REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Boletín *Novedades TIC*

Abril *2019*

Contenido

Sistema de Vigilancia Tecnológica

Ministerio de Comunicaciones

Abril, 2019

INTELIGENCIA ARTIFICIAL

1. FORD DESARROLLA UN CARRITO DE SUPERMERCADO DOTADO CON FRENOS INTELIGENTES

Fecha: 30/04/2019

Para evitar colisiones y desperfectos en los supermercados, Ford ha creado el primer carrito inteligente de la compra, equipado con un sistema de autofrenado automático que se detiene ante los obstáculos.

El carrito de la compra de los supermercados es un artilugio fascinante para los niños. Cuando son muy pequeños solo quieren subirse en él, y cuando son más mayores, quieren conducirlo.

El problema es que no está diseñados para ellos. Los niños llevan los carritos a ciegas, porque normalmente son más altos que ellos y les tapa la visión, así que los accidentes son frecuentes.

Y no hay nada más embarazoso para un padre o una madre, que observar cómo su hijo estrella el carrito contra una pila de botellas de zumo que el reponedor ha tardado un buen rato en colocar. Por suerte, Ford acude al rescate con su novedoso carrito de supermercado con frenos inteligentes.

La compañía americana sigue con su campaña de aplicar las innovaciones de sus automóviles a objetos cotidianos, una estrategia publicitaria que le está dando buenos resultados, porque sus inventos son bastante divertidos y curiosos.

Hace unos días presentó el carro de supermercado de Ford con auto frenado automático. O, en palabras sencillas, un carrito de la compra que frena sin ayuda cuando detecta un obstáculo.

Para crear este práctico utensilio, Ford ha adaptado su tecnología de Asistencia de Pre-colisión que usa en sus vehículos.

Este sistema utiliza un radar y una cámara para detectar peatones y bicicletas. Si detecta un obstáculo emite un aviso, y si el conductor no reacciona es capaz de frenar automáticamente para evitar un atropello.

Ford ha miniaturizado esta tecnología para colocarla en la base del carrito. Como se ve en el vídeo, una cámara situada en la parte inferior detecta cuándo hay un obstáculo cerca.

Llegado el momento, si la persona que maneja el carrito no se detiene los frenos se activan automáticamente, evitando la colisión.

Estamos seguros de que muchos supermercados y tiendas no dudarían en comprar este carro de supermercado de Ford con frenos inteligentes. Pero no será posible, ya que solo es un prototipo y Ford no tiene intención de ponerlo a la venta.

Disponible en:
https://www.ticbeat.com/tecnologias/ford-desarrolla-un-carrito-de-supermercado-dotado-con-frenos-inteligentes/?fbclid=IwAR0LfoNgbj0-T9ptQkt_IVRwoSuC5cG63-1uee7fydPkMuMi-fDg9s5wCN4

2. LA INTELIGENCIA ARTIFICIAL PODRÍA MEJORAR LA CALIDAD DE LA MÚSICA QUE ESCUCHAS

Fecha: 10/04/2019

La música es una de las pocas cosas que hacemos exclusivamente los humanos. En ella se combinan muchos elementos para los que se necesita un aprendizaje especializado, como aprender solfeo, o estudiar a la forma en la que otros artistas combinan las armonías para crear sus obras.

La música también tiene un fuerte componente creativo por ello, a mucha gente le parece imposible que un agente de inteligencia artificial sea capaz de trabajar de forma eficiente y original en un ámbito tan creativo como es el de la música. Sin embargo, ya lo hace.

La inteligencia artificial ya se emplea en mejorar la calidad de la música que escuchas¸ aplicándose a diferentes ámbitos de la creación musical como es la composición, la masterización en el estudio de grabación o la recuperación de audios antiguos para darles un toque más actual.

La historia de la música está llena de ejemplos de grandes obras inacabadas de grandes maestros a los que les sobrevino la muerte antes de poder completar su obra. La Misa de Réquiem de Mozart quedó inacabada a causa de la dolencia renal que llevó a la muerta al genial compositor en 1791.

Otro ejemplo lo encontramos en la famosa Sinfonía n.º 8 “Inacabada” de Schubert, compuesta en 1822, pero trágicamente abandonada antes de su conclusión por la enfermedad del compositor. Ahora, casi 200 años más tarde, la inteligencia artificial ha aceptado el reto de retomarla para finalizarla tal y como habría hecho el propio Schubert.Esta pieza de Schubert se caracteriza por ser una de las más especiales de cuantas compuso Schubert por ser totalmente distinta al resto. Ahí es precisamente donde reside el gran reto musical para la inteligencia artificial de Huawei.

