Número 99 | Febrero 2025

NTT DATA

Radar

El magazine de ciberseguridad

El fraude bancario en la era digital: retos y estrategias de la ciberseguridad

Por Francisco Javier García Lorente

El fraude bancario ha evolucionado de ser un problema puntual a convertirse en una amenaza global que afecta tanto a instituciones financieras como a millones de usuarios en todo el mundo. Impulsado por el crecimiento exponencial de las transacciones digitales, los avances tecnológicos y la vulnerabilidad del factor humano, el fraude bancario representa uno de los mayores desafíos para la ciberseguridad moderna. Este editorial reflexiona sobre los retos asociados a esta problemática y las estrategias necesarias para mitigar su impacto.

La evolución del fraude bancario

En las últimas décadas, el fraude bancario ha pasado de métodos tradicionales, como el robo físico de cheques o tarjetas, a complejas tácticas digitales diseñadas para explotar debilidades tanto tecnológicas como humanas. Actualmente, los ciberdelincuentes utilizan herramientas avanzadas como inteligencia artificial, *machine learning* y *deepfakes* para crear ataques más sofisticados y personalizados.

Entre las técnicas más comunes destacan el *phishing* y su variante más específica, el *spear phishing*, diseñados para engañar a los usuarios y robar credenciales sensibles. También han ganado relevancia ataques como el compromiso de correo electrónico empresarial (BEC, por sus siglas en inglés), donde los atacantes se hacen pasar por ejecutivos de alto rango para ordenar transferencias fraudulentas, y las tácticas de *ransomware* que paralizan los sistemas de instituciones bancarias hasta recibir un pago.

Este cambio en el panorama del fraude ha transformado el concepto de ciberseguridad, que ya no se limita a proteger redes y sistemas, sino que abarca la educación del usuario, la regulación internacional y la adopción de tecnologías avanzadas para anticiparse a las amenazas.

Retos principales de la ciberseguridad frente al fraude bancario

- **Aumento de la sofisticación de los ataques:** los ciberdelincuentes han perfeccionado sus métodos, utilizando inteligencia artificial para analizar patrones de comportamiento y lanzar ataques más efectivos. Por ejemplo, el uso de *deepfakes* puede permitirles eludir sistemas biométricos, mientras que herramientas de automatización les facilitan atacar múltiples objetivos simultáneamente.
- **El factor humano:** a pesar de los avances tecnológicos, el error humano sigue siendo uno de los puntos más vulnerables. Contraseñas débiles, clics en enlaces maliciosos y la falta de conciencia sobre las tácticas de ingeniería social permiten a los atacantes comprometer sistemas que, de otro modo, estarían protegidos.
- **La expansión del perímetro digital:** con el auge de la banca móvil, las APIs abiertas y los sistemas interconectados, el ecosistema digital se ha vuelto más complejo y difícil de proteger. Cada nuevo punto de acceso, desde aplicaciones móviles hasta dispositivos IoT, representa una posible puerta de entrada para los atacantes.
- **Regulación y cooperación internacional:** la naturaleza transfronteriza del fraude bancario complica la investigación y el rastreo de los fondos robados. Además, las disparidades en las leyes de protección de datos y ciberseguridad entre países dificultan la coordinación efectiva para combatir estas amenazas.
- **Riesgo reputacional:** más allá de las pérdidas económicas, las instituciones financieras enfrentan el reto de preservar la confianza de sus clientes. Un incidente de seguridad puede tener un impacto duradero en la reputación de una entidad, afectando su relación con los usuarios y su posición en el mercado.

Estrategias para mitigar el fraude bancario

- **Implementación de tecnologías avanzadas:** herramientas como la inteligencia artificial y el *machine learning* permiten identificar patrones anómalos en tiempo real, detectando transacciones sospechosas antes de que se materialicen. Además, tecnologías como *blockchain* ofrecen soluciones para crear sistemas más seguros y transparentes.

- **Autenticación reforzada:** la autenticación multifactor (MFA) se ha convertido en un estándar para reducir el riesgo de acceso no autorizado. Regulaciones como la PSD2 en Europa han hecho obligatoria la autenticación fuerte para proteger las transacciones digitales.
- **Educación continua del usuario:** invertir en programas de concienciación sobre ciberseguridad es crucial para reducir la eficacia de los ataques basados en ingeniería social. Los clientes deben estar informados sobre cómo identificar intentos de *phishing*, mantener contraseñas seguras y proteger sus dispositivos.
- **Convergencia de la seguridad física y lógica:** la protección de los cajeros automáticos, los sistemas de videovigilancia y los servidores internos debe integrarse con estrategias digitales. Un ejemplo de esta convergencia es la implementación de sistemas que detecten manipulaciones físicas en dispositivos críticos.
- **Respuesta rápida a incidentes:** la capacidad de detectar y responder a incidentes en tiempo real es esencial para limitar el impacto de un ataque. Esto incluye la creación de centros de operaciones de seguridad (SOC) y la adopción de soluciones de detección y respuesta extendida (XDR).
- **Colaboración internacional y regulatoria:** las instituciones deben trabajar de manera conjunta con gobiernos y organismos internacionales para compartir información sobre amenazas emergentes y fortalecer las regulaciones. Iniciativas como el intercambio de inteligencia cibernética entre bancos pueden ser fundamentales para prevenir ataques a gran escala.

