@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. 112 – 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.

25/06/2021

- Hackers sofisticados están atacando firewalls y VPNs de Zyxel.
  https://www.zdnet.com/article/sophisticated-hackers-are-targeting-these-zyxel-firewalls-and-vpns/
- Delincuentes aprovechan un fallo de hace 3 años para borrar los dispositivos de Western Digital.
  https://securityaffairs.co/wordpress/119392/iot/hackers-wipe-western-digital-devices.html
- La filtración de datos de Mercedes-Benz expone los números de SSN y de tarjetas de crédito.
  https://www.bleepingcomputer.com/news/security/mercedes-benz-data-breach-exposes-ssns-credit-card-numbers/ç
- Los hackers están utilizando copias piratas del juego 'Grand Theft Auto V' para minar Monero.
  https://www.cyberscoop.com/grand-theft-auto-hack-sims-monero/

26/06/2021

- **Microsoft descubre que hackers de SolarWinds, vinculados a Rusia, han vulnerado tres nuevas entidades.**
  https://securityaffairs.co/wordpress/119425/apt/solarwinds-nobelium-ongoing-campaign.html
  https://threatpost.com/russian-attackers-breach-microsoft/167340/
- La filtración de datos de Mercedes-Benz afectó a unas 1.000 personas.
  https://securityaffairs.co/wordpress/119436/data-breach/mercedes-benz-data-breach.html

27/06/2021

- Se filtran más de 800 millones de registros de usuarios de WordPress.
  https://www.ehackingnews.com/2021/06/800-million-wordpress-users-records.html
- Un malware generó 2 millones de dólares tras utilizar 222.000 sistemas Windows.
  https://www.ehackingnews.com/2021/06/this-malware-generated-2-million-after.html

28/06/2021

- El lector de noticias personales NewsBlur restablece su servicio después de que un hacker borrara su base de datos.
  https://www.securityweek.com/newsblur-restores-service-after-hacker-wipes-database
- **Documentos confidenciales de la Defensa fueron encontrados en una parada de autobús en Kent, Reino Unido.**
  https://www.infosecurity-magazine.com/news/sensitive-defense-documents-bus/
- Las bandas de ransomware crean ahora sitios web para reclutar miembros.
  https://www.bleepingcomputer.com/news/security/ransomware-gangs-now-creating-websites-to-recruit-affiliates/
- Microsoft aprobó, falla de QA, un controlador de Windows con un malware de tipo rootkit.
  https://www.theregister.com/2021/06/28/microsoft_malware_signing/

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

- La falla de Cisco ASA se explota activamente a medida que cae el PoC.
https://threatpost.com/cisco-asa-bug-exploited-poc/167274/
- El nuevo grupo de ransomware Hive difunde ejemplos de archivos de la empresa de soft Altus.
https://securityaffairs.co/wordpress/119418/cyber-crime/new-ransomware-group-hive-leaks-altus-group-sample-files.html

NOTAS DE INTERÉS

- Nuevas fallas de alta gravedad afectan a 128 modelos de PC y tabletas de Dell.
https://thehackernews.com/2021/06/bios-disconnect-new-high-severity-flaws.html
https://arstechnica.com/information-technology/2021/06/a-well-meaning-feature-leaves-millions-of-dell-pcs-vulnerable/
- **Windows 11 requiere un procesador de seguridad TPM para instalar o actualizar a esa versión.**
https://www.bleepingcomputer.com/news/microsoft/windows-11-wont-work-without-a-tpm-what-you-need-to-know/
- Google amplía la compatibilidad con las cookies de seguimiento de terceras partes hasta 2023.
https://thehackernews.com/2021/06/google-extends-support-for-tracking.html
- Apple afirma que el "*slideloading* (transferencia de archivos entre dispositivos)" de aplicaciones es un riesgo de seguridad "grave".
https://www.bbc.com/news/technology-57597349
- Un error en la tecnología NFC permite piratear un cajero automático agitando un teléfono.
https://arstechnica.com/information-technology/2021/06/nfc-flaws-let-researchers-hack-an-atm-by-waving-a-phone/
- Un nuevo superordenador se ha unido a los cinco dispositivos más potentes del mundo.
https://www.zdnet.com/article/a-new-supercomputer-has-joined-the-top-five-most-powerful-devices-around-the-world/
- Las amenazas mediante dispositivos USB podrían producir impactos críticos en las operaciones de las empresas.
https://www.helpnetsecurity.com/2021/06/28/usb-threats-business-impact/
- GitHub señala que 2020 ha sido el "año más activo hasta la fecha" en la divulgación de vulnerabilidades.
https://www.zdnet.com/article/github-bug-bounties-payouts-surge-past-1-5-million-mark/
- ¿Tiene un viejo Western Digital My Book Live? Desconéctelo de Internet ahora mismo.
https://www.zdnet.com/article/own-a-wd-my-book-disconnect-it-from-the-internet-right-now/
- El nuevo *encriptador* de Linux del ransomware REvil está dirigido a las máquinas virtuales ESXi.
https://www.bleepingcomputer.com/news/security/revil-ransomwares-new-linux-encryptor-targets-esxi-virtual-machines/

ACTUALIZACIONES DE SEGURIDAD

- Citrix publica actualizaciones de seguridad para Hipervisor.
https://us-cert.cisa.gov/ncas/current-activity/2021/06/25/citrix-releases-security-updates-hypervisor
- NVIDIA repara falla de alta gravedad de GeForce en los ataques de suplantación de identidad.
https://threatpost.com/nvidia-high-severity-geforce-spoof-bug/167345/