@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. 106 – 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.

04/06/2021

- Ciberdelincuentes utilizan las noticias del *ransomware* Colonial Pipeline para ataques *phishing*.
  https://www.zdnet.com/article/hackers-use-colonial-pipeline-ransomware-news-for-phishing-attack/
- Fujifilm confirma que el ataque *ransomware* interrumpió las operaciones comerciales.
  https://www.bleepingcomputer.com/news/security/fujifilm-confirms-ransomware-attack-disrupted-business-operations/
  https://www.cyberscoop.com/tokyo-olympics-fujitsu-breach-japan/
- Se sospecha de un ciberataque en los cortes de TV y radio de Cox Media Group.
  https://threatpost.com/cyberattack-cox-outage-tv-radio/166680/
- Atacantes vinculados a China accedieron a la Autoridad de Transporte Metropolitano (MTA) Nueva York utilizando el día cero de Pulse Secure.
  https://securityaffairs.co/wordpress/118579/apt/metropolitan-transportation-authority-hack.html

05/06/2021

- Alerta: *Bug* RCE crítico en VMware vCenter Server bajo ataque activo.
  https://thehackernews.com/2021/06/alert-critical-rce-bug-in-vmware.html
  https://us-cert.cisa.gov/ncas/current-activity/2021/06/04/unpatched-vmware-vcenter-software

06/06/2021

- El portavoz de REvil Ransomware publica una entrevista sobre los recientes ataques.
  https://securityaffairs.co/wordpress/118639/cyber-crime/revil-ransomware-interview.html

07/06/2021

- Una mujer letona fue acusada por su papel en la creación del malware bancario Trickbot.
  https://thehackernews.com/2021/06/latvian-woman-charged-for-her-role-in.html
- Podcast diario de seguridad de redes de SANS (Stormcast) del lunes 7 de junio de 2021.
  https://isc.sans.edu/podcastdetail.html?id=7530
- ¿Se acuerdan de Anonymous? Puede que hayan vuelto y están enfadados con Elon Musk.
  https://www.theregister.com/2021/06/07/anonymous_musk/
- El fabricante estadounidense de camiones y vehículos militares Navistar revela una filtración de datos.
  https://www.bleepingcomputer.com/news/security/us-truck-and-military-vehicle-maker-navistar-discloses-data-breach/

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

- Se encontraron vulnerabilidades en módulo de Realtek.
  https://www.ehackingnews.com/2021/06/vulnerabilties-found-in-realtek-module.html

- Seguridad y comportamiento humano (SHB, por sus siglas en inglés) 2021.
https://www.schneier.com/blog/archives/2021/06/security-and-human-behavior-shb-2021.html

- **Informe: índice de la web oscura (*dark web*) 2021.**
https://securityaffairs.co/wordpress/118574/cyber-crime/dark-web-price-index.html

- La vulnerabilidad de VMware con un índice de gravedad de 9,8 está siendo atacada.
https://arstechnica.com/gadgets/2021/06/under-exploit-vmware-vulnerability-with-severity-rating-of-9-8-out-of-10/
https://www.cyberscoop.com/vmware-exploit-virtual-machine-cisa/

- El nuevo ransomware de Evil Corp imita a la banda PayloadBin para eludir las sanciones estadounidenses.
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/

NOTAS DE INTERÉS

- Fueron encontrados 10 defectos críticos en el software de automatización industrial CODESYS.
https://thehackernews.com/2021/06/10-critical-flaws-found-in-codesys.html
https://www.helpnetsecurity.com/2021/06/04/critical-vulnerabilities-codesys-ics/

- Google permitirá a los usuarios de Android rechazar el seguimiento de anuncios.
https://thehackernews.com/2021/06/google-to-let-android-users-opt-out-to.html

- Estados Unidos tratará el ransomware como si fuera terrorismo.
https://www.infosecurity-magazine.com/news/us-to-treat-ransomware-like/
https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-recent-ransomware-attacks

- La mayoría de las empresas brasileñas carecen de equipos de ciberseguridad.
https://www.zdnet.com/article/most-brazilian-companies-lack-cybersecurity-teams/

- BlackCocaine Ransomware, un nuevo malware en el entorno de las amenazas.
https://securityaffairs.co/wordpress/118617/malware/blackcocaine-ransomware.html

- **TikTok actualiza silenciosamente su política de privacidad para recoger los datos biométricos de los usuarios.**
https://thehackernews.com/2021/06/tiktok-quietly-updated-its-privacy.html

- Google, Microsoft y Mozilla trabajan juntos para mejorar las extensiones del navegador.
https://www.bleepingcomputer.com/news/security/google-microsoft-and-mozilla-work-together-on-better-browser-extensions/

- EE.UU. estudia una respuesta militar a los ataques de ransomware, según funcionarios de Biden.
https://www.theguardian.com/technology/2021/jun/06/us-military-response-ransomware-attacks-biden-russia-putin

- Siloscape: nuevo malware que afecta a los contenedores de Windows para acceder a los clusters de Kubernetes.
https://www.zdnet.com/article/siloscape-this-new-malware-targets-windows-containers-to-access-kubernetes-clusters/

ACTUALIZACIONES DE SEGURIDAD

- Chrome 91 advertirá a los usuarios cuando instalen extensiones no fiables.
https://www.zdnet.com/article/chrome-91-will-warn-users-when-installing-untrusted-extensions/

- Actualizar ya: Los atacantes están a la pesca de este error crítico de VMware vCentre.
https://www.zdnet.com/article/patch-now-attackers-are-hunting-for-this-critical-vmware-vcentre-flaw/