Conclusión

El fraude bancario es una batalla en constante evolución que exige un enfoque integral. Las instituciones financieras deben ir más allá de las soluciones reactivas y apostar por una estrategia proactiva que combine tecnología avanzada, educación del usuario y colaboración intersectorial. Si bien es improbable que el fraude desaparezca por completo, el objetivo es mitigar su impacto al mínimo posible, protegiendo no solo los recursos económicos, sino también la confianza y la seguridad de millones de personas en todo el mundo.

En última instancia, la ciberseguridad no debe ser vista como un gasto, sino como una inversión estratégica. Solo a través de una combinación de innovación, regulación efectiva y un enfoque centrado en el usuario será posible enfrentar los desafíos del fraude bancario en el siglo XXI.

Francisco Javier García Lorente
Cybersecurity Project Manager

Año nuevo, mismos ataques

Cibercrónica por Diego Alonso Fernández y Adrián Álvarez Sánchez

En 2024, los ciberataques experimentaron un notable incremento a nivel mundial. Durante el tercer trimestre, las empresas de todo el mundo registraron una media semanal de 1.876 ataques, lo que representa un aumento del 75% en comparación con el mismo periodo de 2023 y un 15% más que el trimestre anterior. En esta cibercrónica abordamos el cierre de 2024 como anticipo de lo que nos puede deparar este 2025.

En 2024, los ciberataques alcanzaron niveles históricos, con pérdidas globales que superaron los 10.000 millones de euros. La inteligencia artificial (IA) se convirtió en un arma de doble filo, facilitando tanto la defensa como el ataque. Los atacantes emplearon IA para ejecutar operaciones de alta precisión, como troyanos bancarios y fraudes en criptomonedas. Además, servicios como "*Phishing-as-a-Service*" redujeron las barreras de entrada, permitiendo que, incluso actores inexpertos, llevaran a cabo ataques efectivos.

Los sectores más afectados incluyeron manufactura, sanidad y energía. Los ataques dirigidos a infraestructuras críticas generaron una preocupación global, mientras que el incremento del *ransomware* paralizó sistemas esenciales. En Reino Unido, el Servicio Nacional de Salud (NHS) sufrió un ataque que comprometió datos sensibles de pacientes y dificultó la atención sanitaria.

Europa también se vio impactada por tensiones geopolíticas. Reino Unido denunció una "ciberguerra" liderada por Rusia, que empleó IA para atacar telecomunicaciones e instituciones energéticas. En Francia, Anonymous Sudan lanzó ataques masivos en marzo de 2024, afectando servicios gubernamentales clave.

En noviembre, se identificaron vulnerabilidades de día cero en *routers* y dispositivos de grabación de vídeo en red (NVR), explotadas mediante el *malware* Mirai para ejecutar ataques DDoS. Estos incidentes resaltaron la necesidad de estrategias más robustas para proteger infraestructuras digitales.

Ya cerrando el 2024, la CNMC sufrió un ciberataque que tuvo como resultado la filtración de más de 2.000 millones de registros relacionados con usuarios de telefonía móvil, convirtiéndose en uno de los incidentes más graves del año en España.

Este 2025 ha comenzado con un ataque significativo contra Telefónica, una de las mayores compañías de telecomunicaciones del mundo donde, se han sustraído 2,3 GB de datos confidenciales, despertando preocupaciones sobre la seguridad corporativa y la privacidad de los clientes. Aunque la compañía respondió rápidamente, el incidente evidenció vulnerabilidades persistentes incluso en organizaciones con infraestructuras avanzadas.

Según un análisis posterior, el ataque fue facilitado por el uso de un *malware* tipo *infostealer*, que extrajo credenciales y datos críticos. Estas informaciones permitieron a los atacantes implementar tácticas de ingeniería social, ampliando el impacto del incidente. Este caso demuestra cómo las amenazas modernas combinan herramientas tecnológicas avanzadas con manipulación psicológica para maximizar sus efectos.

Este ataque también subrayó el papel de la IA en la automatización de tácticas de intrusión y extracción de datos, permitiendo que los atacantes lograran sus objetivos con rapidez y precisión. La situación reafirmó la necesidad de estrategias proactivas para enfrentar amenazas emergentes.

Por otro lado, la OTAN ha decidido reforzar su presencia en el mar Báltico para proteger las infraestructuras submarinas críticas, después de que en los últimos meses se hayan multiplicado los ataques a cables submarinos. Esta misión, que se denominará "*Baltic Sentry*" (Centinela Báltico) contará con barcos, aviones y "una pequeña flota de drones navales", aunque la Alianza no quiere dar demasiados detalles para no favorecer a los atacantes. El objetivo es mejorar la vigilancia para poder detectar las amenazas de manera coordinada.

Lo que nos espera en 2025: el futuro de la ciberseguridad

De cara al resto del año, los expertos anticipan un incremento en la sofisticación de los ciberataques.

La IA permitirá a los atacantes lanzar operaciones personalizadas y dirigidas, explotando vulnerabilidades específicas a partir de datos masivamente recopilados. Sectores críticos como la sanidad, la energía y las infraestructuras de transporte seguirán siendo objetivos prioritarios debido a su impacto en la sociedad.

