Número 109 | Diciembre 2025

NTT DATA

Radar

El magazine de ciberseguridad

Cuando el hacking evoluciona más rápido que el código

Por Jose Carlos Moral

El desarrollo de *software* ya no es una carrera por lanzar más rápido, sino por lanzar más seguro. En este nuevo paradigma de mejora continua, la seguridad dejó de ser el último control antes del despliegue para convertirse en el hilo que une cada fase del desarrollo.

Vivimos en un ecosistema donde los ataques evolucionan tan deprisa como el código que los intenta detener.

Hoy, los ciberdelincuentes ya no se esconden en sótanos oscuros: están en laboratorios de IA, en foros privados y, muchas veces, dentro de las mismas empresas que buscan protegerse.

Las nuevas técnicas de *hacking —AI-powered phishing, prompt injection, supply chain exploits o deepfakes* operativos— están redefiniendo las reglas del juego.

Ya no basta con pensar en *firewalls* o antivirus; ahora el desafío es adelantarse y crear *software* que piense como un atacante antes de que lo haga uno real.

Shift Left: el código seguro nace desde la primera línea

En desarrollo seguro, el "*shift left*" ya no es un concepto aspiracional, es una necesidad. Integrar seguridad en cada fase del Ciclo de Vida de Desarrollo de *Software* (SDLC), no solo reduce los costes de remediación, sino que también disminuye la superficie de ataque antes incluso de que el producto vea la luz.

Automatizar auditorías, usar SAST y DAST, incorporar *threat modeling* y revisar dependencias de terceros debería ser tan cotidiano como hacer un *commit*.

Porque un fallo en una dependencia puede convertirse en la próxima brecha global. SolarWinds, Log4Shell y XZ Utils son tres recordatorios recientes de que la cadena de suministro digital es tan fuerte como su eslabón más olvidado.

El factor humano: del eslabón débil al escudo inteligente

Por muy avanzadas que sean las técnicas de detección, la ingeniería social sigue siendo la puerta de entrada más efectiva.

Y ahí está el gran giro de esta nueva era: la educación del usuario. No se trata de convertir a todos en expertos en ciberseguridad, sino en cambiar la cultura digital.

El foco debería encontrarse en que un desarrollador sea capaz de identificar cuándo un código es potencialmente vulnerable, o que un empleado desconfíe antes de hacer *clic* en un enlace que no parece demasiado legítimo.

El futuro del *hacking* es colaborativo

El *hacking* ético, los *bug bounty programs* y la colaboración entre comunidades de *white hats* y empresas están impulsando una nueva mentalidad: la de la defensa compartida.

En un mundo donde los ciberataques ya son una industria, solo una respuesta colectiva puede hacerles frente. La seguridad ya no es una capa. Es una actitud.

Y como toda actitud, empieza por la forma en que pensamos en el *software* desde su origen.

Jose Carlos Moral
Cybersecurity Manager Architecture

Cerramos 2025

Cibercrónica por Joel Perez

En la segunda mitad de 2025, el panorama de la ciberseguridad ha entrado en una fase de mutación acelerada. Las viejas recetas de *phishing* masivo o *ransomware* básico ya no bastan; los adversarios están afinando nuevas técnicas de *hacking* —más sofisticadas, multidimensionales y peligrosas— que exigen una vigilancia redoblada y una respuesta urgente.

IA, automatización y *deepfakes*: el arma silenciosa

Los informes más recientes señalan que los ataques apoyados por inteligencia artificial ya no son futurismo: se están desplegando en masa. Según Check Point Software, en 2025 los estados y las bandas criminales "están utilizando tácticas basadas en IA, incluyendo campañas de desinformación y *malware* disruptivo", Check Point Software+1. Por ejemplo:

- Modelos generativos que crean correos de *phishing* casi indistinguibles de los legítimos.
- *Deepfakes* con voz o vídeo para suplantar directivos o empleados y lograr así accesos privilegiados.
- Automatización de procesos de intrusión, reduciendo el tiempo entre descubrimiento y explotación.

