Enero 2021

Ciber Eguraldia
BCSC

⛈ Noticias generales	⛈ Incidentes de ciberseguridad	⛈ Estafas y fraudes
⛈ Malware y vulnerabilidades	🌤 Fugas de información	🌤 Ciberseguridad industrial

Noticias generales

La inversión en ciberseguridad crecerá un 10% este año

Más de 12.000 millones de registros se vieron comprometidos en 2020, mientras que el número de ataques de ransomware conocidos aumentó en casi un 60%. El trabajo y el aprendizaje masivo a distancia y la aceleración de los proyectos de transformación digital mantendrán esta tendencia en 2021.

El 86% de las compañías españolas carecen de una cultura de ciberseguridad

Según un estudio de PwC. el nivel de cultura de ciberseguridad en las compañías en España es de 2,8 puntos sobre 5, el presupuesto medio destinado a concienciar y formar en ciberseguridad supone solo un 9% del total destinado a seguridad de la información y solo el 11% de las compañías miden la concienciación de los empleados en este ámbito.

Detienen al responsable de DarkMarket, el mayor mercado de la Darknet con más de 500,000 usuarios y 2.400 vendedores

El DarkMarket original fue desmantelado en 2008, con su creador en prisión. El nuevo mercado recogió el nombre y ha alcanzado un tamaño varios niveles por encima de lo que tuvo entonces, con más de medio millón de usuarios y unos 2.400 vendedores en el momento de la detención.

La seguridad de los empleados y la prevención de ataques, principales desafíos para 2021

La mitad de los responsables de TI señalan que su enfoque de seguridad no volverá a ser igual que antes de la pandemia. Las principales prioridades hasta 2023 son asegurar el trabajo remoto, la seguridad de los endpoints y dispositivos móviles, y la seguridad de la nube pública y el multicloud.

El 88% de los ciberdelitos son estafas en pagos digitales

El creciente uso de los pagos digitales ha venido acompañado de un incremento de los fraudes porque los estafadores se benefician de sus graves brechas de seguridad. El 88% de los ciberdelitos denunciados en 2019 correspondía a estafas informáticas vinculadas a pagos digitales, que se elevaron hasta superar las 192.000 denuncias.

Incidentes de ciberseguridad

Emotet, "el malware más peligroso del mundo", ha sido desmantelado por una acción policial a nivel mundial

En una acción coordinada a nivel internacional, los investigadores de cuerpos policiales y judiciales de países como Alemania, Estados Unidos, Reino Unido, Francia, Países Bajos, Lituania, Canadá y Ucrania han logrado tomar el control de la infraestructura que controlaba la red. Todo ello bajo la coordinación de Europol y Eurojust, el órgano europeo de coordinación judicial entre países.

Destapada una campaña contra investigadores de seguridad

El grupo de análisis de amenazas de Google hizo pública su investigación acerca de una campaña contra investigadores de seguridad de diferentes compañías. Al parecer, la campaña se habría llevado a cabo en los últimos meses de 2020 y las primeras semanas de este mes de enero. Según el informe, el origen de esta campaña podría encontrase en Corea del Norte, y probablemente haya sido respaldada por el propio gobierno.

El FBI advierte a compañías sobre ataques del ransomware Egregor en todo el mundo

El comunicado advierte a las empresas que el ransomware Egregor, que aparentemente lleva más de 150 víctimas en distintas partes del mundo, está robando información y cifrando archivos para luego solicitar un rescate utilizando diferentes tácticas para lograr sus objetivos.

Estafas y fraudes

Cuidado si te llaman diciendo que te van a poner la vacuna contra la COVID-19 en tu casa: la Guardia Civil dice que es un "intento de estafa"

Según la Guardia Civil, se trata de un "intento de estafa" con el que pretenden "acceder a la vivienda de personas que vivan solas". Estas llamadas coinciden con la campaña de vacunación que se inició el pasado 27 de diciembre en España, según el Ministerio de Sanidad.

Si recibes un email suplantando a la DGT con una supuesta multa, no piques!

Desde INCIBE se ha detectado una campaña de envío de correos electrónicos fraudulentos que tratan de suplantar a la Dirección General de Tráfico (DGT) con el propósito de difundir malware. En dicha campaña, se envía un correo al usuario suplantando al Ministerio del Interior, con el asunto «AVISO – Multa de tráfico no pagada- Nº (XXXXX)]», donde las XXXXX son cifras.

“Detalles del envío”: suplantan a empresas de transporte como DHL y Fedex para robar información

Básicamente consiste en enviar un correo haciéndose pasar por una de estas conocidas empresas de transporte y mensajería indicando que se adjunta un documento relacionado con una factura o justificante de envío, con la esperanza de que el usuario que reciba el email lo abra.

