica estableciendo un conducto secreto entre donde se encuentre (sistema IT o entorno OT/ICS) e Internet), etc. Google ha añadido una nueva API para el sistema operativo Android (versión de 6.0 en adelante) para que la utilicen ciertas APPs que permite que el sistema reconozca que tipo de acceso biométrico (huella, facial, iris, etc.) se utiliza.

EFECTOS NOCIVOS Y DE PROTECCIÓN.

Los principales efectos nocivos (del malware ofensivo) y de protección (del malware defensivo antagónico al ofensivo) que transporta-integra la carga útil del malware inteligente son muy variados:

(1) Instalación de puertas traseras o backdoors, lo que proporciona acceso persistente al dispositivo de computación del objetivo (primario, secundario, etc.) sin necesidad de identificarse, autenticarse y autorizarse. Estas puertas traseras pueden utilizarse para actuar de forma persistente positiva o negativa generando brechas a la confidencialidad similares a un spyware y también a la integridad, disponibi-

CRIPTOGRAFÍA DE CURVAS ELÍPTICAS (ECC) PARA ENTORNOS MALWARE

- **EXPRESIONES PARA SUMAR PUNTOS CON CURVAS ELÍPTICAS**: Existen *tres casos*: (1) *Sumar puntos diferentes*: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ donde $x_1 \neq x_2$. En este caso $x_3 = (d^2 - x_1 - x_2)$; $y_3 = d.(x_1 - x_3) - y_1$; $d = (y_2 - y_1) / (x_2 - x_1)$. (2) *Sumar puntos iguales*: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ donde $x_1 = x_2$, $y_1 = y_2$. En este caso: $x_3 = (d^2 - 2.x_1)$; $y_3 = d.(x_1 - x_3) - y_1$; $d = (3.(x_1)^2 + a) / 2.y_1)$ donde a es el coeficiente de la x en la curva elíptica $y^2 = (x^3 + a.x + b) \bmod p$. (3) *Sumar puntos*: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ donde $x_1 = x_2$, $y_1 = -y_2$. En este caso: (x, y) + (x, – y) = O (*punto origen en el infinito*). Si P = (x, y) entonces – P = (x, – y); P + O = P; 2P = P + P.
- **TABLA DE SUMAS**: Dada la *curva elíptica* no singular de 18 puntos: $y^2 = (x^3 + 13.x + 17) \bmod 23$, el punto G = (22, 7) cumple 18.G = O.

O	(1,10)	(1,13)	(4,8)	(4,15)	(5,0)	(6,9)	(6,14)	(8,9)	(8,14)	(9,9)	(9,14)	(19,4)	(19,19)	(21,11)	(21,12)	(22,7)	(22,16)
(1,10)	(6,9)	O	(21,11)	(8,9)	(6,14)	(5,0)	(1,13)	(22,16)	(4,8)	(22,7)	(19,4)	(21,12)	(9,9)	(19,19)	(4,15)	(8,14)	(9,14)
(1,13)	O	(6,14)	(8,14)	(21,12)	(6,9)	(1,10)	(5,0)	(4,15)	(22,7)	(19,19)	(22,16)	(9,14)	(21,11)	(4,8)	(19,4)	(9,9)	(8,9)
(4,8)	(21,11)	(8,14)	(21,12)	O	(9,9)	(19,19)	(22,7)	(1,10)	(19,4)	(22,16)	(5,0)	(6,14)	(8,9)	(4,15)	(1,13)	(9,14)	(6,9)
(4,15)	(8,9)	(21,12)	O	(21,11)	(9,14)	(22,16)	(19,4)	(19,19)	(1,13)	(5,0)	(22,7)	(8,14)	(6,9)	(1,10)	(4,8)	(6,14)	(9,9)
(5,0)	(6,14)	(6,9)	(9,9)	(9,14)	O	(1,13)	(1,10)	(19,4)	(19,19)	(4,8)	(4,15)	(8,9)	(8,14)	(22,7)	(22,16)	(21,11)	(21,12)
(6,9)	(5,0)	(1,10)	(19,19)	(22,16)	(1,13)	(6,14)	O	(9,14)	(21,11)	(8,14)	(21,12)	(4,15)	(22,7)	(9,9)	(8,9)	(4,8)	(19,4)
(6,14)	(1,13)	(5,0)	(22,7)	(19,4)	(1,10)	O	(6,9)	(21,12)	(9,9)	(21,11)	(8,9)	(22,16)	(4,8)	(8,14)	(9,14)	(19,19)	(4,15)
(8,9)	(22,16)	(4,15)	(1,10)	(19,19)	(19,4)	(9,14)	(21,12)	(9,9)	O	(6,14)	(8,14)	(4,8)	(5,0)	(6,9)	(21,11)	(1,13)	(22,7)
(8,14)	(4,8)	(22,7)	(19,4)	(1,13)	(19,19)	(21,11)	(9,9)	O	(9,14)	(8,9)	(6,9)	(5,0)	(4,15)	(21,12)	(6,14)	(22,16)	(1,10)
(9,9)	(22,7)	(19,19)	(22,16)	(5,0)	(4,8)	(8,14)	(21,11)	(6,14)	(8,9)	(21,12)	O	(1,10)	(19,4)	(9,14)	(6,9)	(4,15)	(1,13)
(9,14)	(19,4)	(22,16)	(5,0)	(22,7)	(4,15)	(21,12)	(8,9)	(8,14)	(6,9)	O	(21,11)	(19,19)	(1,13)	(6,14)	(9,9)	(1,10)	(4,8)
(19,4)	(21,12)	(9,14)	(6,14)	(8,14)	(8,9)	(4,15)	(22,16)	(4,8)	(5,0)	(1,10)	(19,19)	(9,9)	O	(1,13)	(22,7)	(6,9)	(21,11)
(19,19)	(9,9)	(21,11)	(8,9)	(6,9)	(8,14)	(22,7)	(4,8)	(5,0)	(4,15)	(19,4)	(1,13)	O	(9,14)	(22,16)	(1,10)	(21,12)	(6,14)
(21,11)	(19,19)	(4,8)	(4,15)	(1,10)	(22,7)	(9,9)	(8,14)	(6,9)	(21,12)	(9,14)	(6,14)	(1,13)	(22,16)	(8,9)	O	(19,4)	(5,0)
(21,12)	(4,15)	(19,4)	(1,13)	(4,8)	(22,16)	(8,9)	(9,14)	(21,11)	(6,14)	(6,9)	(9,9)	(22,7)	(1,10)	O	(8,14)	(5,0)	(19,19)
(22,7)	(8,14)	(9,9)	(9,14)	(6,14)	(21,11)	(4,8)	(19,19)	(1,13)	(22,16)	(4,15)	(1,10)	(6,9)	(21,12)	(19,4)	(5,0)	(8,9)	O
(22,16)	(9,14)	(8,9)	(6,9)	(9,9)	(21,12)	(19,4)	(4,15)	(22,7)	(1,10)	(1,13)	(4,8)	(21,11)	(6,14)	(5,0)	(19,19)	O	(8,14)

- **PROCESOS DE CIFRADO/DESCIFRADO**:

  Dada la *curva elíptica*: $y^2 = (x^3 + 13.x + 17) \bmod 23$ *sobre GF(23).*

  PROCESOS:

  (1) **GENERACIÓN CLAVES**: Sea G = (22, 7), n_B = 16, $P_B = n_B.G$ = 16.(22, 7) = (8, 14).

  (2) **CIFRADO** del mensaje *M = (8, 9)*. El emisor elige en secreto un valor de un sólo uso *k = 13* → C = (C1, C2) = [k.G, (M + k. P_B)] = [13.(22, 7) , (8, 9)+13.(8, 14)] = [(4, 8), (8, 9) + (21, 11)] = *[(4, 8), (6, 9)]*.

  (3) **DESCIFRADO** del criptograma C. El texto en claro *M* = [C2 – n_B . C1] = (6, 9) – 16.(4, 8) = (6, 9) – (21, 11) = (6, 9) + (21, 12) = *(8, 9) c.q.d.*

FIGURA 6 ▪ CRIPTOGRAFÍA DE CURVAS ELÍPTICAS (ECC) PARA ENTORNOS MALWARE

lidad, no repudio, etc. o inactivando/neutralizando malware ofensivo.

(2) Reemplazar ficheros del objetivo/víctima por ejecutables que aseguren la propagación del malware inteligente, generar algún tipo de visualización en la pantalla, etc. El malware "loveletter" sobre-escribía ficheros con un gran número de extensiones diferentes (.jpg, .mp3, .js, etc.) con scripts Visual Basic, que, si se ejecutaban, entonces re-ejecutaba el código del malware.

(3) Explotar los objetivos para impedir o causar un ciberataque DDoS (Distributed Denial of Service) en uno o varios sistemas elegidos.

(4) Despliegue de keyloggers para capturar todo lo que teclee el usuario/víctima normalmente para obtener contraseñas, códigos PIN, números de tarjetas de crédito, etc. y transmitirla a un sitio Web elegido por el malware. Este tipo de funcionalidad es similar a la del malware spyware y creepware. Desde la perspectiva del malware defensivo realizaría las acciones para evitar la instalación o desinstalar los keyloggers detectados para revertir el proceso ejecutado por el malware ofensivo.

(5) Pintarrajear y hacer cambios en sitios Web objetivo/víctima, por ejemplo el malware "Perl.Santy" sobre-escribe todos los ficheros con extensiones .htm, .asp, .jsp, .php, .shtm, etc. del servidor para que se generare el texto "Este sitio se encuentra pintarrajeado... ". El malware tras descubrir los objetivos a infectar utiliza todas sus técnicas de propagación para enviar dicho malware a esos sistemas de computación objetivos y entonces ejecuta su código en ellos. La transmisión del malware normalmente es automática mientras que su activación puede ser tanto automática como necesitar la ayuda del usuario humano (sabiéndolo o desconociéndolo). Desde la perspectiva del malware defensivo realizaría las acciones contrarias (tanto para impedir, esterilizar, desinfectar, inactivar al malware ofensivo como para deshacer los cambios de dicho malware ofensivo).

PUNTOS DE ACTUACIÓN DEL MALWARE INTELIGENTE OFENSIVO Y DEFENSIVO.

Los lugares y puntos de actuación-infección del malware inteligente (tanto ofensivo como defensivo) van cada día en aumento, son entre otros:

(1) En hardware: microprocesadores/microcontroladores. Explotando las vulnerabilidades de las CPUs, GPUs, DSPs, SIP (System In Package), FPGAs, ASIC, ASSP, SoC (System on Chip), etc. el malware inteligente puede ver información que debería estar protegida como claves que permanecen en memoria con privilegios. Las vulnerabilidades de los procesadores pueden ser explotados de forma local y remota. Las actualizaciones del firmware de chips como SIPs son FOTA (Firmware Over The Air) y son extremadamente vulnerables. Las vulnerabilidades en CPUs/SIMs afectan a cualquier sistema o sistema operativo incluso aunque no haya vulnerabilidades en el software y se hallen habilitadas todas las protecciones a nivel de sistema operativo. Así mismo, el parcheado de vulnerabilidades de los procesadores/microprocesadores puede necesitar la instalación de actualizaciones de firmware, actualizaciones del microcódigo del procesador, actualizaciones del sistema operativo, actualizaciones de la gestión de las máquinas virtuales, actualizaciones del software, de APPs, etc.

(2) En dispositivos USB. Los dispositivos USB pueden estar infectados y contener malware tanto en su software como en su firmware, lo que posibilita que suplanten otros dispositivos USB, que exploten el núcleo del sistema operativo y drivers y puedan incluso entregar malware software o firmware malicioso a otros componentes vulnerables no protegidos (periféricos, dispositivos de red, routers, impresoras 3D (por ejemplo, para fabricar alimentos sintéticos), plotters, PLCs, vehículos conectados/autónomos, drones, etc.).

