@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. 195 – 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 2/12/22 y el 11/12/22

- Rackspace, empresa de servicios en la nube, indica incidente de seguridad que ha provocado una interrupción y que afecta entornos de MS Exchange y a miles de clientes.
https://www.bleepingcomputer.com/news/technology/rackspace-ongoing-exchange-outage-caused-by-security-incident/
- Un ataque DDoS masivo deja fuera de servicio al segundo banco ruso, el VTB
https://www.infosecurity-magazine.com/news/russias-vtb-bank-suffers-biggest/

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

- **Indicadores de compromiso (IOC): cómo los recopilarlos y utilizarlos.**
https://securelist.com/how-to-collect-and-use-indicators-of-compromise/108184/
- El destructor de datos CryWiper ataca tribunales y alcaldías rusas.
https://www.bleepingcomputer.com/news/security/new-crywiper-data-wiper-targets-russian-courts-mayor-s-offices/
- Divulgan un fallo en la cadena de suministro que afecta a las bases de datos en la nube de IBM para PostgreSQL.
https://thehackernews.com/2022/12/researchers-disclose-supply-chain-flaw.html
- **Ataque de drones: pesadilla de ciberseguridad aérea.**
https://securityaffairs.co/wordpress/139196/hacking/drones-abuse.html
- **Se prepara una ciber ofensiva rusa contra Ucrania en el invierno europeo.**
https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/
- Resecurity ha identificado un nuevo mercado clandestino en la Dark Web orientado a desarrolladores de malware para móviles y operadores.
https://securityaffairs.co/wordpress/139310/cyber-crime/dark-web-mobile-malware-marketplace.html
https://resecurity.com/blog/article/in-the-box-mobile-malware-webinjects-marketplace
- ¡Ping de la muerte! FreeBSD corrige un fallo en la herramienta de red.
https://nakedsecurity.sophos.com/2022/12/05/ping-of-death-freebsd-fixes-crashtastic-bug-in-network-tool/
- Se detectan piratas informáticos rusos atacando proveedor de armas y material militar de EE.UU.
https://thehackernews.com/2022/12/russian-hackers-spotted-targeting-us.html
- La semana en ransomware - 9 de diciembre de 2022.
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-9th-2022-wide-impact/

NOTAS DE INTERÉS

- Los autores del ransomware de Cuba se embolsan 60 millones de dólares.
https://www.infosecurity-magazine.com/news/cuba-ransomware-actors-pocket-60m/

- **La OTAN inicia un ejercicio masivo de ciberdefensa.**
https://www.infosecurity-magazine.com/news/nato-launches-massive-cyberdefense/
- Aplicaciones de teclado para Android, con 2 Millones de descargas, pueden hackear remotamente su dispositivo.
https://securityaffairs.co/wordpress/139174/hacking/android-keyboard-apps-flaws.html
- Utilizan archivos comprimidos y contrabando de HTML para eludir las herramientas de detección.
https://www.infosecurity-magazine.com/news/archives-and-html-smuggling-to/
- Nuevo bug de Linux puede encadenarse con otros dos para obtener privilegios completos de root.
https://securityaffairs.co/wordpress/139209/hacking/three-linux-bugs-full-root-privileges.html
- **Los mercados de la Darknet generan ingresos millonarios con la venta de datos personales robados.**
https://arstechnica.com/tech-policy/2022/12/darknet-markets-generate-millions-in-revenue-selling-stolen-personal-data/
- Lazarus APT utiliza falsas aplicaciones de criptomoneda para propagar el malware AppleJeus.
https://securityaffairs.co/wordpress/139290/apt/lazarus-apt-bloxholder-campaign.html
- La vulnerabilidad de SiriusXM permite a los hackers desbloquear y arrancar a distancia los coches conectados.
https://thehackernews.com/2022/12/siriusxm-vulnerability-lets-hackers.html
- Los graves fallos de AMI MegaRAC afectan a servidores de AMD, ARM, HPE, Dell y otros.
https://thehackernews.com/2022/12/new-bmc-supply-chain-vulnerabilities.html
- Ciberataques chinos contra las telecomunicaciones de Oriente Próximo
https://thehackernews.com/2022/12/chinese-hackers-target-middle-east.html
- El nuevo malware Zerobot tiene 21 exploits para dispositivos BIG-IP, Zyxel y D-Link.
https://www.bleepingcomputer.com/news/security/new-zerobot-malware-has-21-exploits-for-big-ip-zyxel-d-link-devices/
- Apple añade la encriptación de extremo a extremo a las copias de seguridad de iCloud.
https://www.theverge.com/2022/12/7/23498580/apple-end-to-end-encryption-icloud-backups-advanced-data-protection
- Los atacantes siguen atentando contra la red eléctrica de EE.UU.
https://www.wired.com/story/attacks-us-electrical-grid-security-roundup/

ACTUALIZACIONES DE SEGURIDAD

- La actualización de emergencia de Google Chrome corrige el noveno día cero del año.
https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-9th-zero-day-of-the-year/
- Boletín de seguridad de Android: diciembre de 2022. Se solucionan 81 vulnerabilidades.
https://source.android.com/docs/security/bulletin/2022-12-01
- Kali Linux 2022.4 añade 6 nuevas herramientas, imágenes Azure y actualizaciones de escritorio.
https://www.helpnetsecurity.com/2022/12/06/kali-linux-2022-4-released/
- Sophos soluciona un fallo crítico en su Firewall versión 19.5
https://securityaffairs.co/wordpress/139362/security/sophos-firewall-critical-flaw.html
- Cisco informa un fallo de alta gravedad que afecta a los teléfonos IP de las series 7800 y 8800.
https://thehackernews.com/2022/12/cisco-warns-of-high-severity-unpatched.html