@mindefarg
argentina.gob.ar/defensa

Ministerio de Defensa
Argentina

Edificio Libertador
Azopardo 250 (CABA)
(54 11) 4346-8836/9

Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 204 – 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 25/2/23 y el 10/3/23

1. Los ciberdelincuentes afirman haber accedido a T-Mobile más de 100 veces en 2022.
https://krebsonsecurity.com/2023/02/hackers-claim-they-breached-t-mobile-more-than-100-times-in-2022/

2. Informe: Un conglomerado brasileño sufre una filtración de datos de 3 TB.
https://www.infosecurity-magazine.com/news/brazilian-conglomerate-3tb-data/

3. Datos confidenciales de miembros de la Cámara y el Senado de los EE. UU. Hackeados.
https://www.theguardian.com/us-news/2023/mar/08/us-house-senate-members-data-leaked-for-sale

4. Medusa ransomware roba datos de escuelas de Minneapolis exigiendo un rescate de $ 1,000,000.
https://www.bleepingcomputer.com/news/security/ransomware-gang-posts-video-of-data-stolen-from-minneapolis-schools/

5. El ataque del ransomware Ransom House afecta al Hospital Clínic de Barcelona.
https://securityaffairs.com/143121/cyber-crime/hospital-clinic-de-barcelona-ransomware.html

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

1. El Gobierno de EE.UU. ha publicado su estrategia sobre ciberseguridad nacional.
https://www.securityweek.com/white-house-releases-national-cybersecurity-strategy/

2. CISA Red Team comparte hallazgos clave para mejorar la supervisión y el refuerzo de las redes
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a

3. Reporte de CISA sobre el ramsonware Royal: TTP, IOC y otros datos útiles para los equipos de ciberseguridad.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

4. Falla crítica de inyección de comandos en teléfonos IP de Cisco.
https://exchange.xforce.ibmcloud.com/collection/04c608e48ecc7ba046c47afce51bbb96

5. Las tácticas cibernéticas de Rusia en Ucrania se orientan hacia el espionaje.
https://www.infosecurity-magazine.com/news/russias-cyber-tactics-shift-to/

NOTAS DE INTERÉS

1. Acer confirma intrusión luego de que se ofreciera una caché de 160 GB de archivos robados.
https://www.theregister.com/2023/03/08/acer_confirms_server_breach/

2. ChatGPT se integra en los productos de ciberseguridad mientras el sector pone a prueba sus capacidades.
https://www.securityweek.com/chatgpt-integrated-into-cybersecurity-products-as-industry-tests-its-capabilities/

3. ¿Quién está detrás del troyano de acceso remoto NetWire?
https://krebsonsecurity.com/2023/03/whos-behind-the-netwire-remote-access-trojan/

4. Rusia prohíbe las aplicaciones de mensajería extranjeras en las organizaciones gubernamentales.
https://www.bleepingcomputer.com/news/security/russia-bans-foreign-messaging-apps-in-government-organizations/

5. CISA advierte sobre falla crítica de VMware RCE.
https://www.bleepingcomputer.com/news/security/cisa-warns-of-critical-vmware-rce-flaw-exploited-in-attacks/

6. Cuando la protección parcial es protección cero: los puntos ciegos de MFA de los que nadie habla.
https://thehackernews.com/2023/03/when-partial-protection-is-zero.html

7. El portero/intercomunicador Akuvox E11 está plagado de vulnerabilidades.
https://arstechnica.com/information-technology/2023/03/go-ahead-and-unplug-this-door-device-before-reading-youll-thank-us-later/

8. GitHub comienza la implementación de 2FA para los contribuyentes de código
https://www.csoonline.com/article/3690329/github-begins-2fa-rollout-for-code-contributors.html

9. 6 complementos de ciberseguridad y privacidad para Firefox que debes conocer.
https://www.helpnetsecurity.com/2023/03/06/cybersecurity-privacy-firefox-add-ons/

ACTUALIZACIONES DE SEGURIDAD

1. Cisco difunde un aviso de seguridad para el software IOS XR.
https://www.cisa.gov/news-events/alerts/2023/03/09/cisco-releases-security-advisory-ios-xr-software

2. Fortinet ha parcheado 15 vulnerabilidades en una variedad de sus productos, incluido CVE-2023-25610.
https://www.helpnetsecurity.com/2023/03/09/cve-2023-25610/

3. Veeam advierte instalar parches para corregir un error en su producto Backup & Replication
https://securityaffairs.com/143218/security/veeam-backup-replication-bug.html

4. US CISA agregó fallas explotadas en Teclib GLPI, Apache Spark y Zoho ManageEngine ADSelfService Plus.
https://securityaffairs.com/143204/security/cisa-known-exploited-vulnerabilities-catalog-2.html