@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. 143 – Año 2021**

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 24/11/21 y el 30/11/21

- Pfizer denuncia que un empleado robó los documentos de la vacuna #COVID19.
  https://www.infosecurity-magazine.com/news/pfizer-insider-stole-vaccine-docs/
- El proveedor de servicios marítimos Swire Pacific Offshore se ve afectado por un ransomware.
  https://portswigger.net/daily-swig/amp/maritime-giant-swire-pacific-offshore-suffers-data-breach-following-cyber-attack
- Las autoridades italianas multan a Google y Apple por su agresiva recopilación de datos.
- https://www.bleepingcomputer.com/news/technology/google-apple-fined-by-italian-authority-for-aggressive-data-collection/
- Panasonic revela una filtración de datos tras un hackeo de la red.
  https://www.infosecurity-magazine.com/news/data-breach-at-panasonic/
- El mercado de la *dark web* Cannazon cierra tras un ataque masivo de DDoS.
  https://www.bleepingcomputer.com/news/security/dark-web-market-cannazon-shuts-down-after-massive-ddos-attack/
- IKEA sufre un ciberataque a su sistema de correo electrónico.
  https://threatpost.com/ikea-email-reply-chain-attack/176625/

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

- La visión cibernética de China, construyendo un nuevo consenso sobre la gobernanza mundial de Internet.
  https://www.aspi.org.au/report/chinas-cyber-vision-how-cyberspace-administration-china-building-new-consensus-global
- Nueve consejos para una negociación eficaz contra el ransomware.
  https://www.csoonline.com/article/3641889/9-tips-for-an-effective-ransomware-negotiation.html#tk.rss_all
- Investigadores de Palo Alto Networks instalaron una infraestructura de *honeypots* con 320 nodos, analizando vulnerabilidades y como quedaron comprometidos en nubes públicas.
  https://securityaffairs.co/wordpress/124959/hacking/vulnerable-honeypot-exposure-analysis.html
- Un nuevo y sigiloso malware JavaScript infecta los PCs de Windows con RATs.
  https://www.bleepingcomputer.com/news/security/stealthy-new-javascript-malware-infects-windows-pcs-with-rats/
- El nuevo CronRAT de Linux se esconde en las tareas temporales cron para evadir la detección.
  https://securityaffairs.co/wordpress/125000/cyber-crime/linux-cronrat-magecart-attacks.html
- Los *criptohackers* utilizan como herramienta Babadeda para hacer indetectable su malware.
  https://thehackernews.com/2021/11/crypto-hackers-using-babadeda-crypter.html
- Hackers *criptomineros* están usando cuentas “comprometidas” en la nube.
  https://www.cnbc.com/2021/11/26/google-warns-crypto-miners-are-using-compromised-cloud-accounts-.html

https://thehackernews.com/2021/11/hackers-using-compromised-google-cloud.html

- El soft espía Chinotto está dirigido a desertores norcoreanos y activistas de derechos humanos.
https://thehackernews.com/2021/11/new-chinotto-spyware-targets-north.html
- AV-Comparatives explica en un informe las implicaciones de las adquisiciones en el sector de la seguridad informática.
https://www.av-comparatives.org/av-comparatives-explains-the-implications-of-takeovers-in-the-it-security-industry/
- Cuatro campañas de troyanos bancarios para Android se centraron en más de 300.000 dispositivos en 2021
https://thehackernews.com/2021/11/4-android-banking-trojan-campaigns.html
- Los hackers furtivos de WIRTE tienen como objetivo los gobiernos de Oriente Medio.
https://www.bleepingcomputer.com/news/security/stealthy-wirte-hackers-target-governments-in-the-middle-east/

## NOTAS DE INTERÉS

- Los piratas informáticos de la APT C-23 utilizan una nueva variante de software espía para Android para atacar a los usuarios de Oriente Medio.
https://thehackernews.com/2021/11/apt-c-23-hackers-using-new-android.html
- Apple demanda a NSO Group por usar el programa espía Pegasus, patrocinado por el Estado.
https://securityaffairs.co/wordpress/124954/laws-and-regulations/apple-sues-nso-group.html
- Japón y Vietnam firman un acuerdo de ciberseguridad para la ciberdefensa contra China.
https://www.securityweek.com/japan-vietnam-look-cyber-defense-against-china
- La AppGallery de Huawei está plagada de juegos infectados con malware.
https://www.theregister.com/2021/11/25/huaweis_appgallery_games_targeting_children/
- Los agujeros en los chips hacen que "un tercio de los smartphones y dispositivos IOT del mundo sean vulnerables a las escuchas".
https://www.forbes.com/sites/thomasbrewster/2021/11/24/mediatek-chip-flaws-left-android-and-iot-devices-vulnerable-to-spying/
- Funcionarios de defensa de EEUU dicen que Israel hackeó el sistema de gas iraní el mes pasado.
https://www.timesofisrael.com/2-us-defense-officials-say-israel-hacked-irans-gas-system-last-month-nyt/
- Microsoft soluciona los problemas que dejaron fuera de servicio a GitHub.
https://betanews.com/2021/11/28/microsoft-fixes-problems-that-took-github-offline/
- Señalan 300 mil infecciones de troyanos bancarios desde Google Play en 4 meses.
https://threatpost.com/banking-trojan-infections-google-play/176630/
- La suplantación de identidad sigue siendo la causa más común de violaciones de datos.
https://www.darkreading.com/edge-threat-monitor/phishing-remains-the-most-common-cause-of-data-breaches-survey-says
- Israel prohíbe la venta de herramientas de piratería y vigilancia a 65 países.
https://thehackernews.com/2021/11/israel-bans-sales-of-hacking-and.html
- Google han encontrado 2 fallos en el software de videoconferencia Zoom.
https://securityaffairs.co/wordpress/125122/security/video-conferencing-software-zoom-flaws.html

## ACTUALIZACIONES DE SEGURIDAD

- Actualización de emergencia del VMware vCenter Server.
https://www.vmware.com/security/advisories/VMSA-2021-0027.html