(3) En tarjetas de red (NICs) y dispositivos PCI (Peripheral Component Interconnect). El bus PCI proporciona la conexión a una amplia variedad de componentes críticos como interfaces de red, GPUs (Graphics Processing Units), etc. El firmware de las tarjetas PCI y de los dispositivos conectados al PCI pueden infectarse tanto por código como por la red. Cuando se ven comprometidos pueden realizarse ciberataques DMA (Direct Access Memory) capaces de leer y escribir la memoria del sistema y ejecutar malware inteligente en el contexto del sistema operativo de la víctima. Los buses de los vehículos conectados (por ejemplo, red Can-bus) pueden infectarse desde dentro y desde fuera (vía satélite, antenas celulares 4G, 5G, etc., WiFi, Bluetooth, etc.) utilizando vulnerabilidades en continuo crecimiento.

(4) En componentes y módulos de los sistemas. Todo dispositivo o componente (DRAM, SRAM, GPUs, interfaces de red, drives, objetos IoT/IIoT/IoMT, etc.) dentro de un sistema se basa en firmware y podrá ser ciber-atacado (o ciber-defendido) por malware inteligente avanzado con resultados que dependen de las funcionalidades que transporte el malware ofensivo o el malware defensivo. El estándar para aumentar la ciberseguridad ETSI-EN-3030 645 establece mínimos de protección para productos de consumo IoT.

(5) En firmware crítico del sistema y de arranque (BIOS/Basic Input/Output System, UEFI/Unified Extensible Firmware Interface, EFI/Extensible Firmware Interface, MBR/Master Boot Record). El firmware crítico es el primer código que se ejecuta al arrancar y si está infectado puede afectar y trastornar al sistema operativo cambiando el código de arranque, parcheando el kernel del sistema operativo, comprometiendo hipervisores y máquinas virtuales. El firmware del sistema también puede utilizarse para entregar firmware infectado (de forma maliciosa o de forma defensiva) a otros componentes del sistema. El BIOS es firmware que maneja físicamente el dispositivo de computación se guarda en memoria flash y PROM e interactúa con el "bootloader" para despertar al sistema operativo (en smartphones con sistema operativo Android e iOS, en equipos Linux, Solaris, Windows, Unix, etc.).

(6) En controladores de gestión de la tarjeta base/madre (BMC/Baseboard Management Controllers). Los BMCs proporcionan gestión fuera de banda en servidores y suelen tener su firmware, recursos y red independiente. El malware inteligente (tanto ofensivo como defensivo) actuando sobre BMCs posibilita el control completo del servidor y de todos los servicios y datos de los niveles superiores que contiene y puede incluso bloquear permanentemente dicho servidor.

(7) En el SMM (System Management Mode). El SMM y firmware similar se enfoca en la operación en tiempo de ejecución del dispositivo y permite que el sistema gestione el comportamiento de bajo nivel del sistema completamente independientemente del sistema operativo. Esto puede permitir al malware inteligente el acceso virtualmente sin trabas al sistema sin el conocimiento y consentimiento del sistema operativo.

(8) En el firmware TXE (Trusted Execution Engine tipo driver), ME (Management Engine), CSME (Converged Security and Management Engine). El ME (en Intel) es un componente común integrado en computadores personales para permitir la gestión fuera de banda del dispositivo. El ME también se denomina TXE y CSME en otras plataformas. El firmware dentro de ME incluye tecnología denominada AMT (Active Management Technology) y sus funciones y capacidades de red son completamente independientes del sistema operativo del dispositivo de computación asociado y los puede utilizar el malware inteligente (ofensivo o defensivo) para funciones y actividades como, por ejemplo, C&C (Command and Control), filtración de datos, establecer canales subliminares y esteganográficos, funciones de inactivación, etc.

(9) En hardware. En forma de troyanos hardware, en circuitos electrónicos maliciosos (o de defensa) activables, en chips patológicos, en electrónica modificada en la cadena de suministro, etc.

(10) En software. En forma de programas (maliciosos-ofensivos o de defensa) compuestos por instrucciones de lenguajes tanto conocidos como diseñados a medida o desconocidos como, por ejemplo: lenguaje máquina, c##, java, fortran, cobol, phyton, etc. Algunos malware ofensivos son The Moon, Santori, CryCryptor, Petya, troyano Peacomm, backdoor Rustock.B, etc. El malware (ofensivo y defensivo) puede actuar (negativa o positivamente) contra el correo electrónico, plugs-in, APIs, macros, scripts, mensajería instantánea (whatsapp, telegram, dust, wickr, threema, confide, tok, cyphr, silence, line, signal, pryvate (con RSA 4096), etc.), redes sociales, video conferencias, etc. El software es muy propenso a vulnerabilidades (que son vectores de ciber-ataque), las APPs son código vivo que evoluciona con el tiempo según las necesidades de las entidades de los ecosistemas IT/OT, por lo que cualquier cambio tiene el potencial de introducir vulnerabilidades que exponen la APP/APIs y su entorno IT/OT.

(11) En memoria (flash, RAM volátil y no volátil, etc.). Caso del malware sin ficheros en memoria principal.

(12) En redes. Mantener la confidencialidad de las transmisiones, sobre todo inalámbricas y de los almacenamientos de información (discos, nubes, satélites, drones, etc.) y datos sensibles-críticos (financieros, de salud, de negocios, etc.) se ha convertido actualmente en una quimera.

(13) Sobre datos. Actuación sobre los datos (violando su soberanía) en entornos muy diversos como nubes (edge-fog-cloud), BigData/Analytics, IoT, IIoT, IoMT, sistemas de contenedores (como Docker), etc. incluso con protección de acceso a la nube CASB, con cifrado (con el sistema BYOK (Bring-Your-Own-Key)), con cifrado totalmente homomórfico multicapa para nubes, etc.

FORMAS DE EXPANSIÓN DEL MALWARE OFENSIVO-DEFENSIVO.

El malware inteligente (tanto ofensivo como defensivo) progresa, se posiciona y evoluciona gracias a infinidad de estrategias, técnicas, tácticas, mecanismos, procedimientos, etc.

Entre dichas opciones se encuentran las vulnerabilidades

(por ejemplo, el malware se camufla en driver como srtsp.sys). La vulnerabilidad SIMjacker (vulnerabilidad registrada en el CVE (Common Vulnerabilities and Exposures) del NIST como CVE-2019-16256/CVE-2019-16257 y por la GSM Association en su proceso CVD (Coordinated Vulnerability Disclosure) como CVD-2019-0026); puede ser explotada en las tarjetas SIM de los móviles que llevan pre-instalada una APP/Applet Java denominada "S@T browser" al recibir del malware/ciber-atacante un SMS denominado "OTA SMS"; esta vulnerabilidad permite ciber-atacar personas, realizar un seguimiento de las localizaciones de la víctima, realizar fraude, espionaje, fuga de datos, DoS, etc.; otra vulnerabilidad similar es "WIBattack" en este caso debida a una APP instalada denominada "WIB APP"). Vulnerabilidades como el almacenamiento de datos de forma no segura en móviles es una de las vulnerabilidades más preocupantes de los "Top-10 de OWASP Mobile", incluye los datos de autenticación que se almacenan de forma no segura.

Vulnerabilidades que permiten el acceso no autorizado para crear archivos y para realizar operaciones sobre datos de proceso y subproceso.

Las vulnerabilidades en el código en APPs al no estar protegidas contra inyección de código y reempaquetado, falta de ofuscación de las APPs permite encontrar datos importantes como nombres de usuario, contraseñas, geolocalización, información personal, financiera de salud y correspondencia, existencia de aplicaciones en red que utilizan cifrado SSL con versiones desactualizadas de OpenSSL, utilizar vulnerabilidades en las aplicaciones más comunes para compartir información (como correo electrónico, mensajería instantánea, redes sociales y video), fuga de información en APPs, transmisión insegura de datos confidenciales-sensibles, aceptar iniciativas BYOD (Bring Your Own Device) donde se permitan dispositivos obsoletos, sin AV, no actualizados, con vulnerabilidades y APPs infectadas, implementación incorrecta de la caducidad de sesión, comunicación insegura entre procesos, protección deficiente e insuficiente ante ciberataques de fuerza bruta, configuración insegura de aplicaciones/APPs, datos confidenciales almacenados en el código fuente de la APP, admisión de teclados de terceros, carencia de "certificated-pinning", validación no existente o insuficiente de entradas, existencia de exploits en Office MS, vectores de infección/exploits basados en ficheros infectados de procesador de textos como Word (macros infectadas), Pdf, HLP, HWP (Hangul Word Processor), etc. deficiente gestión de credenciales, aprovechamiento y abuso de exceso de privilegios, abuso de APIs no auditadas, errores de gestión del buffer, vulnerabilidades que habilitan la inyección SQL, deficiencias y fallos en los sistemas de verificación biométricos (tanto monomodales como multimodales), algoritmos de cifrado deficientes-inadecuados, XSS (Cross-Site-Scripting), existencia de conexiones privilegiadas (por ejemplo, muchas APPs exigen que el usuario conceda máximos privilegios, al liberar un dispositivo se crean máximos privilegios caso de jailbreak/root, ciertos Proveedores de Servicios Gestionados o MSPs exigen el acceso privilegiado a la infraestructura del cliente (lo cual genera vulnerabilidades), validación incorrecta de certificados, almacenamiento de información sensible en texto sin formato, calidad deficiente del código, no integrar las prácticas de ciberseguridad lo antes posible en el diseño y ciclo de desarrollo del software, deficiencias en la configuración de mecanismos de autenticación de correo electrónico como SPF(Sender Policy Framework), DKIM (Domain Keys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting and Conformance), fallos en la configuración de servidores DNS, no utilizar DNS-Sec.

Los sistemas embebidos presentan una superficie de exposición a ciberataques de malware inteligente cada día mayor debido a que presentan un creciente número de vulnerabilidades que los malware inteligentes están preparados para aprovechar y sacar el máximo partido posible, como, por ejemplo:

(**1) A nivel de sensores y actuadores**, aprovecharse del hardware obsoleto, débil, con funcionalidades muy limitadas, etc.

(2) A nivel de red, un orden incorrecto de las operaciones de conexión a red, existencia de datos sin protección, fácil saturación del ancho de banda, facilidad de afección al jitter, al retardo y ralentización, facilidad para intrusiones de red basados en drones, facilidad para manipulaciones maliciosas del QoS, etc.

(3) A nivel de sistema de ficheros, manipulación del path vulnerable, uso de ficheros temporales no seguros, toctou (race condition), etc.

(4) A nivel de entrada del usuario (no validar adecuadamente las entradas de datos, caso de la inyección de código), facilidad de acceso a los datos.

(5) A nivel de software de terceras partes, ejecución de un binario/carga de librerías desde un camino relativo que puede ser controlado por un malware/ciber-atacante externo, facilidad para contaminar datos, dlls, macros, scripts, etc., facilidad para contaminar la cadena de suministro, etc.

(6) Vulnerabilidades en HSM (Hardware Security Module), en cifradores (simétricos y asimétricos), en unidades de esteganografía, en unidades de firma digital-hash y sellado temporal, en generadores de números pseudo-aleatorios (PRNGs) (que generan una salida aleatoria determinista a partir de una semilla constante), uso de memorias con datos sensibles sin limpiar adecuadamente antes de liberarla, etc.

(7) Ciertas funcionalidades de los malware inteligentes explotan la infinidad de vulnerabilidades existentes. Por ejemplo, la vulnerabilidad crítica CVE-2020-1350 permite tomar el control completo de los sistemas y redes. La funcionalidad del malware denominada gusano (o worm) se caracteriza por que se reproduce a sí mismo sobre los dispositivos de computación en una red sin necesitar de infectar y hospedarse específicamente en ficheros.

En la actualidad se detecta una evolución creciente del ciberriesgo debido al malware en nuestro mundo donde la Internet completa (IoE/Internet of Everythings) lo conecta todo. La ciberseguridad nunca ha sido más necesaria y crítica y es un componente clave de la sostenibilidad.

Lo que sucede en nuestra sociedad ante una ciber-pandemia basada en malware inteligente ofensivo, si no hacemos nada, es la llegada del caos y la destrucción de nuestra forma de vivir. El malware defensivo esta aquí para quedarse y protegernos.

CONSIDERACIONES FINALES

El malware inteligente defensivo esta, diseñado para inactivar, neutralizar, anular, bloquear, eliminar, etc. al malware ofensivo.

