@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. 118 – Año 2021

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.

16/07/2021

- El malware de banca móvil Toddler se extiende por toda Europa.
  https://www.zdnet.com/article/toddler-mobile-banking-malware-surges-across-europe/
- **Una empresa israelí ayudó a gobiernos a atacar a periodistas y activistas con días cero y programas espía.**
  https://thehackernews.com/2021/07/israeli-firm-helped-governments-target.html
  https://threatpost.com/nso-group-data-pegasus/167897/
- Víctimas de Kaseya lidiando con el descifrado después de que REvil se volvió invisible.
  https://www.zdnet.com/article/kaseya-victim-struggling-with-decryption-after-revil-goes-dark/
- El ciberataque al Tribunal de Cuentas de Moldavia destruyó las auditorías públicas.
  https://www.bleepingcomputer.com/news/security/cyberattack-on-moldovas-court-of-accounts-destroyed-public-audits/

17/07/2021

- La empresa estatal de telecomunicaciones CNT de Ecuador se ve afectada por RansomEXX.
  https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/
- El ransomware HelloKitty se centra en dispositivos SonicWall vulnerables.
  https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/

18/07/2021

- Facebook informa que ciberdelincuentes iraníes tienen como objetivo el personal militar de EE.UU.
  https://www.ehackingnews.com/2021/07/facebook-says-iranian-hackers-targeted.html
- Virginia Tech publica que fue blanco de dos ciberataques recientes.
  https://www.securityweek.com/virginia-tech-says-it-was-targeted-2-recent-cyberattacks

19/07/2021

- **Biden y el Reino Unido van tras los ciberatacantes chinos.**
  https://www.defenseone.com/policy/2021/07/biden-goes-after-chinas-cyber-attackers/183854/
  https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking
  https://news.sky.com/story/china-accused-of-systematic-cyber-sabotage-by-uk-and-allies-12359056
- La filtración de datos de Saudi Aramco pone a la venta 1 TB de datos robados.
  https://www.bleepingcomputer.com/news/security/saudi-aramco-data-breach-sees-1-tb-stolen-data-for-sale/

- Estudio jurídico de Ford, Boeing, Exxon, Marriott, Walgreens y otros, hackeado en un ataque ransomware.
https://www.zdnet.com/article/law-firm-for-ford-boeing-exxon-marriott-walgreens-and-more-hacked-in-ransomware-attack/

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

- Cloudflare corrige el error de ejecución de código CDN que afecta al 12,7% de todos los sitios.
https://www.bleepingcomputer.com/news/security/cloudflare-fixes-cdn-code-execution-bug-affecting-127-percent-of-all-sites/

NOTAS DE INTERÉS

- El 57% de los incidentes notificados son causados por empleados internos.
https://www.helpnetsecurity.com/2021/07/16/reported-incidents-caused-by-insiders/
- El nuevo "borrado rápido" de Google elimina los últimos 15 minutos de tu historial de búsqueda.
https://www.zdnet.com/article/googles-new-quick-delete-erases-the-last-15-mins-of-your-search-history/
- La mala configuración del almacén en la nube Artwork Archive expuso datos de los usuarios.
https://www.zdnet.com/article/artwork-archive-cloud-storage-misconfiguration-exposed-user-data-revenue-records/
- Las principales CVEs de interés para los ciberdelincuentes.
https://threatpost.com/top-cves-trending-with-cybercriminals/167889/
- Microsoft informa que hay que desactivar la cola de impresión de Windows para evitar hackeos.
https://arstechnica.com/gadgets/2021/07/disable-the-windows-print-spooler-to-prevent-hacks-microsoft-tells-customers/
- **Estados Unidos quiere construir una base de espionaje en el Reino Unido para ayudar a mantener la seguridad de los satélites.**
https://news.sky.com/story/us-wants-to-build-spy-base-in-uk-to-help-keep-satellites-safe-12357419
- Instagram presenta un "chequeo de seguridad" para ayudar a los usuarios a recuperar las cuentas hackeadas.
https://securityaffairs.co/wordpress/120260/security/instagram-security-checkup.html
- Los hackers burlaron Windows *Hello* engañando a una cámara web.
https://arstechnica.com/information-technology/2021/07/hackers-got-past-windows-hello-by-tricking-a-webcam/
- Se descubre otra vulnerabilidad sin parches en el administrador de impresión de Windows.
https://thehackernews.com/2021/07/researcher-uncover-yet-another.html

ACTUALIZACIONES DE SEGURIDAD

- Microsoft: Nuevo error sin parchear en el *"spooler"* de impresión de Windows.
https://threatpost.com/microsoft-unpatched-bug-windows-print-spooler/167855/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481
- D-Link publica un arreglo (*hotfix*) para las vulnerabilidades de varios routers.
https://www.bleepingcomputer.com/news/security/d-link-issues-hotfix-for-hard-coded-password-router-vulnerabilities/
- Cisco libera actualizaciones de seguridad.
https://us-cert.cisa.gov/ncas/current-activity/2021/07/16/cisco-releases-security-updates