@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. 160 – 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 25/3/22 y el 31/3/22

- **Anonymous filtró 28 GB de datos robados del Banco Central de Rusia.**
  https://securityaffairs.co/wordpress/129490/hacking/central-bank-of-russia-data-leak-anonymous.html
- Guerra en Ucrania: Un importante proveedor de Internet, Ukrtelecom, sufre un ciberataque. El "ciberataque masivo" contra el ISP ha sido neutralizado, según el Gobierno.
  https://www.bbc.com/news/60854881
  https://www.zdnet.com/article/massive-cyberattack-against-ukrainian-isp-has-been-neutralized-ukraine-says/
- LAPSUS$ afirma haber accedido a la empresa de TI Globant; filtra 70 GB de datos.
  https://thehackernews.com/2022/03/lapsus-claims-to-have-breached-it-firm.html
  https://www.zdnet.com/article/globant-admits-to-data-breach-after-lapsus-releases-source-code/

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

- La semana del ransomware al 25 de marzo de 2022 - Infraestructuras críticas.
  https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-25th-2022-critical-infrastructure/
- **Tácticas, técnicas y procedimientos de los ciberactores rusos patrocinados por el Estado acusados de atacar el sector energético.**
  https://www.cisa.gov/uscert/ncas/alerts/aa22-083a
- Un fallo de Honda y un ataque de replay, permite a un hacker desbloquear y arrancar su coche.
  https://www.bleepingcomputer.com/news/security/honda-bug-lets-a-hacker-unlock-and-start-your-car-via-replay-attack/#.Yj2EHrzKtFs.twitter
- Definición y ejemplos de ataques Man-in-the-middle (MitM).
  https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html#tk.rss_all
- Una vulnerabilidad crítica de Sophos Firewall permite la ejecución remota de código.
  https://www.bleepingcomputer.com/news/security/critical-sophos-firewall-vulnerability-allows-remote-code-execution/
- Los hackers "Purple Fox" han sido detectados usando una nueva variante de FatalRAT en recientes ataques de malware.
  https://thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html
- **Un nuevo informe sobre el hackeo a Okta, revela el episodio completo del ataque de LAPSUS$.**
  https://thehackernews.com/2022/03/new-report-on-okta-hack-reveals-entire.html
- El malware Mars Stealer se difunde a través de anuncios de OpenOffice en Google.
  https://www.bleepingcomputer.com/news/security/mars-stealer-malware-pushed-via-openoffice-ads-on-google/
  https://thehackernews.com/2022/03/researchers-expose-mars-stealer-malware.html
- Nuevo ransomware cuyo objetivo es la herramienta de visualización de datos Jupyter Notebook.
  https://www.zdnet.com/article/this-new-ransomware-targets-data-visualization-tool-jupyter-notebook/

NOTAS DE INTERÉS

- *Ciberpiratas* norcoreanos usan un *exploit* de día 0 de Chrome en cientos de objetivos de EE.UU.
  https://arstechnica.com/information-technology/2022/03/north-korean-hackers-unleashed-chrome-0-day-exploit-on-hundreds-of-us-targets/
  https://threatpost.com/google-chrome-zero-day-bugs-exploited-weeks-ahead-of-patch/179103/
- El Dpto. de Justicia de EE.UU. acusa a empleados del gobierno ruso de atacar al sector energético.
  https://threatpost.com/doj-indicts-russian-govt-employees-over-targeting-power-sector/179108/
- Los militares rusos habrían hackeado satélites europeos al inicio de la guerra de Ucrania.
  https://www.theverge.com/2022/3/25/22996187/russian-military-hack-viasat-internet-satellite-ukraine
- El ransomware Hive adapta su encriptador VMware ESXi de Linux a Rust.
  https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
- La red de bots Muhstik tiene como objetivo los servidores Redis utilizando una vulnerabilidad recientemente descubierta.
  https://thehackernews.com/2022/03/muhstik-botnet-targeting-redis-servers.html
- Rusia se enfrenta a cortes de Internet debido a la escasez de equipos.
  https://www.bleepingcomputer.com/news/technology/russia-facing-internet-outages-due-to-equipment-shortage/
- Microsoft agrega una opción de seguridad a Windows Defender en Windows 10 y 11.
  https://www.zdnet.com/article/microsoft-is-adding-a-new-driver-blocklist-feature-to-windows-defender-on-windows-10-and-11/
- Ataque a gran escala a la cadena de suministro distribuyó más de 800 paquetes NPM maliciosos.
  https://thehackernews.com/2022/03/a-threat-actor-dubbed-red-lili-has-been.html
- Nueva campaña de piratería del grupo Transparent Tribe dirigida a funcionarios indios.
  https://thehackernews.com/2022/03/new-hacking-campaign-by-transparent.html
- CISA advierte de los continuos ciberataques dirigidos a los dispositivos UPS conectados a Internet.
  https://thehackernews.com/2022/03/cisa-warns-of-ongoing-cyber-attacks.html
  https://threatpost.com/cyberattackers-ups-backup-power-critical-environments/179169/
- **Un bug 0-Day de RCE en Java Spring Framework, sin parches, amenaza la seguridad de las aplicaciones web empresariales.**
  https://thehackernews.com/2022/03/unpatched-java-spring-framework-0-day.html
  https://nakedsecurity.sophos.com/2022/03/30/vmware-spring-cloud-java-bug-gives-instant-remote-code-execution-update-now/

ACTUALIZACIONES DE SEGURIDAD

- Microsoft y Google divulgan parches de emergencia por vulnerabilidades en Edge y Chrome..
  https://betanews.com/2022/03/27/microsoft-and-google-release-emergency-patches-for-security-vulnerabilities-in-edge-and-chrome/
- Western Digital corrige un error crítico que da lugar a un root en los dispositivos NAS My Cloud.
  https://www.bleepingcomputer.com/news/security/western-digital-fixes-critical-bug-giving-root-on-my-cloud-nas-devices/
- Sophos parchea una vulnerabilidad crítica de ejecución remota de código en el Firewall.
  https://www.zdnet.com/article/sophos-patches-critical-remote-code-execution-vulnerability-in-firewall-defense-product/
- **Se publica Google Chrome 100 con nuevas características.**
  https://www.bleepingcomputer.com/news/google/google-chrome-100-released-with-new-features-icon-and-more/