Las perspectivas disruptivas en torno al malware inteligente defensivo pueden mostrar un futuro mejor para nuestra sociedad. El malware inteligente defensivo esta, diseñado para vigilar, inhabilitar, derrotar, bloquear, cazar a todo tipo de entidades dañinas (o malware ofensivo).

Es evidente que muchos malware ofensivos serán eliminados por malware defensivo, pero, ¿quién ganará la batalla a largo plazo? Actualmente, una vez que se extiende el malware éste es imparable. La variante inicial se va mejorando y se van generando nuevas variantes más empoderadas y poderosas.

Desde la variante principal se generan múltiples cambios, por ejemplo, de ganancia de funciones, todos no detectables. Hay que despertar y hacer algo efectivo, hay que prevenir, ser proactivo, predictivo, hay que auto-inactivar y recuperar.

Las nuevas generaciones de malware inteligente defensivo y las correspondientes infecciones malware no detectables definirán nuestra Sociedad (más digital, más conectado a Internet, más basada y definida por software y datos, IoT/IIoT/IoMT, smartphones, PCs, wearables, tablets, vehículos, gadgets, nubes/cloud-fog-edge, PLCs, SCADA, ICS, CPS, SRD (Software Defined Radio), CRM/IT, BDs, ERP/IT, etc.).

El malware inteligente puede ser ciber-endémico si afecta a un cierto país-ecosistema o ser ciber-pandémico si afecta a todos los países.

El malware inteligente (tanto ofensivo como defensivo) es una ciber-arma modular, persistente, no detectable, asintomática, con ganancia de funciones, auto-control y capacidades de comunicación subliminar con el exterior/interior a través de canales esteganográficos subliminares ocultos no detectables, etc.

La compañía Positive Technologies tras analizar-investigar la protección de diversas APPs conocidas tanto para el sistema operativo Android de Google (descargadas de Google Play) como para el sistema operativo de Apple iOS (descargadas de APP Store) concluye que gran parte de las vulnerabilidades detectadas en APPs pueden explotarse sin acceso físico al dispositivo móvil.

Así mismo destaca que por parte del cliente las APPs se encuentran vulnerabilidades de almacenamiento de datos no seguro; de transmisión no segura de datos confidenciales; de implementación incorrecta de la caducidad de sesión; de comunicación no segura entre procesos; de datos confidenciales almacenados sin protección en el código fuente de la APP; de insuficiente protección ante ciber-ataque por fuerza bruta; de configuración no segura de la aplicación.

La totalidad de las APPs analizadas contenían vulnerabilidades de código, indefensión contra inyección de código y de reempaquetado. Las APPs analizadas permiten realizar una captura de la pantalla de las aplicaciones como información de tarjetas y saldos de cuentas.

Desde el lado del servidor que usa dichas APPs la totalidad de las APPs analizadas permiten ciber-ataques a usuarios, en algunas se permite el acceso no autorizado a las aplicaciones, en otras se permite el acceso no autorizado a la información de configuración, en otras se permite el acceso no autorizado a los datos del usuario y en otras se permite la interrupción del funcionamiento de la propia APP.

La IoT posibilita conectar los dispositivos de nuestra vida diaria a Internet y entre si para intercambiarse información valiosa.

La IoT nos permite desde un smartphone y desde cualquier lugar y hora desbloquear puertas, regular temperatura, transmitir datos de salud, etc.

Según Statista para el 2023 habrá 51,11 mil millones de dispositivos conectados en todo el mundo ("que gozada para el malware ofensivo" y un desafío para el malware defensivo). ■

REFERENCIAS

- *Areitio, J. "Seguridad de la Información: Redes, Informática y Sistemas de Información". Cengage Learning-Paraninfo. 2020.*
- *Areitio, J. "Control del creciente empoderamiento del malware: identificación y exploración de los aspectos clave del malware". Revista Conectrónica. Nº 240. Febrero 2021.*
- *Areitio, J. "Peligro del desconocimiento de la existencia de contaminación malware tendente a situaciones ciber-epidemiológicas globales muy graves". Revista Conectrónica. Nº 241. Marzo-Abril 2021.*
- *Areitio, J. "Puntualizaciones sobre el malware, ciber-pandemias y escenarios críticos ciber-epidemiológicos. Protección contra el malware defensa anticipada". Revista Conectrónica. Nº 242. Mayo-Junio 2021.*
- *Areitio, J. "Confluencias entre malware, vulnerabilidades y exploits: indicadores de infiltración, superficie-vector de infección y peligrosidad malware". Revista Conectrónica. Nº 243. Julio 2021.*
- *Areitio, J. ""Adaptación a la variabilidad de los eventos de infección malware no detectados en todo tipo de escenarios, entornos y ecosistemas actuales"". Revista Conectrónica. Nº 244. Septiembre 2021.*
- *Sole, R. and Elena, S.F. "Viruses as Complex Adaptive Systems". Princeton University Press. 2018.*
- *Astra, J.D. "Malware". Shadow Alley Press. 2021.*
- *Ryan, M. "Ransomware Revolution: The Rise of a Prodigious Cyber Threat". Springer. 2021.*
- *Karbab, E.B., Debbabi, M. Derhab, A. and Mouheb, D. "Android Malware Detection using Machine Learning: Data Driven Fingerprinting and Threat Intelligence". Springer. 2021.*
- *Stanford, E. "Crypto Wars: Faked Deaths, Missing Billions and Industry Disruption". Kogan Page. 2021.*
- *Stiennon, R. "Surviving Cyberwar". Bernan Press. 2021.*
- *Mohanta, A. and Saldanha, A. "Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware". Apress. 2020.*
- *Calder, A. "The Ransomware Threat Landscape: Prepare for, Recognise and Survive Ransomware Attacks". IT Governance Publishing. 2021.*
- *David, A.P. "Ghidra Software Reverse Engineering for Beginners: Analyze, Identify, and Avoid Malicious Code and potential threats in your Networks and Systems". Packt Publishing. 2021.*
- *Ludwig, M. "The Giant Black Book of Computer Viruses". American Eagle Books. 2019.*
- *White, G. "Crime Dot Com: From Viruses to Vote Rigging, How Hacking Went Global". Reaktion Books. 2020.*

Redes de Acceso Abierto - Economía colaborativa y telecomunicaciones

Las redes de acceso abierto, o redes neutras, ayudan a aprovechar los beneficios de compartir economía en la industria de las telecomunicaciones acelerando la transformación digital. La economía colaborativa ha atravesado muchas industrias tradicionales. Empresas como Uber se han convertido en líderes del mercado aprovechando este modelo donde la economía colaborativa está cambiando la forma de entender el consumo con eje en las nuevas tecnologías y se ha ido consolidando en una innovadora tendencia.

Artículo cedido por Furukawa

Para el acceso de movilidad en Latinoamérica tenemos varias redes celulares para servicios de voz y datos y también proveedores de fibra óptica que construyen redes cerradas más modernas y en algunos casos privadas. La duplicación de redes aumenta los costos para los clientes. Desde una perspectiva, al ser propietarios de la red de un extremo a otro, también somos propietarios del cliente, sin embargo, el modelo comercial de acceso abierto lo cambia todo al crear una red única de alto rendimiento compartida tanto por los proveedores de la red como por los usuarios públicos y privados.

Se trata, en esencia, de un sistema digital vial de alto rendimiento y performance. Así como todos los vehículos que utilizan una autopista comparten un único sistema vial unificado y optimizan su uso a través de, por ejemplo, la planificación de los viajes con información en tiempo real, una red de acceso abierto comparte el transporte de la misma forma. Las redes de acceso abierto separan y segmentan los servicios diferenciados física y lógicamente. El propietario de la red no es exactamente un proveedor de servicios, inclusive en el modelo comercial de acceso abierto no se requiere la participación taxativa o la propiedad gubernamental de la red, algunas redes privadas pueden operar y lo hacen en este modelo.

Características de las Redes Neutras

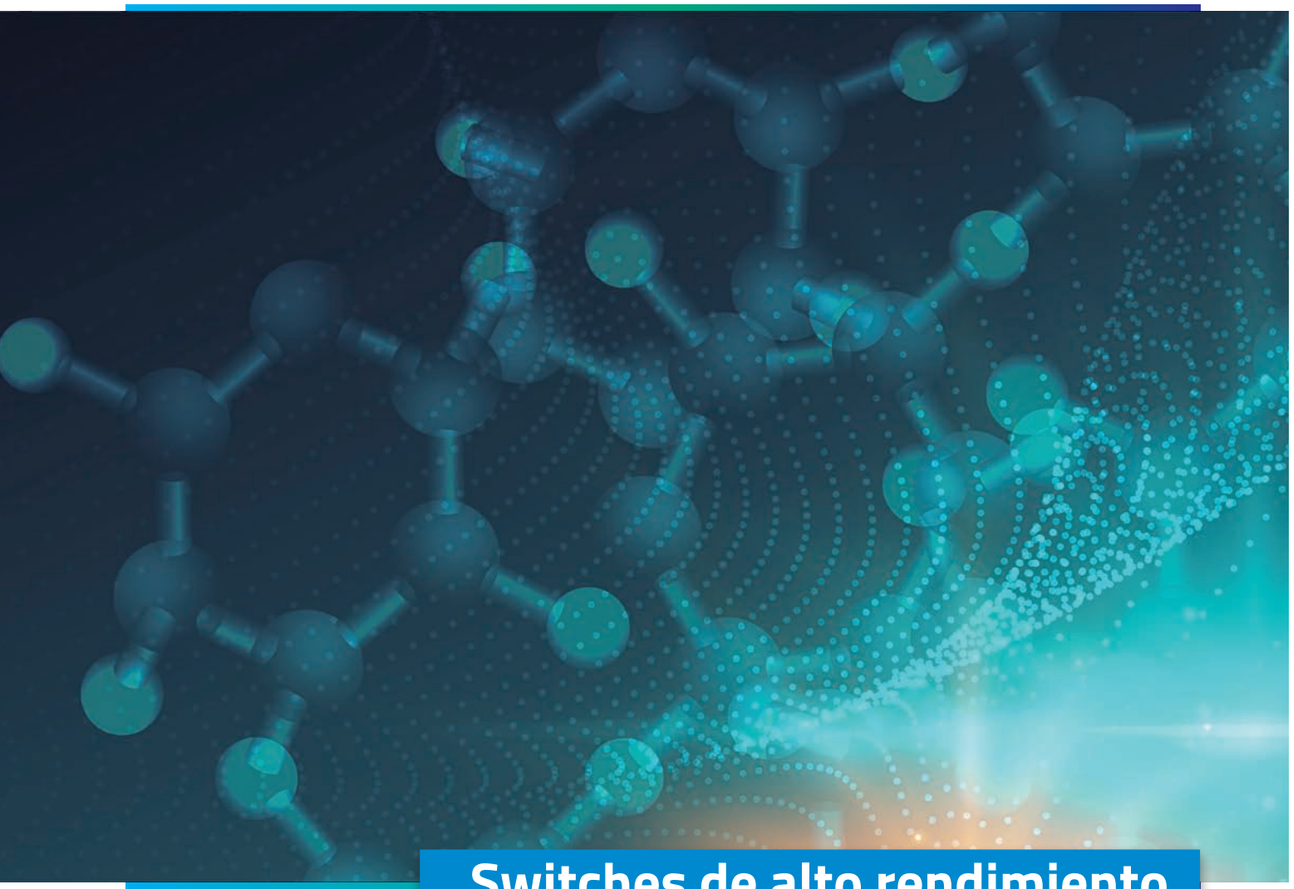
- El administrador de la infraestructura de red asegura que cada proveedor de servicios tenga el ancho de banda necesario para brindar el nivel esperado a cada cliente.
- La combinación de infraestructura de red pasiva y activos ofrece suficiente calidad de servicio (QoS), aumenta el rendimiento y reduce la latencia para determinados servicios.
- Los clientes compran el servicio o los servicios de su elección a uno o más proveedores.
- Los proveedores de servicios contratan el uso de la infraestructura de red para vender múltiples servicios con distintas variantes a sus propios clientes.

