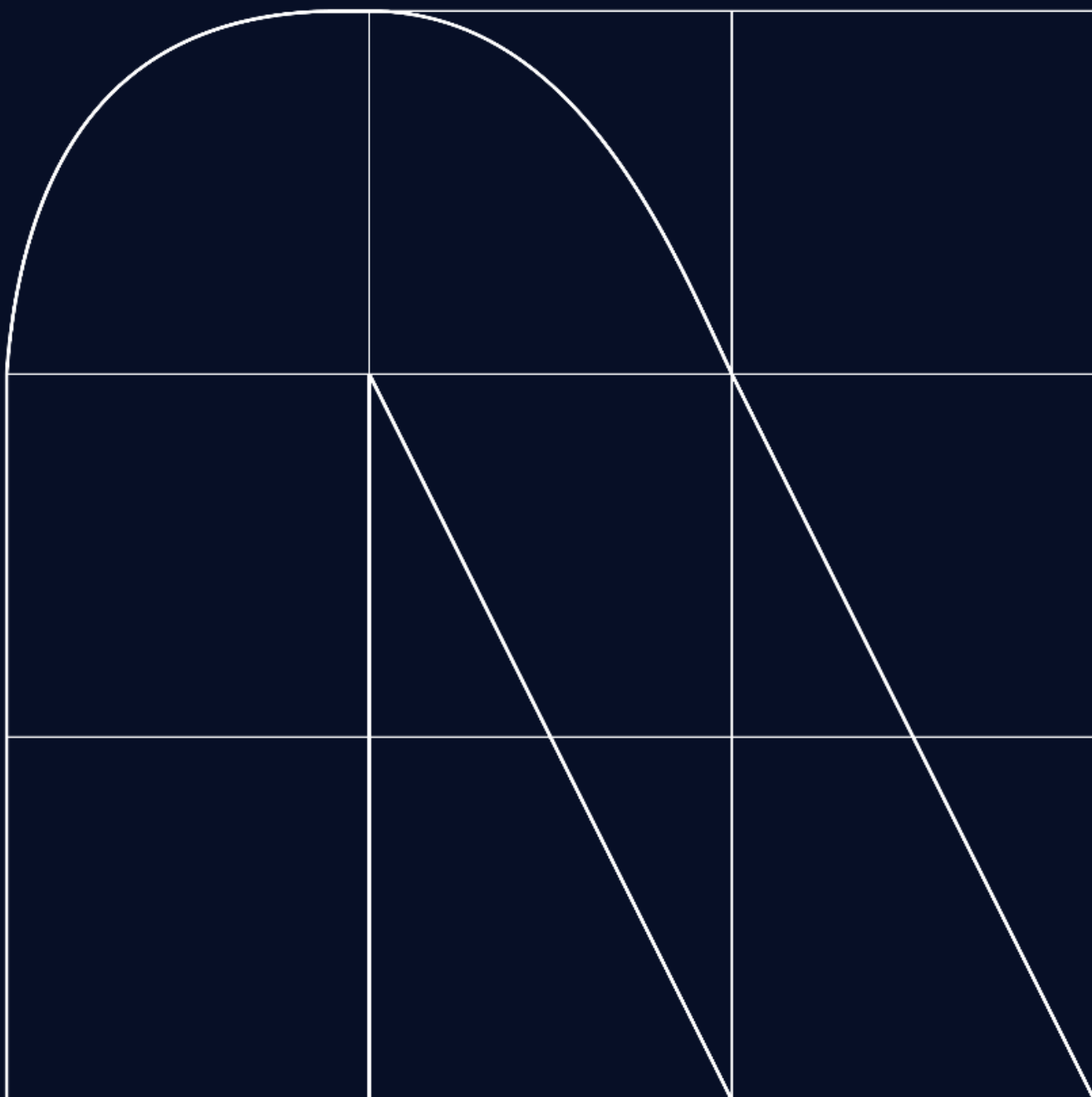
Número 84 | Noviembre 2023

NTT DATA

Radar

El magazine de ciberseguridad



Los cables de comunicaciones submarinas, una infraestructura crítica que necesita protección.