Estas técnicas transforman al "*hacker* tradicional" en algo más parecido a un "orquestador digital": en lugar de lanzar cinco correos masivos, ahora se producen decenas de ataques personalizados, generados por IA, adaptados al objetivo específico.

Multi-plataforma, *supply chain* y ataques sin *malware* clásico

Las tácticas también se están diversificando hacia vectores más complejos que antes. Por ejemplo, según la revista especializada, esta tendencia engloba:

- Ataques en cadena (*supply chain*): comprometen un tercer elemento para llegar al objetivo final.
- Ataques multi-plataforma: consisten en ataques dirigidos a distintos Sistemas Operativos (como Windows, Linux, móviles e incluso en la nube) todo en el mismo ataque.
- Técnicas sin *malware* visible («*fileless*»), que se apoyan en procesos legítimos del sistema, memoria RAM o servicios en la nube para moverse sin dejar la huella tradicional.

Esto significa que muchas defensas tradicionales —antivirus, *firewalls*, firmas de *malware*— ya no son suficientes por sí solas.

Extorsión triple, *infostealers* y ataque al perímetro de la nube

La evolución del *ransomware* también sostiene esta nueva era de *hacking*: no sólo cifrado de discos, sino robo de datos, publicación, presión social y extorsión múltiple. Una de las técnicas clave para 2025 es la "triple extorsión" (robo + cifrado + exposición pública), junto con *deepfakes* y ataques dirigidos.

Asimismo, los llamados "*infostealers*" (programas que roban información sensible) se han multiplicado y actúan como puerta de entrada al ciclo completo de ataque.

Por otro lado, la ampliación de entornos en la nube, IoT y *edge devices* ha abierto nuevos flancos: los atacantes ya no sólo entran por la oficina típica, sino por dispositivos periféricos, servicios SaaS, contenedores y microservicios vulnerables.

Amenaza persistente, colaboración entre actores y reutilización rápida

Los adversarios —ya sean grupos criminales, *hacktivistas* o estados-nación— muestran también una evolución estructural:

- Colaboración entre APTs (grupos persistentes avanzados) y bandas criminales para combinar espionaje y ganancia económica.
- Ciclos de reutilización de herramientas, *kits* modulares listos para usar, y adaptaciones rápidas que permiten que una técnica descubierta hoy se generalice en semanas.
- El factor sorpresa se hace cotidiano: menos ataques "ruidosos" y más operaciones sigilosas, que se extienden en el tiempo y requieren detección proactiva más que reactiva.

¿Qué hacer? Contramedidas para no quedarse atrás

Dado este panorama, la estrategia defensiva debe evolucionar:

- Adoptar monitorización continua y análisis de comportamiento, no solo firmas.
- Integrar IA y automatización para la defensa: si los atacantes usan IA, la defensa también debe apoyarse en inteligencia artificial.
- Segmentar entornos, endurecer el perímetro, pero también asegurar el interior — la nube, los *endpoints*, los servicios de terceros.
- Preparar simulaciones avanzadas, ejercicios de respuesta rápida, y asumir que el "incidente" no será un evento aislado sino una campaña prolongada.
- Formar al personal para reconocer *deepfakes*, *spear-phishing* ultra-personalizados, y ataques que se desarrollan fuera del canal tradicional de correo electrónico.

Conclusión

Estamos ante una nueva era del *hacking* donde la velocidad, la automatización, el uso de IA y la complejidad de los vectores obligan a replantear tanto la forma de atacar como la de defender.

Las técnicas mencionadas ya no son "lo que podría venir"; están aquí y ahora, y los profesionales de ciberseguridad tenemos ante nosotros un escenario dinámico, multidimensional y exigente.

Mic-E-Mouse: cuando el ratón se convierte en micrófono

Artículo por Rodrigo Rey y Alberto Agra

En un mundo donde la inteligencia artificial (IA) avanza más rápido que las medidas de seguridad, cada nuevo descubrimiento en ciberseguridad nos obliga a repensar los límites de la tecnología. El estudio más reciente, conocido como Mic-E-Mouse, ha mostrado una vulnerabilidad inesperada: los sensores de movimiento de los ratones de ordenador pueden ser explotados para capturar sonidos del entorno, convirtiéndolos, en la práctica, en micrófonos improvisados. Esta revelación no solo plantea un desafío técnico, sino también un debate ético sobre los riesgos del ingenio humano en la era de la IA.