En resumen, un propietario de red proporciona el transporte local a varios proveedores de servicios independientes y cada proveedor ofrece, a su vez, múltiples servicios a precios competitivos a sus propios clientes.

Por su naturaleza la red neutra se impone y su velocidad de crecimiento en términos de CAPEX prescinde de un desembolso inmediato. Puede soportar servicios y aplicaciones que anteriormente podían haber sido demasiado costosos. Por ejemplo, una entidad estatal podría usar la red de acceso abierto para desplegar un sistema de ITS, controlar las señales de tráfico, administrar las luces de las calles que ahorran energía, respaldar un sistema de cámaras de seguridad en áreas inseguridad y tener monitoreo en tiempo real para recopilar y analizar datos.

En el pasado, las costosas redes propietarias hacían que este tipo de aplicaciones de Smart City fueran prohibitivamente caras, sin embargo, nuevos modelos emergentes abrieron alternativas.

El crecimiento es constante en el mercado de banda ancha y acompaña a las grandes empresas en búsqueda de alternativas para conseguir una mayor eficiencia económica en el uso de la infraestructura de red. Es sumamente importante para Furukawa brindar red de fibra óptica de óptima calidad con modelos innovadores, y por eso cuenta con ingeniería, consultoría de diseño para los proyectos. Entendemos que además de un producto de calidad, el despliegue debe de ser el más adecuado, según los estándares internacionales. Podemos apoyar en la definición de la topología del proyecto hasta la implementación de los productos y sistemas, por medio del programa “full service” donde la economía de los servicios de transporte sobre redes de acceso abierto marcará la diferencia, vale la pena conocer en profundidad este modelo de economía colaborativo. ■



Switches de alto rendimiento para la red 10 Gigabit del Clúster de Química Computacional de la Universitat de Barcelona

D-Link y su partner SIE (Sistemas Informáticos Europeos) han instalado Switches Enterprise de D-Link en el clúster computacional del Institut de Química Teòrica i Computacional de la Universitat de Barcelona (IQTCUB)

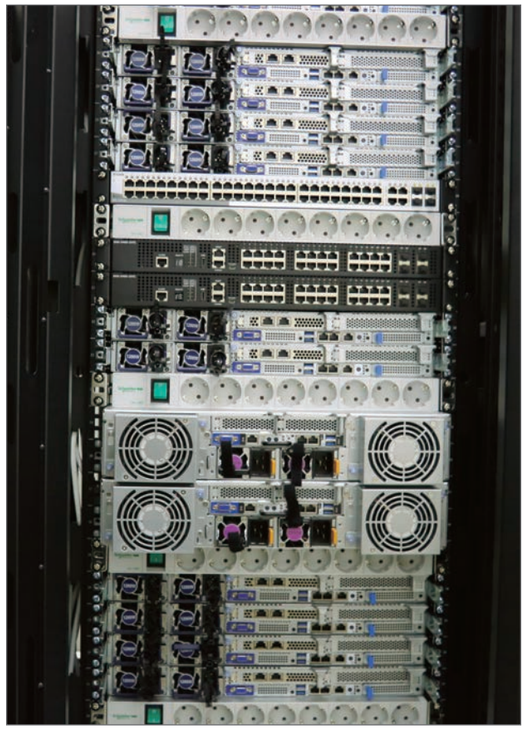
El IQTCUB es uno de los centros más prestigiosos en la investigación de varios campos de la química teórica y computacional. La actividad realizada en el IQTCUB abarca el desarrollo de métodos y herramientas computacionales, la aplicación de varias técnicas de estructuras electrónicas, ciencia de los materiales, el estudio de la reactividad y la dinámica en reacciones químicas, así como de sistemas biológicos y materia blanda. Según su administrador, Jordi Inglés, en el centro trabajan más de 100 investigadores de múltiples nacionalidades y anteriormente al nuevo clúster ya contaba con una potencia de cálculo global de casi 4.000 cores y 37TB de memoria RAM.

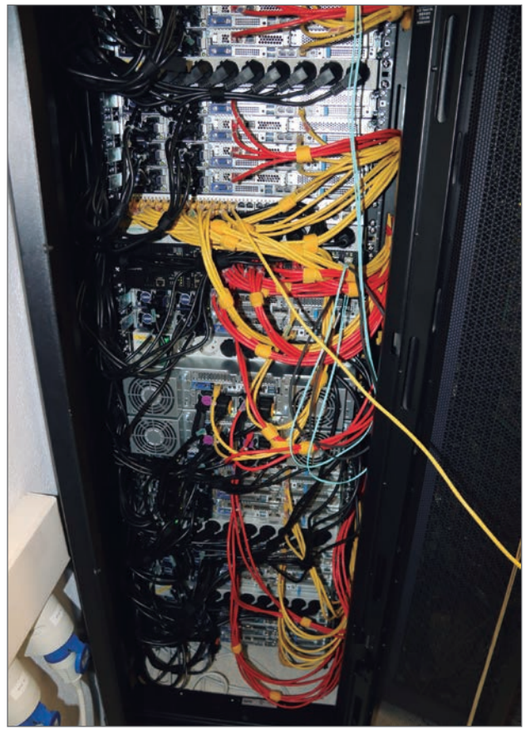
En 2017, el instituto recibió el premio María de Maeztu, concedido por la Agencia Estatal de Investigación de España, que además proporcionó fondos de inversión para expandir las capacidades técnicas destinadas a mejorar la investigación del centro. De esta forma, se decidió aumentar tanto el centro de datos como la capacidad de procesamiento, añadiendo en este caso un nuevo clúster, conocido como IQTC09, que ha aumentado en un 40% el número de núcleos de cálculo y un 70% la memoria RAM.

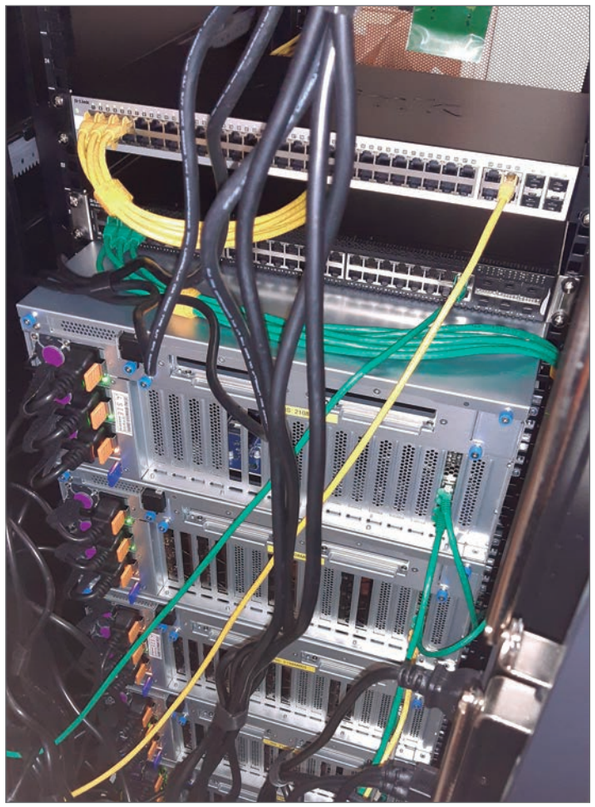
Esta capacidad adicional ha permitido al instituto abrir la investigación a nuevos campos, desde la dinámica molecular, inteligencia artificial, machine learning, diseño de estructuras moleculares en 3D, así como otras aplicaciones diseñadas en entornos virtuales para que los investigadores gestionen e interactúen en un entorno 3D con gafas de realidad virtual.

El clúster se compone de 1.664 núcleos a 2.9 GHz y 26 TB de memoria RAM, desplegados en 26 Nodos desarrollados por SIE Ladón, partner del Programa de Canal VIP+ de D-Link. SIE (Sistemas Informáticos Europeos), es una empresa con más de 30 de experiencia y especializada en soluciones HPC (High Performance Computing). Ya ha instalado más 20.000 Cores de red HPC, así como 60 clúster computacionales en centros de investigación públicos y privados.

Los nodos del clúster se basan en plataformas Gigabyte con procesadores AMD Rome. Estos nodos están integrados en una red 10 Gigabit conectada a fibra hacia el exterior para la distribución hacia los dispositivos conectados tales como ordenadores y estaciones desktop y para ello se han utilizado switches D-Link DXS-3400, una familia de Switches 10 Gigabit de nivel Managed Layer 3 diseñada para entornos Top of the Rack, Campus y Data Center, así como distribución gracias a su apilado físico y amplia densidad de puertos 10 Gigabit. En concreto, en el rack del nuevo clúster computacional se han instalado dos unidades del modelo DXS-3400-24TC. En un esquema de red tan exigente como un clúster computacional era necesario contar con Switches de red de máximo nivel en cuanto a su capacidad de conmutación de Nivel 3, en especial por la implementación de routing en el propio switch, reduciendo así los cuellos de botella que podría generar un router convencional y diseñado para los patrones de tráfico del modelo 20/80, forzando a la mayor parte del tráfico a cruzar los límites de la subred, un sistema ya habitual ante la concentración de servidores en granjas o sistemas cluster de altas prestaciones a los que todos los usuarios deben acceder desde sus respectivas subredes. Gracias a sus funcionalidades de Inter VLAN Routing, Stacking mediante VRRP, Lossless Ethernet (DCB) para ultra baja latencia, Ethernet Ring Protection Switching (ERPS), Switch Resource Management (SRM), los D-Link DXS-3400-24TC garantizaban el rendimiento necesario en el acceso desde el exterior al clúster de computación. La redundancia también era un factor clave, y para ello los D-Link DXS-3400 disponen de ventiladores y fuentes de alimentación intercambiables en funcionamiento (Hot-Swap), aparte de poder configurar el apilado de unidades (hasta 4 Switches) para redundancia. Respecto a su interfaz de gestión, cuentan con







EL CLÚSTER SE COMPONE DE 1.664 NÚCLEOS A 2.9 GHZ Y 26 TB DE MEMORIA RAM, DESPLEGADOS EN 26 NODOS DESARROLLADOS POR SIE LADÓN, PARTNER DEL PROGRAMA DE CANAL VIP+ DE D-LINK

interfaz web y también con acceso por puerto consola para su gestión mediante el estándar de comandos CLI (Full CLI).

En setiembre de 2021 se ha completado una nueva ampliación basada en el Switch D-Link DXS 3610-54T/SI (una familia que viene a evolucionar los DXS-3400 con Open Flow y SDN, puertos 10 Gigabit en cobre y fibra, así como puertos QSFP+/QSFP28 de 40G/100G) y nuevas GPUs. Tras esta actualización, ha pasado de ser una instalación de CPUs a tener 17 GPUs con más de 330 TFlops en simple precisión y más de 178 mil núcleos de CUDA. Además, están interconectados por un HP ProCurve 5406 2l que permite que los demás miembros de la universidad puedan conectarse y gracias al software gestor SNMP de D-Link, D-View 7, se puede tener una monitorización conjunta de los dos clúster.

También era necesario crear una red Gigabit para las comunicaciones IPMI y GSM y para ello se ha instalado un D-Link DGS-1210-48, un Switch Smart Gigabit con 48 puertos Gigabit y gestión de Nivel 2 completa y Nivel 3 Lite con static routing. ■

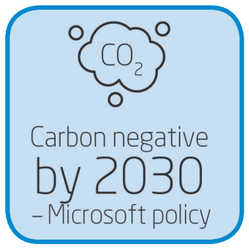
Baterías para centros de datos sostenibles de Microsoft

La tecnología de Saft está desempeñando un papel importante en una nueva asociación estratégica entre el gigante tecnológico Microsoft y la compañía TotalEnergies.

El acuerdo firmado en marzo de 2021 intercambiará experiencia y servicios tecnológicos. Apoyará la transformación digital de TotalEnergies, así como la ambición de Microsoft de convertirse en carbono negativo para 2030. En virtud del acuerdo, Microsoft evaluará la tecnología de Saft en dos áreas para reducir la huella de carbono de sus centros de datos.

Sustituir Grupos Diesel

Microsoft ha anunciado el objetivo de eliminar su dependencia del combustible diésel para 2030. Se utiliza en generadores para proporcionar energía de respaldo a los centros de datos. Además de aumentar su huella de carbono, los generadores diésel requieren un mantenimiento periódico, grandes depósitos de combustible in situ y pueden estar sujetos a normativas que limitan sus operaciones.



