@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. 177 – 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 22/07/22 y el 31/07/22

- Emisoras de radio ucranianas son hackeadas para difundir noticias falsas sobre la salud de Zelensky.
  https://thehackernews.com/2022/07/ukrainian-radio-stations-hacked-to.html
- Un hacker vende los datos de cuentas Twitter de 5,4 millones de usuarios por 30.000 dólares.
  https://securityaffairs.co/wordpress/133593/data-breach/twitter-leaked-data.html
- La APTRoaming Mantis tiene como objetivo a los usuarios de Android y iPhone en Francia.
  https://thehackernews.com/2022/07/roaming-mantis-financial-hackers.html
- **Un grupo de ransomware tuvo como objetivo la agencia tributaria italiana.**
  https://www.cyberscoop.com/lockbit-italy-tax-agency-ransomware/
- El portal de seguros indio, Policybazaar, sufre una brecha.
  https://www.infosecurity-magazine.com/news/indian-insurance-policybazaar/
- **España detiene a posibles ciberdelincuentes que sabotearon el sistema de alerta de radiación.**
  https://www.bleepingcomputer.com/news/security/spain-arrests-suspected-hackers-who-sabotaged-radiation-alert-system/
- Un proveedor de servicios de gestión estadounidense, NetStandard, sufrió un ciberataque.
  https://www.bleepingcomputer.com/news/security/kansas-msp-shuts-down-cloud-services-to-fend-off-cyberattack/
- Un ciberataque al sistema judicial de EE.UU. puso en peligro un sistema de gestión de documentos públicos.
  https://www.infosecurity-magazine.com/news/congress-us-court-records-breach/

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

- Estas son las principales amenazas a la seguridad telefónica en 2022 y cómo evitarlas.
  https://www.zdnet.com/article/here-are-the-top-phone-security-threats-in-2022-and-how-to-avoid-them/
- Hackers norcoreanos atacan objetivos de la UE con el malware Konni RAT.
  https://www.bleepingcomputer.com/news/security/north-korean-hackers-attack-eu-targets-with-konni-rat-malware/
- Expertos descubren un nuevo rootkit de firmware UEFI "CosmicStrand" usado por hackers chinos.
  https://thehackernews.com/2022/07/experts-uncover-new-cosmicstrand-uefi.html
- El reciente Lightning Framework ofrece una amplia gama de funciones de pirateo de Linux.
  https://arstechnica.com/information-technology/2022/07/newly-found-lightning-framework-offers-a-plethora-of-linux-hacking-capabilities/
- Cómo RaaS redefine nuestra comprensión de los incidentes de ransomware.
  https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

- Cómo Tor lucha y vence a la censura rusa.
https://arstechnica.com/information-technology/2022/07/how-tor-is-fighting-and-beating-russian-censorship/

NOTAS DE INTERÉS

- Rusia e Irán debaten sobre la fabricación de tecnología, infoseguridad y la colaboración en materia de gobernanza electrónica.
https://www.theregister.com/2022/07/22/iran_russia_tech_collaboration/
- El grupo TA4563 usa el malware EvilNum para atacar a entidades financieras y de inversión europeas.
https://securityaffairs.co/wordpress/133535/apt/ta4563-group-evilnum-malware.html
- **Una vulnerabilidad 0-Day de Google Chrome ha sido explotada para desplegar software espía.**
https://gbhackers.com/google-chrome-0-day/
- Ahora Microsoft Office bloquea las macros por defecto.
https://www.theverge.com/2022/7/22/23274905/microsoft-office-block-macros-security-malware-default-warning
- Vulnerabilidades críticas de Filewave MDM permiten el control total de los dispositivos móviles.
https://www.darkreading.com/vulnerabilities-threats/critical-filewave-mdm-vulnerabilities-attackers-mobile-device-control
- SmokeLoader infecta los sistemas objetivo con el malware de robo de información Amadey.
https://thehackernews.com/2022/07/smokeloader-infecting-targeted-systems.html
- El malware Luca Stealer se extiende rápidamente después de que el código apareció en GitHub.
https://www.theregister.com/2022/07/26/luca-stealer-rust-cyble/
- **Las extensiones maliciosas de IIS ganan popularidad entre los ciberdelincuentes.**
https://thehackernews.com/2022/07/malicious-iis-extensions-gaining.html
- **El tráfico de la red de Apple se desvía misteriosamente a su paso por Rusia.**
https://www.theregister.com/2022/07/27/apple_networking_traffic_russia_bgp/
https://www.manrs.org/2022/07/for-12-hours-was-part-of-apple-engineerings-network-hijacked-by-russias-rostelecom/
- Estados Unidos amplía su asociación en materia de ciberseguridad con Ucrania.
https://www.infosecurity-magazine.com/news/us-cybersecurity-partnership/
- **CISA añade una nueva vulnerabilidad explotada activamente al catálogo.**
https://www.cisa.gov/uscert/ncas/current-activity/2022/07/29/cisa-adds-one-known-exploited-vulnerability-catalog
- Paquetes Npm maliciosos explotados de nuevo para atacar a los usuarios de Discord.
https://threatpost.com/malicious-npm-discord/180327/
- El auge de los satélites comerciales hace que el espacio sea vulnerable a los hackers
https://therecord.media/the-commercial-satellite-boom-is-leaving-space-vulnerable-to-hackers/

ACTUALIZACIONES DE SEGURIDAD

- Error crítico de Samba puede permitir que alguien se convirtiera en administrador de un dominio.
https://nakedsecurity.sophos.com/2022/07/27/critical-samba-bug-could-let-anyone-become-domain-admin-patch-now/
- LibreOffice publica una actualización de software para arreglar 3 nuevas vulnerabilidades.
https://thehackernews.com/2022/07/libreoffice-releases-software-security.html
- **Importantes actualizaciones de IBM**
https://www.ibm.com/support/pages/node/6607135