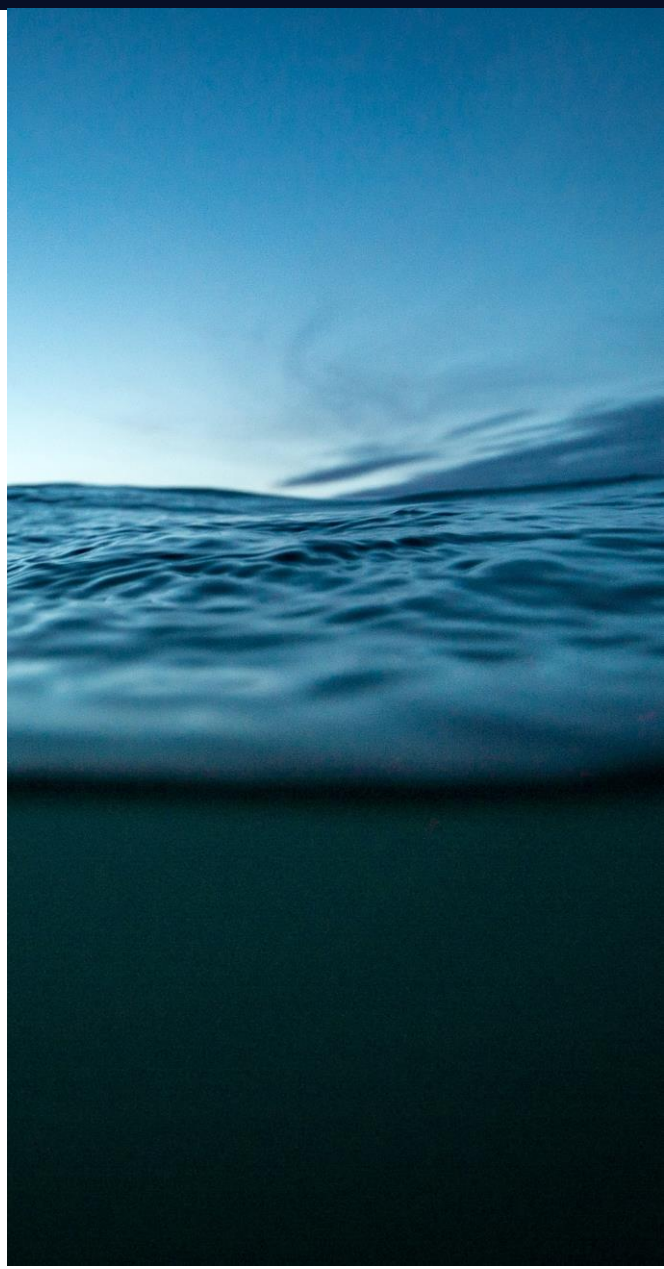
Por: Jorge Trujillo Ramirez

La comunicación global depende en gran medida de una infraestructura crítica que a menudo pasa desapercibida: los cables de comunicaciones submarinos.

Estos cables, que se extienden por miles de kilómetros en el fondo del océano, son la columna vertebral de la conectividad mundial, permitiendo la transmisión de datos, voz y video a través de los océanos. Sin embargo, y aunque la ubicación exacta de los mismos se mantiene en secreto y se utilizan técnicas de cifrado para proteger la información, la creciente dependencia de estas redes submarinas, el 99 % de las comunicaciones digitales del mundo transitan por la red, ha aumentado la preocupación sobre los riesgos de ciberseguridad que enfrentan, y es que este de la seguridad de los cables ha sido un elemento poco estudiado en la seguridad internacional (según advierte un informe del parlamento europeo "Security threats to undersea communications cables and infrastructure – consequences for the EU" June 2022), y no es nada sencillo, ya que afecta a la gobernanza de los océanos, la soberanía digital, la política de infraestructuras críticas y diversos aspectos de la acción exterior, desde la política de defensa hasta la política de seguridad.

En el mundo hay unos 400 cables, de los cuales 250 pasan por Europa, España con 32 puntos de aterrizaje conecta 4 continentes: Europa, África, Asia y Norteamérica y es el punto estratégico de conexión global de la Unión Europea.

La media anual de incidentes que causan cortes es de aproximadamente un centenar. La gran mayoría se producen por negligencias en las operaciones pesqueras cerca de ellos, pero la acumulación de cortes en los últimos meses ha vuelto a poner encima de la mesa la posibilidad de otro tipo de ataques o sabotajes aumentando la alerta sobre este tipo de infraestructuras, lo que ha motivado el último informe de ENISA, "SUBSEA CABLES - WHAT IS AT STAKE? publicado a finales de julio de este año, en este documento se señalan que casi el 40% de los fallos en los cables se deben a fondeos o pesca, mientras que en casi la otra mitad no hay una causa específica. En total, el 87% de los incidentes son causados por la intervención humana, ya sean errores no intencionados o acciones maliciosas intencionadas, sólo el 4% de las incidencias se atribuyen a fallos del sistema (fallos de planta) y el 5 % se deben a fenómenos naturales.



Las inteligencias artificiales (IA), como ChatGPT, no están necesariamente diseñadas específicamente para el ámbito de la ciberseguridad, pero pueden ser entrenadas para realizar tareas relacionadas con la seguridad informática.

El entrenamiento de una IA para la ciberseguridad implica enseñarle a reconocer patrones y anomalías en los datos, y a tomar decisiones basadas en esa información. Esto se logra a través de la alimentación de la IA con grandes cantidades de datos de seguridad, como registros de actividad de red, registros de eventos de seguridad, registros de aplicaciones y datos de amenazas conocidas.