La investigación, publicada a mediados de septiembre de 2025 por un grupo de expertos en ciberseguridad de varias universidades, tenía un objetivo simple pero inquietante: explorar si los sensores ópticos y de movimiento presentes en ratones comunes podían registrar vibraciones mínimas causadas por ondas sonoras.

Estos sensores, diseñados originalmente para captar desplazamientos sobre una superficie, registran cambios lumínicos a gran velocidad —en algunos modelos, hasta 30.000 veces por segundo—. Los investigadores se dieron cuenta de que esas fluctuaciones podían, en determinadas condiciones, reflejar vibraciones producidas por la voz o por sonidos cercanos.

El hallazgo se ha difundido rápidamente en medios especializados como TechSpot, Kaspersky, GBHackers o The Indian Express, sorprendiendo a la comunidad tecnológica y recordando que las amenazas cibernéticas no siempre provienen de *software* malicioso, sino a veces de los propios dispositivos físicos.

El ataque descrito por los investigadores se basa en un principio físico: cualquier sonido genera una vibración mecánica en las superficies cercanas. Cuando un ratón con sensor óptico de alta resolución se encuentra sobre una mesa, esas vibraciones microscópicas pueden afectar al reflejo de la luz que el sensor utiliza para calcular el movimiento.

Los científicos desarrollaron un modelo de IA capaz de analizar las señales captadas por el sensor —en apariencia simples coordenadas de movimiento— y filtrarlas para reconstruir patrones de frecuencia asociados con sonidos humanos. Con suficiente entrenamiento, la red neuronal logró identificar fragmentos de voz y reconocer palabras específicas, con una precisión sorprendente en entornos controlados.

El ataque, denominado Mic-E-Mouse, no requiere acceso físico al micrófono del ordenador, ni siquiera a componentes de audio. Bastaría con comprometer el *firmware* del ratón o interceptar los datos de movimiento transmitidos al equipo. Si bien el proceso todavía es experimental y su ejecución práctica resulta compleja, demuestra que, incluso los periféricos más cotidianos, pueden convertirse en herramientas de espionaje.

El experimento Mic-E-Mouse no es simplemente una demostración técnica: es una advertencia sobre el futuro de la privacidad digital. La capacidad de convertir un ratón en un dispositivo de escucha refleja hasta qué punto la IA puede reinterpretar los límites físicos de la tecnología.

Aunque el ataque no representa, por ahora, una amenaza masiva, su existencia nos recuerda que la seguridad debe concebirse como un sistema integral, donde cada componente —por trivial que parezca— puede ser una puerta abierta al riesgo. En última instancia, este estudio nos invita a reflexionar sobre nuestra relación con la tecnología. No se trata solo de crear máquinas más inteligentes, sino de garantizar que su inteligencia no se vuelva en nuestra contra.
.

Rodrigo Rey
Cybersecurity Lead Architect

Alberto Agra
Cybersecurity Expert Architect

Conciencia cuántica

Espacio cuántico
por María Gutiérrez

Cerramos este año 2025 de la Ciencia y las Tecnologías cuánticas con el convencimiento de que lo cuántico es presente. Recientemente, hemos visto casos prácticos en sanidad, energía, logística, finanzas, comunicaciones... parece que la física cuántica no se despliega solo en fórmulas, laboratorios o centros de investigación, sino que empieza a estar en nuestra vida cotidiana. Es más, puede que siempre haya estado presente en nuestras vidas, en concreto en nuestro cerebro... los fenómenos cuánticos, superposición, entrelazamiento o de coherencia, podrían jugar un papel esencial en los procesos que dan lugar a la experiencia subjetiva, esa misteriosa cualidad que nos hace "ser" y "sentir". Y es que no hablamos solo de información o procesamiento neuronal, sino del sustrato último de la mente consciente, ¿podría ser eso que llamamos conciencia?