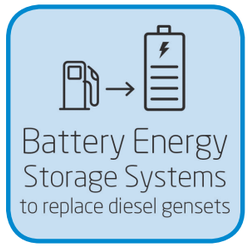
Microsoft considera a Saft como socio al tener soluciones de almacenamiento de energía de batería (BESS), desde su contenedor de alta energía Intensium Max 20 hasta el diseño e instalación completos de BESS, incluyendo ingeniería, PCS y transformadores. La madurez y experiencia de Saft en tecnología de Li-ion, así como en el desarrollo de software en gestión de energía, ayudarán a incorporar las capacidades conectadas a la red como servicios adicionales a los requisitos de backup.

Para lograr un sistema de respaldo de mayor duración, será necesario desarrollar sistemas de batería con una gran capacidad de almacenamiento de energía y sistemas de control avanzados. Los expertos de Saft están trabajando ahora con Microsoft para evaluar la viabilidad a largo plazo de tales sistemas. Estos tendrán que estar en una escala similar a algunos de los proyectos de almacenamiento de energía conectada a la red al tiempo que se satisfacen las necesidades particulares de los centros de datos.

Especificación de la sostenibilidad con Flex'ion Gen 2

Microsoft también prevé la posibilidad de que nuestras baterías de respaldo más recientes mejoren la sostenibilidad de sus centros de datos. El objetivo es utilizar nuestro sistema Flex'ion Gen 2 para ahorrar energía, garantizar la máxima se-

guridad, autoalimentación y monitorización remota. Nuestros expertos están trabajando en estrecha colaboración con los ingenieros de los centros de datos de Microsoft para formar parte de sus especificaciones, así como con los proveedores de SAIs preferidos. “Hemos lanzado el sistema Flex'ion Gen 2 en noviembre de 2020 para proporcionar un cambio gradual en el rendimiento de la energía de las baterías UPS sin comprometer la seguridad”, afirmó François Danet, director de ventas y desarrollo de negocios en Saft.



“Pero también ofrece beneficios de sostenibilidad. Microsoft ve oportunidades para reducir los requisitos de refrigeración en los centros de datos. Esto se debe a que el sistema Flex'ion Gen 2 se basa en la electroquímica de Li-ion de Saft, que puede funcionar a 35 ˚C con el nivel adecuado de normas de seguridad. Como resultado, los operadores del centro de datos pueden ahorrar energía y agua que antes se necesitaba para refrigerar la sala de baterías y, por tanto, reducir las emisiones de CO2. Otra ventaja es la reducción de materias primas críticas como el cobalto, gracias a nuestra química basada en LFP (fosfato de hierro de litio).

Otra característica útil para Microsoft es el sistema autoalimentado de supervisión de baterías. El sistema se alimenta de la propia batería, por lo que es independiente de la alimentación de red y tiene la misma disponibilidad que el propio sistema de respaldo. Esto es importante para los operadores del centro de datos, ya que optimiza la disponibilidad del sistema.

Densidad de potencia como sostenibilidad

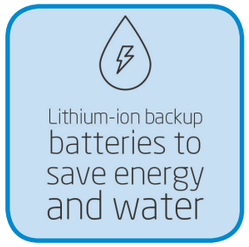
Si bien puede no parecer obvio a primera vista, la alta densidad de potencia del sistema Flex'ion Gen 2 libera otro beneficio de sostenibilidad. El sistema de alto rendimiento energético en un espacio reducido minimiza el espacio del SAI. A su vez, esto reduce el tamaño del edificio del centro de datos en todos los niveles, desde la base hasta el techo.

“Hay una cantidad significativa de CO2 incrustados en el acero y el hormigón que se utilizan para la construcción”, dice François, “El uso de un sistema de baterías con alta densidad de potencia puede reducir los requisitos de ingeniería civil. Como alternativa, simplemente puede liberar espacio para otros servicios”.

Con una densidad de potencia de 220 kW por armario, el sistema Flex'ion Gen 2 ofrece alrededor de un 40% más de rendimiento que la primera generación de Flex'ion.

Otro factor importante para reducir la huella total del SAI es la seguridad. Debido a su alto nivel de seguridad (estándar UL 9540A), Flex'ion Gen 2 no necesita que los ingenieros de centros de datos incluyan una separación de aire de aproximadamente 1 metro (tres pies) entre armarios ni protección contra incendios. Esto suele ser necesario para la seguridad contra incendios cuando se utilizan otros sistemas de batería de Li-ion.

Mirando al futuro



Con varias oportunidades para explorar, la asociación entre las compañías TotalEnergies y Microsoft será interesante de ver. Microsoft ya ha adjudicado a TotalEnergies un contrato para suministrar 47 MW de energía renovable a instalaciones eléctricas en España. Y mirando hacia el futuro, los socios están trabajando juntos para combinar tecnologías emergentes y soluciones digitales en un enfoque que acelerará el camino de la red cero. ■

Analizador de espectro SPECTRAN V6 con certificación MIL

El nuevo analizador de espectro en tiempo real SPECTRAN® V6 MIL de Aaronia se utiliza en todos los casos en los que se exige la máxima velocidad de medición, ancho de banda en tiempo real, robustez y estabilidad. Por ejemplo, para la protección de objetos, la supervisión de VIPs o conferencias, la defensa contra ataques de escucha, la supervisión de accionamientos o incluso para los técnicos de servicio que comprueban la calidad de las antenas de transmisión de telefonía móvil.

Para ello, el SPECTRAN® V6 MIL ha sido probado y certificado de forma independiente según MIL-STD-810G e IP65. La carcasa endurecida de alta calidad se ha diseñado para que el analizador sea a prueba de golpes, vibraciones y caídas. Un sellado adicional protege completamente el sistema contra el polvo y la humedad. Ya sea para la contrainteligencia, la vigilancia de seguridad o el uso intensivo en exteriores, el SPECTRAN V6 MIL permite su uso incluso en las condiciones más difíciles, por ejemplo, en el desierto, en la selva o en las regiones polares. Esto se debe a que el SPECTRAN® V6 MIL sigue siendo plenamente operativo a temperaturas desde -20 °C a +60 °C y, además, ofrece una enorme capacidad de almacenamiento para grabaciones a largo plazo.

El SPECTRAN® V6 MIL no sólo es un potente analizador de espectro en tiempo real y de barrido con un ancho de banda en tiempo real de 245 MHz (I/Q), que barre 6 GHz en menos de 5 msg (1 THz/sg), incluido el registrador IQ. También es un equipo portátil bien equipado que puede utilizarse como un ordenador normal con Windows si es necesario. Para ello, está equipado con un procesador Intel® Xeon® E-2176, 64 GB de RAM, una tarjeta gráfica dedicada NVIDIA GTX 1050 con 4 GB de memoria GDDR5, así como un disco duro de sistema SSD de 1 TB y un almacenamiento de grabación SSD de 2 TB u 8 TB. Por lo tanto, no se necesita otro ordenador para posibles tareas adicionales.

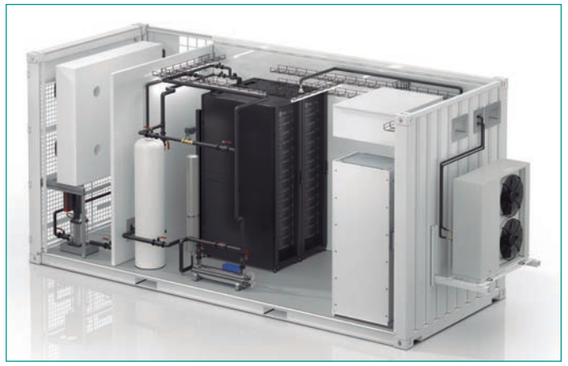
Ha sido desarrollado para el análisis del espectro de banda ancha. El analizador de espectro portátil para exteriores se entrega con el software RTSA-Suite PRO preinstalado. En combinación con este software, es posible monitorizar un amplio rango de frecuencias en tiempo real o barrer la banda completa de 10 MHz a 6 GHz (opcionalmente 8 GHz) en muy poco tiempo utilizando la función de barrido superrápido. Esto permite detectar y localizar de forma fiable incluso las señales más cortas con una antena direccional adecuada. Al mismo tiempo, el RTSA-Suite PRO permite visualizar y analizar las señales en tiempo real de muy diversas maneras. El software se actualiza constantemente y se amplía con nuevas funciones. De este modo, se pueden encontrar y desactivar con precisión los dispositivos de interferencia o de escucha y seguimiento.

El bajo PDI del SPECTRAN® V6 MIL es ideal para detectar micrófonos ocultos, dispositivos externos u otros dispositivos de vigilancia. Se puede configurar una función de alarma adicional de forma que avise en cuanto aparezcan señales llamativas, por ejemplo en los rangos de frecuencia de 2G, 3G, 4G, 5G, WLAN 2.4 o WLAN 5. La grabación puede continuar incluso cuando la pantalla está apagada. De este modo, la vigilancia puede continuar de forma discreta y se puede emitir una señal acústica a través de la salida de audio (o del altavoz) si se activa uno de los disparadores automáticos. Además, existe la opción de demodulación de audio si se desea supervisar la comunicación por radio. Gracias a la ampliación opcional del disco duro, es posible almacenar a largo plazo todos los datos brutos I/Q en cualquier momento.

El SPECTRAN® V6 MIL ahora también está disponible en las variantes SPECTRAN® V6 MIL PRO y SPECTRAN® V6 MIL ENTERPRISE.

Centro de datos de refrigeración líquida EcoStruxure™ Modular Data Center

Schneider Electric ha anunciado el lanzamiento de un centro de datos modular todo en uno con refrigeración líquida EcoStruxure. Integrado por Avnet y con refrigeración de inmersión de precisión a nivel de chasis de Iceotope, el nuevo módulo prefabricado permitirá desplegar las aplicaciones edge computing de alto rendimiento (HPC) más intensivas en CPU y GPU en entornos difíciles y remotos.



Ubicada en un armario estándar ISO de 20 pulgadas, la nueva solución All-In-One tiene capacidad para una carga informática estándar de 60 kW, con una capacidad informática de hasta 336 kW disponible como solución a medida. El sistema también incluye un SAI trifásico Galaxy VS de 80 kW, una batería de reserva completa, protección contra incendios, rechazo de calor integrado y refrigeración redundante. La supervisión y la gestión remotas tanto del entorno físico como de los equipos informáticos se realizan con el premiado software EcoStruxure.

El nuevo módulo All-In-One combina una alta eficiencia con un PUE ultrabajo <1,15, y en algunos emplazamientos se puede alcanzar también un PUE de 1,03. El uso de refrigeración líquida elimina la necesidad de ventiladores.

Utilizando el chasis refrigerado por líquido Ku:l 2 de Iceotope, integrado con el sistema de rack refrigerado con líquido NetShelter de Schneider Electric, los equipos informáticos de función crítica se aíslan del entorno y se refrigeran por inmersión con precisión en una caja sellada e impermeable al polvo, los gases y la humedad. Los equipos informáticos, de almacenamiento y de red, seguros y a prueba de interferencias, cuentan con un nivel adicional de seguridad física y de conexión de E/S.

Schneider Electric ha anunciado previamente una alianza con Iceotope y Avnet, que permite que los servidores de nivel empresarial de una serie de fabricantes de equipos originales se integren con una infraestructura de refrigeración por inmersión de precisión a nivel de chasis antes del montaje, lo que aumenta la velocidad y la comodidad de las instalaciones y reduce los riesgos de servicio asociados a la instalación sobre el terreno de los equipos de servidor.

Proyector de láser puro M 4K25 RGB

Christie® ha presentado el paquete “todo en uno” de proyector RGB más pequeño, ligero y silencioso del mercado. El nuevo M 4K25 RGB avanza en la línea de fiabilidad, resistencia e innovación de la Serie M.

