@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. 109 – 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.

15/06/2021

- El mayor distribuidor de propano de EE.UU. revela una filtración de datos de "8 segundos". https://www.bleepingcomputer.com/news/security/largest-us-propane-distributor-discloses-8-second-data-breach/
- El sospechoso de "Face of Anonymous" es deportado desde México para enfrentarse a cargos de piratería informática en Estados Unidos. https://nakedsecurity.sophos.com/2021/06/15/face-of-anonymous-suspect-deported-from-mexico-to-face-us-hacking-charges/
- CISA advierte a los fabricantes de la vulnerabilidad *ThroughTek*. https://www.zdnet.com/article/cisa-warns-manufacturers-of-throughtek-vulnerability/ https://us-cert.cisa.gov/ics/advisories/icsa-21-166-01
- **Fujifilm restablece sus operaciones tras el reciente ataque de ransomware del día 2 de junio.** https://securityaffairs.co/wordpress/119005/cyber-crime/fujifilm-ransomware-attack.html

16/06/2021

- **Un fallo en la cadena de suministro de IoT afecta a millones de cámaras.** https://www.infosecurity-magazine.com/news/iot-supply-chain-bug-millions/
- Ucrania detiene a los miembros de la banda de ransomware Clop y confisca los servidores. https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/
- El ataque con malware a entidades surcoreanas fue obra del grupo Andariel. https://thehackernews.com/2021/06/malware-attack-on-south-korean-entities.html

17/06/2021

- Un nuevo software espía se enfoca en los usuarios de Telegram y Psiphon VPN en Irán. https://thehackernews.com/2021/06/a-new-spyware-is-targeting-telegram-and.html
- Cruceros Carnival sufre una filtración de datos y alerta del riesgo de uso indebido de los mismos.
- https://www.darkreading.com/attacks-breaches/carnival-cruise-line-reports-security-breach-/d/d-id/1341335
- Las páginas web de las principales aerolíneas de Estados Unidos se ven interrumpidas. Los servicios bancarios “on line” en Australia vuelven a funcionar tras la interrupción mundial. https://www.reuters.com/business/aerospace-defense/websites-major-us-airlines-face-outage-downdetector-2021-06-17/ https://www.infosecurity-magazine.com/news/australia-suffers-widespread/

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

- Un fallo de Instagram permitía a cualquiera ver cuentas privadas sin necesidad de seguirlas.

https://thehackernews.com/2021/06/instagram-bug-allowed-anyone-to-view.html

- El código fuente del ransomware Paradise se ha publicado en un foro de hackers. https://www.bleepingcomputer.com/news/security/paradise-ransomware-source-code-released-on-a-hacking-forum/
- La vulnerabilidad de las bicicletas fijas Peloton permitía la captura completa de sus dispositivos. https://threatpost.com/peloton-bike-bug-hackers-control/166960/ https://nakedsecurity.sophos.com/2021/06/16/clop-ransomware-suspects-busted-in-ukraine-money-and-motors-seized/
- **El malware Vigilante bloquea a las víctimas para que no descarguen software pirata.** https://www.bleepingcomputer.com/news/security/vigilante-malware-blocks-victims-from-downloading-pirated-software/ https://arstechnica.com/gadgets/2021/06/newly-discovered-vigilante-malware-outs-software-pirates-and-blocks-them/
- Los Smart Switches de Cisco están plagados de graves agujeros de seguridad. https://threatpost.com/cisco-smart-switches-security-holes/167031/

NOTAS DE INTERÉS

- Google Workspace añade una nueva protección contra la suplantación de identidad y el cifrado del lado del cliente. https://www.bleepingcomputer.com/news/security/google-workspace-adds-new-phishing-protection-client-side-encryption/
- **La OTAN advierte que considerará una respuesta militar a los ciberataques.** https://www.infosecurity-magazine.com/news/nato-warns-military-response-cyber/
- Los PDFs dañinos inundan la web y conducen al robo de contraseñas. https://threatpost.com/rotten-pdfs-flood-web-password-snarfing/166932/
- Microsoft Defender ATP ahora advierte acerca de los iPhones y iPads con código de "*jailbreak*". https://www.bleepingcomputer.com/news/security/microsoft-defender-atp-now-warns-of-jailbroken-iphones-ipads/
- **Google publica herramientas y bibliotecas de código abierto para el cifrado totalmente homomórfico.** https://www.securityweek.com/google-releases-open-source-tools-and-libraries-fully-homomorphic-encryption
- La mayoría de las empresas se enfrentan a un segundo ataque de ransomware tras pagar el primero. https://www.zdnet.com/article/most-firms-face-second-ransomware-attack-after-paying-off-first/
- Cómo la IA está transformando la gobernanza de los datos en el mundo actual. https://securityaffairs.co/wordpress/119048/security/how-ai-transforming-data-governance.html
- Los investigadores descubren el 'Process Ghosting', una nueva técnica de evasión de malware. https://thehackernews.com/2021/06/researchers-uncover-process-ghosting.html

ACTUALIZACIONES DE SEGURIDAD

- Apple emite parches urgentes para fallos de día cero que se explotan en la red. https://thehackernews.com/2021/06/apple-issues-urgent-patches-for-2-zero.html https://www.bleepingcomputer.com/news/security/apple-fixes-ninth-zero-day-bug-exploited-in-the-wild-this-year/