La proliferación de dispositivos conectados al Internet de las Cosas (IoT) abre nuevas puertas a los atacantes, quienes podrían utilizar redes vulnerables para realizar ataques masivos, como los DDoS.

Como respuesta, las organizaciones deben invertir en tecnologías de detección temprana, educar a sus empleados sobre mejores prácticas de ciberseguridad y colaborar con gobiernos e instituciones para compartir información sobre amenazas.

Conclusiones

El panorama de ciberseguridad en 2024 y el inicio de 2025 han demostrado que las amenazas evolucionan rápidamente, mientras que las defensas a menudo se quedan rezagadas.

La colaboración entre sector público y privado, junto con inversiones significativas en tecnologías avanzadas y educación en ciberseguridad, será esencial para construir un ecosistema digital más resiliente.

En un mundo donde las oportunidades tecnológicas y los riesgos van de la mano, solo aquellos que estén preparados podrán prosperar. Frente a un futuro digital incierto, la proactividad y la adaptabilidad serán nuestras mejores defensas.

Diego Alonso Fernández
Cybersecurity Analyst

Adrián Álvarez Sánchez
Cybersecurity Architect

Medidas preventivas contra las estafas

Artículo por Alejandra Romero Gutiérrez

La detección de las estafas, con carácter preventivo, es muy compleja dado que es el propio usuario legítimo el que está efectuando la operación. En este artículo, realizaremos una revisión de diferentes medidas que pueden permitir un mayor índice de detección de las estafas, teniendo en consideración la fricción con el cliente y el apetito al riesgo de la entidad financiera.

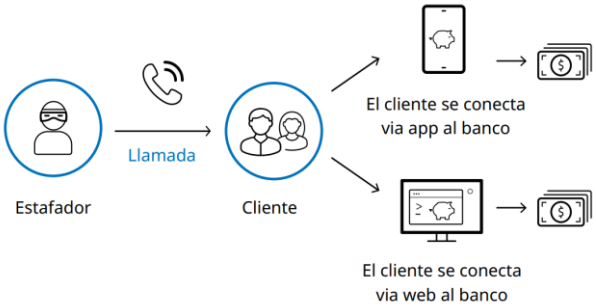
El gran incremento de estafas frente al fraude convencional está provocando una gran erosión a nivel reputacional en las entidades financieras, preocupación por la posible asunción de pérdidas a futuro y un gran daño a la sociedad en general. Esto es debido al bajo coste que suponen las campañas de estafa para los equipos organizados de defraudadores, junto a grandes beneficios económicos.

Frente al fraude convencional, en donde los criminales buscan hacerse con las claves del usuario por distintos métodos, en las estafas es el propio usuario el que realiza la operación de engaño. Métodos como la inteligencia del dispositivo, la geolocalización o modelos de Inteligencia Artificial destinados a la prevención de fraude, entre otros, por sí mismos no arrojan buenos resultados para detectar las estafas, ni prevenir que estas se produzcan.

A continuación, analizamos los principales vectores de ataque y soluciones que han arrojado buenos resultados.

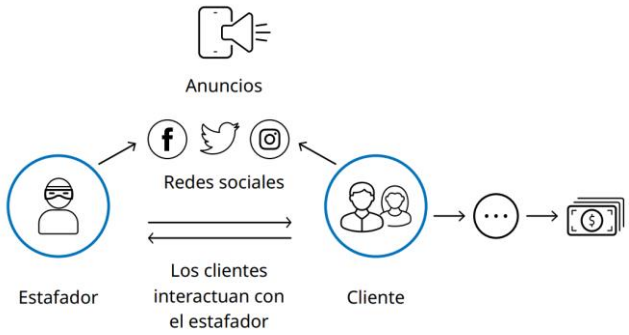
Estafa mediante llamada telefónica

El estafador, mediante una llamada a la víctima, genera una situación de estrés para que acceda al banco (vía app o web) y transfiera una cantidad de dinero.



Estafa mediante anuncios / redes sociales

El estafador, mediante anuncios y comunicaciones en redes sociales, atrae a las potenciales víctimas con las que interactúa hasta finalmente convencerles de transferir su dinero. Este método es muy usual en las estafas de inversión, como por ejemplo en la compra de bienes y de alquileres. También debe tenerse en consideración dentro de los vectores de ataque a aquellos estafadores que abren cuentas en entidades financieras, online o en oficina, con el fin de recibir el dinero que han ganado de las estafas.



Medidas Preventivas

Creación de modelos de *scoring*

Las entidades pueden plantearse la creación de modelos de *scoring* específicos que permitan mejorar, por ejemplo, la detección de posibles estafadores y mulas o de potenciales víctimas de estafas. En base a datos históricos pueden analizarse diversos datos como ocupación, productos contratados, tipo de alta, tipo de comunicación con su entidad (inclusión de consultas y campañas), edad, histórico de transaccionalidad e inversiones, etc., con el fin identificar patrones comunes para, posteriormente, extrapolarlos.

Estos modelos, además de ayudar en la prevención de estafas, pueden mejorar falsos positivos, solventar la problemática de los bloqueos y contribuir al cumplimiento de la identificación y reporte de cuentas mula.

Biometría del comportamiento

Los patrones de comportamiento como los movimientos del ratón o del dispositivo, patrones de tecleo o duración de la sesión pueden indicar signos de estrés, vacilación o distracción, que son señales que suelen observarse cuando un cliente actúa guiado por un delincuente.

