@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. 108 – 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.

11/06/2021

- Nuevo grupo de ciberespionaje que tiene como objetivo los Ministerios de Asuntos Exteriores.
https://thehackernews.com/2021/06/new-cyber-espionage-group-targeting.html
- Piratas informáticos roban el código fuente y las herramientas de FIFA 21 en un ataque a EA.
https://threatpost.com/hackers-fifa-21-source-code/166829/
- Una falla de seguridad dejó al descubierto la información personal de los clientes del minorista estadounidense Carter's.
https://www.zdnet.com/article/lax-security-around-url-shortener-exposed-pii-of-us-retailer-carters-customer-base/
- McDonald's sufre una filtración de datos en Estados Unidos, Corea del Sur y Taiwán.
https://www.bleepingcomputer.com/news/security/mcdonalds-discloses-data-breach-after-theft-of-customer-employee-info/
https://www.theverge.com/2021/6/11/22529656/mcdonalds-data-breach-us-south-korea-taiwan

12/06/2021

- Los legisladores de EE.UU. presentan proyectos de ley contra las grandes empresas tecnológicas.
https://www.bbc.com/news/technology-57450345
- La filtración de datos de Audi y Volkswagen afecta a 3,3 millones de clientes.
https://securityaffairs.co/wordpress/118887/data-breach/volkswagen-data-breach.html
- Piratas informáticos iraníes atacaron sitios web de un banco africano y una biblioteca federal estadounidense.
https://www.ehackingnews.com/2021/06/iranian-hackers-attacked-websites-of.html

13/06/2021

- Interpol cierra miles de falsas farmacias que estaban disponibles “en línea”.
https://www.bleepingcomputer.com/news/security/interpol-shuts-down-thousands-of-fake-online-pharmacies/
- Se cree que hackers chinos están detrás del segundo ciberataque a Air India
https://thehackernews.com/2021/06/chinese-hackers-believed-to-be-behind.html

14/06/2021

- El ransomware REvil afecta a un contratista de armas nucleares y a una empresa multinacional de energía renovable, ambas estadounidenses.
https://www.bleepingcomputer.com/news/security/microsoft-scammers-bypass-office-365-mfa-in-bec-attacks/
https://www.infosecurity-magazine.com/news/revil-claims-responsibility-for/#.YMfiRaa56gc.twitter
- CISA advierte de la amenaza que supone el ransomware para los sistemas industriales.

https://www.securityweek.com/cisa-warns-threat-posed-ransomware-industrial-systems

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

- Los 11 proveedores de ciberseguridad a los que hay que prestar atención en 2021.
- https://www.darkreading.com/edge/theedge/11-cybersecurity-vendors-to-watch-in-2021/b/d-id/1341265
- Los ciberatacantes de la APT "Fancy Lazarus" se intensifican con intentos DDoS.
  https://threatpost.com/fancy-lazarus-cyberattackers-ransom-ddos/166811/
- El ransomware Avaddon se desactiva y libera las claves de descifrado.
  https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/
- Codecov abandona Bash Uploader por un ejecutable NodeJS.
  https://www.bleepingcomputer.com/news/security/codecov-ditches-bash-uploader-for-a-nodejs-executable/
  https://www.zdnet.com/article/codecov-debuts-new-uploader-dismisses-bash-script-as-source-of-supply-chain-attack-risk/

NOTAS DE INTERÉS

- Investigadores crean una red cuántica "*inhackeable*" a lo largo de cientos de kilómetros utilizando fibra óptica.
  https://www.zdnet.com/article/researchers-created-an-un-hackable-quantum-network-over-hundreds-of-kilometers-using-optical-fiber/
- Una falla de Linux, de 7 años atrás, permite a usuarios no privilegiados obtener acceso a la raíz.
  https://thehackernews.com/2021/06/7-year-old-polkit-flaw-lets.html
- Los ataques DDoS aumentan un 341% en medio de la pandemia.
  https://www.helpnetsecurity.com/2021/06/11/ddos-attacks-increase-pandemic/
- El monumental ataque a la cadena de suministro de las aerolíneas se debe a un autor estatal.
  https://threatpost.com/supply-chain-attack-airlines-state-actor/166842/
- Estados Unidos crea un grupo nacional de trabajo sobre IA.
  https://www.infosecurity-magazine.com/news/us-launches-national-ai-task-force/
- El ataque a la cadena de suministro de NoxPlayer es probablemente obra del grupo Gelsemium.
  https://thehackernews.com/2021/06/noxplayer-supply-chain-attack-is-likely.html
- Los delincuentes se saltan la protección MFA de Office 365 en los ataques BEC.
  https://www.bleepingcomputer.com/news/security/microsoft-scammers-bypass-office-365-mfa-in-bec-attacks/

ACTUALIZACIONES DE SEGURIDAD

- Actualizar Chrome ya, pues tiene un exploit de día cero.
  https://betanews.com/2021/06/10/chrome-zero-day-exploit/
- NVIDIA deja de dar soporte a los controladores de Windows 7 y Windows 8.
  https://www.bleepingcomputer.com/news/software/nvidia-is-dropping-support-for-windows-7-and-windows-8-drivers/
- Microsoft dará soporte a Internet Explorer durante un año más.
  https://betanews.com/2021/06/14/microsoft-will-support-internet-explorer-for-one-more-year-but-now-is-the-time-to-move-on/