@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. 116 – 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.

09/07/2021

- Lazarus tiene como objetivo a los ingenieros que buscan trabajo usando documentos maliciosos. https://threatpost.com/lazarus-engineers-malicious-docs/167647/
- El gigante de los seguros CNA informa de una violación de datos tras un ataque de ransomware. https://securityaffairs.co/wordpress/119913/data-breach/cna-data-breach.html
- El error crítico "PrintNightmare" de Windows sigue causando dolores de cabeza. https://www.cyberscoop.com/printnightmare-print-spooler-microsoft-patch/
- El FBI advierte a dueños de criptomonedas y a casas de cambio de ataques que se están produciendo. https://www.bleepingcomputer.com/news/security/fbi-warns-cryptocurrency-owners-exchanges-of-ongoing-attacks/

10/07/2021

- Mint Mobile sufre una filtración tras la transferencia de números y el acceso a los datos. https://www.bleepingcomputer.com/news/security/mint-mobile-hit-by-a-data-breach-after-numbers-ported-data-accessed/
- **Consejo distrital del municipio de Anhalt-Bitterfeld declara la primera "cibercatástrofe" de la historia de Alemania.** https://www.rappler.com/world/europe/germany-anhalt-bitterfield-declare-cyber-catastrophe-2021
- El sistema ferroviario iraní sufrió un gran ciberataque, los hackers publicaron mensajes falsos sobre retrasos. https://securityaffairs.co/wordpress/119942/hacking/irans-railroad-system-cyberattack.html

11/07/2021

- Cibercriminales chinos atacan a las empresas de telecomunicaciones taiwanesas. https://www.ehackingnews.com/2021/07/chinese-hackers-target-taiwanese.html

12/07/2021

- El minorista de moda Guess divulga una filtración de datos tras un ataque de ransomware. https://www.bleepingcomputer.com/news/security/fashion-retailer-guess-discloses-data-breach-after-ransomware-attack/
- Delincuentes roban 600 millones de perfiles de LinkedIn y ahora los están vendiendo "*on line*". https://securityaffairs.co/wordpress/120009/cyber-crime/600m-linkedin-profiles-scraped.html

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

- Advertencia: 1 de cada 3 empleados es susceptible a caer en una estafa de phishing. https://www.techrepublic.com/article/warning-1-in-3-employees-are-likely-to-fall-for-a-phishing-scam/

- Los datos de 1,2 millones de pacientes fueron robados antes del ataque del ransomware de un proveedor externo.
https://www.scmagazine.com/home/health-care/data-of-1-2m-patients-stolen-prior-to-third-party-vendor-ransomware-attack/

- Hackers propagan el malware BIOPASS a través de sitios chinos de juego en línea.
https://thehackernews.com/2021/07/hackers-spread-biopass-malware-via.html

- **Análisis del teléfono An0m del FBI.**
https://www.schneier.com/blog/archives/2021/07/analysis-of-the-fbis-anom-phone.html
https://www.vice.com/en/article/n7b4gg/anom-phone-arcaneos-fbi-backdoor

- El plugin de gestión de archivos de WordPress está plagado de errores críticos.
https://threatpost.com/frontend-file-manager-wordpress-bugs/167687/

NOTAS DE INTERÉS

- **Europa aprueba ley de vigilancia masiva en WhatsApp, Telegram y Gmail.**
https://www.criptonoticias.com/regulacion/europa-aprueba-ley-vigilancia-masiva-whatsapp-telegram-gmail/

- Se ha informado de fallos críticos en los sistemas de imagen médica Philips Vue PACS.
https://thehackernews.com/2021/07/critical-flaws-reported-in-philips-vue.html

- El grupo Magecart oculta los datos de tarjetas de crédito robadas en imágenes.
https://thehackernews.com/2021/07/magecart-hackers-hide-stolen-credit.html

- Un nuevo troyano roba millones de credenciales de acceso.
https://www.techradar.com/news/malware-steals-millions-of-login-credentials-for-popular-websites
https://www.darkreading.com/edge/theedge/i-smell-a-rat!-new-cybersecurity-threats-for-the-crypto-industry/b/d-id/1341421

- **Ciberpolígono 2021: Hacia un desarrollo seguro de los ecosistemas digitales.**
https://threatpost.com/cyber-polygon-2021-towards-secure-development-of-digital-ecosystems/167661/

- Las TI, la sanidad y la industria son los principales objetivos de los ciberataques.
https://www.helpnetsecurity.com/2021/07/12/cyberattacks-top-targets/

- Un instituto holandés expone los defectos de la plataforma Kaseya - VSA.
https://www.ehackingnews.com/2021/07/dutch-institute-exposes-flaws-in-kaseya.html

- SolarWinds afirma que los piratas informáticos utilizaron un fallo de día cero para realizar "ataques dirigidos" en una nueva intrusión.
https://www.cyberscoop.com/solarwinds-hacked-again-zero-day/

ACTUALIZACIONES DE SEGURIDAD

- Los fallos de Cisco BPA y WSA permiten ciberataques remotos.
https://threatpost.com/cisco-bpa-wsa-bugs-cyberattacks/167654/

- Índice de prioridad de parches de Tripwire de junio de 2021.
https://www.tripwire.com/state-of-security/vert/tripwire-patch-priority-index-for-june-2021/

- Kaseya “corrige” los días cero utilizados en los ataques de REvil.
https://threatpost.com/kaseya-patches-zero-days-revil-attacks/167670/