Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 209 – Año 2023

Este boletín periódico es un resumen seleccionado de las últimas vulnerabilidades, incidentes de seguridad e informes recopilados de fuentes internacionales conocidas dedicadas a la seguridad informática. Está destinado a las áreas de ciberseguridad de la Defensa como información de interés general para su difusión.

NOTICIAS DE CIBERSEGURIDAD entre el 24/6/23 y el 9/7/23

1. Hackers chinos atacan embajadas europeas con una técnica de pirateo de HTML.
https://therecord.media/html-smuggling-china-espionage-europe

2. Microsoft niega que se haya producido una filtración de 30 millones de clientes.
https://www.infosecurity-magazine.com/news/microsoft-denies-major-30-million/

3. La Comisión Europea insta a tomar medias de seguridad con las redes 5G.
https://cybersecuritynews.es/la-comision-europea-insta-a-tomar-medias-de-seguridad-con-las-redes-5g/

4. Nueva herramienta explota el error de Microsoft Teams para enviar malware a los usuarios.
https://www.bleepingcomputer.com/news/security/new-tool-exploits-microsoft-teams-bug-to-send-malware-to-users/

TRABAJOS, ESTUDIOS Y ANÁLISIS ABOCADOS A LAS TEMÁTICAS DE LA CIBERSEGURIDAD

1. ¿Quién está detrás de la estafa de correo masivo de DomainNetworks?
https://krebsonsecurity.com/2023/07/whos-behind-the-domainnetworks-snail-mail-scam/

2. El error de Ghostscript podría permitir que los documentos no autorizados ejecuten comandos del sistema.
https://nakedsecurity.sophos.com/2023/07/04/ghostscript-bug-could-allow-rogue-documents-to-run-system-commands/?utm_source=dlvr.it&utm_medium=twitter

3. Más de dos tercios de los firewalls de FortiGate aún están en riesgo
https://www.infosecurity-magazine.com/news/two-thirds-fortigate-risk/

4. La nueva herramienta de Python verifica los paquetes de NPM en busca de problemas de confusión manifiesta.
https://www.bleepingcomputer.com/news/security/new-python-tool-checks-npm-packages-for-manifest-confusion-issues/

5. Mozilla publica recomendaciones de seguridad para Thunderbird, Firefox y Firefox ESR.
https://www.cisa.gov/news-events/alerts/2023/07/06/mozilla-releases-security-advisories-thunderbird-firefox-and-firefox-esr

6. CISA y sus asociados difunden un aviso conjunto de ciberseguridad sobre las nuevas variantes identificadas del malware Truebot.
https://www.cisa.gov/news-events/alerts/2023/07/06/cisa-and-partners-release-joint-cybersecurity-advisory-newly-identified-truebot-malware-variants

7. Snappy: una herramienta para detectar puntos de acceso WiFi no autorizados en redes abiertas.
https://www.bleepingcomputer.com/news/security/snappy-a-tool-to-detect-rogue-wifi-access-points-on-open-networks/

NOTAS DE INTERÉS

1. La campaña del troyano OpenSSH se centra en sistemas Linux y dispositivos IoT.
https://www.malwarebytes.com/blog/news/2023/06/openssh-trojan-campaign-targets-linux-systems-and-iot-devices

2. El nuevo Meduza Stealer de Windows se centra en decenas de billeteras de criptomonedas y gestores de contraseñas.
https://securityaffairs.com/148059/cyber-crime/meduza-stealer-malware.html

3. China frena exportaciones de materiales clave para chips informáticos.
https://www.bbc.com/news/business-66093114

4. TSA quiere expandir el reconocimiento facial a cientos de aeropuertos en la próxima década.
https://www.theregister.com/2023/07/03/tsa_facial_recognition_airport/

5. Amazon tiene un gran problema ya que los libros generados por IA inundan ***Kindle Unlimited.***
https://www.securityweek.com/in-other-news-healthcare-product-flaws-free-email-security-testing-new-attack-techniques/

ACTUALIZACIONES DE SEGURIDAD

1. El complemento de WordPress permite a los usuarios convertirse en administradores: ¡actualice temprano, actualice a menudo!
https://nakedsecurity.sophos.com/2023/07/03/wordpress-plugin-lets-users-become-admins-patch-early-patch-often/

2. CISA agrega errores de Samsung y D-link a su catálogo de vulnerabilidades conocidas explotadas.
https://securityaffairs.com/148079/security/cisa-adds-samsung-and-d-link-bugs-to-its-known-exploited-vulnerabilities-catalog.html

3. Google lanza actualización de parche de Android para 3 vulnerabilidades explotadas activamente.
https://thehackernews.com/2023/07/google-releases-android-patch-update.html

4. TackRot es una nueva vulnerabilidad de seguridad en el kernel de Linux.
https://securityaffairs.com/148231/security/stackrot-linux-kernel-privilege-escalation-bug.html