La inteligencia artificial es una auténtica especialista en encontrar patrones de datos que apuntan hacia determinadas tendencias. Esto le ha servido de base a Huawei para completar Sinfonía n.º 8 “Inacabada” de Schubert utilizando la inteligencia artificial que integra su Huawei Mate 20 Pro.

Dado que esta pieza se considera muy diferente al resto de obras de Schubert, la inteligencia artificial de Huawei no podía utilizar los datos de la obra anterior del compositor, por lo que solo disponía de los dos primeros movimientos para completar el tercer y cuarto movimiento que supuestamente faltaría.

Dicho y hecho, tras un análisis exhaustivo de la estructura, armonías y melodías originales del autor, generó los movimientos tercero y cuarto. A partir de los datos obtenidos, Huawei contó con la colaboración del compositor Lucas Cantor, ganador de premios Emmy, para escribir la partitura completa de orquesta e interpretarla por primera vez al completo ante un público en directo casi 200 años después de que se empezara a escribir la primera nota.

La inteligencia artificial en la producción musical

El trabajo de estudio es casi tan importante que el que los artistas hacen antes. Se puede tener entre manos una composición excelente, pero si el técnico de producción no hace un buen trabajo con la mezcla, el resultado será mediocre o directamente desastroso.

En esta tarea se combina el talento con el dominio de la técnica a la hora de dar a cada pista la importancia que se merece. Muchos comparan a esta tarea a editar una foto, en la que puedes establecer que el azul del cielo sea más intenso o el verde los campos sea más verde.

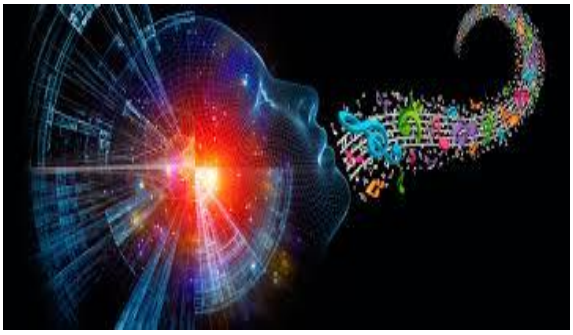
Si bien todavía no llega a sustituir el "toque creativo" de los grandes profesionales de la producción musical, la inteligencia artificial consigue ahorrar muchas horas de estudio y economizar gastos a artistas independientes que no cuentan con muchos recursos.

La inteligencia artificial es capaz de analizar las pistas grabadas y, tras unas sencillas indicaciones del tipo de sonido que se quiere conseguir, realiza un primer acercamiento al resultado final que se busca. Después, el técnico puede darle los toques finales.

Esto reduce drásticamente el tiempo que el técnico debe emplear en la maquetación inicial, limitando su intervención a dar el visto bueno o los últimos detalles a la producción. Un trabajo que podría llevar varios días, resuelto en solo unas horas y con resultados que, en muchos casos, ni siquiera requiere la intervención del técnico para obtener resultados de excelente calidad musical.

Para conseguir esto se debe entrenar a la inteligencia artificial con millones de horas de música de diferentes estilos para que aprenda los matices y patrones de los diferentes estilos y su forma de combinar los instrumentos.

Además, la inteligencia artificial se está utilizando dentro de los estudios de grabación para completar pistas rellenando con fragmentos de instrumentos que realmente no se han grabado, como *loops* con batería o acordes de guitarra que realmente no se han grabado. De ese modo también se contribuye a reducir el número de horas que se utiliza el estudio y, por tanto, también se reduce el coste de la producción musical



Restaurar audio mediante inteligencia artificial

La inteligencia artificial ha conseguido recuperar fotos históricas e incluso se ha logrado reconstruir el color que tendrían de haberse capturado con negativos a color "pintando" las fotos en base a las tonalidades de gris o a datos históricos.

También se ha logrado recuperar películas históricas y colorearlas para crear una nueva versión remasterizada con mejor calidad que las originales gracias a la inteligencia artificial. Con la música también se están consiguiendo hazañas similares. Gracias a la inteligencia artificial se consiguen filtrar los audios procesando las señales para eliminar ruidos y potenciar los diálogos mediante aprendizaje automático profundo y la direccionalidad del sonido.

Por ejemplo, mediante el procesamiento del audio con inteligencia artificial, se ha

conseguido que una pista de sonido grabada en sonido monoaural (mono), pueda ser interpretada por el oído humano como sonido envolvente.