Una vez que la IA ha sido entrenada en la identificación de patrones y anomalías, puede aplicarse a diversas tareas de ciberseguridad, como la detección de intrusiones, la identificación de malware, la monitorización de la actividad de red, la predicción de comportamientos maliciosos, y la respuesta automática a eventos de seguridad.

Para mantener una IA de ciberseguridad efectiva, es necesario que se actualice regularmente con nuevos datos y técnicas de amenazas. También es importante que las decisiones tomadas por la IA se supervisen y se ajusten según sea necesario para garantizar la precisión y la efectividad en la protección de los sistemas informáticos y los datos.

Para ChatGPT, el modelo GPT-3.5 se entrena en una gran cantidad de datos no estructurados de diferentes fuentes, que incluyen páginas web, libros, artículos de noticias, foros y redes sociales, con el objetivo de aprender patrones y asociaciones en el lenguaje natural. A través de esta capacitación continua, el modelo se vuelve cada vez más preciso y efectivo en su capacidad para entender y generar lenguaje natural.

En resumen, los cables submarinos de comunicaciones son una parte fundamental de la infraestructura global de telecomunicaciones que permite la comunicación a larga distancia en todo el mundo. Su seguridad y confiabilidad son de suma importancia para la economía global y la sociedad actual, los riesgos de ciberseguridad son una preocupación creciente en un mundo cada vez más interconectado y en el que según el informe de parlamento europeo no se ha puesto suficiente foco hasta ahora. Proteger esta infraestructura crítica es esencial para garantizar la seguridad y la continuidad de nuestras comunicaciones globales, por eso proponemos que se añada en los análisis de riesgos las amenazas relacionadas con este tema y además de se haga un exhaustivo seguimiento y monitorización de la evolución de los mismos para detectar y alertar lo antes posible.

Jorge Trujillo Ramirez
Project Leader de Ciberseguridad en NTT DATA Perú

Cibercrónica

Por: NTT DATA Europe & Latam

La inteligencia artificial se ha convertido en una herramienta muy potente tanto para realizar ataques como para las defensas cibernéticas a gran escala.

En conflictos recientes hemos podido ver cómo se han utilizado tácticas de guerra cibernética para obtener ventajas estratégicas. Estos ciberataques incluyen la infiltración de sistemas, la desinformación y la interrupción de servicios en línea.

La inteligencia artificial (IA en adelante) ha sido una herramienta clave en estos ciberataques, ya que permite automatizar y optimizar sus operaciones. A continuación, se detallan algunos ejemplos de uso de IA en ciberataques:

Ataques de phishing avanzados: La IA se utiliza para crear correos electrónicos de phishing altamente personalizados y convincentes, diseñados para engañar a los destinatarios y obtener información confidencial.

> “La guerra cibernética en estos conflictos es un recordatorio de cómo la tecnología y la inteligencia artificial están siendo utilizadas en el campo de batalla moderno.

Malware inteligente: Los ciberdelincuentes emplean IA para desarrollar malware capaz de evadir las defensas tradicionales y adaptarse a las condiciones en tiempo real.

Detección de vulnerabilidades: Los actores cibernéticos pueden utilizar la IA para buscar constantemente vulnerabilidades en sistemas informáticos y redes, lo que les permite identificar y explotar debilidades.

Ataques de denegación de servicio (DDoS): La IA se utiliza para coordinar y amplificar ataques DDoS, lo que hace que sean más difíciles de mitigar.

Desinformación y manipulación en redes sociales: La IA puede automatizar la creación y difusión de noticias falsas y desinformación en plataformas de redes sociales, lo que puede influir en la opinión pública.

En estos casos, también se usa la inteligencia artificial para fortalecer sus defensas cibernéticas. La IA se utiliza para detectar amenazas, identificar patrones anómalos y mejorar la seguridad de los sistemas críticos.

La guerra cibernética en estos conflictos es un recordatorio de cómo la tecnología y la inteligencia artificial están siendo utilizadas en el campo de batalla moderno. Estos desarrollos plantean desafíos significativos para la ciberseguridad y ponen de manifiesto la importancia de la cooperación internacional en la prevención y mitigación de ciberataques en tiempos de conflicto.

FraudeGPT

Hablando de otros temas, en el radar pasado hablábamos de unas herramientas nuevas en el mercado, como “FraudeGPT”. Estas herramientas implementan la tecnología IA para la detección y prevención de fraude, y ya muchas empresas españolas han empezado a confiar en ellas.

Estudios realizados en nuestro país demuestran que el fraude sigue siendo una de las mayores preocupaciones tanto para empresas como consumidores. Uno de cada cinco españoles admite haber sido víctima de fraude en alguno de sus pagos, dejando la media de dinero estafado alrededor de los 160$
Otro de estos estudios resalta que los intentos de fraude han ido aumentando a lo largo de estos últimos años. Aun así, un 60% de minoristas confía en que sus sistemas de detección de fraude son eficaces, habiendo solo un 24% de ellos que afirmen haber invertido en sistemas de prevención y respuesta en el último año.

