@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. 105 – 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.

01/06/2021

- **Un ciberataque obliga a un productor de carne, JBS, a cerrar sus operaciones en Estados Unidos y Australia.**
  https://threatpost.com/cyberattack-meat-producer-shut-down/166560/
  https://www.cyberscoop.com/meatpacking-hack-jbs-ransomware-australia/
  https://exchange.xforce.ibmcloud.com/collection/0725bf1dacc8073b8e44056dabaabb5d
- Soldados estadounidenses revelaron información sobre el arsenal de armas nucleares.
  https://www.ehackingnews.com/2021/06/us-soldiers-exposed-information-about.html
- Crítico "*día cero*" del plugin de WordPress que está bajo una utilización activa.
  https://www.bleepingcomputer.com/news/security/critical-wordpress-plugin-zero-day-under-active-exploitation/
- Aparece una nueva variante de ransomware *Barebones*.
  https://www.darkreading.com/vulnerabilities---threats/new-barebones-ransomware-strain-surfaces/d/d-id/1341181

02/06/2021

- Las escuelas estadounidenses obtienen subsidios de IBM para protegerse contra el ransomware.
  https://www.zdnet.com/article/us-schools-land-ibm-grants-to-protect-themselves-against-ransomware/
- Foros clandestinos rusos organizan concursos de criptodivisas y *hackeos* a NFT (*no fungible token*).
  https://www.zdnet.com/article/russian-underground-forums-launch-competitions-for-cryptocurrency-hacks/
  https://thehackernews.com/2021/06/cybercriminals-hold-115000-prize.html
- Los equipos USB LTE de Huawei son vulnerables a los ataques de escalada de privilegios.
  https://www.bleepingcomputer.com/news/security/huawei-usb-lte-dongles-are-vulnerable-to-privilege-escalation-attacks/
- FUJIFILM cierra la red tras un presunto ataque de ransomware.
  https://www.bleepingcomputer.com/news/security/fujifilm-shuts-down-network-after-suspected-ransomware-attack/

03/06/2021

- El FBI atribuye el ataque del ransomware de JBS al grupo REvil.
  https://www.zdnet.com/article/fbi-attributes-jbs-ransomware-attack-to-revil/
- El mayor servicio de ferry de Massachusetts sufre un ataque de ransomware.
  https://www.infosecurity-magazine.com/news/ransomware-massachusetts-largest/
- Servidores Exchange atacados por el malware "Epsilon Red".
  https://threatpost.com/exchange-servers-epsilon-red-ransomware/166640/

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

- **Lista de filtraciones de datos y ciberataques en mayo de 2021.**
https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-may-2021-116-million-records-breached
- Un malware puede utilizar este recurso para eludir la defensa contra el ransomware en las soluciones antivirus.
https://thehackernews.com/2021/06/malware-can-use-this-trick-to-bypass.html
- Ahora Firefox bloquea el rastreo *cross-site* por defecto en la navegación privada.
https://www.bleepingcomputer.com/news/security/firefox-now-blocks-cross-site-tracking-by-default-in-private-browsing/
- El malware de criptominería aumenta y el malware financiero disminuye en el primer trimestre de 2021, según Kaspersky.
https://www.techrepublic.com/article/cryptomining-malware-up-financial-malware-down-in-q1-2021-kaspersky-finds/
- Prometheus y Grief: dos nuevas bandas de ransomware emergentes que apuntan a las empresas y publican datos del gobierno mexicano para su venta.
https://securityaffairs.co/wordpress/118446/cyber-crime/prometheus-grief-ransomware.html
- Se ha encontrado una vulnerabilidad XSS en un popular editor tipo WYSIWYG de sitios web.
https://www.zdnet.com/article/xss-vulnerability-found-in-popular-wysiwyg-website-editor/

NOTAS DE INTERÉS

- **Informe: El servicio secreto danés ayudó a la NSA a espiar a políticos europeos.**
https://thehackernews.com/2021/06/report-danish-secret-service-helped-nsa.html
- Microsoft adquiere ReFirm Labs para mejorar la seguridad del IoT.
https://www.microsoft.com/security/blog/2021/06/02/microsoft-acquires-refirm-labs-to-enhance-iot-security/
- **Ahora el antivirus Norton 360 permite minar la criptomoneda Ethereum.**
https://www.bleepingcomputer.com/news/cryptocurrency/norton-360-antivirus-now-lets-you-mine-ethereum-cryptocurrency/
- Expertos descubren otra campaña de espionaje china dirigida al sudeste asiático.
https://thehackernews.com/2021/06/experts-uncover-yet-another-chinese.html
- Ciberdelincuentes chinos pasaron tres años creando una nueva herramienta que se usa en actividades de ciberespionaje.
https://www.zdnet.com/article/chinese-cybercriminals-spent-three-years-creating-a-new-backdoor-to-spy-on-governments/
- El *bot* Necro Python se ha renovado con nuevos exploits de VMWare y servidores.
https://www.zdnet.com/article/necro-python-bot-revamped-with-new-vmware-smb-exploits/

ACTUALIZACIONES DE SEGURIDAD

- Se publica Kali Linux 2021.2. Nuevas herramientas y mejoras.
https://www.helpnetsecurity.com/2021/06/02/kali-linux-2021-2-released/
- Cisco anuncia actualizaciones de seguridad para varios productos.
https://us-cert.cisa.gov/ncas/current-activity/2021/06/02/cisco-releases-security-updates-multiple-products