Esto es posible engañando al cerebro para que interprete el sonido de forma que parece que viene de distintos orígenes (estéreo) cuando en realidad la fuente se encuentra en mono (un solo origen). El cerebro interpreta de forma subconsciente esta direccionalidad del sonido basándose en diferentes valores, como la diferencia de tiempo de llegada del sonido o diferencia de tiempo interaural. Por ejemplo, si el sonido proviene del lado derecho, lo percibirás antes por el oído derecho que por el izquierdo. Cuanto mayor sea esta diferencia, más se balancea el sonido hacia ese lado.

Lo mismo sucede con la diferencia de volumen o diferencia interaural de intensidad en la que, cuando un sonido procede del lado derecho, el cerebro lo percibe con un mayor volumen en el oído derecho que en el izquierdo.

El cerebro también diferencia si el sonido es frontal o desde de detrás. Si viene de delante, las orejas dirigen el sonido directamente al canal auditivo mientras que, si proviene de detrás, choca con la oreja y se produce una pequeña distorsión antes de llegar al canal auditivo. La inteligencia artificial es capaz de tener todos esos datos en cuenta y, tras analizar pistas de audio grabado en mono, separar los distintos sonidos y modular su volumen, retraso o intensidad para engañar al cerebro y hacerle creer que los sonidos provienen de varias direcciones creando una sensación similar a la obtenida por un sistema de audio 3D.

Esto podría tener infinidad de usos, pero el más evidente es el de crear espacios personales de sonido envolvente que permitirían, mediante inteligencia artificial, mejorar la calidad de la música que escuchas creando la sensación de encontrarte en el centro del estudio de grabación, mientras los artistas clásicos interpretan sus canciones a tu alrededor.

Disponible en:
https://computerhoy.com/patrocinado/tecnologia/inteligencia-artificial-podria-mejorar-calidad-musica-escuchas-401471

TELEFONÍA MÓVIL

1. LA ÚLTIMA ACTUALIZACIÓN DE WINDOWS 10 MEJORA LA SINCRONIZACIÓN CON MÓVILES ANDROID

Fecha: 29/04/2019

Microsoft está buscando nuevas perspectivas en los últimos tiempos.No debemos quedarnos solo con la multitud de problemas encontrados en las últimas actualizaciones de Windows 10, también se debe anotar la apuesta por reducir el hermetismo en su visión de negocio y aumentar la relación con la competencia, como la mejora en la sincronización con Android.

Uno de los últimos ejemplos ha sido el cambio a núcleo Chromium de Microsoft Edge que ha incorporado la posibilidad de ver Chromecast mediante Microsoft Edge. Otro más reciente, la opción de que Windows muestre las notificaciones de los móviles Android.

Llama la atención este cambio en la aplicación Your Phone de Windows 10. Se podrá configurar para que las alertas de Android sean previsualizadas en el

escritorio y así evitar la necesidad de estar pendiente del teléfono en todo momento. Las notificaciones irán apareciendo en la barra de menú y se podrá configurar el modo de alerta visual y sonora a nuestro gusto.

A pesar de la novedad, esta se verá limitada de momento a la simple visualización de las notificaciones, no se podrá interactuar con ellas ni responder a los mensajes. Aunque todo apunta a que en un futuro esta sincronización entre dispositivos servirá para contestar vía escritorio a WhatsApp o Snapchat -que no tiene presencia en Windows-.
Posiblemente quedará para posteriores actualizaciones de Windows.
Para poder disfrutar de esta novedad hará falta disponer como mínimo de la versión 1803 de Windows 10 y un teléfono con Android 7.0 Nougat y 1GB de RAM o superior.

De todas formas, esta clase de actualizaciones queda ensombrecida por la delicada situación de Windows tras los problemas que han llegado en el último año con las novedades implementadas y a la espera de la nueva actualización de Windows 10 que llegará en Mayo.

Disponible en:
https://computerhoy.com/noticias/tecnologia/ultima-actualizacion-windows-10-mejora-sincronizacion-moviles-android-412837

SEGURIDAD INFORMÁTICA

1. EL 81% DEL TRÁFICO MALICIOSO ONLINE SE DIRIGE AL FAMOSO LENGUAJE PHP

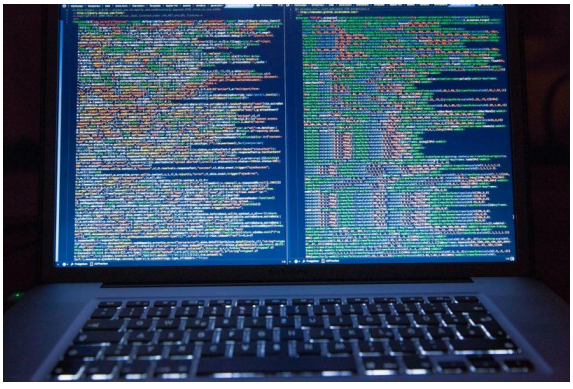
Fecha: 24/04/2019

PHP es el lenguaje más popular en desarrollo web, prácticamente omnipresente a la hora de navegar por Internet. Eso hace que sea uno de los blancos principales de los hackers malintencionados, que no han dudado en aprovechar las numerosas vulnerabilidades que presenta.