El lanzamiento en 2007 de la Serie M representó un cambio radical en el sector del audiovisual profesional. “La Serie M traía, en un paquete pequeño, gran cantidad de prestaciones”, cuenta Larry Paul, director ejecutivo de Tecnología y Secciones Customizadas de Christie. “Por ejemplo, aspectos que hasta entonces nadie incluía, como un sistema de lentes inteligentes o el Twist, una herramienta que permite realizar blending y warping. Si a ello le añadimos su pequeño tamaño y poco peso, comprenderemos por qué la Serie M se ha convertido en la línea de proyectores y lentes más vendida de Christie”.

Ahora, con la nueva resolución 4K UHD y los 25.000 lúmenes de potencia del proyector de láser puro M 4K25 RGB, Christie reinventa esa serie, incorporando soluciones técnicas que ningún otro competidor está en condiciones de ofrecer, en un pequeño paquete de menos de 44 kilos sin rival en el mercado. La tecnología RGB de láser puro redobla la apuesta cromática de la Serie M original. El resultado son unas imágenes brillantes y vivas que se acercan al volumen de color Rec. 2020, un estándar que se aproxima a lo que el ojo humano realmente ve.

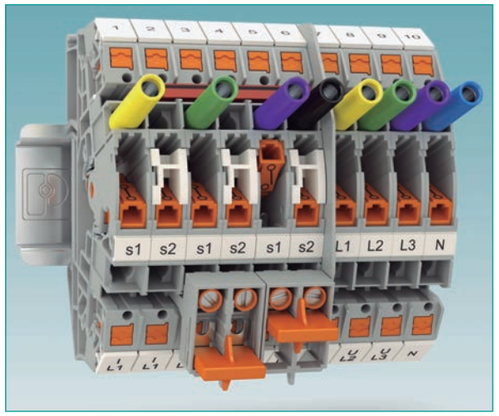
La incorporación de la electrónica TruLife+ completa las conexiones necesarias, ahorrándonos con ello tener que recurrir a tarjetas de entradas opcionales. Además, TruLife+ viene con ECC (convergencia de colores electrónica), un aspecto que permite al usuario corregir deficiencias en la convergencia de colores y ajustar individualmente, y desde la distancia, el rojo, el verde y el azul, librándonos con ello de la necesidad de subirnos a una escalera para efectuar ajustes. Nuestro sistema inteligente de lente ILS1 facilita el cambio de lentes (una gran ventaja para el sector del rental y los espectáculos en vivo) y ofrece la posibilidad de zoom, enfoque y offset motorizados y por control remoto. Las lentes de las Series M, J y Crimson, al igual que la estructura de rigging de la Serie M, son compatibles con el nuevo M 4K25 RGB, una gran ventaja para quienes estén ya usando esas soluciones.

Con su gran precisión, la tecnología pixel-shift patentada de Christie elimina distorsiones que otras tecnologías pixel-shift se muestran incapaces de solucionar y ofrece resolución 4K UHD a 60Hz. Con la actualización opcional del Mirage, el proyector M 4K25 RGB puede soportar 4K UHD a 120 Hz en aplicaciones estereoscópicas 2D y 3D. En el caso de la actualización opcional Mirage Pro, es posible alcanzar frecuencias de imagen de hasta 480Hz con resolución UHD.

Bornas de medición con conexión push-in lateral

Las bornas de medición seccionables PTVME de Phoenix Contact son una ampliación de la gama PTV. Su campo de aplicación abarca todas las aplicaciones del cableado secundario de instalaciones de conmutación para transformadores y señales.

La modernización de las instalaciones se simplifica mediante la conexión push-in vertical de las bornas. Gracias a su diseño compacto, permiten una anchura similar a las bornas de tornillo. Gracias a la tensión nominal de 1.000 V se logra una seguridad elevada. Con el patín deslizante sin tornillos, las bornas se accionan rápida y fácilmente. El estado de conmutación es claramente reconocible. Con las bornas de medición seccionables con conexión de conductores lateral pueden conectarse secciones de cable de 0,5 mm² a 6 mm². Puede elegir entre bornas con conectores hembra de pruebas integrados u opcionales. El accesorio estándar Clipline complete también se utiliza en estas bornas.



Antenas de banda ultra ancha para mediciones isotrópicas radiales de 150 MHz a 18 GHz

Aaronia amplia la serie de antenas de banda ancha OmniLOG con las antenas OmniLOG PRO. Aaronia ofrece la nueva serie en ocho versiones. Todas ellas tienen en común que consisten en una antena de banda ultra-ancha optimizada en frecuencia que también puede ser utilizada como antena de transmisión (1W o 100W). Gracias a su ancho de banda de hasta 18 GHz, sólo se necesita una antena para la monitorización completa de la frecuencia. Las soluciones de monitorización de banda ancha (monitorización de salas de conferencias, radiogoniometría, monitorización del espectro, monitorización multibanda, etc.) se convierten en un juego de niños. Gracias a su potencia de transmisión opcional de hasta 100 W, también son posibles las aplicaciones de transmisión de banda ancha hasta la interferencia reactiva.

Las pequeñas y ligeras antenas de la serie OmniLOG PRO son aptas para su uso en exteriores. Un chasis de antena con certificación IP65 proporciona una protección segura contra las influencias ambientales. La base magnética de la antena permite una instalación fija temporal, por ejemplo en el techo de un coche durante las mediciones.

Los datos completos de calibración (pasos de 50 MHz) para todas las antenas se pueden descargar del sitio web de Aaronia. Esto también hace que la antena sea adecuada para las mediciones de EMC.

Todas las antenas de banda ancha son desarrolladas, fabricadas individualmente y calibradas por Aaronia en Alemania. Esto garantiza los más altos estándares de calidad, permitiendo a Aaronia ofrecer a cada cliente una garantía completa de 2 años para todas las antenas EMC.

La serie OmniLOG PRO de Aaronia: Cubre todas las fuentes de RF hasta la banda K.

Características

- LTE800
- ISM868
- GSM900
- GSM1800
- GSM1900
- DECT
- UMTS
- WLAN
- Microondas
- Bluetooth

FRITZ! Repeater 6000

FRITZ!Repeater 6000 es el primer repetidor inalámbrico del fabricante AVM que está equipado con Wi-Fi 6 y la tecnología de red inteligente Mesh.

El nuevo estándar Wi-Fi 6 (IEEE 802.11ax) responde al constante aumento del número de dispositivos Wi-Fi en los hogares y oficinas. Desde smartphones, tablets, ordenadores, televisores 4K y altavoces, pasando por lámparas inteligentes, cada vez se utilizan más dispositivos simultáneamente en la red inalámbrica. Con velocidades de datos Wi-Fi de hasta 6 Gbit/s.

Por ejemplo, la modulación OFDMA con QAM-1024 de Wi-Fi 6 garantiza un flujo de datos rápido y estable, evitando las interferencias con otras redes inalámbricas vecinas. Por otro lado, los tiempos de respuesta y ejecución cortos de los paquetes IP que permite Wi-Fi 6 mejoran el rendimiento en aplicaciones muy exigentes como los juegos. Por supuesto, el FRITZ!Repeater 6000 también es compatible con los estándares Wi-Fi anteriores (IEEE 802.11ac/n/g/a), para asegurar el correcto funcionamiento de los dispositivos existentes junto con los nuevos dispositivos con Wi-Fi 6.

Además, el FRITZ!Repeater 6000 dispone de un puerto LAN de 2,5 gigabits y un puerto LAN de 1 gigabit, para conectar al repetidor otros dispositivos de la red local a través de cable, como sistemas NAS o impresoras en red.

Equipado con tres unidades de radio y 12 antenas, el nuevo repetidor tribanda FRITZ!Repeater 6000 es una obra maestra en su categoría, que lleva las redes inalámbricas al siguiente nivel para garantizar una cobertura estable y de máximo alcance. Incluso con múltiples aplicaciones de streaming y juegos ejecutándose al mismo tiempo, el Wi-Fi siempre funciona sin problemas.

El FRITZ!Repeater 6000 cuenta con tres unidades de radio: una para la banda de 2,4 GHz y dos más para la banda de 5 GHz. Gracias a los cuatro flujos en cada banda, las tres unidades de radio del FRITZ!Repeater 6000 permiten una velocidad máxima de datos de hasta 6000 Mbit/s: hasta 2400 Mbit/s por unidad de radio en la banda de 5 GHz y hasta 1200 Mbit/s en la banda de 2,4 GHz. Las 12 antenas integradas en el dispositivo aseguran el máximo alcance y cobertura del Wi-Fi, incluso en oficinas o viviendas muy grandes o de varias plantas. Por otro lado, la compatibilidad con el estándar de cifrado WPA3 y la tecnología OWE garantiza la máxima seguridad y privacidad de la red y los datos transmitidos en ella, también en el caso de las redes Wi-Fi públicas.

Gracias a su compatibilidad con la tecnología Wi-Fi Mesh, el FRITZ!Repeater 6000 permite la creación de redes en malla inteligentes combinando diversos puntos de acceso inalámbricos como routers, repetidores, adaptadores PLC, etc. en una única red Wi-Fi inteligente. Los puntos de acceso compatibles trabajan en una sola red, intercambian información entre ellos y mejoran el rendimiento de todos los dispositivos inalámbricos. Esto significa que, incluso en grandes espacios interiores y en condiciones estructurales complejas, todos los dispositivos de la oficina o del hogar navegan a la máxima velocidad.

La selección automática de canales y la repetición de banda cruzada, entre otras tecnologías inteligentes, garantizan que todos los dispositivos Wi-Fi estén siempre conectados al punto de acceso inalámbrico óptimo dentro de la red.

Configuración rápida y fácil, con solo pulsar un botón

Fluke renueva su promoción Compre un Fluke y reciba otro gratis

Fluke ha lanzado la promoción de temporada de este otoño y anima a sus clientes a solicitar un producto gratuito al adquirir un instrumento Fluke entre el 1 de septiembre y el 15 de diciembre de 2021. Los clientes disponen de una amplia gama de instrumentos para aplicaciones industriales y eléctricas, comprobadores de redes y equipos de calibración para uso doméstico y comercial que permitirán a los ingenieros de instalación, mantenimiento, resolución de problemas y reparación trabajar de forma eficiente y segura.

Los clientes que adquieran instrumentos a través de distribuidores autorizados de Fluke pueden utilizar su factura original para solicitar un producto gratis a través de la web de Fluke.

Nuevas opciones de productos Fluke gratuitos

La promoción "Compre un Fluke y reciba otro gratis" se divide en seis niveles en función del valor del producto comprado incluido en la promoción. El precio mínimo para que los clientes puedan solicitar un producto gratuito es de 100 €. Entre los artículos incluidos en esta promoción se encuentran los instrumentos de Fluke para aplicaciones industriales y eléctricas, así como los productos de Fluke Networks y Fluke Calibration. Los clientes podrán solicitar un segundo producto entre una selección de instrumentos gratuitos disponibles, como pinzas amperimétricas, multímetros digitales, comprobadores avanzados y accesorios como, por ejemplo, estuches para los equipos.

¿Cómo funciona?

En cada uno de los seis niveles de cualificación se ofrece una gama fija de productos dependiendo del valor de la compra original realizada a través de un distribuidor autorizado de Fluke. Por ejemplo, tras gastar entre 100 € y 549,99 € en uno de los productos incluidos los clientes podrán solicitar un producto gratuito de nivel uno, como una exclusiva correa magnética Fluke TPAK™, un estuche flexible de transporte para proteger el instrumento recién adquirido, un detector de tensión sin contacto Fluke 2AC VoltAlert™ o un kit Fluke Networks Protool IS40.

El nivel más alto permite a los clientes de Fluke solicitar un avanzado instrumento de medida gratuito, como el kit para resolución de problemas DMM (formado por un multímetro industrial de verdadero valor eficaz 87V, una pinza amperimétrica de verdadero valor eficaz 325, un comprobador de tensión T6-1000 y un comprobador de dos polos T150), un servicio de asistencia Gold durante 1 año para DSX-5000, un multímetro digital de precisión 8845A o una selección de lentes teleobjetivo y gran angular para cámaras termográficas.

Solución de colaboración VIA Connect 2

Kramer ha lanzado la solución VIA Connect 2 orientada a facilitar las reuniones híbridas y el aprendizaje de la denominada Generación H. La nueva solución VIA Connect 2, que destaca por su gran facilidad de uso y por su grado de seguridad, hace posible la participación de múltiples modos, puesto que transforma cualquier sala en un espacio colaborativo.