El cerebro, a temperatura corporal, parecía un entorno demasiado cálido y ruidoso para mantener coherencia cuántica. Sin embargo, en los últimos años han aparecido resultados experimentales que invitan a reabrir el debate. En biología cuántica se ha comprobado la existencia de coherencia en sistemas vivos, como la fotosíntesis o la navegación de ciertas aves, lo que demuestra que la vida puede aprovechar fenómenos cuánticos incluso en condiciones "no ideales".

La idea tomó forma en los años noventa, cuando el físico Roger Penrose y el anestesista Stuart Hameroff propusieron la teoría Orch-OR (Orchestrated Objective Reduction). Según esta hipótesis, la conciencia surgiría de procesos cuánticos en los microtúbulos, estructuras del citoesqueleto celular, que permitirían estados de superposición en el cerebro. Dichos estados colapsarían de forma orquestada, generando momentos discretos de conciencia.

Esto ha impulsado una corriente de investigación que algunos denominan neurobiología cuántica, en la que se exploran los límites de la decoherencia en estructuras neuronales y la posible interacción entre procesos cuánticos y cognición. Aunque aún estamos lejos de una demostración sólida, la sola posibilidad está modificando la manera en que concebimos la mente.

Estas ideas rozan lo metafísico, pero también plantean un reto empírico: ¿podemos diseñar experimentos que diferencien un cerebro clásico de uno "cuántico"? Algunos proyectos, todavía en fase conceptual, intentan buscar firmas de entrelazamiento en redes neuronales o correlaciones no clásicas en la actividad cerebral.

La dificultad técnica es inmensa, pero el impacto potencial sería revolucionario. Porque en un momento en el que parece que la inteligencia ya no es lo que nos define como humanos (la IA nos supera en memoria, capacidad, velocidad, aunque requiere más energía para aprender…), en la búsqueda de aquello que nos hacer ser únicos y diferentes nos topamos con la conciencia.

¿Será la conciencia la que realmente nos diferencie?, pero ¿y si resulta ser un tema de complejidad, de colapso de estados cuánticos?, ¿podría ser que ser que la computación cuántica (que viene a resolver temas complejos) pueda dotar a la IA de conciencia? Por lo que tampoco sea esta la que nos haga ser "únicos "y "diferentes".

La conciencia cuántica no es hoy una teoría demostrada, sino una invitación a pensar. Y ese pensamiento, a medio camino entre la física, la biología y la filosofía, será sin duda uno de los grandes escenarios de debate científico en las próximas décadas, termina el año 2025, ¡pero ni mucho menos termina el debate cuántico!

Evasión de EDR: la Nueva Frontera de la Seguridad Ofensiva

Tendencias por Jesús Murciano

Durante 2025, una tendencia ha captado la atención de los investigadores en ciberseguridad: la evasión de los EDR (Endpoint Detection & Response). Estas plataformas, que representan la primera línea de defensa contra amenazas avanzadas, están siendo estudiadas tanto por investigadores como por atacantes que buscan evadir sus mecanismos de detección y respuesta. El auge de herramientas como EDRFreeze simboliza el comienzo de una nueva etapa en la carrera armamentística entre la ofensiva y la defensa. Ya no se trata solo de ocultar *malware*, sino de neutralizar temporalmente al guardián que protege los sistemas.

¿En qué consiste esta técnica?

Hasta hace poco, las estrategias más comunes para evadir los EDR consistían en el uso de controladores vulnerables (conocidos como BYOVD, Bring Your Own Vulnerable Driver) que otorgaban privilegios de *kernel* para desactivar los servicios de seguridad. Sin embargo, este enfoque requería acceso avanzado y dejaba rastros detectables.

El cambio de paradigma llega con métodos como EDRFreeze, que operan completamente en modo usuario. Aprovechando mecanismos legítimos del sistema operativo, como el servicio Windows Error Reporting (WER), estas herramientas pueden suspender o "congelar" los procesos de seguridad sin necesidad de explotar vulnerabilidades del *kernel* ni cargar controladores firmados.