Según un informe publicado por F5 Labs y compartido con este medio, el número de ataques contra PHP no ha parado de aumentar en los últimos años, en la mayoría de los casos siguiendo un proceder muy similar. Prácticamente el 80% de las webs utiliza este lenguaje, así que el potencial de los exploits es devastador.

El 81% de todo el tráfico malicioso en Internet en 2018 fue dirigido directamente hacia PHP, un aumento de nada menos que del 23% en un sólo año, y no parece que vaya a parar.

De esta forma, PHP se ha convertido en el Talón de Aquiles del mundo digital y de Internet, y es que con ciertos conocimientos y aprovechando las vulnerabilidades, es relativamente fácil para un atacante hacerse con el control de un sistema.



La clave está en una herramienta llamado phpMyAdmin, que concede acceso a bases de datos MySQL. Si el atacante consigue permisos de administrador y acceso a la primera, el sistema se convierte en una presa fácil.

Lo curioso de todo este asunto está en el origen de los ataques contra PHP, localizados en su mayoría en un campus universitario en Norteamérica, según F5 Labs. El 87% del tráfico malicioso procedía de dos únicas IP con ese origen, algo bastante llamativo.

Por ahora no se sabe exactamente quién está detrás de este ataque ni qué pretende exactamente, aunque lo que está claro es que su proceder ha servido para identificar algunos exploits en sistemas PHP que hasta ahora habían pasado desapercibidos. Con cada vez más personas formándose en distintos lenguajes de programación, hoy en día hay más opciones que nunca a la hora de elegir. Todo parece indicar que PHP seguirá reinando, al menos durante un tiempo.

Disponible en:
https://www.ticbeat.com/seguridad/el-81-del-trafico-malicioso-online-se-dirige-al-famoso-lenguaje-php/

2. "EN LOS PRÓXIMOS 4 O 5 AÑOS TODA LA INFORMACIÓN SE ALMACENARÁ EN LA NUBE"

Fecha: 24/04/2019

Pero falta seguridad. Según un informe de Check Point, prácticamente una quinta parte de las empresas mundiales sufre incidentes de seguridad en la nube.

"En los próximos 4 o 5 años toda la información se almacenará en la nube". Así lo afirma Eusebio Nieva, director técnico de Check Point para España y Portugal.

Y este cambio de paradigma trae consigo retos de seguridad que superar. Entre otras cosas, porque se genera una mayor movilidad y libertad de acceso y también porque se amplía la diversidad de los dispositivos utilizados.

El propio Nieva advierte de que "no todas las empresas son realmente conscientes de lo importante que es proteger toda la información disponible en entornos *cloud*" y explica que las nuevas infraestructuras exigen "contar con soluciones de seguridad flexibles y capaces de adaptarse a cualquier situación".

Según un informe publicado por Check Point (Security Report 2019), prácticamente una quinta parte de las empresas mundiales sufrió un incidente de seguridad cloud el año pasado. La cifra exacta es del 18 %.

Para evitar estas situaciones, los expertos recomiendan, en primer lugar**,** la "defensa del host" con la combinación de soluciones antivirus, antispyware y de prevención de intrusiones con herramientas para filtrado de contenidos web y monitorización de registros. También se aconseja el análisis dinámico de ficheros y contenidos en descarga y la tecnología para detectar anomalías en el comportamiento.

En segundo lugar, habría que añadir "control de acceso", incluyendo la gestión de cuentas, las verificaciones de identidades y las restricciones a usuarios no autorizados.

Para proteger los datos, deberían aplicarse soluciones de cifrado. Y, por último, Check Point apunta a la simplificación de procesos. “Una de las reglas fundamentales para todas las empresas es que su estrategia de seguridad debe ser coherente, transparente y operativa”, recalca, además de “sencilla” de gestionar.

Disponible en:
https://www.silicon.es/en-los-proximos-4-o-5-anos-toda-la-informacion-se-almacenara-en-la-nube-2394743

3. LOS CIBERDELICUENTES SE ENFOCAN EN EL CORREO

Fecha:13/04/2019

Los ciberdelincuentes han descubierto una nueva manera de extorsionar a los usuarios: mandan un correo que amenaza con difundir grabaciones comprometidas de su webcam. Éste es sólo un ejemplo de los ciberataques que llegan a través del e-mail.

