@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. 154 – 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 12/2/22 y el 20/2/22

- Los *San Francisco 49ers* de la NFL se ven afectados por el ataque del ransomware Blackbyte.
https://www.bleepingcomputer.com/news/security/nfls-san-francisco-49ers-hit-by-blackbyte-ransomware-attack/
- La marca deportiva Mizuno sufre un ataque de ransomware que retrasa los pedidos.
https://www.bleepingcomputer.com/news/security/sports-brand-mizuno-hit-with-ransomware-attack-delaying-orders/
- Los principales bancos de Canadá se desconectan varias horas durante un misterioso apagón.
https://www.bleepingcomputer.com/news/security/canadas-major-banks-go-offline-in-mysterious-hours-long-outage/
- Estados Unidos y Gran Bretaña acusan a Rusia de ciberataques dirigidos a Ucrania.
https://www.securityweek.com/white-house-accuses-russia-cyberattacks-targeting-ukraine

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

- Un error de seguridad RCE de alta gravedad en el software de base de datos Apache Cassandra.
https://jfrog.com/blog/cve-2021-44521-exploiting-apache-cassandra-user-defined-functions-for-remote-code-execution/
- La Cruz Roja relaciona el hackeo recibido con una vulnerabilidad de Zoho sin parchear.
https://www.zdnet.com/article/red-cross-traces-hack-back-to-zoho-vulnerability/
- Cómo el iPhone de una mujer saudí reveló el hackeo en todo el mundo.
https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/
- **Los hackers se infiltran en los chats de Microsoft Teams para distribuir malware.**
https://www.bleepingcomputer.com/news/security/hackers-slip-into-microsoft-teams-chats-to-distribute-malware/
- La red de bots basada en Golang ya está generando 3.000 dólares al mes para los operadores.
https://threatpost.com/golang-botnet-pulling-in-3k-month/178509/
- **La NSA publica una guía para la selección de tipos de contraseñas fuertes de Cisco.**
https://www.darkreading.com/vulnerabilities-threats/nsa-issues-guidance-for-selecting-strong-cisco-password-types

NOTAS DE INTERÉS

- La policía española desmantela una red de intercambio de tarjetas SIM que vaciaba cuentas bancarias.
https://arstechnica.com/information-technology/2022/02/police-in-spain-dismantle-a-sim-swapping-ring-that-drained-bank-accounts/
- Las computadoras pueden escribir su propio código, entonces, ¿los programadores son obsoletos?
https://www.theguardian.com/commentisfree/2022/feb/12/computers-can-write-their-own-code-so-are-programmers-now-obsolete

- FBI: El ransomware BlackByte vulneró las infraestructuras críticas de EE.UU.
https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/
- Ucrania afirma estar en el punto de mira de una "ola masiva de guerra híbrida".
https://www.bleepingcomputer.com/news/security/ukraine-says-it-s-targeted-by-massive-wave-of-hybrid-warfare-/
- **APT2541: grupo que lleva años atacando a la industria aeroespacial y de defensa.**
https://thehackernews.com/2022/02/experts-warn-of-hacking-group-targeting.html
https://threatpost.com/ta2541-apt-rats-aviation/178422/
- Los piratas informáticos "Moses" se centran en las organizaciones israelíes con fines de ciberespionaje.
https://thehackernews.com/2022/02/moses-staff-hackers-targeting-israeli.html
- EE.UU. afirma que piratas informáticos rusos roban datos sensibles de contratistas de defensa.
https://www.theverge.com/2022/2/16/22937554/russian-hackers-target-us-defense-contractors-nsa-cisa
https://thehackernews.com/2022/02/us-says-russian-hackers-stealing.html
- Las empresas del metaverso se enfrentaron el año pasado a un 60% más de ataques.
https://www.techrepublic.com/article/metaverse-companies-face-60-more-attacks-last-year-and-5-other-online-fraud-statistics/
- El escaneo de código de GitHub ahora encuentra más vulnerabilidades de seguridad.
https://www.bleepingcomputer.com/news/security/github-code-scanning-now-finds-more-security-vulnerabilities/
- Los servidores VMware Horizon son víctimas de una explotación activa por parte de hackers del Estado iraní.
https://arstechnica.com/information-technology/2022/02/iranian-state-hackers-are-using-log4shell-to-infect-unpatched-vmware-servers/
- El control del funcionamiento de Trickbot está ahora a cargo del ransomware Conti.
https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html
- El cambio en la ciberseguridad: 5 predicciones basadas en datos.
https://www.tripwire.com/state-of-security/security-data-protection/the-changing-state-of-cybersecurity-5-data-backed-predictions/

ACTUALIZACIONES DE SEGURIDAD

- Adobe publica una solución de emergencia para el día cero explotable en Commerce y Magento.
https://www.zdnet.com/article/patch-now-adobe-releases-emergency-fix-for-exploited-commerce-magento-zero-day/
- QNAP amplía las actualizaciones críticas para algunos dispositivos NAS no soportados.
https://www.bleepingcomputer.com/news/security/qnap-extends-critical-updates-for-some-unsupported-nas-devices/
- Nuevo error de día 0 de Chrome está bajo ataque activo. Piden actualizarlo lo antes posible.
https://thehackernews.com/2022/02/new-chrome-0-day-bug-under-active.html
- Se presenta Kali Linux 2022.1: Nuevas herramientas, "*kali-linux-todo*" y cambios visuales.
https://www.helpnetsecurity.com/2022/02/15/kali-linux-2022-1-released/
- **Se publican parches de VMware para varias vulnerabilidades detectadas.**
https://thehackernews.com/2022/02/vmware-issues-security-patches-for-high.html
- Se descubre un fallo crítico en el *plugin* de copia de seguridad de WordPress utilizado por más de 3 millones de sitios.
https://thehackernews.com/2022/02/critical-flaw-uncovered-in-wordpress.html
- La herramienta de paquetes Linux Snap corrige los errores de *make-me-root*.
https://www.theregister.com/2022/02/19/linux_snap_ubuntu/