@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. 95/2021**

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.

### 27/04/2021

- Dos ataques de phishing se han centrado en los clientes de Chase Bank.
  https://www.techrepublic.com/article/phishing-attacks-target-chase-bank-customers/
- MangaDex revela la filtración después de que su base de datos robada se compartiera en línea.
  https://www.bleepingcomputer.com/news/security/mangadex-discloses-data-breach-after-stolen-database-shared-online/
- Los piratas informáticos BABUK amenazan con liberar los datos robados a la policía de Washigton DC, en un aparente ataque ransomware.
  https://www.theverge.com/2021/4/27/22405339/washington-dc-police-hack-data-department-ransomeware-babuk
  https://thehackernews.com/2021/04/hackers-threaten-to-leak-dc-police.html

### 28/04/2021

- La red ferroviaria británica Merseyrail podría estar afectada por el ransomware Lockbit.
  https://www.bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/
- El Departamento de Salud de Wyoming (WDH), EE.UU., ha anunciado la exposición accidental de información sanitaria personal.
  https://www.infosecurity-magazine.com/news/data-breach-impacts-1-in-4/
- La vulneración de datos de DigitalOcean expone la información de facturación de los clientes.
  https://www.bleepingcomputer.com/news/security/digitalocean-data-breach-exposes-customer-billing-information/

### 29/04/2021

- Pacientes con cáncer derivados tras un ciberataque a una empresa de tecnología médica.
  https://www.infosecurity-magazine.com/news/cancer-patients-diverted-attack/
- La banda DoppelPaymer divulga los archivos del fiscal general de Illinois tras la ruptura de las negociaciones del rescate.
  https://threatpost.com/doppelpaymer-leaks-illinois-ag/165694/
- A los clientes de First Horizon Bank les han vaciado los fondos de sus cuentas.
  https://www.infosecurity-magazine.com/news/first-horizon-bank-customers/
- En Australia los anti-vacunas piratean los códigos QR en los lugares de registro de COVID-19.
  https://threatpost.com/anti-vaxxer-hijacks-qr-codes-covid19/165701/
- **El sistema judicial de Rio Grande do Sul de Brasil se ve afectado por el ransomware REvil.**
  https://www.bleepingcomputer.com/news/security/brazils-rio-grande-do-sul-court-system-hit-by-revil-ransomware/

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

- *Hackers* aprovechan el defecto de *día cero* del Gatekeeper para atacar ordenadores macOS.
  https://thehackernews.com/2021/04/hackers-exploit-0-day-gatekeeper-flaw.html
- El FBI comparte 4 millones de direcciones de correo electrónico utilizadas por Emotet.
  https://www.bleepingcomputer.com/news/security/fbi-shares-4-million-email-addresses-used-by-emotet-with-have-i-been-pwned/
- **Ciberespías atacan a las organizaciones militares con un nuevo *backdoor*.**
  https://thehackernews.com/2021/04/chinese-hackers-attacking-military.html
  https://www.cyberscoop.com/chinese-military-hackers-naikon-bitdefender-military/
- Microsoft Office SharePoint es objeto de ataques de phishing y ransomware de elevado riesgo.
  https://threatpost.com/sharepoint-phish-ransomware-attacks/165671/
- RotaJakiro: Una puerta trasera de Linux que ha permanecido oculta durante años.
  https://www.zdnet.com/article/rotajakiro-a-linux-backdoor-that-has-flown-under-the-radar-for-years/
- Los delincuentes de LuckyMouse se centraron en bancos, empresas y gobiernos en 2020.
  https://thehackernews.com/2021/04/luckymouse-hackers-target-banks.html

## NOTAS DE INTERÉS

- El FBI y el CISA descubren las tácticas empleadas por los hackers de la inteligencia rusa.
  https://thehackernews.com/2021/04/fbi-cisa-uncover-tactics-employed-by.html
  https://us-cert.cisa.gov/ncas/alerts/aa21-116a
- Un argentino compra el dominio de Google por 2 libras (esta noticia es conocida, pero ha aparecido en muchos medios internacionales)
  https://www.theguardian.com/technology/2021/apr/27/argentinian-buys-googles-domain-name-for-2-pounds
- El Pentágono explica la extraña transferencia de 175 millones de direcciones IP a una empresa poco conocida.
  https://arstechnica.com/information-technology/2021/04/pentagon-explains-odd-transfer-of-175-million-ip-addresses-to-obscure-company/
- Una vulnerabilidad del kernel de Linux expone la "*stack memory*" y causa pérdidas de datos.
  https://www.zdnet.com/article/linux-kernel-vulnerability-exposes-stack-memory/
- Los ciberdelincuentes utilizan ampliamente la macro de Excel 4.0 para distribuir malware.
  https://thehackernews.com/2021/04/cybercriminals-widely-abusing-excel-40.html
- Una coalición de expertos en seguridad comparte acciones para desbaratar el ransomware.
  https://www.bleepingcomputer.com/news/security/security-expert-coalition-shares-actions-to-disrupt-ransomware/
  https://threatpost.com/gov-task-force-ransomware-economy/165715/

## ACTUALIZACIONES DE SEGURIDAD

- Importante actualización del navegador Chrome - 26 de abril de 2021.
  https://exchange.xforce.ibmcloud.com/collection/3ae3c4e83b477bcfa6bd700dbdffc87d
  https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html
- Apple corrige un defecto de día cero en MacOS que puede eludir las defensas antimalware.
  https://threatpost.com/apple-patches-macos-bug-bypass-defenses/165611/