De esta forma, el uso de la biometría comportamental permite tener una idea de las emociones o intenciones de un usuario durante una sesión e identificar en tiempo real las estafas de ingeniería social. Varias soluciones del mercado han invertido en esfuerzos de investigación y desarrollo en modelar patrones específicos de comportamiento que predicen las estafas.

Normalmente estas herramientas funcionan mejor si se orquestan sus señales biométricas de comportamiento con perfiles transaccionales utilizando motores de riesgo, capaces de puntuar el riesgo de estafas potenciales y desencadenar tratamientos de intervención en tiempo real.

Análisis de enlaces

Esta medida vincula una o más características de identificación asociadas a un presunto ataque fraudulento con características de identificación de mulas o defraudadores denunciados.

Existen varias soluciones que aprovechan las redes de características de dispositivos vinculados con personas etiquetadas con marcadores indicativos de asociación con fraude por otros miembros del consorcio. Presentan buenos resultados para detectar posibles estafas, puntuando el riesgo de los pagos salientes en función de los vínculos entre las características de la cuenta o el dispositivo del beneficiario y las características de la cuenta o el dispositivo de las personas denunciadas.

Call in progress

Existen soluciones que detectan cuando un usuario se encuentra en una llamada telefónica y está operando con su banca, a fin de prevenir posibles situaciones de estafa. Algunas son capaces de detectar si la llamada es por WhatsApp.

Esta funcionalidad debe estar acompañada de reglas para disminuir la fricción con los clientes y los falsos positivos, a modo de ejemplo, si está en la lista de beneficiarios usuales.

Intervenciones interactivas con el usuario

La solución que empieza a plantear el mercado pasa por ampliar la fricción con los clientes (normalmente, para los grupos vulnerables de ser estafados), alterando el flujo de finalización de operación enviando a los usuarios mensajes específicos sobre la operación y requiriendo factores adicionales.

Para cada una de las tipologías de estafa deberían identificarse los patrones más comunes de manera que pudiera enviarse un mensaje al usuario en tiempo real solicitando un segundo factor de autenticación sin paralizar la operación. Este cambio en el *journey* permitiría generar dudas al cliente víctima de una posible estafa, añadir fricción adicional a porcentaje limitado de clientes, reducir las revisiones por parte de equipo de operación y una mayor facilidad en el proceso de reclamaciones.

Colaboración

La colaboración entre las entidades financieras en la lucha contra el crimen financiero compartiendo datos confirmados como fraude, generará una importante mejora en la prevención del fraude. La colaboración entre entidades financieras y no financieras y entes públicos involucrados en la lucha contra el fraude aportará una mayor seguridad a la hora de operar por parte de los clientes.

Concienciación

La educación y formación de los consumidores es fundamental en la lucha contra el fraude ya que el cliente suele ser la pieza más débil en la cadena de seguridad.

Conocer los métodos más habituales de fraude y estafas permite que los consumidores detecten estas señales y actúen antes de ser víctimas. Asimismo, conocer cómo protegerse mitiga la ansiedad y el estrés asociado a la posibilidad de ser engañado.

NTT DATA dispone de un equipo altamente especializado en la prevención, detección y gestión del fraude. Nuestra experiencia multidisciplinar nos permite asesorar a las organizaciones en la toma de decisiones estratégicas, así como en la selección, adaptación e implementación de soluciones tecnológicas personalizadas. Gracias a nuestro profundo conocimiento del ecosistema integral, ofrecemos una visión 360° y un enfoque de extremo a extremo (e2e) para garantizar la máxima efectividad en la mitigación del fraude.

Alejandra Romero Gutierrez
Director FinCrime

Altos estándares de ciberseguridad

Tendencias por Gerard Marín

El sector financiero se enfrenta a importantes desafíos de ciberseguridad en 2025 marcados por el uso de inteligencia artificial y el aumento de la superficie de riesgo debido a ecosistemas cada vez más amplios. A esto se suma la implementación del Reglamento de Resiliencia Operativa Digital (DORA) que busca fortalecer la capacidad del sector para gestionar amenazas complejas. La transición hacia modelos de confianza cero y el avance en criptografía resistente a la computación cuántica serán claves para garantizar la protección frente a riesgos presentes y futuros.

Los dos grandes retos del 2025 serán el uso de la IA por parte de los ciberdelincuentes y la ampliación de la superficie de riesgo.

Los bancos e instituciones financieras están utilizando cada vez más la inteligencia artificial (IA) para la detección y mitigación de amenazas. Sin embargo, los ciberdelincuentes han respondido con técnicas de aprendizaje automático (ML) para superar las medidas de seguridad tradicionales. Estos ataques se están volviendo más sofisticados, personalizados y difíciles de detectar, atacando vulnerabilidades con precisión. Este uso adversarial de la IA subraya la necesidad de soluciones de seguridad innovadoras que puedan anticipar y contrarrestar las amenazas en evolución.

Además, en su búsqueda de rentabilidad, el sector financiero amplía fronteras y cada vez establece más relaciones con terceros, proveedores y proveedores de terceros. Este hecho aumenta la superficie de riesgo, ya que es cierto que los bancos disponen de mejores medidas de prevención, detección y reacción a los ciberataques, pero puede que otros *partners* no las tengan.

