@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. 135 – 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.

Noticias de ciberseguridad entre el 1/10/21 y el 7/10/21

- El malware Hydra se enfoca en los clientes del segundo banco más grande de Alemania. https://www.bleepingcomputer.com/news/security/hydra-malware-targets-customers-of-germanys-second-largest-bank/
- Cibercriminales robaron criptomonedas de al menos 6.000 clientes de Coinbase. https://www.ft.com/content/43ab875b-2e96-48b7-926d-be17e925f1c3
- Una banda de ransomware encripta servidores VMware ESXi con un script de Python. https://www.bleepingcomputer.com/news/security/ransomware-gang-encrypts-vmware-esxi-servers-with-python-script/
- The Telegraph deja al descubierto una base de datos de 10 TB con información de suscriptores. https://www.theregister.com/2021/10/05/telegraph_newspaper_10tb_data_breach/
- **Más de 1.500 millones de datos personales de usuarios de Facebook se encuentran a la venta en un foro de hackers.** https://www.techrepublic.com/article/over-1-5-billion-facebook-users-personal-data-found-for-sale-on-hacker-forum/
- **Hackean la página de Facebook de un buque de guerra de EE.UU. para retransmitir el juego 'Age of Empires'.** https://threatpost.com/navy-warships-facebook-age-empires-gaming/175409/
- Las empresas británicas sufren un ataque cada 47 segundos. https://www.infosecurity-magazine.com/news/uk-firms-one-attack-every-47/

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

- Creando señales inalámbricas con cable Ethernet para robar datos de los sistemas con cobertura aérea. https://thehackernews.com/2021/10/creating-wireless-signals-with-ethernet.html
- **¿Qué pasó con Facebook, Instagram y WhatsApp?** https://krebsonsecurity.com/2021/10/what-happened-to-facebook-instagram-whatsapp/ https://blog.cloudflare.com/october-2021-facebook-outage/
- Lista de vulneraciones de datos y ciberataques en septiembre de 2021: 91 millones de registros afectados. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-september-2021-91-million-records-breached
- **SharpML - Red de Aprendizaje Automático Comparte el Kit de Búsqueda de Contraseñas.** https://www.kitploit.com/2021/09/sharpml-machine-learning-network-share.html

- Hackers iraníes aprovechan Dropbox en ciberataques contra empresas aeroespaciales y de telecomunicaciones.
  https://thehackernews.com/2021/10/iranian-hackers-abuse-dropbox-in.html
- **El código fuente de Twitch y las ganancias de sus creadores, es exp4kunesta en una filtración de 125 GB.**
  https://arstechnica.com/information-technology/2021/10/twitch-admits-to-major-leak-exposing-source-code-creator-earnings/

NOTAS DE INTERÉS

- Las conexiones 5G alcanzaron los 429 millones en el segundo trimestre de 2021.
  https://www.helpnetsecurity.com/2021/10/01/5g-connections-q2-2021/
- El jefe de ciberseguridad de la NSA informa que los hackers utilizan, cada vez más, herramientas comerciales para mantenerse ocultos.
  https://www.nextgov.com/cybersecurity/2021/09/nsa-cyber-chief-warns-hackers-increasingly-use-commercial-tools-stay-hidden/185733/
- Falso antivirus de Amnistía Internacional para Pegasus que hackea computadoras con malware.
  https://thehackernews.com/2021/10/beware-of-fake-amnesty-international.html
- "Mariana Trench", la herramienta de detección de errores de Android y Java, ahora en código abierto.
  https://www.zdnet.com/article/android-java-bug-bunting-tool-mariana-trench-becomes-open-source/
- La nueva APT ChamelGang tiene como objetivo las organizaciones rusas de energía y aviación.
  https://threatpost.com/apt-chamelgang-targets-russian-energy-aviation/175272/
- Los servidores Apache Airflow mal configurados filtran miles de credenciales
  https://www.bleepingcomputer.com/news/security/misconfigured-apache-airflow-servers-leak-thousands-of-credentials/
- Un nuevo grupo de hacking APT orientado a las industrias del combustible, la energía y la aviación.
  https://thehackernews.com/2021/10/a-new-apt-hacking-group-targeting-fuel.html
- El troyano bancario Flubot para Android se propaga a través de falsas actualizaciones de seguridad.
  https://securityaffairs.co/wordpress/122839/malware/flubot-android-trojan-fake-updates.html
- Investigadores de BlackBerry vinculan una campaña de malware dirigida a víctimas de la India con un grupo de ciberespionaje chino.
  https://www.zdnet.com/article/blackberry-ties-malware-campaign-targeting-victims-in-india-to-chinese-cyberespionage-group/

ACTUALIZACIONES DE SEGURIDAD

- Apache corrige una vulnerabilidad de día cero activamente aprovechada.
  https://exchange.xforce.ibmcloud.com/collection/a196fc565350685b57d872292b783e67
- Google impulsa una actualización de emergencia para resolver "días cero" de Chrome.
  https://www.cyberscoop.com/google-chrome-zero-days/
- El parche de octubre de Android corrige tres errores críticos, 41 fallos en total.
  https://www.bleepingcomputer.com/news/security/android-october-patch-fixes-three-critical-bugs-41-flaws-in-total/