@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. 168 – 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 20/5/22 y el 26/5/22

- **El banco ruso Sberbank informa que se enfrenta a oleadas masivas de ataques DDoS.**
  https://www.bleepingcomputer.com/news/security/russian-sberbank-says-it-s-facing-massive-waves-of-ddos-attacks/
- Hackers prorrusos atacan sitios web gubernamentales críticos en Italia.
  https://www.infosecurity-magazine.com/news/pro-russian-hackers-italy/
- El ataque de "credential stuffing" a General Motors en EE.UU., expone datos personales de los propietarios de vehículos.
  https://www.infosecurity-magazine.com/news/general-motors-hit-by-cyber-attack/
- Pasajeros de la aerolínea india SpiceJet, quedan varados tras un ataque de ransomware.
  https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/

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

- Los 5 mejores navegadores para la privacidad: Navegación segura por la web.
  https://www.zdnet.com/article/best-browser-for-privacy/
- Un PDF que propaga el malware Snake Keylogger utiliza un astuto nombre de archivo engañoso.
  https://www.zdnet.com/article/this-malware-spreading-pdf-uses-a-sneaky-file-name-to-trick-the-unwary/
- El nuevo grupo RansomHouse crea un mercado de extorsión y suma sus primeras víctimas.
  https://www.bleepingcomputer.com/news/security/new-ransomhouse-group-sets-up-extortion-market-adds-first-victims/
- Se descubre una nueva variante del ransomware Chaos "Yashma".
  https://thehackernews.com/2022/05/new-chaos-ransomware-builder-variant.html
- **CISA añade 41 vulnerabilidades a la lista de *bugs* utilizados en ciberataques.**
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Cómo manipular los sistemas de aprendizaje automático mediante el orden de los datos de entrenamiento.
  https://www.schneier.com/blog/archives/2022/05/manipulating-machine-learning-systems-through-the-order-of-the-training-data.html
- El nuevo ransomware Linux "Cheers" se concentra en los servidores VMware ESXi.
  https://www.bleepingcomputer.com/news/security/new-cheers-linux-ransomware-targets-vmware-esxi-servers/

NOTAS DE INTERÉS

- El ransomware de Conti cierra la operación y se reagrupa en unidades más pequeñas.
  https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/
- La India reafirma su compromiso con las nuevas normas de ciberseguridad.

https://www.zdnet.com/article/india-reaffirms-commitment-to-new-cybersecurity-rules/

- Los hackers aprovechan VMware Horizon para atacar a Corea del Sur con el backdoor NukeSped.
https://thehackernews.com/2022/05/hackers-exploiting-vmware-horizon-to.html
- El spyware Predator de Cytrox se enfoca en los usuarios de Android con exploits de día cero.
https://thehackernews.com/2022/05/cytroxs-predator-spyware-target-android.html
- **Alrededor de 380 mil servidores de API de Kubernetes, están expuestos a la Internet pública.**
https://threatpost.com/380k-kubernetes-api-servers-exposed-to-public-internet/179679/
- **Microsoft advierte del aumento del malware XorDdos centrado en los dispositivos Linux.**
https://thehackernews.com/2022/05/microsoft-warns-rise-in-xorddos-malware.html
- Dominios falsos ofrecen instaladores de Windows 11, pero en su lugar entregan malware.
https://www.zdnet.com/article/fake-domains-offer-windows-11-installers-but-deliver-malware-instead/
- Hackers chinos "Twisted Panda" son sorprendidos espiando institutos de defensa rusos.
https://thehackernews.com/2022/05/chinese-twisted-panda-hackers-caught.html
- **Un paquete malicioso del repositorio de Python, PyPI, introduce Cobalt Strike en sistemas Windows, macOS y Linux.**
https://www.darkreading.com/application-security/malicious-package-python-repository-cobalt-strike-windows-macos-linux
- El sistema Lumos puede encontrar cámaras ocultas y dispositivos IoT en su habitación de Airbnb u hotel.
https://thehackernews.com/2022/05/lumos-system-can-find-hidden-cameras.html
- **El jefe del comando de inteligencia artificial del Departamento de Defensa de EE.UU. advierte que el Pentágono debe mejorar para vencer a China en materia de IA.**
https://www.cyberscoop.com/head-of-dod-artificial-intelligence-pentagon-must-improve/
- La adquisición por parte de China del mayor productor de microchips del Reino Unido se enfrenta a la revisión de la seguridad nacional.
https://news.sky.com/story/chinese-takeover-of-uks-largest-microchip-producer-faces-national-security-review-12621350
- Advierten del aumento del malware ChromeLoader que se apodera de los navegadores de los usuarios.
https://thehackernews.com/2022/05/experts-warn-of-rise-in-chromeloader.html

ACTUALIZACIONES DE SEGURIDAD

- Cisco recomienda a los administradores que parcheen el día cero de IOS XR utilizado en ataques.
https://www.bleepingcomputer.com/news/security/cisco-urges-admins-to-patch-ios-xr-zero-day-exploited-in-attacks/
- **Nueva versión: Tor Browser 11.0.13.**
https://blog.torproject.org/new-release-tor-browser-11013/
- Mozilla corrige los días cero de Firefox y Thunderbird vulnerados por Pwn2Own.
https://www.bleepingcomputer.com/news/security/mozilla-fixes-firefox-thunderbird-zero-days-exploited-at-pwn2own/
- Actualizar Zoom, pues un bug podría permitir el hackeo de usuarios con sólo un mensaje.
https://thehackernews.com/2022/05/new-zoom-flaws-could-let-attackers-hack.html
- Google Chrome 102 llega con 32 correcciones de seguridad, una de ellas crítica.
https://www.zdnet.com/article/time-to-update-google-chrome-102-arrives-with-32-security-fixes-one-critical/