Para combatir esta creciente amenaza, se está implementando la IA en herramientas de detección de fraude. Según las encuestas realizadas, ya un 53% de los minoristas españoles aprovechan las capacidades de la inteligencia artificial para defenderse ante el fraude, además de softwares de gestión de chargeback para la gestión y reducción del coste asociado. Viendo la situación y las previsiones de futuro, se recomienda que las empresas inviertan en no solo herramientas de gestión y prevención, sino en adaptar estas a sus necesidades específicas, aprovechar el aprendizaje automático y trabajar en la distinción de compradores legítimos de otros actores maliciosos.

Resiliencia en blockchain: ¿Es necesario un plan de recuperación ante desastres?

ANÁLISIS

Uno de los grandes retos para las compañías es estar preparadas ante una disrupción que pueda poner en peligro la continuidad de sus procesos críticos, y cuyas respuestas de recuperación mitiguen lo máximo posible los impactos negativos (reputacional, económicos, operativos, legales, etc.) que ha generado o puede generar la contingencia.

El contexto actual que tenemos a nivel mundial (efectos medioambientales extremos, falta de energía, tensiones políticas, aumento del cibercrimen…) pone en evidencia el riesgo que tienen las compañías de sufrir algún tipo de disrupción. Las organizaciones están tomando conciencia y focalizando sus esfuerzos en identificar los riesgos que pueden afectar a su operativa para trazar una estrategia que los mitigue aquellos riesgos que puedan poner en peligro la disponibilidad de los servicios tecnológicos de las compañías.

Una de las estrategias más comunes y recurrentes para las compañías son los planes de Recuperación ante Desastres (DRP, por sus siglas en inglés). Estos planes constituyen una parte esencial de la estrategia operativa y de seguridad de cualquier negocio, ya que diseñados para asegurar que las operaciones se recuperan con celeridad en caso de disrupciones inesperadas (desastres naturales o causados por humanos). Sin embargo, con la aparición del Blockchain y la decisión de algunos negocios de construir sus modelos basándose esta tecnología, o incluso de trasladar sus modelos existentes a esta nueva tecnología, se plantea un posible cambio en las prácticas respecto a los DRP.

Una de las principales características de las redes Blockchain es la capacidad de resistir fallos. Esta cualidad se deriva de su diseño, que se forma a partir de nodos independientes q formados por redes descentralizadas y distribuidas. A diferencia de los sistemas tradicionales centralizados, en los que un fallo puede paralizar todo el sistema, los sistemas Blockchain son fundamentalmente resistentes a este tipo de interrupciones. En una empresa cuyos sistemas se encuentren basados en Blockchain, como por ejemplo las *dApps* (aplicaciones que funcionan en una red Blockchain de forma descentralizada), el concepto de la distribución desempeña un papel muy importante en su planificación ante un posible desastre. Para que una red Blockchain caiga es necesario que todos los nodos que la componen caigan, pues cada nodo contiene una copia entera del Blockchain y es capaz de operar de forma independiente.
Ethereum, una de las redes Blockchain más grandes y populares en el mundo empresarial por su capacidad de guardar los llamados “Contratos Inteligentes” (programas autoejecutables almacenados en una red Blockchain que se activan cuando se cumplen ciertas condiciones predefinidas), tiene varios miles de nodos distribuidos por el mundo. Para forzar la caída de esta red Blockchain sería necesario comprometer sus nodos a través de uno de los siguientes métodos:

•Que se produzca un fenómeno natural a nivel mundial que arrasase todos los nodos. Este evento debe afectar a todas las zonas geográficas que tengan nodos y debe comprometer el suministro eléctrico o la conexión a internet, ambos factores esenciales para la red Blockchain. Este fenómeno provocaría una caída de servicio de la red Blockchain por no haber nodos operativos que puedan sostener la red.

•También se podría comprometer la red mediante algún ataque que, en función del mecanismo de consenso de la red Blockchain, busque tomar el control de la red. Aunque esto no afectaría necesariamente a la disponibilidad del servicio, sí comprometería la confiabilidad de los datos, ya que un actor malintencionado con suficiente control sobre la red podría intentar manipular las transacciones o incluso revertir las ya realizadas, rompiendo la confianza inherente al sistema. Aunque se podría comprometer un único nodo con relativa facilidad (ej. Tomar el control físicamente del nodo), para comprometer la red entera se deberían comprometer un gran número de nodos (el 51% de los nodos en un *Proof of Work* o aquellos nodos que sumen el 51% de los tokens de la red en un *Proof of Stake*). Esto sería un proceso extremadamente costoso y que con práctica certeza sería identificado por la comunidad, quienes podrían entonces tomar medidas para prevenirlo.

Cabe destacar que ambos casos, tanto el desastre natural a nivel global como el ataque masivo a los nodos, se plantean como hipótesis con una probabilidad muy baja.