El lanzamiento de esta solución crea una experiencia de colaboración y comunicación unificadas (UC&C), con flexibilidad de compartir, interactuar y colaborar de forma inalámbrica en cualquier lugar del mundo, desde cualquier dispositivo con acceso a internet, a través de la plataforma de videoconferencia que se desee. Además, VIA Connect 2 dispone de una entrada HDMI con cable que permite cambiar de manera automática de un dispositivo a una pantalla 4K o HD.

VIA Connect 2 posibilita a los usuarios la oportunidad de orquestar su propia reunión utilizando la apliaciíon VIA compatible con cualquier sistema operativo o a través de Airplay y Miracast. Gracias a la función VIA Versa, podrán utilizarse los dispositivos AV de la sala o aula que se encuentren conectados al equipo via USB-pantallas, cámaras, micrófonos, altavoces, etc.- Cabe destacar que los usuarios de Zoom, Google o Teams pueden conectarse directamente a las reuniones híbridas a través de VIA Connect 2 con tan solo un clic.

La nueva solución tecnológica es compatible con cualquier dispositivo Windows, Mac, Chromebook, Android o iOS. De la misma manera que ocurre con el resto de las soluciones VIA de la compañía, VIA Connect 2 puede ser implementado, administrado y configurado de modo centralizado mediante VIA Site Management (VSM). Dicha plataforma de gestión de software avanzada posibilita a los administradores e integradores de TI la opción de controlar el hardware de forma remota a través de la nube o de las redes locales.

Prácticas soluciones de manipulación y transporte de cables de LAPP

El portfolio de productos de LAPP incluye más de 40.000 productos: un sinfín de tipos de cables, conectores y prensaestopas, así como otros productos para facilitar su instalación e identificación… pero ¿sabía que LAPP también ofrece soluciones y servicios logísticos? Soluciones que pueden ayudarle a transportar, apilar y desenrollar bobinas de cable. Estos productos de LAPP le ayudarán a mantener su almacén ordenado y a la vez contribuyen a tener un espacio de trabajo seguro.

CHAMPION: El desenrollador universal de bobinas que le permite una manipulación de cables profesional y cuidadosa. Tire del extremo del cable y la bobina comienza a girar suavemente y el cable se desenrolla, con un mínimo esfuerzo. El CHAMPION está disponible en dos modelos diseñados para bobinas de cable con un ancho máximo de 52 o 67 cm. En caso de que quiera manipular bobinas más grandes simplemente se pueden poner en dos CHAMPIONS, uno para cada lateral de la bobina. Cuenta con una capacidad de carga de hasta 200 kg y rodillos portadores fácilmente ajustables con 6 posiciones diferentes para ofrecerle versatilidad. Además, el diseño híbrido de aluminio y poliamida reforzada lo convierte en una solución extremadamente ligera. También es posible instalar 4 ruedas giratorias para ofrecer mayor flexibilidad en el transporte de las bobinas.

Caja de cartón de desbobinado: ¿Le gustaría tener la opción de desbobinar los cables de forma segura y profesional, aunque no tenga un bobinero? ¿Necesita una solución flexible para desbobinar? La caja de cartón de desbobinado de LAPP es justo lo que usted necesita. Esta le permite desenrollar directamente las bobinas cable de hasta 30 kg y con un diámetro de hasta 40 cm. La bobina gira dentro de la caja, por lo que desenrollarlo es extremadamente sencillo. Puede transportar estas prácticas cajas con las dos asas y apilar hasta tres cajas para crear un estante. De esta manera los cables estarán cuidadosamente ordenados y protegidos contra la suciedad.

TRONIC: Sistemas de ordenación y manipulación para cables unipolares

Los sistemas TRONIC se componen de cajas individuales, módulos apilables y carros de transporte. De esta manera puede almacenar, transportar y desenrollar fácilmente las bobinas cables unipolares, protegiendo los cables. Con TRONIC ahorrará tiempo, espacio y le ayudarán a tener entornos de trabajo más eficientes, ordenados y limpios.

Soluciones Vertiv™ Liebert® RXA y Liebert® MBX de distribución de alimentación para centros de datos Edge, Colocation y de tamaño mediano

Vertiv ha presentado dos nuevos sistemas de distribución de alimentación para simplificar la gestión y escalabilidad de centros de datos. El panel de alimentación remoto (remote power panel, RPP) Liebert® RXA es una solución flexible y segura para aplicaciones de alimentación de alta densidad con uno de los tamaños más reducidos del sector, mientras que el sistema de blindobarras (busway) Liebert® MBX facilita la distribución suspendida de alimentación en centros de datos de cualquier tamaño, dejando la superficie libre para los equipos. Ambos productos se encuentran ya disponibles en Europa, Oriente Medio y África (EMEA).

Tradicionalmente, muchos centros de datos han utilizado sistemas de distribución eléctrica creados a medida para suministrar energía a los racks de servidores. Sin embargo, las soluciones a medida requieren tiempos de espera más largos y no están pre-certificadas por los fabricantes de equipos originales (OEMs), lo cual puede generar complicaciones durante el mantenimiento.

Una alternativa demostrada a los sistemas creados a medida, en especial para las aplicaciones de alta densidad, es un RPP estandarizado, como el nuevo Liebert RXA de tamaño reducido, el cual se puede instalar de forma flexible en centros de datos, salas de servidores o armarios de red. Pre-construido y configurado, certificado y testeado, el Liebert RXA proporciona una solución de distribución eléctrica lista para usar una vez conectada a circuitos derivados, simplificando el arranque y expansión de instalaciones y la gestión general de redes de centros de datos de mayor escala. La solución ofrece características flexibles y múltiples opciones de configuración para acomodar las necesidades de diferentes espacios y su crecimiento futuro, al tiempo que permite optimizar el espacio disponible. Además, esta nueva generación de RPPs estandarizados proporciona capacidades integradas de control inteligente. A través de la supervisión de alimentación inteligente y el sistema de control Vertiv™ Liebert® DPM, esta solución es capaz de responder con mayor rapidez ante cualquier desequilibrio de carga, aumentando la disponibilidad de sistemas críticos y evitando situaciones que podrían dañar equipos y servidores valiosos, además de causar interrupciones no planificadas. Gracias a su innovador diseño, Liebert RXA cuenta con uno de los volúmenes más reducidos del sector, mientras que las características de seguridad contra contactos en los dedos proporcionan mayor protección a los operadores.

Switches gestionados aptos para tiempo real con Time Sensitive Networking

Phoenix Contact presenta los nuevos FL Switch TSN 2300 son los primeros switches Ethernet para el Time Sensitive Networking (TSN) de Phoenix Contact. Permiten crear aplicaciones con sincronización temporal y hacen posible una comunicación con tiempo real en la red Ethernet, además de aumentar la disponibilidad en sus redes de automatización.

Con las funciones Frame Preemption, Stream Management y una sincronización temporal precisa según IEEE 802.1AS, los switches respaldan desde el primer momento el perfil TSN Profinet. De este modo, permiten una configuración TSN fácil para el usuario mediante la ingeniería Profinet 2.4, comparable fácilmente con el Profinet RT clásico.

Además, el amplio conjunto de propiedades de los switches gestionados de la serie 2000, como en el resto de switches Phoenix Contact, hace que sea posible un uso universal de los switches TSN también en aplicaciones clásicas. De este modo, las soluciones de red actuales pueden migrarse fácilmente en el futuro a arquitecturas TSN modernas.

Kits de nodos extensores Wi-Fi 6

D-Link ha anunciado el lanzamiento de los kits D-Link COVR-X1862 (2 nodos) y D-Link COVR-X1863 (3 nodos) que crean una red WiFi 6 unificada en malla con hasta 1.800 Mbps de velocidad e itinerancia automática entre los puntos de acceso (nodos) para estar siempre conectado al que tenga mejor intensidad de señal y no quedarse conectado al router aunque estemos muy alejados.

Otra de de las grandes ventajas técnicas de Wi-Fi 6 es que también opera en la banda de 2,4GHz (el anterior Wi-Fi 5 sólo se activaba en la banda de 5 GHz, bajando a Wi-Fi N en las conexiones 2.4 GHz) y debido a que en largas distancias con respecto al emisor es más óptimo usar la banda 2.4 GHz esto supone un notable incremento de prestaciones. Además, Wi-Fi 6 incorpora MU-MIMO uplink/downlink (la última versión de Wi-Fi 5 Wave 2 también integraba MU-MIMO pero sólo para el downlink), que junto a OFDMA y 1024-QAM reducen considerablemente la latencia y aumentan el rendimiento y la capacidad de la red.

Características destacadas de los kits D-Link COVR-X1862 y COVR-X1863:

- Red Wi-Fi en malla sin interrupciones, roaming automático entre nodos
- Sistema extensible hasta 4 nodos, también permite añadir el extensor de pared D-Link DAP-X1860 Wi-Fi 6 Mesh
- Wi-Fi 6 de doble banda de última generación, hasta 1.8 Gbps
- Smart Roaming, OFDMA, 1024QAM, BSS coloring, MU-MIMO uplink/downlink
- Dos modos de uso: extensores mesh desde el router de cualquier operadora o modo router+extensor/es mesh para usar uno de los nodos como router neutro (dejando el router de la operadora en modo bridge o mediante triple VLAN)
- 1 puerto LAN Gigabit y 1 puerto WAN Gigabit en cada nodo
- Soporta Ethernet Backhaul para interconectar los nodos por cable LAN y que sean puntos de acceso sin pérdida de señal entre nodos (red troncal a 1 Gigabit) ideal para las casas que ya integran conexion de red LAN RJ-45 en cada habitación, ya obligatorio en las viviendas de nueva construcción.
- Instalación sencilla desde app D-Link WiFi, no necesita ordenador, compatible con cualquier router u operadora.
- Gestión mediante interfaz web o app D-Link WiFi. Si se configura un nodo como router de la red, dispone de funciones de priorización de tráfico (QoS), control parental, WiFi de invitados, acceso seguro por VPN, etc.
- Nuevo protocolo de encriptación WPA3 para máxima seguridad.
- Control por voz con Amazon Alexa y Google Assistant

Los kits D-Link COVR Wi-Fi 6 ya se encuentran a la venta a un precio PVP recomendado de 175€ para el COVR-X1862 de dos nodos y de 265€ para el COVR-X1863 de tres nodos. El extensor de pared D-Link DAP-X1860, compatible con estos kits COVR, así como con la gama de routers Wi-Fi 6 de D-Link, también se encuentra ya a la venta con un PVP de 79€.

Ecosistema Vertiv™ Avocent® ADX para gestión en remoto de activos de TI

Vertiv ha presentado el Ecosistema VertivTM Avocent® ADX, una plataforma de gestión de TI de nueva generación que responde a las necesidades en constante evolución de los centros de datos. El ecosistema Avocent ADX es un conjunto de dispositivos y software diseñado para las arquitecturas de red híbridas más complejas de hoy en día y con el objetivo de satisfacer las demandas de los trabajadores en remoto. Ya está disponible en Europa, Oriente Medio y África (EMEA).

Sobre la base de Avocent y la especialización en la que los clientes han confiado durante años, el nuevo Ecosistema Avocent ADX está diseñado para su uso en entornos empresariales, de Edge Computing, cloud y Colocation. Admite una experiencia de trabajo en remoto segura y sólida al permitir que los trabajadores accedan a los datos y los controlen de forma rápida y fluida, como requieren la ingeniería y el diseño avanzados, la edición de vídeo y otras aplicaciones de retransmisión de alta resolución. El ecosistema Avocent ADX incluye el KVM 4K más rápido y con más funciones en un solo dispositivo, con la gestión de dispositivos de TI más amplia del mercado.

