@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. 72/2021

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.

26/01/2021

- Un *bug* de TikTok podría haber expuesto datos del perfil y números de teléfono de los usuarios. https://securityaffairs.co/wordpress/113869/mobile-2/tiktok-privacy-flaw.html
- La banda de ransomware Nefilim se lleva el premio grande con una cuenta fantasma. https://threatpost.com/nefilim-ransomware-ghost-account/163341/
- El gigante minorista asiático Dairy Farm sufre un ataque del ransomware REvil. https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revil-ransomware-attack/
- La filtración del condado de Cook, en EE.UU., expone casos criminales y de violencia doméstica. https://threatpost.com/criminal-domestic-case-cook-county-leak23k-sensitive-court-records/163336/

27/01/2021

- La Comisión Australiana de Valores e Inversiones (ASIC) ha declarado que uno de sus servidores fue vulnerado el 15 de enero. https://www.zdnet.com/article/asic-reports-server-breached-via-accellion-vulnerability/
- Un error de Sudo de hace 10 años permite a los usuarios de Linux obtener acceso a nivel *root*. https://www.helpnetsecurity.com/2021/01/27/cve-2021-3156/ https://www.cyberscoop.com/sudo-flaw-cyber-command-nsa-buffer-overflow/
- Emotet: La red de malware más peligrosa del mundo fue desbaratada en una gran operación policial. https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/ http://www.ddosinfo.com/ddos-news/international-law-enforcement-effort-pulls-off-emotet-botnet-takedown
- El grupo TeamTNT oculta malware con una herramienta de código abierto. https://threatpost.com/teamtnt-cloaks-malware-open-source-tool/163414/

28/01/2021

- Autoridades de EE.UU. y Bulgaria incautan un sitio de la “dark web” vinculado al ransomware Netwalker. https://thehackernews.com/2021/01/authorities-seize-dark-web-site-linked.html
- El CERT de Italia advierte de un nuevo malware para Android que roba credenciales. https://thehackernews.com/2021/01/italy-cert-warns-of-new-credential.html
- El CISA publicó un aviso de seguridad sobre fallas de alta gravedad en algunos productos SCADA/HMI de la empresa japonesa Fuji Electric.

https://securityaffairs.co/wordpress/113950/ics-scada/fuji-electric-hmi-flaws.html
https://us-cert.cisa.gov/ics/advisories/icsa-21-026-01

- La unidad cibernética de Hezbollah hackeó telecomunicaciones e ISPs.
https://www.zdnet.com/article/hezbollahs-cyber-unit-hacked-into-telecoms-and-isps/

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

- Nueva campaña dirigida a investigadores de seguridad para robar información no divulgada.
https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/
https://thehackernews.com/2021/01/n-korean-hackers-targeting-security.html

- Así es como un investigador entró en el GitHub de Microsoft VS Code.
https://www.bleepingcomputer.com/news/security/heres-how-a-researcher-broke-into-microsoft-vs-codes-github/

- La guía del hacker de satélites para la industria espacial: que no cunda el pánico (todavía).
https://cybernews.com/security/the-satellite-hackers-guide-to-the-space-industry-dont-panic-yet/

NOTAS DE INTERÉS

- Mastercard presenta especificaciones resistentes a tecnología cuántica para mejorar la seguridad *contactless*.
https://www.infosecurity-magazine.com/news/mastercard-quantum-resistant/

- Firefox 85 elimina Flash y añade protección contra las supercookies.
https://www.zdnet.com/article/firefox-85-removes-flash-and-adds-protection-against-supercookies/

- El malware DanaBot vuelve a ser protagonista.
https://threatpost.com/danabot-malware-roars-back/163358/

- **Los principales ciberataques de 2020.**
https://thehackernews.com/2021/01/top-cyber-attacks-of-2020.html

- Malware para Linux utiliza una herramienta de código abierto para evadir la detección.
https://www.bleepingcomputer.com/news/security/linux-malware-uses-open-source-tool-to-evade-detection/

- Una nueva herramienta de ciberdelincuencia puede crear páginas de phishing en tiempo real.
https://securityaffairs.co/wordpress/113961/cyber-crime/logokit-phishing-kit.html

ACTUALIZACIONES DE SEGURIDAD

- Google corrige una grave vulnerabilidad RCE de "*Go language*" en Windows.
https://www.bleepingcomputer.com/news/security/google-fixes-severe-golang-windows-rce-vulnerability/

- Apple corrige otros tres *zero-days* del iOS del nuevo iPhone.
https://www.zdnet.com/article/apple-fixes-another-three-ios-zero-days-exploited-in-the-wild/

- Nvidia elimina un fallo de alta gravedad de DoS.
https://threatpost.com/nvidia-squashes-high-severity-jetson-dos-flaw/163360/

- Mozilla difunde actualizaciones de seguridad para Firefox, Firefox ESR y Thunderbird.
https://us-cert.cisa.gov/ncas/current-activity/2021/01/27/mozilla-releases-security-updates-firefox-firefox-esr-and