Hace algunos años, se popularizó una imagen en la que se podía ver a Mark Zuckerberg sentado frente a su portátil. La particularidad de aquella foto era que en ella se podía apreciar que el fundador de Facebook tenía tapada la cámara y el micrófono de su equipo.

Dicha instantánea provocó un debate acerca de la seguridad de estos dispositivos y la posibilidad de que se aprovechase su vulnerabilidad para grabar a los usuarios y, llegado el caso, chantajearlos con la posibilidad de publicar estos registros si se no paga cierta cantidad para evitarlo.

Parece que los ciberdelicuentes están aprovechando este miedo para extorsionar a sus víctimas. Según el ‘Barómetro Mensual ESET NOD32’, elaborado por la compañía de software de seguridad, desde el pasado verano se está observando un aumento considerable del envío de correo electrónico fraudulento, que amenaza con difundir supuestas grabaciones realizadas mientras se visitan webs de contenido pornográfico.

Aunque dicha amenaza no sea real, ya que los ciberdelincuentes no disponen de estas imágenes, el propio contenido del mensaje, unido a que muchos de estos correos suplantan la identidad del remitente o de alguna cuenta corporativa, hace que la víctima se atemorice y acabe cediendo a la extorsión.

Pero éste no es el único ejemplo de ataque a través del correo electrónico. Por ejemplo,

ESET señala que el pasado mes de marzo recibió un e-mail remitido desde una dirección perteneciente a la Junta de Andalucía. La finalidad de este mensaje era que se introdujera la dirección de correo y la contraseña en un formulario. Los investigadores de la compañía descubrieron que estos correos se enviaban desde direcciones legítimas pertenecientes a centros educativos de Andalucía en los que, al menos en uno de los casos, el servidor de correo se había visto comprometido por los atacantes.

Además, la empresa de ciberseguridad recuerda que siguen llegando algún correo que suplanta a empresas o marcas conocidas. En este sentido, el pasado mes detectó una campaña de phishing que suplantaba a Amazon, avisando de un problema con la información de cobro asociada a la cuenta. Los ciberdelincuentes

pretendían que la víctima introdujese los datos de su tarjeta de crédito para usarla en su propio beneficio.

Por otro lado, el informe de ESET advierte acerca de las vulnerabilidades del Internet de las Cosas (IoT, en sus siglas en inglés). Por ejemplo, el pasado mes se descubrieron vulnerabilidades importantes en algunos modelos de marcapasos fabricados por Medtronic. Dichas brechas de seguridad permitirían que un atacante dentro del rango de alcance del dispositivo pudiese interceptar la comunicación que el marcapasos realiza por radiofrecuencia con la consola que proporciona el fabricante. Podría derivar en la posibilidad de leer y escribir en cualquier ubicación de la memoria del dispositivo y modificar su comportamiento.

También despiertan recelos los automóviles conectados. Se ha demostrado la existencia de fallos graves en algunos fabricantes de sistemas de alarmas para coches, pudiendo geolocalizar un vehículo, hacer que se detenga y secuestrarlo, forzando al propietario a abandonarlo.

Asimismo, ESET habla del descubrimiento de una nueva variante de la botnet Mirai, que atenta contra dispositivos IoT como routers, cámaras IP, grabadores de vídeo y equipos de almacenamiento en red. Además, algunas variantes recientes de Mirai tenían como objetivo a los sistemas de presentación inalámbrica WePresent WiPG-1000 y a las televisiones LG Supersign, utilizadas en comercios para mostrar publicidad a la vez que la señal del canal o de la fuente seleccionada. Anteriores variantes incorporaban exploits contra Apache Struts y SonicWall, por lo que algunos investigadores concluyen que los operadores de esta botnet tienen al sector empresarial en su punto de mira.

El estudio también informa de varios casos donde los delincuentes han utilizado una vulnerabilidad en el manejo de ficheros .ACE, que han explotado especialmente en el compresor de ficheros WinRAR, como la distribución del ransomware JNEC.a. ESET especifica que los atacantes engañan a sus víctimas invitándoles a descomprimir un archivo .RAR que contiene el malware junto a una imagen aparentemente corrupta.

Además, la compañía advierte que hay varios foros especializados en la publicación, compra y venta de este tipo de herramientas, pudiendo ser utilizadas posteriormente en actividades delictivas y facilitando que ciberdelincuentes sin conocimientos técnicos desplieguen ataques de manera sencilla.

Por último, el informe recuerda el ataque que recibieron varios usuarios de ordenadores Asus a través de la propia herramienta oficial de actualización de la compañía. Los atacantes aprovecharon para infectar y acceder a unos pocos cientos de equipos, a pesar de que el número total de usuarios a los que se les instaló una puerta trasera a través de esta brecha de seguridad era mucho mayor.