El ecosistema Avocent ADX se desarrolla sobre la base de una arquitectura común, con los estándares abiertos, plataformas y API que los usuarios precisan, al tiempo que permite implementaciones rápidas, seguras y adaptables de dispositivos de TI desde la empresa hasta el Edge Computing. El Ecosistema Avocent ADX incorpora la tecnología Avocent® Core Insight (Avocent® ACI) para mejorar aún más la comunicación con los dispositivos habilitados para Redfish. Estas tecnologías permiten a Avocent ADX superar los obstáculos más persistentes para la gestión en remoto de las arquitecturas distribuidas e híbridas, incluida la adaptación de sistemas al crecimiento de la red, permitiendo así un acceso seguro a los usuarios designados y proporcionando capacidades de vídeo de alta resolución para adaptarse a las tecnologías modernas, incluyendo los conectores USB-C.

El ecosistema Avocent ADX incluye varios componentes individuales, cada uno de los cuales puede desplegarse de forma independiente o en conjunto, para una experiencia de usuario más sólida. La plataforma ofrece una gestión y un control seguros y eficientes de la infraestructura de TI virtual y física, y gestiona tanto las sesiones KVM como las de serie para hasta 100 o más usuarios simultáneos; el Rack Manager proporciona de forma resiliente una consolidación de IP para diversos dispositivos, así como una vía para la adaptabilidad; y el KVM 4K en remoto aumenta la productividad y funciona a mayor velocidad y con un mayor ancho de banda en comparación con los KVM 4K estándar de la competencia.

El sistema funciona con una eficiencia y seguridad que marcará un nuevo hito para el sector, y es especialmente eficiente para las implantaciones de Edge Computing, donde la escala y el crecimiento son retos habituales.

Plataforma de gestión Avocent® ADX MP1000:

Simplifica la gestión, el control, la seguridad y la automatización de la infraestructura de TI virtual y física en toda la empresa y en implantaciones de Edge Computing. Gestiona procesadores de servicio, máquinas virtuales, módulos KVM IP y dispositivos de acceso en remoto.

Rack Manager Avocent® ADX RM1048P:

Conecta y gestiona diversos dispositivos de TI en el rack y puede implementarse con o sin Avocent ADX MP1000. Consolida las direcciones IP para mitigar cualquier deficiencia a medida que se añaden más equipos al rack. Utiliza la alimentación a través de Ethernet (PoE) para reducir el número de cables en el rack.

Switch Avocent® ADX IPUHD 4K IP KVM:

Esta nueva incorporación al portfolio de Vertiv™ KVM puede dar acceso a más de 100 usuarios y 48 objetivos únicos en una sola sesión, ofreciendo vídeo 4K y rendimiento de alta velocidad (20 GB en enlace ascendente) para permitir la gestión de dispositivos y datos en remoto en tiempo real. Cada switch está equipado con conectores USB-C con longitudes de cable más cortas. Con la consolidación de PoE e IP, los requisitos de cableado se reducen drásticamente.

Módulo Advantech 5G AIW-355

Advantech presenta el nuevo miembro de la serie AIW-300: el AIW-355. Este innovador módulo 5G marca un hito para Advantech Industrial Wireless (AIW) y está diseñado para soluciones AIoT que requieren conectividad ubicua, movilidad dinámica y seguridad extrema. AIW-355 es una excelente opción para su uso en dispositivos edge computing, pasarelas y diversos dispositivos móviles desplegados globalmente.

El AIW-355 utiliza el 5G para proporcionar capacidades y potencia que antes no estaban disponibles con el 4G. El 5G ofrece una velocidad diez veces mayor (10 Gbps frente a 1 Gbps del 4G) y admite la conexión de hasta un millón de dispositivos por kilómetro cuadrado. Además, 5G permite un aumento de 100 veces en la capacidad, una disminución de 10 veces en la latencia, y reduce los tiempos de retraso a sólo 1 milisegundo (en comparación con 10 ~ 20 milisegundos para 4G).

Advantech AIW-355 cuenta con el módem Snapdragon X55 5G y es compatible con las frecuencias 5G NR SUB6 tanto en operaciones 5G autónomas (Stand Alone -SA) como no autónomas (NSA). Es compatible con los estándares LTE y WCDMA; y es retrocompatible con las redes LTE-A y 3G. AIW-355 ayuda a optimizar la inversión del cliente en la fase inicial de la construcción de 5G y se adapta a las demandas del mercado emergente.

El módulo inalámbrico 5G AIW-355 de Advantech cuenta con una interfaz USB M.2 3052 de factor de forma M.2 Key B. Este módulo M.2 se adapta a la mayoría de los operadores principales y facilita la integración de 5G. AIW-355 también integra un receptor GNSS multiconstelación e interfaces USB 3.1 de alta velocidad.

Diseñado para Aplicaciones Industriales y de Ciudades Inteligentes

El módulo 5G AIW-355 de Advantech ofrece capacidades de alta velocidad para aplicaciones de monitorización industrial, tratamiento médico remoto, transporte y sistemas de vigilancia de alta calidad. AIW-355 proporciona las capacidades 5G necesarias para soportar los sistemas de videovigilancia basados en la ciudad. Estos sistemas son vitales para la seguridad pública y requieren una transmisión de alta velocidad y baja latencia. El 5G satisface estas necesidades a la vez que admite tecnologías de información innovadoras que mejoran los tiempos de respuesta de la administración. En resumen, AIW-355 es capaz de aumentar la eficiencia de la infraestructura de seguridad pública.

El alcance de las aplicaciones de supervisión de la seguridad se ha ampliado para incluir el uso de datos de supervisión dimensional y la supervisión de vehículos en tiempo real. El AIW-355 de Advantech también da cabida a estas aplicaciones, al tiempo que ayuda a las empresas a reducir costes mediante la supervisión eficaz de zonas restringidas y potencialmente peligrosas.

Hay tres versiones de AIW-355 disponibles para aplicaciones en Norteamérica, Europa y China. Cada versión es compatible con las arquitecturas de red 5G SA y NSA y ofrece velocidades de transmisión más rápidas, mejor capacidad de transporte y menor latencia de red. Cada modelo puede funcionar en amplios rangos de temperatura (-30 ~ 75 °C/-22 ~ 167 °F) y es compatible con Windows y Linux.

Características Principales

- Conjunto de chips Qualcomm SDX55 5G NR SUB6
- Amplio soporte de temperatura de funcionamiento -30 ~ 75 °C/-22 ~ 167 °F (compatible con 3GPP, con un diseño térmico adecuado)
- Proporciona factor de forma M.2 3052 Key B e interfaces USB 3.1
- Compatibilidad con diversos O/S: Windows y Linux (Ubuntu 20.04)
- Soporta capacidades de posicionamiento GNSS

Plataforma VIAVI 5P16 para pruebas de arquitectura PCIe 5.0

Viavi Solutions Inc ha anunciado que la plataforma VIAVI Xgig 5P16 admite ahora la bifurcación del analizador y la funcionalidad multiusuario, lo que permite realizar múltiples usuarios y pruebas simultáneas en una sola plataforma. Estas mejoras permiten el análisis simultáneo de protocolos para el tráfico de datos PCI Express® (PCIe) 5.0 en todas las capas de la pila, lo que acelera el tiempo de comercialización y controla el coste total de propiedad (TCO) para el desarrollo y la producción de productos de próxima gener.

La capacidad de acomodar a varios usuarios en la misma plataforma, ya sea de forma local o remota, crea una amplia gama de posibles configuraciones de prueba y permite una depuración y desarrollo más rápidos de los equipos. Las pruebas simultáneas de múltiples enlaces PCIe 5.0 aumentan la productividad de cada chasis de analizador para reducir las métricas de coste por prueba/coste por usuario, lo que impulsa la eficiencia operativa y de costes para mejorar el retorno de la inversión.

Las nuevas capacidades de bifurcación y multiusuario son compatibles tanto con la plataforma VIAVI Xgig 5P16 como con la Xgig 5P8, ofreciendo una mayor flexibilidad para gestionar la configuración de los dispositivos, la asignación y los gastos de software. Exclusiva de VIAVI, la plataforma multifuncional Xgig integra las funciones de analizador, ejercitador y jammer en el mismo chasis. Este diseño permite a los usuarios optimizar aún más los equipos para satisfacer mejor los requisitos operativos y presupuestarios.

Analizador de espectro óptico Yokogawa AQ6380

El OSA AQ6380 de Yokogawa ofrece un rendimiento óptico que permite a los ingenieros y científicos desarrollar y mejorar la velocidad, el ancho de banda y la calidad de la próxima generación de redes de comunicación, al tiempo que su facilidad de uso garantiza su rapidez y eficacia.

El AQ6380 tiene una resolución de longitud de onda óptica de hasta 5 picómetros (pm), lo que permite separar y medir con precisión las señales ópticas que se encuentran muy próximas. Con el AQ6380, las formas de onda que antes ni siquiera eran visibles en un OSA típico, como los picos laterales de modulación en el espectro del láser, pueden ahora visualizarse con precisión.

También ofrece una gama de longitudes de onda de 1200 a 1650 nm, lo que permite que una unidad satisfaga diversas necesidades de medición de longitudes de onda. Gracias a la posibilidad de modificar la resolución de la longitud de onda de 5 pm a 2 nm, se puede admitir una amplia gama de aplicaciones, desde mediciones de picos y puntos de banda estrecha hasta mediciones espectrales de banda ancha.

El AQ6380 cuenta con una calibración integrada basada en una fuente de luz incorporada. La calibración de la longitud de onda se realiza automáticamente a intervalos establecidos mediante la conmutación de la ruta óptica con un switch óptico interno.

Otro parámetro importante en el análisis de formas de onda ópticas es el rango dinámico cercano, definido como la diferencia en el nivel de potencia medido desde el pico de la señal hasta el ruido a una distancia específica de la longitud de onda de pico.

Incorpora un monocromador de nuevo diseño con características espectrales más nítidas que las disponibles hasta ahora, consiguiendo un rango dinámico de proximidad de hasta 65 dB.

El nuevo monocromador también ofrece una supresión muy alta de la luz parásita, un criterio importante en la medición óptica. Por ejemplo, en situaciones como la medición de SMSR láser, en la que se miden varios espectros ópticos con diferentes niveles al mismo tiempo, la luz parásita puede interferir en la medición. El AQ6380 ofrece un valor de supresión de luz parásita de 80 dB, el mejor de su clase.

El AQ6380 captura los puntos de datos en sólo 0,23 segundos, en comparación con los 5,4 segundos del modelo existente (AQ6370D) en determinadas condiciones. También se ha diseñado para facilitar y hacer más eficiente su uso, asegurando que el esquema de medición se pueda configurar y que los datos se puedan adquirir fácilmente.

La pantalla táctil LCD de 10,4 pulgadas, de alta resolución y gran capacidad de respuesta, hace que el dispositivo sea tan fácil e intuitivo de manejar como una tablet.

A la hora de analizar los resultados, el AQ6380 cuenta con funciones de análisis integradas para caracterizar el espectro óptico de una gran variedad de sistemas y dispositivos ópticos, como el sistema WDM, DFB-LD, EDFA y filtros.

Las funciones de análisis incluyen: DFB-LD; FP-LD; LED; Ancho espectral (pico/punto); SMSR; Potencia óptica; WDM (OSNR); EDFA (Ganancia y NF); Filtro (pico/pie) y Filtro WDM (pico/pie).

El AQ6380 también cuenta con un menú de aplicación “Modo APP”, que facilita enormemente la configuración de las mediciones. Al pulsar el botón APP, aparece un resumen de las aplicaciones de prueba preinstaladas: WDM, DFB-LD, FP-LD y pruebas de LED. Un asistente guía conduce al usuario a través de un sencillo proceso de configuración de mediciones y análisis específicos.

Las aplicaciones de prueba nuevas o adicionales estarán disponibles para su descarga en el sitio web de Yokogawa y podrán añadirse al AQ6380 mediante futuras actualizaciones de firmware.

El nuevo estándar para la tecnología de automatización

Conectores M12 Push-Pull

Conexión sencilla, bloqueo rápido: los conectores M12 con bloqueo rápido Push-Pull permiten una conexión segura y sin herramientas. Las variantes especiales con bloqueo interior permiten realizar diseños de carcasas compactos también en espacios estrechos y con una gran densidad de cableado.

Más información en **phoenixcontact.com/M12PushPull**

PHOENIX CONTACT
INSPIRING INNOVATIONS