@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. 148 – Año 2022

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 29/12/21 y el 4/1/22

- **La empresa noruega de medios de comunicación Amedia sufre una caída por un ciberataque.**
https://www.securityweek.com/norwegian-media-firm-amedia-suffers-disruption-due-cyberattack
- Empresa financiera *hackeada*, por log4j, se niega a pagar un rescate de 5 millones de dólares.
https://www.bleepingcomputer.com/news/security/fintech-firm-hit-by-log4j-hack-refuses-to-pay-5-million-ransom/
- La Universidad de Kioto, en Japón, pierde 77 TB de datos de investigación por un error en las copias de seguridad.
https://www.bleepingcomputer.com/news/security/university-loses-77tb-of-research-data-due-to-backup-error/
- PulseTV, de EE.UU., divulga un posible riesgo que involucra a 200.000 tarjetas de crédito.
https://www.bleepingcomputer.com/news/security/pulsetv-discloses-potential-compromise-of-200-000-credit-cards/
- Sega dejó abierta a los hackers una enorme base de datos de información de los usuarios.
https://www.techradar.com/news/sega-left-a-huge-database-of-user-information-open-to-hackers
- **La cuenta de Twitter del director de la NASA fue *hackeada* por el grupo "Poderoso Ejército Griego".**
https://securityaffairs.co/wordpress/126243/hacking/nasa-director-hacked-by-powerful-greek-army.html
- Medios de comunicación israelíes son *hackeados* en el aniversario del asesinato de Soleimani.
https://securityaffairs.co/wordpress/126267/hacking/soleimani-anniversary-attack-israeli-media.html
- **El ciberataque a la Academia de Defensa del Reino Unido causó daños importantes.**
https://www.theguardian.com/uk-news/2022/jan/02/cyber-attack-on-uks-defence-academy-caused-significant-damage
https://www.zdnet.com/article/ex-officer-reveals-cyberattack-against-uk-ministry-of-defence-training-academy/
- Los medios de comunicación portugueses "Impresa" son atacados por piratas informáticos.
https://www.reuters.com/business/media-telecom/portugals-impresa-media-outlets-hit-by-hackers-2022-01-03/
- UScellular revela la segunda violación de datos en un año.
https://securityaffairs.co/wordpress/126317/data-breach/uscellular-second-data-breach-2021.html

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

- El escáner Log4j de Microsoft Defender provoca falsas alertas positivas.
https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-log4j-scanner-triggers-false-positive-alerts/
- La vulnerabilidad número cuatro de Log4Shell: "Mucho ruido y pocas nueces".
https://nakedsecurity.sophos.com/2021/12/29/log4shell-vulnerability-number-four-much-ado-about-something/
- **Veintidós (22) estadísticas de ciberseguridad que hay que conocer para 2022.**
https://www.welivesecurity.com/2021/12/30/22-cybersecurity-statistics-know-2022/

- Nuevo Rootkit iLOBleed afecta servidores empresariales HP con ataques de borrado de datos.
https://thehackernews.com/2021/12/new-ilobleed-rootkit-targeting-hp.html
- Uber ignora la vulnerabilidad que permite enviar cualquier correo electrónico desde uber.com
https://www.bleepingcomputer.com/news/security/uber-ignores-vulnerability-that-lets-you-send-any-email-from-ubercom/
- **Los peores ciberataques de 2021.**
https://securityaffairs.co/wordpress/126253/hacking/the-worst-cyber-attacks-of-2021.html
- Detección de malware evasivo en dispositivos IoT mediante emanaciones electromagnéticas.
https://thehackernews.com/2022/01/detecting-evasive-malware-on-iot.html
- La computación cuántica es para mañana, pero el riesgo relacionado con ella ya está aquí.
https://www.securityweek.com/quantum-computing-tomorrow-quantum-related-risk-here-today
- No copie y pegue comandos de páginas web: lo pueden *hackear*.
https://www.bleepingcomputer.com/news/security/dont-copy-paste-commands-from-webpages-you-can-get-hacked/
- El *backdoor* Purple Fox se propaga a través del falso instalador de Telegram.
https://securityaffairs.co/wordpress/126299/cyber-crime/purple-fox-telegram-installer.html
- Un fallo en el software de Apple Home podría bloquearle el iPhone.
https://nakedsecurity.sophos.com/2022/01/04/apple-home-software-bug-could-lock-you-out-of-your-iphone/

NOTAS DE INTERÉS

- La APT BlackTech, vinculada a China, utiliza el nuevo malware Flagpro en sus recientes ataques.
https://securityaffairs.co/wordpress/126121/apt/blacktech-apt-flagpro-malware.html
- Ataque de criptominería aprovecha la incorrecta configuración de la API de Docker desde 2019.
https://threatpost.com/cryptomining-attack-exploits-docker-api-misconfiguration-since-2019/177299/
- LastPass asegura que ninguna contraseña se ha visto comprometida tras el incidente.
https://www.theverge.com/2021/12/28/22857485/lastpass-compromised-breach-scare
- La APT 'Aquatic Panda' tiene como objetivo universidades con herramientas para Log4Shell.
https://threatpost.com/aquatic-panda-log4shell-exploit-tools/177312/
- T-Mobile confirma que los ataques de intercambio de SIMs condujeron a una filtración.
https://www.zdnet.com/article/t-mobile-confirms-sim-swapping-attacks-led-to-breach/
- Netgear deja vulnerabilidades sin resolver en el router Nighthawk.
https://www.bleepingcomputer.com/news/security/netgear-leaves-vulnerabilities-unpatched-in-nighthawk-router/
- ¿Recuerda el efecto Y2K? Microsoft confirma un nuevo problema denominado Y2K22.
https://news.sky.com/story/remember-the-y2k-bug-microsoft-confirms-new-y2k22-issue-12507401
- **La importancia de la IoT crece rápidamente, pero su seguridad sigue siendo débil.**
https://www.securityweek.com/iots-importance-growing-rapidly-its-security-still-weak
- Asegurar las ciudades inteligentes: Lo que hay que saber.
https://www.tripwire.com/state-of-security/security-data-protection/iot/securing-smart-cities-what-you-need-to-know/

ACTUALIZACIONES DE SEGURIDAD

- Microsoft publica una solución de emergencia para el error de Exchange del año 2022.
https://thehackernews.com/2022/01/microsoft-issues-fix-for-exchange-y2k22.html