En la práctica, esto significa que un atacante puede detener la monitorización del EDR el tiempo suficiente para ejecutar código malicioso, moverse lateralmente o exfiltrar información, todo sin generar alertas inmediatas.

¿Por qué es tan efectiva esta tendencia?

La efectividad de esta técnica radica en su bajo perfil y en el uso de componentes legítimos del sistema operativo. Al apoyarse en procesos nativos de Windows y ejecutarse con permisos estándar, el atacante reduce significativamente las probabilidades de ser detectado por las defensas tradicionales.

Este enfoque, alineado con la filosofía de "vivir de la tierra" (*living off the land*), representa una evolución natural de las técnicas de evasión, donde se prioriza el uso discreto de los recursos del propio sistema en lugar de herramientas externas.

Además, estas herramientas eliminan la necesidad de conocimientos profundos del *kernel*, ampliando su adopción entre actores menos sofisticados. Al mismo tiempo, la investigación en comunidades ofensivas ha acelerado la publicación de pruebas de concepto y *scripts* que replican el comportamiento de suspensión de procesos, lo que sugiere que actores maliciosos con menos conocimientos técnicos podrán ejecutar ataques cada vez más sofisticados.

Conclusión

La evasión de EDR marca una evolución significativa en las tácticas de los atacantes y obliga a los defensores a adaptarse rápidamente. Proteger los propios mecanismos de defensa se convierte en una prioridad estratégica. Las organizaciones deben reforzar los controles de integridad de procesos, aplicar listas de bloqueo de controladores vulnerables, vigilar el uso anómalo de servicios del sistema y, sobre todo, detectar los "silencios del EDR" —los periodos en los que la telemetría deja de reportar— como posibles indicadores de ataque.

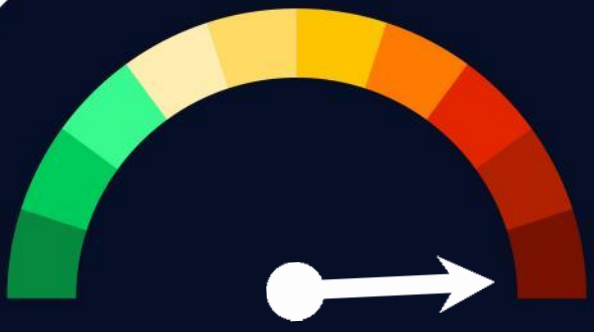
En un entorno cada vez más sofisticado, donde el objetivo ya no es solo comprometer el sistema, sino desactivar a quienes lo protegen, la resiliencia de las defensas será el verdadero factor diferenciador. La carrera por "congelar el EDR" apenas comienza.

Jesús Murciano
Cybersecurity Analist

Vulnerabilidades

Vulnerabilidad crítica en React Native Metro CLI

Fecha: 3 de noviembre de 2025
CVE: CVE-2025-11953



CVSS: 9.8

CRÍTICA

Descripción

La vulnerabilidad **CVE-2025-11953** de severidad crítica, permite a atacantes remotos ejecutar código arbitrario en las máquinas de los desarrolladores que ejecutan el servidor de desarrollo Metro de React Native.

El origen de la vulnerabilidad ocurre debido a que el servidor no valida correctamente el parámetro *lineNumber* y *file*. En Windows, el servidor invoca el editor mediante *child_process.spawn* de Node.js y pasa el archivo y línea como argumentos; si lineNumber incluye metacaracteres de *shell*, *cmd.exe* los interpreta y permite ejecutar comandos arbitrarios. No es necesario autenticación y se pueden lanzar comandos de forma remota si pueden acceder al puerto del servidor (por defecto, 8081).

Solución

Realizar los siguientes pasos mitigará la vulnerabilidad CVE-2025-11953:

- Actualizar @react-native-community/cli-server-api a la versión 20.0.0 o superior, que incluye la corrección para esta vulnerabilidad
- Para mejorar la seguridad, o en caso de que no sea posible actualizar, configurar el servidor de desarrollo para que se vincule explícitamente a la interfaz *localhost*, incluyendo la opción --host 127.0.0.1

Productos afectados

Esta vulnerabilidad crítica afecta a todas las versiones anteriores del *commit* que resuelve la falta de validación de los parámetros de entrada, resuelto en **React Native CLI**, específicamente en el componente de **Metro Development Server versiones anteriores a la 20.0.0**. La explotación de la vulnerabilidad es más grave en sistemas Windows.

