@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. 151 – Año 2022**

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 19/1/22 y el 25/1/22

- El grupo de marketing RRD confirma el robo de datos en el ataque del ransomware Conti.
https://www.bleepingcomputer.com/news/security/marketing-giant-rrd-confirms-data-theft-in-conti-ransomware-attack/
- El hackeo de Crypto.com afectó a 483 cuentas y provocó un robo de 34 millones de dólares.
https://securityaffairs.co/wordpress/126956/hacking/crypto-com-crypto-heist.html
- Ciberataque a la Cruz Roja expone datos de 515 mil personas altamente vulnerables.
https://securityaffairs.co/wordpress/126947/data-breach/red-cross-cyberattack.html
- El banco central de Indonesia confirma un ataque de ransomware, y Conti filtra datos.
https://www.bleepingcomputer.com/news/security/indonesias-central-bank-confirms-ransomware-attack-conti-leaks-data/
- La filtración de datos de OpenSubtitles afectó a 7 millones de abonados.
https://securityaffairs.co/wordpress/127092/data-breach/opensubtitles-data-breach.html
- **Hackers afirman haber encriptado los servidores de los FF.CC. bielorrusos.**
https://arstechnica.com/information-technology/2022/01/hactivists-say-they-hacked-belarus-rail-system-to-stop-russian-military-buildup/
- El Ministerio de Asuntos Exteriores de Canadá ha sido hackeado.
https://www.bleepingcomputer.com/news/security/canadas-foreign-affairs-ministry-hacked-some-services-down/

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

- Las vulnerabilidades de Zoom afectan a los clientes y a los servidores de MMR.
https://www.zdnet.com/article/zoom-vulnerabilities-impact-clients-mmr-servers/
https://googleprojectzero.blogspot.com/2022/01/zooming-in-on-zero-click-exploits.html
- El reciente malware BHUNT tiene como objetivo las criptocarteras y las contraseñas.
https://www.bleepingcomputer.com/news/security/new-bhunt-malware-targets-your-crypto-wallets-and-passwords/
- Hackers rusos utilizan el sistema de dirección de tráfico malicioso para distribuir malware.
https://thehackernews.com/2022/01/russian-hackers-heavily-using-malicious.html
- **CISA publica la versión final de la guía: Consideraciones sobre IPv6 para TIC 3.0.**
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/20/cisa-releases-final-version-guidance-ipv6-considerations-tic-30
- ATP chinos han sido descubiertos utilizando el nuevo firmware UEFI en ataques dirigidos.
https://thehackernews.com/2022/01/chinese-hackers-spotted-using-new-uefi.html
- 4 amenazas clave de ciberseguridad para las nuevas monedas digitales de los bancos centrales.
https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies/
- TrickBot refuerza las defensas por capas para evitar la detección por inyección.

https://securityintelligence.com/posts/trickbot-bolsters-layered-defenses-prevent-injection/

- El malware centrado en Linux aumenta un 35% en 2021.
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/
- El malware para Android BRATA borra tu dispositivo después de robar los datos.
https://www.bleepingcomputer.com/news/security/android-malware-brata-wipes-your-device-after-stealing-data/
- **ISO27001:2021 - Una nueva forma de trabajar.**
https://www.tripwire.com/state-of-security/controls/iso27001-2022-a-new-way-of-working/

## NOTAS DE INTERÉS

- CISA añade al catálogo 17 vulnerabilidades explotadas en ataques.
https://www.bleepingcomputer.com/news/security/cisa-adds-17-vulnerabilities-to-list-of-bugs-exploited-in-attacks/
- **Los ataques a la cadena de suministro de software se dispararon más del 300% en 2021.**
https://www.helpnetsecurity.com/2022/01/20/software-supply-chain-attacks-2021/
https://arstechnica.com/information-technology/2022/01/supply-chain-attack-used-legitimate-wordpress-add-ons-to-backdoor-sites/
- ProtonMail presenta un nuevo sistema de bloqueo de rastreadores de correo electrónico.
https://www.bleepingcomputer.com/news/security/protonmail-introduces-a-new-email-tracker-blocking-system/
- El FBI advierte a las organizaciones de los ataques de ransomware Diavol.
https://www.securityweek.com/fbi-warns-organizations-diavol-ransomware-attacks
- Error en McAfee Agent permite ejecutar código con privilegios de SISTEMA de Windows.
https://threatpost.com/mcafee-bug-windows-system-privileges/177857/
- El grupo Molerats esconde ataques de espionaje detrás de la infraestructura de la nube pública.
https://thehackernews.com/2022/01/molerats-hackers-hiding-new-espionage.html
- Encuentran similitudes estratégicas entre los ataques NotPetya y WhisperGate en Ucrania.
https://thehackernews.com/2022/01/experts-find-strategic-similarities-bw.html
- El exploit de Dark Souls 3 podría permitir a los hackers tomar el control de todo tu ordenador.
https://www.theverge.com/2022/1/22/22896785/dark-souls-3-remote-execution-exploit-rce-exploit-online-hack
- Error de programación de Rust de alta gravedad podría conducir a la eliminación de archivos y directorios.
https://thehackernews.com/2022/01/high-severity-rust-programming-bug.html
- Sofisticados atacantes utilizaron el backdoor DazzleSpy de macOS en ataques "watering hole".
https://securityaffairs.co/wordpress/127166/cyber-crime/dazzlespy-macos-backdoor.html

## ACTUALIZACIONES DE SEGURIDAD

- Oracle publica la actualización de parches críticos de enero de 2022.
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/18/oracle-releases-january-2022-critical-patch-update
- Microsoft: SolarWinds corrige el bug de Serv-U utilizado para ataques a Log4j.
https://thehackernews.com/2022/01/microsoft-hackers-exploiting-new.html
- Error crítico de Cisco StarOS que permite el acceso a la raíz a través del modo de depuración.
https://threatpost.com/critical-cisco-staros-bug-root-access-debug-mode/177832/
https://www.securityweek.com/cisco-patches-critical-vulnerability-rcm-staros
- **Se ha encontrado y corregido un grave error en el kernel de Linux.**
https://www.zdnet.com/article/nasty-linux-kernel-bug-found-and-fixed/