Cabe destacar que en el mundo de la seguridad siempre se habla sobre las tres dimensiones de la seguridad: disponibilidad, integridad y confidencialidad. La disponibilidad es la garantía de acceso a la información cuando hace falta, la integridad habla de protección de la información ante manipulaciones no deseadas y la confidencialidad se refiere a asegurar que el acceso solo se permite a aquellas personas autorizadas. Teniendo esto en cuenta, podemos comprobar que las características básicas del Blockchain protegen la disponibilidad mediante la distribución de nodos y la integridad de la información ya que cada nodo contiene una copia entera del Blockchain criptográficamente protegida (para asegurar su inmutabilidad). La confidencialidad, sin embargo, es un desafío mayor debido a la transparencia inherente de las redes Blockchain (sí existen medidas alternativas para asegurar la confidencialidad, pero acostumbran a tener una mayor complejidad). Por tanto, las empresas que den especial importancia a la disponibilidad y la integridad de la información deberían considerar la posibilidad de incorporar Blockchain en sus operaciones o trasladar su modelo a esta tecnología.

María Lezana Juberías
Cybersecurity Expert NTT DATA Europe & Latam

Óscar Marimon Rius
Cybersecurity Consultant NTT DATA Europe & Latam

La preocupante sofisticación del vishing con la Inteligencia Artificial Generativa.

TENDENCIAS

El phishing y sus diversas mutaciones continúan siendo una de las estrategias más utilizadas por ciberdelincuentes en la actualidad. A pesar de los esfuerzos crecientes de las empresas para educar a sus empleados sobre estos ataques, aún presenciamos numerosos ejemplos de esta técnica en acción.

Durante este año, hemos sido testigos de campañas de phishing que suplantan la identidad de instituciones respetadas como la Agencia Tributaria y la Dirección General de Tráfico (DGT), empleando envíos masivos de sms fraudulentos que alegan sanciones monetarias inexistentes y dirigen a los usuarios a sitios web maliciosos.

En particular, en los últimos meses, las técnicas de vishing han ganado notoriedad. El vishing es un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima. Ejemplo de ello es una campaña que suplantaba al Instituto Nacional de Ciberseguridad de España (INCIBE) con el objetivo de robar datos personales de usuarios. Esta estratagema combinaba vishing y phishing, comenzando con llamadas telefónicas en las que los atacantes se hacían pasar por representantes del INCIBE, intentando persuadir a los usuarios para que proporcionaran información, incluyendo sus direcciones de correo electrónico, como parte de su esquema fraudulento.

Otro incidente destacado es el hackeo de MGM Resorts International, un conglomerado que gestiona algunos de los casinos más grandes de Las Vegas. El grupo de atacantes, conocido como "Scattered Spider", investigó a los empleados de MGM en LinkedIn y utilizó la identidad de uno de ellos para llamar al servicio de asistencia técnica y solicitar un restablecimiento de contraseña. En apenas 10 minutos, los ciberdelincuentes habían logrado acceder a la red.

El uso de la voz e imágenes de individuos para fines fraudulentos no es novedoso, pero resulta sorprendente la facilidad con la que los atacantes pueden manipular estas tecnologías para sus propios propósitos. A lo largo de este año, hemos sido testigos de múltiples campañas de estafas que emplean la voz e imagen de celebridades, como Elon Musk, quien ha sido objeto frecuente de estos engaños, especialmente en el ámbito de las criptomonedas. Algunos de los ataques más notorios involucran el pirateo de canales de YouTube con una amplia audiencia que, de la noche a la mañana, empiezan a difundir contenido fraudulento.

Recientemente, una campaña falsa se volvió viral, utilizando la identidad de Jimmy Donaldson, conocido como MrBeast, para supuestamente sortear un iPhone 15 Pro entre 10,000 personas. Lo impactante de estas campañas es la rapidez con la que un ciberdelincuente puede ejecutarlas utilizando herramientas como HeyGen.

Esta tecnología, cuando está en manos de actores maliciosos con mayores conocimientos y recursos, puede ser utilizada para influir en conflictos internacionales. Un ejemplo se vivió en Rusia, donde se hackearon emisoras de radio y canales de televisión para difundir deepfakes de Vladimir Putin, anunciando información falsa sobre retiradas y movilizaciones masivas.

El vishing, combinado con herramientas de inteligencia artificial generativa, ha evolucionado rápidamente y se ha convertido en una amenaza significativa. Estos ataques aprovechan la suplantación de identidad, el uso de figuras públicas y la manipulación de la voz para engañar a las víctimas. La facilidad de creación de deepfakes y campañas fraudulentas plantea desafíos adicionales para la ciberseguridad.

