@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. 99/2021

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.

11/04/2021

- Las agencias de inteligencia de Estados Unidos advierten sobre las debilidades de la red 5G.
  https://thehackernews.com/2021/05/us-intelligence-agencies-warn-about-5g.html
- Nuevo malware para Android que ataca a los bancos de Italia, España, Alemania, Bélgica y los Países Bajos.
  https://www.zdnet.com/article/new-android-malware-targeting-banks-in-italy-spain-germany-belgium-and-the-netherlands/
- Los problemas de configuración de AWS conducen a la divulgación de 5 millones de registros.
  https://www.scmagazine.com/home/security-news/cloud-security/aws-configuration-issues-lead-to-exposure-of-5-million-records/
- Empresa de tecnología energética noruega fue afectada por un ataque de ransomware.
  https://www.wsj.com/articles/energy-tech-firm-hit-in-ransomware-attack-11620764034

12/05/2021

- Investigadores encuentran tres fallas en el sistema de voto electrónico de ACT en Australia que podrían afectar a los resultados de las elecciones.
  https://www.zdnet.com/article/researchers-find-three-flaws-in-act-e-voting-system-that-could-affect-election-outcomes/
- Una banda de ransomware filtra datos de la Policía de Washington, tras fracasar las negociaciones.
  https://thehackernews.com/2021/05/ransomware-gang-leaks-metropolitan.html

13/05/2021

- Colonial Pipeline restablece las operaciones interrumpidas por el ransomware.
  https://www.zdnet.com/article/colonial-pipeline-restarts-operations-brought-down-by-ransomware/
- Falsas aplicaciones para Android e iOS prometen rentables inversiones mientras roban tu dinero.
  https://www.zdnet.com/article/fake-android-ios-apps-promise-lucrative-investments-while-stealing-your-money/
- La empresa de seguros CNA restablece sus sistemas tras un ataque de ransomware.
  https://www.bleepingcomputer.com/news/security/insurance-giant-cna-fully-restores-systems-after-ransomware-attack/

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

- **Ataque al oleoducto Colonial: Todo lo que necesita saber el profesional de la ciberseguridad.**
  https://www.darkreading.com/operations/colonial-pipeline-cyberattack-what-security-pros-need-to-know/d/d-id/1340970

https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

- Una falsa aplicación de Chrome sirve de base para el ciberataque "Smish".
https://threatpost.com/fake-chrome-app-worming-smish-cyberattack/166038/
- DarkSide Ransomware: Mejores prácticas para prevenir la interrupción del negocio por ataques de ransomware.
https://us-cert.cisa.gov/ncas/alerts/aa21-131a
- Investigadores de FireEye documentaron 5 grupos separados sospechosos de estar conectados a DarkSide, la red de Ransomware responsable del incidente de seguridad de Colonial Pipeline.
https://www.zdnet.com/article/researchers-track-down-five-affiliates-of-darkside-ransomware-service/
- Casi todos los dispositivos Wi-Fi son vulnerables a los nuevos ataques FragAt.
https://thehackernews.com/2021/05/nearly-all-wifi-devices-are-vulnerable.html
https://www.zdnet.com/article/new-ransomware-cisa-warns-over-fivehands-file-encrypting-malware-variant/

NOTAS DE INTERÉS

- Los hackers de oleoducto de EE.UU. dicen que quieren dinero, no caos.
https://thehill.com/policy/national-security/552684-pipeline-hackers-say-they-want-money-not-mayhem
- Microsoft lanza un nuevo proyecto de código abierto para llevar la herramienta de Linux eBPF a Windows.
https://betanews.com/2021/05/11/microsoft-open-source-project-linux-tool-ebpf-on-windows/
- Ahora Microsoft Defender ATP asegura los dispositivos Linux y macOS en red.
https://www.bleepingcomputer.com/news/security/microsoft-defender-atp-now-secures-networked-linux-macos-devices/
- GitHub se prepara para ir más allá de las contraseñas.
https://threatpost.com/github-security-keys-passwords/166054/
- Casi la mitad de los proyectos de IoT no comprueban la seguridad del software.
https://betanews.com/2021/05/12/half-iot-projects-dont-test-software-security/
- La Casa Blanca se propone reforzar la ciberseguridad del país tras el *hackeo* del oleoducto.
https://www.defenseone.com/technology/2021/05/white-house-aims-beef-nations-cybersecurity-after-pipeline-hack/174003/

ACTUALIZACIONES DE SEGURIDAD

- VLC Media Player 3.0.14 soluciona el problema del actualizador automático de Windows.
https://www.bleepingcomputer.com/news/software/vlc-media-player-3014-fixes-broken-windows-automatic-updater/
- Adobe corrige la vulnerabilidad de día cero de Reader.
https://www.bleepingcomputer.com/news/security/adobe-fixes-reader-zero-day-vulnerability-exploited-in-the-wild/
- Microsoft: parches de mayo de 2021 con 55 fallas corregidos, cuatro de ellas críticas.
https://www.zdnet.com/article/microsofts-may-2021-patch-tuesday-55-flaws-fixed-four-critical/
https://threatpost.com/wormable-windows-bug-dos-rce/166057/
- Parches de Seguridad de SAP - Mayo 2021.
https://exchange.xforce.ibmcloud.com/collection/596141e9e139121f64c97999ce107e1a
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=576094655