Referencias

- nvd.nist.gov
- jfrog.com

TLP:WHITE

Vulnerabilidades

Vulnerabilidades críticas en el producto UCCX de Cisco

Fecha: 5 de noviembre de 2025
CVE: CVE-2025-20354 y 1 más

CVSS: 9.8

CRÍTICA

Descripción

Cisco ha publicado dos vulnerabilidades de severidad crítica que afectan a su producto Unified Contact Center Express.

La vulnerabilidad CVE-2025-20354 permitiría a un atacante remoto sin permisos subir archivos maliciosos y ejecutar código con permisos de administrador. La vulnerabilidad se debe a un fallo en la autenticación de UCCX.

Por otro lado, la vulnerabilidad con identificador CVE-2025-20358 permitiría a un atacante realizar un bypass de la autenticación y obtener permisos de administración. La vulnerabilidad es causada por un fallo en la autenticación entre el componente CCX Editor y el servidor UCCX.

Solución

El fabricante ha publicado un parche mitigando la vulnerabilidad. Por ello, se recomienda actualizar de manera inmediata a una de las siguientes versiones:

- 12.5 SU3 ES07.
- 15.0 ES01.

Productos afectados

La vulnerabilidad afecta a todas las instalaciones de UCCX, independientemente de la configuración que se disponga.

Referencias

- sec.cloudapps.cisco.com

TLP:WHITE

ShopLentor para Wordpress corrige una vulnerabilidad crítica

Fecha: 4 de noviembre de 2025
CVE: CVE-2025-12493

Crítica

Descripción

ShopLentor (anteriormente conocido como WooLentor) es un **destacado complemento de WordPress** que integra WooCommerce con los editores de páginas Elementor y Gutenberg. Con millones de descargas y una amplia base de usuarios activos, constituye un componente fundamental dentro del ecosistema del comercio electrónico en WordPress.

Recientemente, se identificó la vulnerabilidad **CVE-2025-12493**, una falla de **inclusión de archivos locales (LFI)** que afecta a todas las **versiones hasta la 3.2.5**. El problema se origina en la función *load_template*, que, no valida correctamente las rutas de archivo proporcionadas por el usuario, permitiendo el uso de secuencias como ../ para acceder a archivos internos del servidor, como *wp-config.php*.

Clasificada como **CWE-22**, esta vulnerabilidad podría permitir la **exposición de información sensible** o incluso la **ejecución remota de código**, sin necesidad de autenticación, lo que aumenta su gravedad. Hasta el momento, no se han publicado pruebas de concepto ni código de explotación, aunque se recomienda actualizar el *plugin* de inmediato a una versión corregida.

Productos afectados

El complemento afectado es **ShopLentor – WooCommerce Builder** para Elementor y Gutenberg. La vulnerabilidad impacta a **todas las versiones hasta la 3.2.5 (incluida)**, y puede explotarse en cualquier sitio WordPress que tenga activa una versión vulnerable del *plugin*

Solución

Actualizar el *plugin* ShopLentor de WordPress a la versión más reciente (3.2.6 o superior). En caso de no poder actualizar inmediatamente el *plugin*, se recomienda deshabilitarlo e implementar reglas específicas de WAF para bloquear posibles intentos de explotación.

Referencias

- nvd.nist.gov
- wordfence.com

Google corrige vulnerabilidad en Chrome

Fecha: 5 de noviembre de 2025
CVE: CVE-2025-12725, CVE-2025-12727 y 3 mas

Alta

Descripción

Google publicó recientemente un parche de seguridad que aborda 5 vulnerabilidades que afectan a diferentes componentes del navegador como WebGPU, JavaScript V8 y Omnibox. Estas vulnerabilidades podrían permitir la ejecución remota de código.