La UE tomó la iniciativa a mediados de este año para impulsar la primera ley europea sobre inteligencia artificial, prevista para finales de año y que regula varios aspectos de los usos de esta tecnología e incluye bajo vigilancia a sistemas como ChatGPT. Bajo esta ley los proveedores deberán identificar y mitigar los potenciales riesgos y cumplir con requisitos de transparencia avisando de que contenido ha sido generado mediante IA y ayudar a distinguir las imágenes reales de las “Deepfake”.

Además de esto, como reacción al auge del contenido generado mediante IA han aparecido cada vez más herramientas para detectar este. Twitter ya ha lanzado herramientas para combatir la desinformación en su plataforma y Google lanzó SynthID, otra herramienta especialmente enfocada en la detección de imágenes generadas por IA.

Además de las implicaciones en la seguridad personal, el vishing puede ser utilizado para influir en conflictos internacionales al difundir información falsa. Esto subraya la necesidad de mantenerse alerta y adoptar medidas de seguridad sólidas para protegerse contra estas amenazas en constante evolución. La educación sobre la identificación de estafas y la implementación de medidas de seguridad cibernética robustas son cruciales en un mundo donde la tecnología de manipulación de voz e imágenes está al alcance de los ciberdelincuentes.

Vulnerabilidades

Reciba nuestro boletín completo de parches y vulnerabilidades suscribiéndose aquí.

Vulnerabilidad crítica en Cisco Emergency Responder
Fecha: 4 de octubre de 2023
Gravedad**: CRÍTICA**
CVE: CVE-2023-20101

Descripción:
El pasado 4 de octubre Cisco publicó una vulnerabilidad crítica en la aplicación Cisco Emergency Responder debida a la existencia de credenciales estáticas del usuario root que no pueden ser cambiadas ni eliminadas; estas credenciales están destinadas normalmente a su utilización durante el desarrollo.

Con la explotación de esta vulnerabilidad un atacante remoto no autenticado podría iniciar sesión en el dispositivo afectado con el usuario root permitiendo así que ejecute comandos con permisos elevados.

El Equipo de Respuesta ante Incidentes de Seguridad de Protocolos (PSIRT) de Cisco informan que no se han encontrado divulgaciones públicas de esta vulnerabilidad.

Enlace

Productos afectados:
Esta vulnerabilidad únicamente afecta a la versión 12.5(1)SU4 de Cisco Emergency Responder.

Solución:
La solución recomendada para hacer frente a esta vulnerabilidad consiste en actualizar las instalaciones vulnerables; siendo la primera versión fija la versión 12.5(1)SU5.

Vulnerabilidad en Google Chrome
Fecha: 3 de octubre de 2023
Gravedad**: ALTA**
CVE: CVE-2023-5346

Descripción:
El pasado martes 03 de septiembre, Chrome lanzó una actualización para la aplicación de escritorio de Google Chrome. En esta actualización, se informa de la corrección de una vulnerabilidad alta. Esta vulnerabilidad podría permitir a un atacante llevar a cabo ejecución remota de código al explotar la corrupción de la memoria en la pila de ejecución del navegador haciendo uso de una página HTML especialmente diseñada.

Se trata de una vulnerabilidad debida a un problema en el motor JavaScript de Google Chrome (V8), dado que interpreta incorrectamente el tipo de datos.

Otros navegadores como Microsoft Edge, al estar basados en Chromium, también se han visto afectados por esta vulnerabilidad y desde Microsoft ya han lanzado una actualización de seguridad para el mismo.

Enlace
Enlace

Productos afectados.:
Los recursos afectados por esta vulnerabilidad son los siguientes:

Google Chrome, versiones anteriores a la versión 117.0.5938.149.

Microsoft Edge, versiones anteriores a la versión 117.0.2045.55.

Solución:
La solución consiste en la actualización de los navegadores Google Chrome a la versión 117.0.5938.149 y Microsoft Edge a la versión 117.0.2045.55.

Parches

Boletín de seguridad mensual de Android
Fecha: 2 de octubre de 2023
Gravedad**: CRÍTICA**

Descripción:

Android ha publicado el pasado día 2 su boletín de seguridad correspondiente al mes de octubre. En este aviso informa de un total de 51 vulnerabilidades, entre las que se encuentran 5 vulnerabilidades críticas y 46 altas.

Entre las vulnerabilidades críticas se encuentran las siguientes:

CVE-2023-40129 y CVE-2023-4863: Son dos vulnerabilidades críticas que podrían permitir a un atacante realizar ejecución remota de código. Ambas vulnerabilidades afectan al componente system.

CVE-2023-24855: Esta vulnerabilidad crítica se debe la corrupción de memoria en el módem durante el proceso de configuración de seguridad previo a AS Security Exchange.

CVE-2023-28540: Esta vulnerabilidad se debe a una autenticación incorrecta durante el protocolo de enlace TLS que provoca problemas criptográficos en el módem de datos.

CVE-2023-33028: Se trata de una vulnerabilidad debida a la corrupción de memoria en el firmware WLAN durante el proceso de realización de una copia de memoria de la caché pmk.