Esto podría llevar a que los bancos, más allá de recibir ciberataques directos, se conviertan en víctimas de ciberataques dirigidos a su ecosistema de alianzas, proveedores, etc.

La implantación del DORA conllevará mayor inversión en ciberseguridad

En respuesta a estas crecientes amenazas, los organismos regulatorios están introduciendo marcos más estrictos para fortalecer la resiliencia en todo el sector financiero. Un hito clave en 2025 es la implementación del Reglamento de Resiliencia Operativa Digital (DORA, por sus siglas en inglés), que ha entrado en vigor el 17 de enero. Esta regulación tiene como objetivo armonizar los requisitos de gestión de riesgos TIC, garantizando que las entidades financieras estén mejor preparadas para manejar riesgos sistémicos, entre ellos, los cibernéticos.

Se espera que el sector financiero aumente significativamente sus inversiones en ciberseguridad. Además, se enfatiza la implantación de estrategias de resiliencia operativa robustas, sobre todo cuando se adopten tecnologías emergentes, con el fin de mitigar el impacto de los riesgos que llevan asociadas.

Las pautas integrales de DORA servirán como piedra angular en esta evolución regulatoria, obligando a las instituciones a adoptar medidas proactivas de gestión de riesgos.

Las nuevas amenazas requerirán arquitecturas de confianza cero

Los modelos tradicionales de seguridad basados en perímetros están demostrando ser inadecuados frente a la complejidad de las amenazas cibernéticas modernas. Para 2025, muchas organizaciones están en transición hacia una Arquitectura de Confianza Cero (ZTA, por sus siglas en inglés), un modelo que exige una verificación de identidad estricta para cada usuario y dispositivo que intente acceder a recursos en redes privadas.

Se espera un aumento de la investigación cuántica para hacer frente a los riesgos de 2030

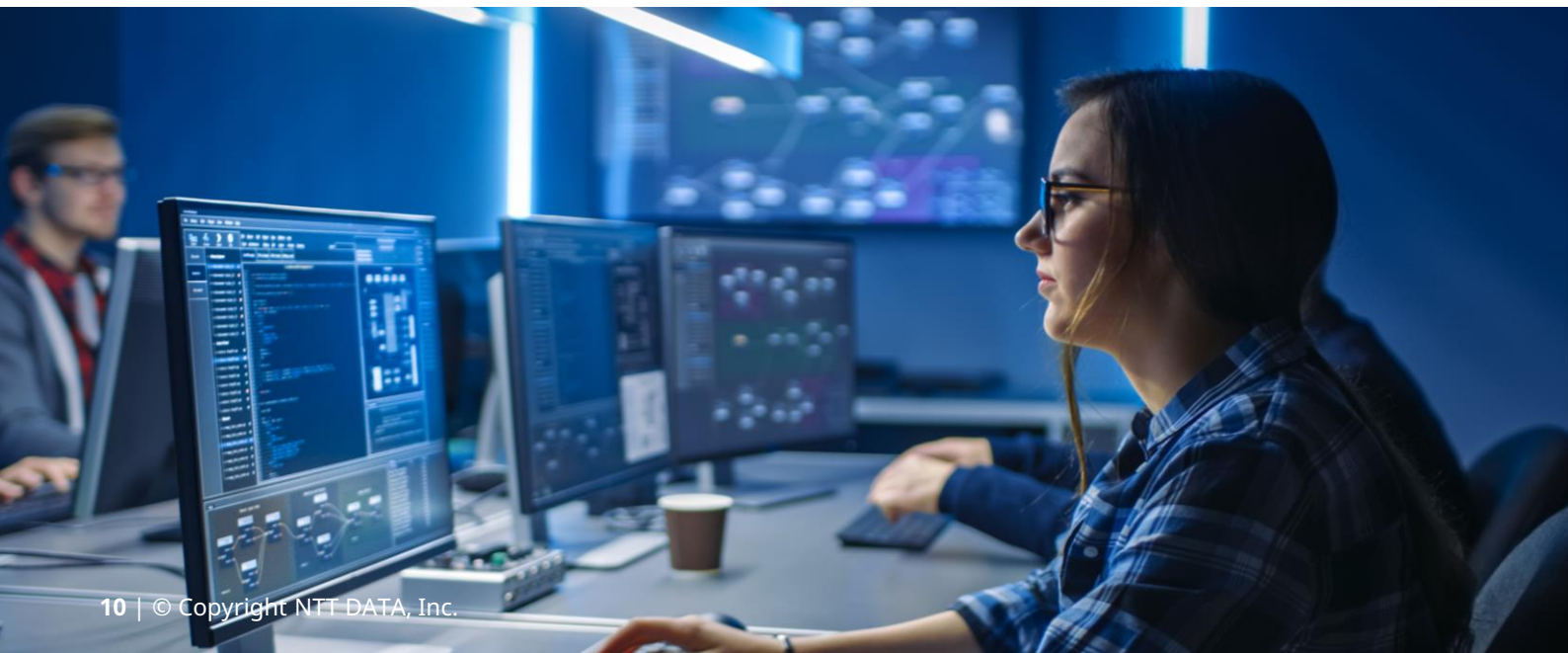
A medida que la computación cuántica se acerca a la viabilidad general, su potencial para interrumpir los estándares actuales de cifrado se cierne como una gran amenaza. Teóricamente, las computadoras cuánticas podrían romper algoritmos de cifrado ampliamente utilizados, como RSA y ECC, en cuestión de minutos, lo que supone un riesgo sin precedentes para la seguridad de los datos.

