@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. 157 – 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 4/2/22 y el 10/3/22

- El grupo Lapsus$ ha difundido hoy una enorme recopilación de datos confidenciales que, según ellos, son de Samsung Electronics. Samsung confirma el robo de código fuente.
  https://threatpost.com/samsung-lapsus-ransomware-source-code/178791/
  https://thehackernews.com/2022/03/samsung-confirms-data-breach-after.html
- Coinbase bloqueó 25.000 direcciones de *blockchain* vinculadas a personas y entidades rusas.
  https://securityaffairs.co/wordpress/128775/digital-id/coinbase-blocked-25000-russian-addresses.html
- La red de estaciones de servicio rumanas de Rompetrol se ve afectada por el ransomware Hive.
  https://www.bleepingcomputer.com/news/security/rompetrol-gas-station-network-hit-by-hive-ransomware/
  https://exchange.xforce.ibmcloud.com/collection/542f9d9289b7d9e53dd4a9fb3f184ee0
- El servicio digital PressReader regresa parcialmente tras el ciberataque que afectó a más de 7.000 publicaciones.
  https://www.zdnet.com/article/pressreader-service-partially-returns-after-cyberattack-causes-outage/
- Ciberdelincuentes acceden a 300 mil cuentas de Mercado Libre y Mercado Pago: dicen tener más datos de la compañía.
  https://www.bleepingcomputer.com/news/security/e-commerce-giant-mercado-libre-confirms-source-code-data-breach/
- CISA actualiza la alerta del ransomware Conti con casi 100 nombres de dominio.
  https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/

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

- CISA añade otros 95 errores a su lista de vulnerabilidades conocidas.
  https://www.bleepingcomputer.com/news/security/cisa-warns-organizations-to-patch-95-actively-exploited-bugs/
  https://www.zdnet.com/article/get-patching-now-cisa-adds-another-95-flaws-to-its-known-exploited-vulnerabilities-list/
- Rusia actualiza la lista de IPs y dominios que atacan su infraestructura con ataques DDoS.
  https://thehackernews.com/2022/03/russia-releases-list-of-ips-domains.html
- Vulnerabilidad en el Kernel de Linux: "cgroups". Linux ha sido afectado por su vulnerabilidad de mayor gravedad en años, Dirty Pipe.
  https://thehackernews.com/2022/03/new-linux-kernel-cgroups-vulnerability.html
  https://arstechnica.com/information-technology/2022/03/linux-has-been-bitten-by-its-most-high-severity-vulnerability-in-years/
- Rusia-Ucrania: La amenaza de que las operaciones cibernéticas regionales se conviertan en una ciberguerra mundial.
  https://www.securityweek.com/russia-ukraine-threat-local-cyber-operations-escalating-global-cyberwar
- Ahora los ataques DDoS utilizan un nuevo vector de amplificación.

https://www.zdnet.com/article/in-the-wild-ddos-attack-can-be-launched-from-a-single-packet-to-create-terabytes-of-traffic/

- Los hackers chinos del APT41 entraron en al menos 6 gobiernos estatales de Estados Unidos
https://thehackernews.com/2022/03/chinese-apt41-hackers-broke-into-at.html
- Agentes de phishing chinos (grupo TA416) se centran sistemáticamente en diplomáticos de la UE.
https://www.bleepingcomputer.com/news/security/chinese-phishing-actors-consistently-targeting-eu-diplomats/

NOTAS DE INTERÉS

- Microsoft suspenderá todas sus ventas y servicios en Rusia.
https://news.sky.com/story/microsoft-to-suspend-all-sales-and-services-in-russia-12557408
- La ONU estudia la propuesta de Rusia para un tratado sobre ciberdelincuencia.
https://www.theregister.com/2022/03/07/russia-un-cybercrime-treaty/
- Según Google, para detener el phishing y el malware estamos cambiando nuestras notificaciones de comentarios.
https://www.zdnet.com/article/google-to-stop-phishing-and-malware-were-changing-our-comment-notifications/
- El gobierno de Biden busca dinero para reforzar la ciberseguridad relacionada con la guerra de Ucrania en el país y en el extranjero.
https://www.cyberscoop.com/biden-ukraine-cybersecurity-supplemental-fiscal-2022-assistance/
- Una aplicación de Google Play con más de 10.000 descargas contenía un RAT que robaba datos.
https://arstechnica.com/information-technology/2022/03/google-play-app-drops-data-stealing-teabot-rat-on-10000-android-phones/
- Tres proveedores ofrecen servicios gratuitos a las organizaciones en riesgo de ciberataques rusos.
https://www.darkreading.com/cloud/trio-of-vendors-offer-free-services-to-organizations-at-risk-of-russian-cyberattacks
- Informe de Google: grupos estatales de Rusia, China y Bielorrusia han atacado Ucrania y Europa.
https://www.bleepingcomputer.com/news/security/google-russia-china-belarus-state-hackers-target-ukraine-europe/
- Los errores críticos de Firefox de día cero permiten el RCE.
https://threatpost.com/firefox-zero-day-bugs-rce-sandbox-escape/178779/
- El grupo ransomware Ragnar Locker ha accedido a las redes de al menos 52 organizaciones de múltiples sectores de infraestructuras críticas de Estados Unidos.
https://securityaffairs.co/wordpress/128796/cyber-crime/fbi-ragnar-locker-ransomware.html
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/fbi-releases-indicators-compromise-ragnarlocker-ransomware
- Errores de "cero clic" en dispositivos UPS muy utilizados amenazan la infraestructura crítica.
https://threatpost.com/zero-click-flaws-ups-critical-infratructure/178810/
- Se descubrieron, en millones de dispositivos HP, 16 fallos de firmware UEFI de alta gravedad.
https://thehackernews.com/2022/03/new-16-high-severity-uefi-firmware.html

ACTUALIZACIONES DE SEGURIDAD

- Microsoft corrige 71 vulnerabilidades y parches de otras empresas de software.
https://thehackernews.com/2022/03/critical-security-patches-issued-by.html
https://www.zdnet.com/article/microsoft-march-2022-patch-tuesday-71-vulnerabilities-fixed/
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/08/sap-releases-march-2022-security-updates
https://isc.sans.edu/podcastdetail.html?id=7912