Las tres últimas vulnerabilidades afectan al componente Qualcomm closed-source.

Enlace

Productos afectados:

Las vulnerabilidades corregidas en este boletín afectan a los siguientes recursos:
Android Open Source Project (AOSP) versiones 11, 12, 12L y 13.
Componentes: framework, system, Sistema de actualizaciones de Google Play, Arm, MediaTek Qualcomm (incluidos closed-source)

Actualización

Actualizar los dispositivos afectados con los parches de seguridad publicados por el fabricante.

Actualizacion de una vulnerabilidad 0 day en Apple
Fecha: 4 de octubre de 2023
Gravedad**: ALTA**

Descripción:

Apple ha publicado una actualización de seguridad para iOS y iPadOS que corrige una vulnerabilidad zero-day CVE-2023-42824.

La vulnerabilidad identificada como CVE-2023-42824 afecta al kernel y podría otorgar a un atacante local la capacidad de aumentar sus niveles de privilegios en los dispositivos afectados. Desde Apple informan de que este fallo de seguridad puede haber sido utilizado contra las versiones de iOS vulnerables.

Esta actualización de seguridad también cubre la vulnerabilidad CVE-2023-5217, un fallo de seguridad zero-day de Google Chrome del pasado 28 de septiembre. Esta vulnerabilidad se origina debido a un desbordamiento de búfer de pila en la codificación vp8, que se encuentra en libvpx, una biblioteca de códecs de video desarrollada conjuntamente por Google y Alliance for Open Media (AOMedia). Este problema se resolvió actualizando a libvpx 1.13.1.

Enlace
Enlace

Productos afectados.:

La vulnerabilidad afecta a todas las versiones anteriores a la versión 16.6. En concreto afecta a los siguientes productos:

iPhone XS y posteriores.
iPad Pro-12.9 pulgadas, segunda generación y posteriores.
iPad Pro-10.5 pulgadas
iPad Pro-11 pulgadas, primera generación y posteriores.
iPad Air tercera generación y posteriores.
iPad sexta generación y posteriores.
iPad mini quinta generación y posteriores.

Solución:

iOS 17.0.3 and iPadOS 17.0.3

Eventos

Black Hat MEA
14-16 Noviembre

La edición de Black Hat MEA (Medio Oriente y África) se llevará a cabo en Riyadh, Arabia Saudita, del 14 al 16 de noviembre. Este evento líder en la región promoverá el intercambio de conocimientos y la difusión de nuevas tecnologías a través de conferencias y talleres impartidos por expertos de la industria. .

Enlace

National Cyber League España
25 octubre – 16 noviembre

La National Cyber League es una competición organizada en España por la Guardia Civil que se lleva a cabo desde el 22 de octubre hasta el 16 de noviembre. Esta competición tiene como objetivo potenciar el talento de los jóvenes a través de una perspectiva multidisciplinaria, abordando aspectos técnicos, legales y de comunicación.

Enlace

Cyber Security & Cloud Expo
30 noviembre – 1 diciembre

Cyber Security & Cloud Expo es un evento que se lleva a cabo en Londres del 30 de noviembre al 1 de diciembre, donde se abordan diversos temas, tales como la inteligencia artificial, blockchain y el Internet de las Cosas (IoT), enfocados en múltiples sectores, incluyendo la ciberseguridad.

Enlace

Recursos

Nuevos Metodos de ingenieria social mediante la IA

Hoy en día, la inteligencia artificial te brinda la capacidad de asumir la identidad de otra persona en tiempo real. Esto se logra mediante aplicaciones como VoiceX, que te permite modificar tu voz, y DeepfakeVFX, que te permite alterar tu rostro de manera convincente. Gracias a estas tecnologías, es posible suplantar la identidad de alguien y, de esta manera, obtener información que pueda ser usada de forma maliciosa.

Enlace

La RNS comparte más de 30 alertas diarias sobre ciberamenazas activas

La Red Nacional de Operaciones de Ciberseguridad (RNS), bajo la dirección del Centro Criptológico Nacional (CCN), informa sobre más de 30 ciberamenazas diarias en curso, brindando a las entidades participantes la oportunidad de tomar medidas para mitigar posibles riesgos.

Enlace

Raspberry Pi5

A finales de octubre, estará disponible para su venta la Raspberry Pi 5, una computadora de placa única con un rendimiento sustancialmente mejorado en comparación con su predecesora. Este avance tecnológico permitirá a los entusiastas y profesionales de la informática realizar una amplia gama de proyectos con mayor eficiencia y versatilidad.