Disponible en:
https://www.silicon.es/ciberdelicuentes-enfocan-correo-2394101

4. ¿ES POSIBLE HACKEAR CUALQUIER CÁMARA DE VIGILANCIA POR INTERNET?

Fecha:08/04/2019

Si tienes una cámara de vigilancia en casa y ésta está conectada a Internet, deberías estar preocupado. Todo dispositivo conectado es vulnerable en mayor o menor medida, pero es que además las llamadas cámaras IP son especialmente jugosas para los atacantes, y es que permiten invadir la intimidad de las personas sin que éstas sean conscientes de ello.

No obstante, ¿es posible hackear cualquiera cámara de vigilancia a través de Internet? La lógica dice que sí, y es que como ya hemos dicho, cualquier dipositivo de potencialmente vulnerable. Sin embargo, no todos lo son en la misma medida.

Normalmente, los hackers y atacantes de todo pelaje se centran en tomar el control de dispositivos cuya seguridad ni es ni mucho menos férrea. Romper una clave segura con dígitos alfanuméricos y varios caracteres distintos toma su tiempo y su esfuerzo, así que lo normal es ir directamente a por aquellas webcam cuya seguridad deja mucho que desear.

En Internet es relativamente fácil encontrar páginas web con cámaras de vigilancia pirateadas, aunque no vamos a citarlas expresamente aquí para no generar interés en esta actividad. La gran cantidad de webcams que están emitiendo online sin que sus propietarios lo sepan nos da una idea de lo fácil que es piratear una cámara que está conectada a Internet.

De hecho, existen buscadores especializados en los que aparecen listados interminables de dispositivos conectados y vulnerables, el paraíso para cualquier persona con los conocimientos necesarios. De ahí a acceder a la señal de la cámara y "rebotarla" a otra página web sólo hay un paso.

Detectar si tu cámara está siendo hackeada en estos instantes es difícil de saber, a no ser que te topes con la emisión online en algunas de esas webs. Por eso, lo mejor es prevenir antes que curar y tomar todas las medidas posibles para evitar que esto ocurra.

Aquí van algunos consejos para que esto no te ocurra

La primera forma de evitar que tu webcam sea pirateada es no conectarla a Internet a menos que sea estrictamente imprescindible. Puedes configurar una red local o almacenar las grabaciones en una tarjeta de memoria. De esta forma, al no tener conexión a la red, nadie puede acceder a ella de forma remota.

Es perfecto si lo que necesitas es una cámara de vigilancia para ver qué ocurre en un lugar concreto pero no necesitas verlo en tiempo real.

Si la conectas, cambia la clave por defecto

Con estas cámaras de vigilancia conectadas a Internet ocurre exactamente lo mismo que con los routers: si no cambias la contraseña por defecto, eres vulnerable. Existen listados de claves de fabricante que sólo tienes que probar para poder piratear un router o webcam, así que si la tuya es "123456789", debes modificarla.

La inmensa mayoría de estas cámaras pirateadas simplemente jamás dieron un paso para mejorar su seguridad.

Disponible en:
https://computerhoy.com/reportajes/tecnologia/posible-hackear-cualquier-camara-vigilancia-internet-401709

5. SI TU CONTRASEÑA ES DE 8 CARACTERES PODRÍAN DESCIFRARLA EN MENOS DE 2 HORAS

Fecha:04/04/2019

Los expertos en ciberseguridad subrayan la importancia de contar con credenciales robustas, carentes de referentes personales y largas. Sin embargo, puede que cualquier clave sea más vulnerable de lo que pensamos.

Resulta una obviedad que qwerty, 123456 o la fecha de tu cumpleaños no son opciones idóneas para elaborar tu contraseña -pese a que sean claves muy usadas por los españoles-.

Desdeñar las credenciales débiles y optar por combinaciones lo suficientemente largas -los expertos recomiendan al menos entre 12 y 14 caracteres-, carentes de significado y de referencias personales, robustas y que no se repitan en los diferentes servicios digitales, así como ricas en mayúsculas, minúsculas, números y símbolos parece de sentido común a la hora de reforzar tu seguridad online.

Pero muchos usuarios optan por una extensión de contraseña bastante escueta, escogiendo por pereza o comodidad –o dificultad a la hora de rerenerla en la memoria– la longitud mínima exigida, de ocho caracteres. Para todos ellos, tenemos una mala noticia: sus claves pueden ser descifradas en un plazo menor a dos horas y en gran parte de los casos, en tan solo unos minutos.

