@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. 140 – 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.

Noticias de ciberseguridad entre el 4/11/21 y el 10/11/21

- Amazon es víctima de un nuevo ataque.
https://www.infosecurity-magazine.com/news/amazon-spoofed-in-new-attack/
- Electronic Warfare, proveedor de defensa de EE.UU. se ve afectado por una filtración de datos.
https://www.bleepingcomputer.com/news/security/us-defense-contractor-electronic-warfare-hit-by-data-breach/
- El gigante minorista de la electrónica MediaMarkt sufre un ataque de ransomware.
https://www.bleepingcomputer.com/news/security/electronics-retail-giant-mediamarkt-hit-by-ransomware-attack/
- El trader Robinhood sufre una filtración de datos a través de la app, exponiendo información de 7 millones de usuarios.
https://thehackernews.com/2021/11/robinhood-trading-app-suffers-data.html
- Investigadores descubren el malware PhoneSpy, que espía a los ciudadanos surcoreanos.
https://thehackernews.com/2021/11/researchers-discover-phonespy-malware.html

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

- **CISA comparte un catálogo de 306 vulnerabilidades activamente explotadas.**
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- El fallo (CVE-2021-43267) existe en un tipo de mensaje TIPC que permite a los nodos de Linux enviar claves criptográficas entre sí.
https://threatpost.com/critical-linux-kernel-bug/176000/
- Los eventos DDoS bloqueados aumentaron un 75% en los primeros nueve meses de 2021.
https://www.helpnetsecurity.com/2021/11/05/blocked-ddos-events-up-2021/
- El papel de la IA en la seguridad moderna de los “end points” de las redes.
https://www.csoonline.com/article/3639843/the-role-of-ai-in-modern-endpoint-security.html
- La lucha por el *streaming* continúa: ¿qué pasa con las ciberamenazas?
https://securelist.com/streaming-related-cyberthreats-report-2021/104833/

NOTAS DE INTERÉS

- El CERT de Francia advierte de los ataques de ransomware Lockean contra empresas de ese país.
https://securityaffairs.co/wordpress/124171/malware/cert-fr-warns-lockean-ransomware.html
- Ucrania identifica a los agentes del FSB ruso involucrados en los ciberataques de Gamaredon.
https://www.securityweek.com/ukraine-names-russian-fsb-officers-involved-gamaredon-cyberattacks
- El Samsung Galaxy S21 fue hackeado en el segundo día del evento “Pwn2Own de Austin”.

https://www.bleepingcomputer.com/news/security/samsung-galaxy-s21-hacked-on-second-day-of-pwn2own-austin/

- Estados Unidos prohíbe el comercio con la empresa responsable del programa espía Pegasus. https://threatpost.com/pegasus-spyware-blacklisted-us/175999/
- **Microsoft acaba de ampliar su protección contra el malware para los servidores Linux.** https://www.zdnet.com/article/microsoft-just-expanded-its-malware-protection-for-linux-servers/
- El software de información sanitaria, Tasy EMR, de Philips es vulnerable a "SQL injection". https://www.bleepingcomputer.com/news/security/philips-healthcare-infomatics-solution-vulnerable-to-sql-injection/
- OneDrive dará fin al soporte bajo Windows 7 y 8, en enero próximo. https://securityaffairs.co/wordpress/124263/hacking/philips-tasy-emr-sql-injection.html
- BlackBerry descubre un broker de acceso inicial vinculado a 3 grupos de hackers distintos. https://thehackernews.com/2021/11/blackberry-uncover-initial-access.html
- El último de una larga lista de ciberataques de *hacking* de activistas, en contra de palestinos. https://www.theguardian.com/world/2021/nov/08/hacking-activists-latest-long-line-cyber-attacks-palestinians-nso-group-pegasus-spyware
- **Un dron fue modificado para afectar la red eléctrica de EE.UU. según boletín de inteligencia.** https://securityaffairs.co/wordpress/124245/security/drone-attack-u-s-power-grid.html
- El Pentágono anuncia la versión 2.0 de su polémico programa CMMC (Certificación del Modelo de Madurez de Ciberseguridad, por sus siglas en inglés). https://csoonline.com/article/3639603/pentagon-announces-version-2-0-of-its-controversial-cmmc-program.html
- **El futuro de la seguridad OT en un mundo convergente IT-OT.** https://www.theregister.com/2021/11/09/securing_ics_in_the_cloud/
- Oficial: el Gobierno de Taiwán se enfrenta a 5 millones de ciberataques diarios. https://www.securityweek.com/taiwan-government-faces-5-million-cyberattacks-daily-official

ACTUALIZACIONES DE SEGURIDAD

- Cisco ha publicado parches de seguridad para errores que afectan a varios productos. https://thehackernews.com/2021/11/hardcoded-ssh-key-in-cisco-policy-suite.html
- Se publica la versión 91.3 de Mozilla Thunderbird para corregir defectos de alto impacto. https://www.bleepingcomputer.com/news/security/mozilla-thunderbird-913-released-to-fix-high-impact-flaws/
- Las vulnerabilidades recién descubiertas en los servidores Nagios deben ser actualizadas. https://www.csoonline.com/article/3639613/update-and-isolate-your-nagios-servers-now.html
- Adobe publica actualizaciones de seguridad para varios productos. https://us-cert.cisa.gov/ncas/current-activity/2021/11/09/adobe-releases-security-updates-multiple-products
- SAP publica las actualizaciones de seguridad de noviembre de 2021. https://us-cert.cisa.gov/ncas/current-activity/2021/11/09/sap-releases-november-2021-security-updates
- Noviembre de 2021, martes de parches de Microsoft. https://isc.sans.edu/forums/diary/Microsoft+November+2021+Patch+Tuesday/28018/