Factura pendiente de Vodafone y Burofax online. Vuelven las campañas de troyanos bancarios

En su retorno a la acción los delincuentes no han innovado demasiado, ya que han reutilizado plantillas de correos ya conocidas y usadas en campañas anteriores, como son las que suplantan la identidad de la empresa de telecomunicaciones Vodafone actualizando, eso sí, las fechas que se incluyen en el correo pero sin corregir varias faltas de ortografía.

“Confirmación del pedido” Utilizan correo suplantando a Amazon para obtener tu tarjeta de crédito

En esta ocasión nos encontramos con un correo que simula la confirmación de un pedido realizado a Amazon, con una fecha de entrega y número de pedido para tratar de hacerlo más creíble para el usuario que lo reciba.

Detienen a 18 personas en Vizcaya por un centenar de estafas en internet, también en Cantabria

Los estafadores contactaban con sus víctimas a través de conocidos portales de compraventa y acordaban la venta de productos que no llegaban a pagar y que posteriormente vendían.

Malware y vulnerabilidades

Vulnerabilidades zero-days en iOS

Apple ha hecho públicas tres vulnerabilidades de tipo zero-day catalogadas como críticas que afectan a productos con sistemas operativos macOS e IOS. La primera de ellas afecta al kernel, parte fundamental del sistema operativo que permite al resto del software acceder al hardware. Las otras dos vulnerabilidades se descubrieron en el motor del navegador WebKit, desarrollado por Apple para Safari. El propio fabricante insta a actualizar a las versiones iOS 14.4 y iPadOS 14.4 cuanto antes para solucionar estos fallos.

Vulnerabilidad en SUDO

Investigadores de seguridad de la empresa Qualys han alertado sobre una vulnerabilidad crítica en la utilidad SUDO, presente en casi la totalidad de sistemas operativos basado en Unix y Linux. Este programa permite ejecutar instrucciones con los privilegios de seguridad del usuario root (usuario que tiene acceso administrativo al sistema) siempre y cuando se tengan privilegios o se conozca la contraseña de dicho usuario.

Vulnerabilidad día cero afecta soluciones VPN de SonicWall. ¿Cómo mitigar el riesgo de explotación?

El equipo de seguridad de SonicWall emitió una alerta de seguridad relacionada con un grupo de hackers que ha estado explotando una falla día cero en sus soluciones de red privada virtual (VPN) que podría permitir el despliegue de ataques internos. Los productos de SonicWall son empleados por toda clase de pequeñas y medianas y grandes empresas, por lo que los expertos consideran que este es un problema de gran alcance.

Vulnerabilidad en el core de Drupal

Se han publicado una vulnerabilidad de severidad crítica, en la librería Archive_Tar, que afecta al core de Drupal. La comprobación inadecuada de los enlaces simbólicos en la librería Archive_Tar podría permitir operaciones de escritura con Directory Traversal . Se ha asignado el identificador CVE-2020-36193 para esta vulnerabilidad.

Microsoft corrige zero day y otras 83 vulnerabilidades en actualización de enero

En esta edición del popularmente conocido Patch Tuesday, la compañía reparó un total de 83 vulnerabilidades presentes en distintos productos. Del total de vulnerabilidades reparadas, 10 fueron catalogadas como críticas. Uno de los fallos corregidos es una zero-day que afecta a Microsoft Defender.

Hallan una puerta trasera en más de 100000 firewalls y VPN Zyxel

Afecta al fabricante de equipamiento de red Zyxel, del que se habría filtrado credenciales “hardcodeadas” (escritas en claro) dentro del código de su software, y que pondrían en manos ajenas, potencialmente, unos 100000 dispositivos o más.

Fugas de información y privacidad

Encuentran una vulnerabilidad en TikTok que deja al descubierto datos como el número de teléfono y la información de los perfiles de usuarios

Concretamente, el error estaría en la función "Encontrar amigos", explica la compañía, que permitiría a ciberdelincuentes acceder a la información del perfil de los usuarios. Esta incluye el número de teléfono, nombre, foto de perfil, avatar, identificaciones únicas e incluso configuración del perfil.

Multa récord de la Agencia de Protección de Datos a Caixabank: 6 millones de euros por forzar la cesión de datos personales

Es la mayor multa de la Agencia Española de Protección de Datos, con 6 millones de euros. Un mes después de sancionar al BBVA, la AEPD multa a Caixabank con varias sanciones relacionadas con el uso indebido de los datos.

Ubiquiti pide cambiar la contraseña por una filtración de datos

El motivo de esto es un ataque sufrido por parte de sus sistemas alojados en un proveedor de nube externo. Esto ha provocado que los datos de los usuarios hayan podido filtrarse, de ahí la importancia de cambiar las claves de inmediato y evitar problemas mayores.

Ciberseguridad industrial

Las auténticas razones por la que los ciberdelincuentes están multiplicando sus ataques contra las vacunas

Los ciberdelincuentes habían comenzado a centrar sus ataques informáticos en las farmacéuticas que ultiman sus fármacos contra el coronavirus. También contra las cadenas de frío, infraestructuras logísticas indispensables para garantizar la distribución de muchas de las dosis.