Por qué la contraseña "ji32k7au4a83"es sorprendentemente insegura

Desde Panda Security nos hablan de HashCat, una herramienta de código abierto originalmente concebida para la recuperación de claves pero que puede emplearse también con el propósito de descifrar contraseñas hash de ocho caracteres de Windows NTLM en menos de dos horas y media. NTLM es un antiguo protocolo de autenticación de Microsoft que ya ha sido reemplazado por Kerberos, pero de todos modos ha sembrado dudas en todas las compañías que dependen de Windows y Active Directory.

En un hilo publicado en Twitter, los responsables del proyecto de software apuntaron a que la versión 6.0.0 beta de HashCat superaba el punto de referencia de velocidad de cracking NTLM de 100GH/s (gigahashes por segundo), gracias a que utiliza ocho GPUs Nvidia GTX 2080Ti. Llegando a dicha velocidad de computación es posible probar diversas combinaciones de caracteres por segundo y conseguir cualquier credencial de ocho caracteres en horas o minutos.

Según los datos de HashCat, si tienes una contraseña de ocho caracteres totalmente aleatoria con mayúsculas, minúsculas, números y símbolos, la herramienta la descifrará en el promedio de una hora y quince minutos. Si eliges palabras o nombres con la primera letra en mayúscula y un número al final -un esquema habitual que repiten muchos usuarios-, se identificará de forma instantánea.

La moraleja de esta historia es la importancia de ampliar la extensión de las contraseñas. De hecho, las propias agencias reguladoras deberán corregir su

perspectiva. Organismos como el Instituto Nacional de Estándares y Tecnología de EEUU lo aconsejaban, lo que ha derivado en miles de compañías recomendando esa política.

A partir de ahora, opta por extensiones superiores a 12 caracteres -y si puedes a 15-, recuerda emplear gestores de contraseña, grupos de palabras sin conexión aparente y símbolos, números, mayúsculas y minúsculas. Es fundamental activar siempre la autenticación en dos pasos.

Disponible en:
https://www.ticbeat.com/seguridad/contrasena-menos-8-caracteres-horas/

USO SOCIAL DE LAS TIC

1. CÓMO SERÁN LAS FUTURAS CASAS EN MARTE DE LA NASA IMPRESAS EN 3D

Fecha: 02/05/2019

Fueron ideadas como parte de un concurso para instalar colonias humanas, la Agencia Espacial de EEUU presentó los tres proyectos finalistas. En mayo se conocerá al ganador

La idea de colonizar Marte está cada vez más adelantada. Y los proyectos para que eso suceda en un futuro muy próximo se viven con intensidad.

Como parte de un concurso para instalar colonias humanas en el planeta rojo en la próxima década, la Agencia Espacial de EEUU presentó los tres proyectos finalistas, todos con la tecnología de la impresión 3D.

Así, los equipos que compiten en el 3D-Printed Habitat Challenge de la NASA completaron el último nivel de la competencia: construcción virtual completa, y los tres primeros ganaron una parte del premio de 100.000 dólares.

Esta nueva etapa requería que los equipos crearan un diseño de hábitat a gran escala, utilizando software de modelado. Este nivel se construyó sobre una etapa anterior que también requería modelado virtual.

En total hubo once propuestas que fueron evaluadas según el diseño arquitectónico, la programación, el uso eficiente del espacio interior y la escalabilidad de impresión en 3D y la capacidad de construcción del hábitat.

Además, los equipos realizaron la presentación de los hábitats en videos con información sobre sus diseños, así como modelos en miniatura impresos en 3D que se separaron para mostrar el diseño interior. También se otorgaron puntos por representación estética y realismo.

El Equipo SEArch +/Apis Cor, de Nueva York quedó en primer puesto. La forma única de su hábitat permite un refuerzo continuo de la estructura. La luz entra a través de puertos en forma de canal en los lados y la parte superior, según la NASA.

El Equipo Zopherus, de Arkansas resultó en segunda posición. El diseño del equipo sería construido por una impresora itinerante autonoma que imprime una estructura y luego se mueve al siguiente sitio.

Finalmente, el Equipo Mars Incubator, de Connecticut, quedó en tercero con un diseño que representa un aspecto modular de las viviendas espaciales y permite una gran cantidad de luz natural.

Disponible en:
https://www.infobae.com/tendencias/innovacion/2019/04/16/como-seran-las-futuras-casas-en-marte-de-la-nasa-impresas-en-3d/?fbclid=IwAR3mux3th0kYiy0GqS3hW3Xaaq8KyVF2Tmn7tCeIYl8pc9vJM1-vbxdvFbM

2. GOOGLE MAPS YA LOCALIZA PUNTOS DE CARGA DE COCHES ELÉCTRICOS

Fecha: 1/05/2019

Informa de cuantos puertos están disponibles.

