@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. 86/2021

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.

23/03/2021

- Stratus Technologies, fabricante de servidores de alta disponibilidad, sufrió un ataque de ransomware que ha obligado a desconectar los sistemas.
https://www.bleepingcomputer.com/news/security/high-availability-server-maker-stratus-hit-by-ransomware/
- Un ransomware detiene la producción del fabricante de IoT Sierra Wireless.
https://www.zdnet.com/article/ransomware-attack-halts-production-at-iot-maker-sierra-wireless/
- La Universidad de Northampton, en el reino Unido, sufre un ciberataque.
https://www.bbc.com/news/uk-england-northamptonshire-56500434
- El sitio de MangaDex quedó fuera de servicio tras un incidente de *hackeo*.
https://threatpost.com/mangadex-site-offline-hacking/164983/
- La empresa de seguros CNA sufre un ciberataque y sus operaciones se ven afectadas.
https://www.bleepingcomputer.com/news/security/cna-insurance-firm-hit-by-a-cyberattack-operations-impacted/

24/03/2021

- El malware Purple Fox ataca a las máquinas Windows con nuevas capacidades de gusano.
https://threatpost.com/purple-fox-malware-windows-worm/164993/
- Filtración en la Oficina de Contralor del Estado de California.
https://www.infosecurity-magazine.com/news/breach-at-california-state/
- Brasil lidera los ataques de phishing.
https://www.zdnet.com/article/brazil-leads-in-phishing-attacks/

25/03/2021

- El ransomware Black Kingdom a la caza de servidores Microsoft Exchange sin parches.
https://thehackernews.com/2021/03/black-kingdom-ransomware-hunting.html
- QNAP advierte de los continuos ataques de fuerza bruta contra los dispositivos NAS.
https://www.bleepingcomputer.com/news/security/qnap-warns-of-ongoing-brute-force-attacks-against-nas-devices/
- El equipo de investigación de CyberNews encontró 62.174 servidores Microsoft Exchange potencialmente vulnerables y sin parches.
https://securityaffairs.co/wordpress/115965/hacking/microsoft-exchange-servers-unpatched.html
- Facebook eliminó innumerables perfiles falsos destinados a propagar programas maliciosos de espionaje.
https://threatpost.com/facebook-disrupts-spy-uyghurs/165032/

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

- Una empresa fue atacada por un ransomware. Esto es lo que hicieron después y por qué no pagaron.
https://www.zdnet.com/article/this-company-was-hit-with-ransomware-heres-what-they-did-next-and-why-they-didnt-pay-up/
- ¿Quién está en tus cuentas de Facebook e Instagram?
https://usa.kaspersky.com/blog/suspicious-login-attempt-facebook-instagram/24271/
- CISA añade dos shells web a la guía de Exchange Server.
https://www.darkreading.com/risk/cisa-adds-two-web-shells-to-exchange-server-guidance/d/d-id/1340525
https://us-cert.cisa.gov/ncas/current-activity/2021/03/25/webshells-observed-post-compromised-exchange-servers
- La migración a la nube del sector manufacturero abre la puerta a importantes riesgos cibernéticos.
https://threatpost.com/manufacturing-cloud-migration-cyber-risk/165028/

NOTAS DE INTERÉS

- La vulnerabilidad "*slicing*" de la red 5G deja a las empresas expuestas a ciberataques.
https://www.helpnetsecurity.com/2021/03/24/5g-network-slicing-vulnerability/
- El lanzamiento de Firefox 87 incluye la navegación privada 'SmartBlock'.
https://www.zdnet.com/article/firefox-87-launch-packed-with-private-browsing-smartblock/
- Google Chrome utilizará HTTPS como protocolo de navegación por defecto.
https://www.bleepingcomputer.com/news/google/google-chrome-will-use-https-as-default-navigation-protocol/
- *Exploits* activos afectan a los sitios de WordPress vulnerables a los fallos de Thrive Themes.
https://threatpost.com/active-exploits-wordpress-sites-thrive-themes/165013/
- El mercado mundial de Wi-Fi alcanzará los 25.244 millones de dólares en 2026.
https://www.helpnetsecurity.com/2021/03/25/wi-fi-market-2026/
- Las estafas con criptomonedas casi se duplican en 2020 y hay más en marcha.
https://betanews.com/2021/03/25/cryptocurrency-scams-almost-double/
- En EE.UU. los fiscales estatales presionan a Facebook y Twitter para que hagan más por frenar la desinformación sobre los virus.
https://www.cyberscoop.com/vaccine-misinformation-coronavirus-facebook-twitter/

ACTUALIZACIONES DE SEGURIDAD

- OpenSSL corrige graves vulnerabilidades de DoS y de validación de certificados.
https://www.bleepingcomputer.com/news/security/openssl-fixes-severe-dos-certificate-validation-vulnerabilities/
https://www.openssl.org/news/secadv/20210325.txt
- Samba anuncia actualizaciones de seguridad.
https://us-cert.cisa.gov/ncas/current-activity/2021/03/25/samba-releases-security-updates
- Se corrigió el escalar privilegios de PsExec en Windows Corregido
https://exchange.xforce.ibmcloud.com/collection/e97cd1b85394822631fcc1589f7ff16d