Aunque a nivel gubernamental ya se ha empezado a trabajar en ello, el sector financiero debería priorizar el desarrollo y adopción de criptografía resistente a la cuántica para contrarrestar este riesgo inminente. Si bien los expertos predicen que los ataques cuánticos podrían volverse prácticos hacia 2030, la base para la resiliencia debe comenzar ahora para proteger la infraestructura crítica contra futuras interrupciones.

Conclusión

Los desafíos de ciberseguridad del sector financiero en 2025 son formidables, pero no insuperables. Abordar el panorama de amenazas en escalada, adaptarse a los cambios regulatorios como DORA, adoptar Arquitectura de Confianza Cero y prepararse para riesgos cuánticos son pasos esenciales para garantizar la resiliencia. Al priorizar la innovación, la colaboración y la gestión proactiva de riesgos, la industria puede proteger sus sistemas y continuar prosperando en un mundo cada vez más digital.

Gerard Marín Raventos
Cybersecurity Consultant



Vulnerabilidades

Vulnerabilidad de ejecución remota de código en Webmin

Fecha: 20 de diciembre de 2024
CVE: CVE-2024-12828

CVSS: 9.9

CRÍTICA

Descripción

Desde el equipo de Zero Day Initiative han identificado una vulnerabilidad en el producto Webmin.

Esta vulnerabilidad permite a un atacante ejecutar código arbitrario en Webmin. Se requiere autenticación para explotar esta vulnerabilidad.

El fallo específico existe en las peticiones CGI en Webmin. La vulnerabilidad ocurre debido la falta de validación de una cadena proporcionada por el usuario antes de utilizarla para ejecutar una llamada al sistema. Un atacante podría aprovechar esta vulnerabilidad para ejecutar código en el contexto de *root*.

Solución

Webmin ha publicado una actualización para corregir la vulnerabilidad.

La actualización está disponible en una nueva versión en el GitHub oficial del fabricante.

Productos afectados

Esta vulnerabilidad afecta a los siguientes productos Webmin:

- El fabricante ha indicado que Webmin está afectado, sin especificar ninguna versión.

Referencias

- incibe.es
- nvd.nist.gov
- zerodayinitiative.com

TLP:WHITE

Vulnerabilidades

Vulnerabilidad crítica en SonicWall Firewall

Fecha: 7 de enero de 2025
CVE: CVE-2024-53704 y 3 más

CVSS: 8.2

ALTA

Descripción

El proveedor SonicWall ha alertado a sus clientes para que actualicen sus dispositivos *firewall* SonicOS para corregir una vulnerabilidad crítica.

Mediante esta vulnerabilidad, existe la posibilidad de realizar un *bypass* de autenticación que afecta a las conexiones SSL de VPN y administración de servicios SSH.

Dicha vulnerabilidad ha sido corregida por el fabricante el pasado 7 de enero de 2025, y el proveedor sugiere la actualización inmediata de este nuevo parche para corregir esta vulnerabilidad y otras no tan críticas.

Solución

Esta vulnerabilidad ha sido corregida en el último parche de seguridad del fabricante.

Para corregir esta vulnerabilidad se debe actualizar a las siguientes versiones:

- Gen 6 / 6.5 *hardware firewalls*: SonicOS 6.5.5.1-6n o más reciente.
- Gen 6 / 6.5 NSv *firewalls*: SonicOS 6.5.4.v-21s-RC2457 o más reciente.
- Gen 7 *firewalls*: SonicOS 7.0.1-5165; 7.1.3-7015 o más reciente.
- TZ80 *firewalls*: SonicOS 8.0.0-8037 o más reciente.

Productos afectados

Esta vulnerabilidad afecta a las siguientes versiones del *software:*

- 6.5.4.15-117 y versiones anteriores
- 7.1.1-7058 y versiones anteriores.
- Versión 7.1.2-7019.

Referencias

- psirt.global.sonicwall.com
- www.incibe.es

TLP:WHITE

Actualización crítica de SHARP para mitigar vulnerabilidades en *routers*

Fecha: 22 de diciembre de 2024
CVE: CVE-2024-46873 y 2 más

Crítica

Descripción

Desde la compañía SHARP han publicado un aviso relacionado con múltiples vulnerabilidades críticas que afectan a algunos modelos de sus *routers*.

En caso de ser explotadas estas vulnerabilidades, un atacante podría lograr la ejecución de comandos con privilegios de administrador, acceso no autorizado y la posibilidad de llegar a realizar ataques de denegación de servicio. Las vulnerabilidades con más riesgo son: CVE-2024-45721, CVE-2024-46873, CVE-2024-54082.

La ejecución de estas vulnerabilidades podría dar lugar a que los atacantes roben información sensible, afecten al servicio mediante ataques de denegación de servicio y consigan el control remoto no autorizado.

