@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. 156 – 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 26/2/22 y el 3/3/22

- Nvidia, el gigantesco fabricante de chips de EE.UU., está investigando un posible ciberataque.
https://www.bleepingcomputer.com/news/security/nvidia-confirms-data-was-stolen-in-recent-cyberattack/
- El grupo de ransomware Conti anuncia su apoyo a Rusia y dice que cualquier "actividad bélica" contra Rusia hará que utilicen su capacidad de acceso para "devolver el golpe"
https://twitter.com/GossiTheDog/status/1497248121763635226
- Anonymous ha accedido a la red interna de los ferrocarriles bielorrusos y afirma haber bloqueado todos los servicios hasta que las tropas rusas abandonen el territorio de Bielorrusia.
https://securityaffairs.co/wordpress/128486/hacktivism/anonymous-breached-belarusian-railways.html
- Toyota suspende todas las operaciones de la fábrica de Japón tras un presunto ciberataque.
https://www.bleepingcomputer.com/news/security/toyota-halts-production-after-reported-cyberattack-on-supplier/
- Ucrania es atacada por el novedoso troyano "FoxBlade" horas antes de ser invadida.
https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/
- Nvidia afirma que su "información propietaria" está siendo filtrada por hackers.
https://www.theverge.com/2022/3/1/22957212/nvidia-confirms-hack-proprietary-information-lapsus

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

- Se detecta un nuevo gusano (HermeticWizard) y un malware de limpieza (IsaacWiper) de datos que afecta a las redes ucranianas.
https://securityaffairs.co/wordpress/128553/malware/isaacwiper-data-wiper.html
- Podcast diario de seguridad de redes de SANS (Stormcast) del lunes 28 de febrero de 2022.
https://isc.sans.edu/podcastdetail.html?id=7898
- Se filtran los chats internos del ransomware Conti tras aliarse con Rusia.
https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/
- Ciberespías chinos atacan a gobiernos con su puerta trasera "más avanzada": Daxin.
https://thehackernews.com/2022/03/china-linked-daxin-malware-targeted.html
- Axis Communications, de Suecia, comparte detalles sobre un ciberataque disruptivo recibido.
https://www.bleepingcomputer.com/news/security/axis-communications-shares-details-on-disruptive-cyberattack/
- La NSA detalla las mejores prácticas de infraestructura de red.
https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2949885/nsa-details-network-infrastructure-best-practices/
- Analistas han identificado una nueva y alarmante tendencia en los ataques DDoS que tienen como objetivo los dispositivos de inspección de paquetes y filtrado de contenidos.

https://arstechnica.com/information-technology/2022/03/unending-data-floods-and-complete-resource-exhaustion-ddoses-get-meaner/

- Un investigador ucraniano filtra el código fuente del ransomware Conti.
https://www.bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/
- Los exploits de Log4shell ahora se usan para las redes de bots DDoS y las criptomonedas.
https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
- Casi el 75% de las bombas de infusión en hospitales están afectadas por vulnerabilidades graves.
https://thehackernews.com/2022/03/report-nearly-75-of-infusion-pumps.html
- Desencriptor gratuito para las víctimas de HermeticRansom en Ucrania.
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-hermeticransom-victims-in-ukraine/

## NOTAS DE INTERÉS

- CISA: Malware destructivo centrado en organizaciones de Ucrania.
https://www.cisa.gov/uscert/ncas/current-activity/2022/02/26/cisa-releases-advisory-destructive-malware-targeting-organizations
- La red de malware TrickBot se detiene y sus desarrolladores se pasan a un malware más furtivo.
https://thehackernews.com/2022/03/trickbot-malware-gang-upgrades-its.html
- El malware Electron Bot está haciendo estragos en la Microsoft Store, abriendo puertas traseras en las computadoras de las víctimas.
https://betanews.com/2022/02/25/electron-bot-malware-is-running-rampant-in-the-microsoft-store-opening-backdoors-on-victims-computers/
- Expertos crean un clon de AirTag de Apple que puede eludir las medidas anti-seguimiento.
https://thehackernews.com/2022/02/experts-create-apple-airtag-clone-that.html
- Las contraseñas y los códigos 2FA de Instagram están en riesgo frente a estafadores.
https://nakedsecurity.sophos.com/2022/02/28/instagram-scammers-as-busy-as-ever-passwords-and-2fa-codes-at-risk/
- E-mails malintencionados advierten a los usuarios de Microsoft de una "actividad de inicio de sesión inusual" procedente de Rusia, buscan sacar provecho de la crisis ucraniana.
https://threatpost.com/microsoft-accounts-targeted-russian-credential-harvesting/178698/
- Ucrania pide a Musk terminales Starlink mientras la invasión rusa interrumpe la banda ancha.
https://arstechnica.com/tech-policy/2022/02/ukraine-asks-musk-for-starlink-terminals-as-russian-invasion-disrupts-broadband/
- La ICANN rechaza la petición de Ucrania de bloquear a Rusia de Internet.
https://www.zdnet.com/article/icann-rejects-ukraines-request-to-block-russia-from-the-internet/
- El grupo APT Conti celebró al filtrar los datos de las víctimas. Ahora han cambiado las cosas.
https://arstechnica.com/information-technology/2022/03/conti-cybergang-gloated-when-leaking-victims-data-now-the-tables-are-turned/
- Ciberataque al organismo de control ético de Nueva York.
https://www.infosecurity-magazine.com/news/cyber-attack-on-new-york-ethics/

## ACTUALIZACIONES DE SEGURIDAD

- Se publicaron parches críticos para los productos Cisco Expressway Series y TelePresence VCS.
https://thehackernews.com/2022/03/critical-patches-issued-for-cisco.html