Enlace

Filtración del ransomware HelloKitty

El día 9 de octubre de 2023 se filtró el ransomware HelloKitty en un foro de hacking, que este malware ha provocado muchos dolores de cabeza para empresas como CD Proyect en 2021 y Cloudflare en 2022. Gracias a esta filtración muchos cibercriminales podrán aprovecharse para poder desarrollar su propio malware sin tener tantos conocimientos avanzados, pudiendo provocar un aumento en los ataques de esta índole.
Enlace

Responsables Ciber

María Pilar Torres Bruna

Directora de Ciberseguridad en NTT DATA Latam y Perú
maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schawarzer

Directora de Ciberseguridad en NTT DATA Brasil
carla.passosschwarzer@emeal.nttdata.com

Miguel Angel Garzón Ramírez

Manager de Ciberseguridad en NTT DATA Colombia
miguel.angel.garzon.ramirez@emeal.nttdata.com

Fernando Vilchis Rivero

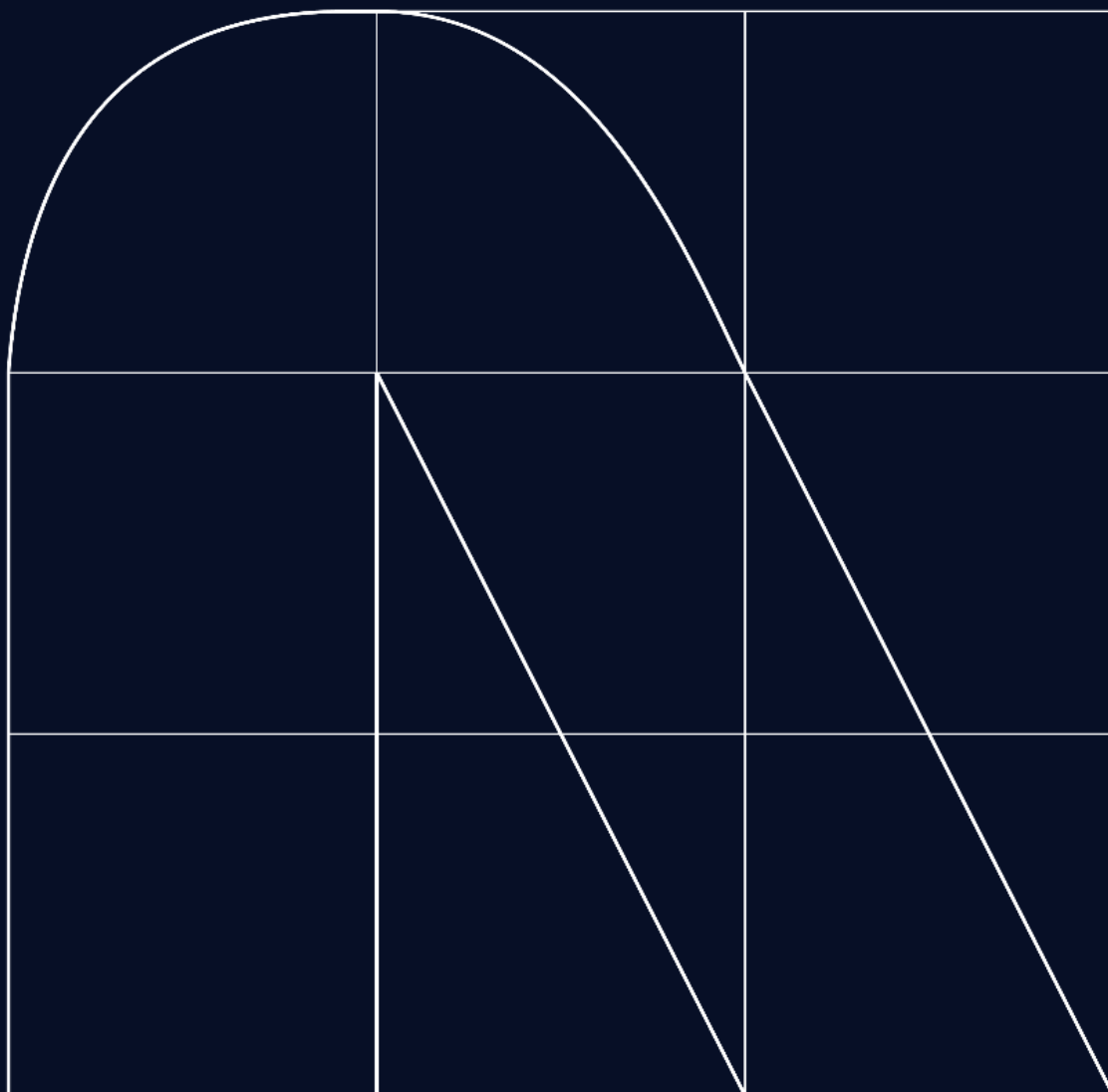
Manager de Ciberseguridad en NTT DATA México
fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Ciberseguridad en NTT DATA USA
nestor.ordonez.ramirez@emeal.nttdata.com

Jose Uzcategui

Manager de Ciberseguridad en NTT DATA Chile
jose.uzcategui@emeal.nttdata.com



Powered by the cybersecurity NTT DATA team

es.nttdata.com