Productos afectados

Los productos afectados por estas vulnerabilidades son:

- NTT Docomo, Inc: Wi-Fi STATION SH-05L, SH-52B, SH-54C y home 5G HR02
- SoftBank Corp: Pocket Wi-Fi 809SH
- KDDI Corporation: Speed Wi-Fi NEXT W07

Solución

Se recomienda actualizar todos los productos afectados a la versión más reciente dependiendo del producto afectado, siguiendo las recomendaciones del fabricante.

Referencias

- unaaldia.hispasec.com
- nvd.nist.gov
- incibe.es

TLP:WHITE

Parches de seguridad para productos Palo Alto Networks (PAN)

Fecha: 27 de diciembre de 2024
CVE: CVE-2024-3393

Alta

Descripción

Palo Alto Networks ha publicado parches para mitigar una vulnerabilidad crítica en su *software* de gestión de dispositivos.

Concretamente, la vulnerabilidad se encuentra en la sección "DNS Security" dentro de su *software*, donde permitiría a un atacante no autenticado explotar los *firewalls* bajo paquetes de datos creados de manera manual. La ejecución de estas instrucciones forzaría al dispositivo a su reinicio. Repetir esto en cadena forzaría al dispositivo a entrar en modo mantenimiento, causando una denegación de servicio en el mismo (DoS).

Debido a la gravedad de la vulnerabilidad, se ha evaluado con una puntuación de 8.7 en la escala de CVSS, sabiendo que además está siendo explotada activamente.

Productos afectados

Las actualizaciones de seguridad afectan a las siguientes versiones:

- PAN-OS 11.2 y anteriores
- PAN-OS 11.1 y anteriores
- PAN-OS 10.2 y anteriores
- PAN-OS 10.1 y anteriores

Solución

PAN recomienda la actualización a las siguientes versiones:

- PAN-OS 11.2.3
- PAN-OS 11.1.5
- PAN-OS 10.2.10-h12 y 10.2.13-h2
- PAN-OS 10.1.14-h8

Referencias

- gbhackers.com
- security.paloaltonetworks.com
- socradar.io

Eventos

EspañaSec Cyber Summit
11 – 12 de febrero

EspañaSec Cyber Summit tiene como objetivo principal reunir a más de 100 líderes de ciberseguridad de diversas industrias, como banca, automoción, servicios públicos y fabricación, fomentando la colaboración entre profesionales con ideas afines.

Durante dos días, el evento se centrará en explorar las principales tendencias en estrategias, herramientas y estándares de ciberseguridad. La agenda estará compuesta por sesiones educativas e interactivas diseñadas para promover la generación de conocimientos, la planificación estratégica y el intercambio de experiencias entre expertos del sector.

Enlace

CyberTech Latin America 2025
19 - 20 febrero

Desde su creación en 2017, CyberTech América Latina ha sido el puente que conecta los principales ecosistemas de ciberseguridad, negocios e innovación de la región.

Este evento, realizado en colaboración con la Embajada de Israel en Panamá, la Ciudad del Saber, SENACYT, AIG, y otros destacados socios regionales, es un acceso a una reunión exclusiva. En el evento se encontrarán funcionarios gubernamentales, líderes de la industria, académicos, empresas consolidadas y *start-ups* dinámicas bajo un mismo techo.

Enlace

CIBER2C MX
26 de febrero

El Congreso CIBER2C MX es un evento clave en ciberseguridad que reúne a expertos, representantes gubernamentales y líderes de la industria para abordar amenazas y soluciones en sectores esenciales como energía, transporte y salud. Su objetivo es salvaguardar los sistemas que sostienen la economía y la vida diaria.

Bajo el lema "Las infraestructuras críticas, en la diana: el gran desafío de la ciberseguridad", el congreso fomenta el intercambio de estrategias y la colaboración público-privada, promoviendo una cultura de innovación y resiliencia ante los retos de un mundo interconectado.

Enlace

HackOn 2025
28 de febrero al 1 de marzo

HackOn es un evento nacido en 2019 dirigido a profesionales y entusiastas de la ciberseguridad que combina conferencias, talleres prácticos y CTF.

En su próxima edición, HackOn explorará temas como inteligencia artificial aplicada a la seguridad, *hacking* ético y ciber resiliencia. Con actividades para todos los niveles, este evento promete ser una experiencia formativa y colaborativa que impulsa la innovación tecnológica y la construcción de redes profesionales.

Enlace

Recursos

➢ AttackGen

AttackGen es una herramienta de código abierto que ayuda a las organizaciones a prepararse para las ciber amenazas. Utiliza modelos avanzados de IA y el marco ATT&CK de MITRE para crear escenarios de respuesta a incidentes adaptados al tamaño de la organización, sector y actores de amenazas seleccionados. Con funciones como plantillas rápidas para ataques comunes y un asistente integrado para refinar los escenarios, AttackGen hace que la planificación de incidentes sea fácil y eficaz. Es compatible con sistemas empresariales e industriales, lo que ayuda a los equipos a estar preparados para las amenazas del mundo real.

