@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. 162 – 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 8/4/22 y el 17/4/22

- Sitios de la empresa TrustFord de Irlanda del Norte afectados por una banda de ransomware.
  https://www.infosecurity-magazine.com/news/northern-ireland-trustford/
- Ataque DDoS interrumpe los sitios del gobierno finlandés durante el discurso de Zelensky.
  https://www.cyberscoop.com/finland-denial-of-service-zelenskyy/
- Funcionarios de la Unión Europea fueron atacados con el programa espía Pegasus.
  https://www.infosecurity-magazine.com/news/eu-officials-pegasus-spyware/

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

- Raspberry Pi acaba de hacer un gran cambio para aumentar la seguridad.
  https://zdnet.com/article/raspberry-pi-just-made-a-big-change-to-boost-security/
- AWS Lambda sufre su primer ataque de malware, Denonia, y no se sabe cómo llegó.
  https://www.techrepublic.com/article/aws-lambda-sees-first-malware-attack-denonia-we-dont-know-how-got-there/
- Grupos de hackers chinos siguen atacando los activos de la red eléctrica india.
  https://thehackernews.com/2022/04/chinese-hacker-groups-continue-to.html
- Hackers utilizan el ransomware filtrado por Conti para atacar a empresas rusas.
  https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/
- CISA advierte a las organizaciones de EE.UU. acerca del bug de WatchGuard aprovechado por los hackers estatales rusos.
  https://www.bleepingcomputer.com/news/security/cisa-warns-orgs-of-watchguard-bug-exploited-by-russian-state-hackers/
- Un nuevo malware utiliza un error de Windows para ocultar las tareas programadas.
  https://www.bleepingcomputer.com/news/security/microsoft-new-malware-uses-windows-bug-to-hide-scheduled-tasks/
- **EE.UU. advierte de que grupos APT tienen como objetivo los sistemas ICS/SCADA con malware especializado.**
  https://thehackernews.com/2022/04/us-warns-of-apt-hackers-targeting.html
- **Nuevas redes de bots EnemyBot DDoS que capta routers e IoTs en su ejército y Fodcha, que ataca más de 10 víctimas por día.**
  https://www.bleepingcomputer.com/news/security/new-enemybot-ddos-botnet-recruits-routers-and-iots-into-its-army/
  https://www.bleepingcomputer.com/news/security/new-fodcha-ddos-botnet-targets-over-100-victims-every-day/
- La banda de ransomware OldGremlin apunta a Rusia con un nuevo malware.

https://www.bleepingcomputer.com/news/security/oldgremlin-ransomware-gang-targets-russia-with-new-malware/

- La semana en el ransomware - 15 de abril de 2022 - La encriptación de Rusia.
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-15th-2022-encrypting-russia/

NOTAS DE INTERÉS

- El nuevo troyano bancario Octo se propaga a través de aplicaciones falsas en Google Play Store.
https://thehackernews.com/2022/04/new-octo-banking-trojan-spreading-via.html
- Microsoft: Casi todos los grupos estatales rusos se centran ahora en Ucrania.
https://www.infosecurity-magazine.com/news/russian-state-targeting-ukraine/
- Google borró 6 aplicaciones falsas para Android que afectan a usuarios del Reino Unido e Italia.
https://threatpost.com/google-play-bitten-sharkbot/179252/
- La prevista función de seguridad Smart App Control de Windows 11 tiene un problema importante.
https://betanews.com/2022/04/08/windows-11s-upcoming-smart-app-control-security-feature-has-a-major-issue/
- Las huellas digitales podrían ayudar a los hackers a infiltrarse en las redes informáticas.
https://thenextweb.com/news/your-digital-footprints-could-help-hackers-infiltrate-computer-networks
- **OpenSSH ahora protege por defecto contra los ataques de los ordenadores cuánticos.**
https://www.zdnet.com/article/openssh-now-defaults-to-protecting-against-quantum-computer-attacks/
- El bug de Spring4Shell está siendo utilizado para propagar el malware botnet Mirai.
https://www.zdnet.com/article/spring4shell-flaw-is-now-being-used-to-spread-this-botnet-malware/
- Más de 16.500 sitios hackeados para distribuir malware mediante el servicio de redirección web.
https://thehackernews.com/2022/04/over-16500-sites-hacked-to-distribute.html
- Los responsables del proyecto NGINX corrigen fallos en la implementación de referencia de LDAP.
https://securityaffairs.co/wordpress/130117/hacking/nginx-ldap-reference-implementation-bug.html
- Microsoft ha anunciado que Windows Autopatch, un servicio diseñado para mantener actualizado automáticamente el software de Windows y Office, se activará en julio de 2022.
https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-autopatch-steals-the-fun-from-patch-tuesdays/
- **Se cierra el foro de hacking RaidForums y detienen a su fundador en una operación policial.**
https://thehackernews.com/2022/04/fbi-europol-seize-raidforums-hacker.html
- Grupos atacantes están explotando el RCE de VMware para distribuir malware.
https://www.helpnetsecurity.com/2022/04/14/cve-2022-22954/
- APT Lazarus de Corea del Norte orienta sus ataques al sector químico.
https://www.securityweek.com/north-korea-apt-lazarus-targeting-chemical-sector

ACTUALIZACIONES DE SEGURIDAD

- Microsoft ha publicado parches para 128 vulnerabilidades de seguridad para su abril de 2022.
https://threatpost.com/microsoft-zero-days-wormable-bugs/179273/
- Google publica actualizaciones de seguridad para Chrome.
https://www.cisa.gov/uscert/ncas/current-activity/2022/04/15/google-releases-security-updates-chrome
- Cisco ha publicado parches para contener una vulnerabilidad de seguridad crítica en WLC.
https://thehackernews.com/2022/04/critical-auth-bypass-bug-reported-in.html