@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. 119 – 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.

20/07/2021

- FBI: Los grupos de amenazas pueden tener como objetivo los Juegos Olímpicos de Tokio 2020.
  https://www.bleepingcomputer.com/news/security/fbi-threat-actors-may-be-targeting-the-2020-tokyo-summer-olympics/
- Cientos de máquinas expendedoras de billetes de tren con pantalla táctil están fuera de servicio tras un ataque de ransomware al norte de Inglaterra.
  https://www.theregister.com/2021/07/20/northern_trains_ticketing_system/
- Un nuevo fallo en el kernel de Linux permite acceder al root en la mayoría de las distribuciones.
  https://www.bleepingcomputer.com/news/security/new-linux-kernel-bug-lets-you-get-root-on-most-modern-distros/

21/07/2021

- Podcast diario de seguridad de redes de SANS (Stormcast) del miércoles 21 de julio de 2021.
  https://isc.sans.edu/podcastdetail.html?id=7594
- Se ha detectado el malware de fraude de facturación Joker en Google Play Store.
  https://www.zdnet.com/article/joker-billing-fraud-malware-found-in-google-play-store/

22/07/2021

- Se acusa al gobierno de Modi de India de espiar a críticos y opositores con el programa Pegasus.
  https://www.zdnet.com/article/modi-government-accused-of-spying-on-critics-opponents-using-pegasus-spyware/
- Una APT distribuyó un troyano para Android a través de un portal electrónico de gobierno sirio
  https://thehackernews.com/2021/07/apt-hackers-distributed-android-trojan.html
- Mil GB de datos de municipios han sido expuestos por empresa de software de Massachusetts.
  https://www.zdnet.com/article/1000-gb-of-local-government-data-exposed-by-massachusetts-software-company/
- **Miles de sitios web, incluyendo HSBC, Airbnb y British Airways, afectados por cortes globales.**
  https://news.sky.com/story/several-high-profile-websites-including-hsbc-airbnb-and-british-airways-hit-by-outages-12361521
  https://www.lanacion.com.ar/tecnologia/una-falla-en-un-sistema-de-distribucion-de-contenido-apago-media-internet-nid22072021/
  https://www.bbc.com/news/technology-57929544

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

- Operaciones cibernéticas patrocinadas por el Estado chinos. Tácticas, técnicas y procedimientos de los responsables de la APT40.
  https://us-cert.cisa.gov/ncas/alerts/aa21-200b
  https://us-cert.cisa.gov/ncas/alerts/aa21-200a

- El grupo NSO fue *hackeado*.
https://www.schneier.com/blog/archives/2021/07/nso-group-hacked.html
https://threatpost.com/nso-pegasus-spyware-bans-apple-accountability/167965/
- Nuevas fallas críticas afectan al software de automatización industrial CODESYS.
https://thehackernews.com/2021/07/several-new-critical-flaws-affect.html
- MITRE actualiza la lista de los 25 errores de software más peligrosos.
https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html

NOTAS DE INTERÉS

- Nuevo malware se oculta entre las exclusiones de Windows Defender para evadir la detección.
https://thehackernews.com/2021/07/this-new-malware-hides-itself-among.html
https://www.bleepingcomputer.com/news/security/new-mosaicloader-malware-targets-software-pirates-via-online-ads/
- Google utiliza el "aprendizaje de máquina" y nuevas herramientas para detener ataques DDoS.
https://www.zdnet.com/article/google-is-using-machine-learning-to-stop-ddos-attacks/
https://www.zdnet.com/article/google-cloud-rolls-out-new-security-tools-as-threat-landscape-heats-up/
- El nuevo servicio de privacidad del e-mail de DuckDuckGo reenvía mensajes sin rastro.
https://www.bleepingcomputer.com/news/security/duckduckgos-new-email-privacy-service-forwards-tracker-free-messages/
- El malware MosaicLoader para Windows, para robo de contraseñas, se distribuye a través de anuncios en los resultados de las búsquedas.
https://www.zdnet.com/article/this-password-stealing-windows-malware-is-distributed-via-ads-in-search-results/
- La red de datos espacial está lista para comenzar a operar.
https://www.techrepublic.com/blog/forrester/the-space-wide-web-is-ready-to-launch/
- Kaseya obtiene un descifrador universal para las víctimas del ransomware REvil.
https://www.bleepingcomputer.com/news/security/kaseya-obtains-universal-decryptor-for-revil-ransomware-victims/

ACTUALIZACIONES DE SEGURIDAD

- Fortinet corrige un error que permitía a los hackers no autentificados ejecutar código como root.
https://www.bleepingcomputer.com/news/security/fortinet-fixes-bug-letting-unauthenticated-hackers-run-code-as-root/
- Parches para el iPhone de Apple, pero sin noticias de si se solucionó el reciente fallo del Wi-Fi.
https://nakedsecurity.sophos.com/2021/07/20/apple-iphone-patches-are-out-no-news-if-recent-wi-fi-bug-is-fixed/
- Chrome 92 acaba de añadir nuevas funciones de seguridad y privacidad.
https://www.zdnet.com/article/chrome-browser-just-added-these-new-security-and-privacy-features/
- Oracle advierte de fallos críticos del servidor Weblogic explotables de forma remota.
https://thehackernews.com/2021/07/oracle-warns-of-critical-remotely.html
- Microsoft publica una solución para este importante fallo de Windows 10.
https://www.zdnet.com/article/microsoft-just-published-a-workaround-for-this-important-windows-10-flaw/