Los puntos de interés de los usuarios siempre son cambiantes y cada vez más amplios. Si alguien sabe de eso es Google, que cuenta con nuestros datos, le pese a quien le pese, y que ha actualizado Google Maps para que los usuarios puedan buscar cuál es su estación de recarga eléctrica más cercana.

Para ver dónde encuentran todos los cargadores registrados solo hay que introducir en el buscador “EV charging stations” (buscando en español por “estaciones de carga EV” los resultados son menos numerosos) y aparecerán todos los existentes de diversas empresas entre las que se encuentran EVgo, Chargemaster, SemaConnect, ACS Group o Threeforce. Eso, claro está, además de los puntos de carga de Tesla.

El concurso culminará con una estructura de subescala impresa cara a cara del 1 al 4 de mayo de 2019 y la entrega de un premio de 800.000 euros al ganador.

Lo más destacado, sin embargo, es el hecho de que también dé el dato de cuántos puertos están disponibles, por lo que los poseedores de un vehículo electrificado ya no tendrán que lidiar con la situación de circular hasta un punto solo para comprobar que está ocupado por otro coche.

Google ya ha habilitado esta nueva función y está activa en navegadores y dispositivos móviles, tanto Android como iOS, además de estar integrada en Android Auto.

Disponible en:
https://computerhoy.com/noticias/motor/google-maps-ya-localiza-puntos-carga-coches-electricos-412899?fbclid=IwAR0vwimqY0lSGrDXpbb-8Ygd29KhPInE75U6d6ihrLtKaYsZjQZEJUnPM0U

3. CONCLUYE LA CONSTRUCCIÓN DEL NUEVO CABLE DE DATOS INTERCONTINENTAL CURIE.

Fecha: 29/04/2019

Este cable submarino, financiado completamente por Google, forma parte de la estrategia de la compañía para mejorar la prestación de sus servicios en Latinoamérica. La infraestructura conecta Los Ángeles con Chile, un país que está atrayendo las inversiones en interconexión global de otros gigantes tecnológicos como AWS o Huawei.

En los últimos años, la industria de interconexión global ha visto como nuevos actores han comenzado a invertir en sus propias redes de datos intercontinentales, sin ser compañías dedicadas especialmente a las telecomunicaciones.

Entre ellas se cuentan los principales proveedores de servicios en la nube, como Google, que ha invertido en diversos proyectos de esta naturaleza. El último en concluirse ha sido el cable submarino Curie, que une el centro de datos de Equinix en Los Ángeles con el datacenter de Google en Quilicura, cerca de la capital de Chile, con una estación de aterrizaje en Valparaíso.

Este cable permitirá a Google mejorar la cobertura de sus servicios en América Latina. Además, se prevé la incorporación de un futuro ramal que conectará esta infraestructura con Panamá. Según comentó Jayne Stowell, de Google, “Aunque este cable es uno de los trece financiados por Google e instalados en el mundo, Curie nos convierte en la primera empresa de tecnología que, sin ser un especialista en telecomunicaciones, invierte en el desarrollo de infraestructura de este tipo 100% privado”.

La construcción de este cable, de más de 10.000 kilómetros de longitud, corrió a cargo de SubCom, una empresa especializada en la instalación de redes submarinas, y tuvo un coste final de unos 47.000 millones de dólares. Esto, finalmente, superó las previsiones iniciales anunciadas por Google, que eran de unos 30.000 millones, pero la compañía lo considera un gran logro en su estrategia de expansión global. Por su parte, el gobierno de Chile valoró positivamente las posibilidades que esta infraestructura brindará al país, tanto a las empresas como a los usuarios de en general.

Este país tiene en sus planes mejorar drásticamente su infraestructura de Internet, lo que está atrayendo las inversiones de otras grandes compañías tecnológicas, que reconocen el potencial que representa Chile en el mercado latinoamericano. Un ejemplo de ello es el cable proyectado por Huawei Marine denominado FOA (Fiber Optic Austral), que para finales de 2019 conectará diferentes regiones del sur del país, con el que será el cable submarino más meridional del planeta. Y la compañía ya tiene planes para un futuro proyecto más ambicioso, que llevaría la conexión hasta China. La mejora de las infraestructuras de interconexión en esta región de globo reforzará el potencial de la nube en Asia Pacífico, proporcionando nuevas vías de entrada a los mercados americanos.

Disponible en:
https://almacenamientoit.ituser.es/noticias-y-actualidad/2019/04/concluye-la-construccion-del-nuevo-cable-de-datos-intercontinental-curie?fbclid=IwAR0s6gFAnpCjG6GINbQT82KIxqpHx-2uEAPayEAnMmylvDHkHIV0oTAmP9A

REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Sistema de Vigilancia Tecnológica