Enlace

➢ Brainstorm

Brainstorm es una herramienta que hace que el *fuzzing* web sea más eficaz mediante el uso de LLM locales como Ollama junto con ffuf. Analiza los enlaces de un sitio web de destino y genera conjeturas inteligentes para archivos ocultos, directorios y API *endpoints*. Al aprender de cada descubrimiento, reduce el número de peticiones necesarias a la vez que encuentra más puntos finales en comparación con las listas de palabras tradicionales. Esta herramienta es perfecta para optimizar las tareas de fuzzing, ahorrar tiempo y evitar la detección

Enlace

➢ FuzzyAI

Herramienta que ofrece a las organizaciones un enfoque sistemático para probar modelos de IA frente a diversas entradas de adversarios, descubrir posibles puntos débiles en sus sistemas de seguridad y hacer que el desarrollo y el despliegue de la IA sean más seguros. En el corazón de FuzzyAI se encuentra un potente *fuzzer* capaz de exponer vulnerabilidades encontradas a través de más de diez técnicas de ataque distintas, desde eludir filtros éticos hasta exponer indicaciones ocultas del sistema.

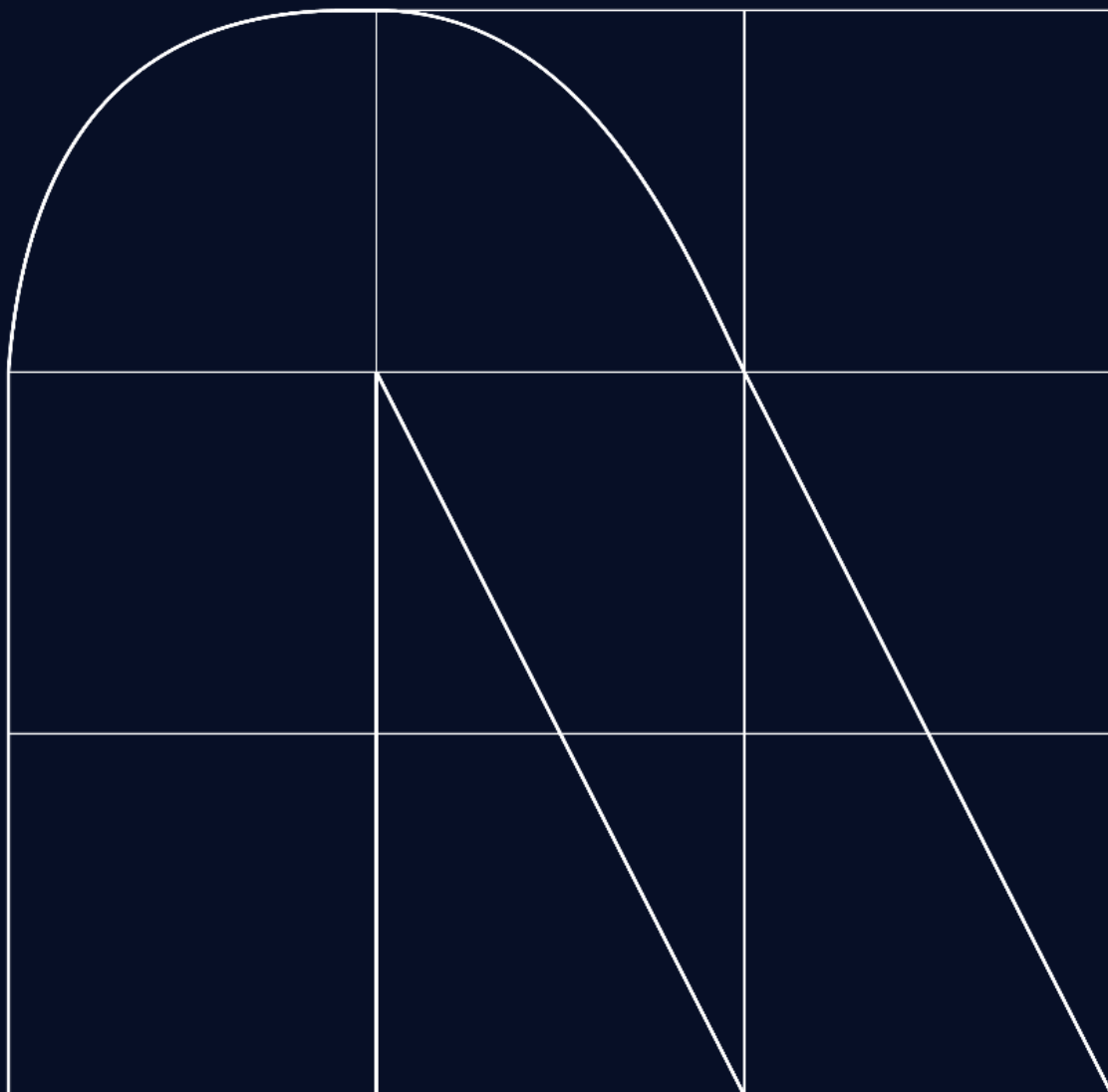
Enlace

➢ Vulnhuntr

Analizador estático de código Python que aprovecha la potencia de los grandes modelos de lenguaje (LLM) para encontrar y explicar vulnerabilidades complejas de varios pasos. Gracias a las capacidades de modelos como Claude 3.5, AI ha descubierto más de una docena de vulnerabilidades 0-day explotables de forma remota dirigidas a proyectos de código abierto en el ecosistema de AI con más de 10.000 estrellas de GitHub en tan solo unas horas de funcionamiento.

Enlace

Suscríbete a RADAR
up.nttdata.com/suscribetearadar



Powered by the cybersecurity NTT DATA team

es.nttdata.com