Las vulnerabilidades parcheadas más relevantes son las siguientes:

- CVE-2025-12725 (CVSS 8,8): vulnerabilidad que permitiría a un atacante ejecutar código de manera remota debido a un fallo de escritura que permitirá escribir Out of Bounds.
- CVE-2025-12727 (CVSS 8,8): Esta vulnerabilidad permitiría a un atacante ejecutar código de manera remota debido a un fallo en el motor de Javascript V8.

Productos afectados

Las versiones afectadas del producto son las siguientes:

- Versiones anteriores a las 142.0.7444.134/.135 en Windows.
- Versiones anteriores a la 142.0.7444.135 en macOS.
- Versiones anteriores a la 142.0.7444.134 en Linux.

Solución

El fabricante recomienda actualizar a las siguientes versiones:

- 142.0.7444.134/.135 en Windows.
- 142.0.7444.135 en macOS.
- 142.0.7444.134 en Linux.

Referencias

- chromereleases.googleblog.com
- cybersecuritynews.com

Eventos

SANS CyberThreat Summit 2025
3 - 4 de diciembre

El emblemático estadio Stamford Bridge en Londres acogerá un congreso de dos días pensado específicamente para profesionales de la ciberseguridad tanto ofensiva como defensiva. Organizado por SANS Institute, este evento ofrece una inmersión técnica profunda, permitiendo a los asistentes explorar las últimas tácticas, herramientas y casos reales de ataque y defensa en un entorno de alto nivel. Ideal para quienes están camino a ser gerentes de ciberseguridad: dos jornadas intensas, *networking* de primer nivel y la tradición de SANS respaldando la calidad.

Enlace

Black Hat Europe 2025
8 – 11 de diciembre

Londres se convierte de nuevo en el epicentro europeo de la ciberseguridad con este evento de alto impacto. Ubicado en el ExCeL London, incluye desde entrenamientos especializados de dos y cuatro días hasta conferencias principales (*briefings*) los días 10 y 11 donde se revelan investigaciones punteras, demostraciones de herramientas *open-source* (“Arsenal”), salas de exposiciones y amplias oportunidades de conexión profesional.

Enlace

León Cybersecurity Conference
20 de diciembre

El sábado 20 de diciembre de 2025, en Cañada de Mariches #3435, León de los Aldama (Guanajuato, México), se celebrará esta conferencia de un día que marca un “antes-y-después” para el Bajío en materia de seguridad digital.

Este evento reúne voces nacionales e internacionales para empoderar tanto a personas como a organizaciones frente a los retos del entorno digital, con un enfoque en formar, actualizar e inspirar.

Enlace

Recursos

➢ AdaptixC2

Adaptix es un marco extensible de postexplotación y emulación adversaria creado para los evaluadores de penetración. El servidor Adaptix está escrito en Golang y permite flexibilidad al operador. El cliente GUI está escrito en C++ QT, lo que permite su uso en los sistemas operativos Linux, Windows y MacOS.

Enlace

➢ LLM Red Teaming Framework

DeepTeam incorpora las últimas investigaciones para simular ataques adversarios utilizando técnicas SOTA, como *jailbreaking* e inyecciones de comandos, con el fin de detectar vulnerabilidades como sesgos y fugas de información de identificación personal, que de otro modo podrían pasar desapercibidas. Una vez descubiertas las vulnerabilidades, DeepTeam ofrece medidas de protección para evitar problemas en la producción.

Enlace

➢ DumpGuard

Darktrace ha evolucionado su plataforma para detectar amenazas mediante el aprendizaje del comportamiento normal de la red, sin depender de firmas de ataques conocidas. Su capacidad de respuesta autónoma Antigena puede contener ataques de manera dirigida sin interrumpir las operaciones comerciales.

La plataforma utiliza análisis comportamental para identificar anomalías de alto riesgo, incluyendo amenazas sofisticadas impulsadas por IA y estableciendo modelos únicos para cada entorno digital empresarial.

Enlace 1

Enlace 2

Informe de Tendencias de Ciberseguridad H1 2025

Desvelamos los principales datos del informe.

https://bit.ly/49BGCUB

Suscríbete a RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com