@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. 132 – 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 10/09/21 y el 16/09/21

- Los datos de los clientes de MyRepublic se ven comprometidos por una brecha de seguridad de terceros.
https://www.zdnet.com/article/myrepublic-customers-compromised-in-third-party-data-breach/
- Polonia extradita a Estados Unidos al presunto operador de una red de bots.
https://www.infosecurity-magazine.com/news/poland-extradites-alleged-botnet/
- El *ransomware* BlackMatter afecta al gigante de la tecnología médica Olympus.
https://threatpost.com/blackmatter-ransomware-olympus/169423/
- **El *ransomware* REvil vuelve a atacar y hay nuevas víctimas.**
https://securityaffairs.co/wordpress/122106/cyber-crime/revil-ransomware-resumed-operations.html
- Los ciberataques se centran cada vez más en las infraestructuras críticas de Australia.
https://www.theguardian.com/technology/2021/sep/15/significant-threat-cyber-attacks-increasingly-targeting-australias-critical-infrastructure
- Tres ex oficiales de inteligencia estadounidenses admiten haber *hackeado* para los EAU.
https://www.zdnet.com/article/doj-fines-nsa-hackers-who-assisted-uae-in-attacks-on-dissidents/
- **Un ransomware encripta toda la red del Departamento de Justicia de Sudáfrica.**
https://www.bleepingcomputer.com/news/security/ransomware-encrypts-south-africas-entire-dept-of-justice-network/

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

- SOVA: Aparece un nuevo troyano bancario para Android con mayores capacidades.
https://threatpost.com/sova-sophisticated-android-trojan/169366/
- WhatsApp dejará por fin que los usuarios cifren las copias de seguridad de sus chats en la nube.
https://thehackernews.com/2021/09/whatsapp-to-finally-let-users-encrypt.html
- El nuevo ataque SpookJS elude la protección de *aislamiento* de sitios de Google Chrome.
https://thehackernews.com/2021/09/new-spookjs-attack-bypasses-google.html
- **Un defecto de Travis CI expuso los secretos de miles de proyectos de código abierto.**
https://arstechnica.com/information-technology/2021/09/travis-ci-flaw-exposed-secrets-for-thousands-of-open-source-projects/
- **OWASP actualiza el ranking de las 10 principales vulnerabilidades por primera vez desde 2017.**
https://www.zdnet.com/article/owasp-updates-top-10-vulnerability-ranking-for-first-time-since-2017/

NOTAS DE INTERÉS

- Relacionan los ataques de malware de Sidewalk con el grupo de hackers chinos Grayfly.
https://thehackernews.com/2021/09/experts-link-sidewalk-malware-attacks.html

- Google estrena las nuevas funciones de Private Compute para reforzar la seguridad de Android. https://www.zdnet.com/article/google-debuts-new-private-compute-features-to-ramp-up-android-security/
- Un tercio de los sistemas de control industrial fueron atacados en el primer semestre de 2021. https://www.infosecurity-magazine.com/news/third-industrial-control-systems/
- TikTok está eliminando los vídeos educativos de hacking. https://www.vice.com/en/article/akgppp/tiktok-hacking-learn-to-hack
- Los ataques de bots crecen un 41% en el primer semestre de 2021. https://www.zdnet.com/article/bot-attacks-grow-41-in-first-half-of-2021-lexisnexis/
- **Nueva variante de ZLoader más sigilosa que se propaga a través de falsos anuncios de descarga de TeamViewer. El virus deshabilita al Windows Defender.** https://thehackernews.com/2021/09/new-stealthier-zloader-variant.html
- Criptografía cuántica: un cable de fibra óptica lleno de aire puede transportar claves inviolables. https://www.zdnet.com/article/quantum-cryptography-this-air-filled-fiber-optic-cable-can-transport-un-hackable-keys-say-researchers/
- El futuro sin contraseña ya es presente para su cuenta de Microsoft. https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/
- Se descubren fallos críticos en la aplicación de Azure que Microsoft instaló en secreto en las máquinas virtuales de Linux. https://thehackernews.com/2021/09/critical-flaws-discovered-in-azure-app.html
- El nuevo malware Capoae tiene como blanco instalaciones de WordPress y los sistemas Linux. https://www.zdnet.com/article/new-go-malware-capoae-targets-wordpress-installs-linux-systems/

ACTUALIZACIONES DE SEGURIDAD

- WordPress anuncia una actualización de seguridad. https://us-cert.cisa.gov/ncas/current-activity/2021/09/10/wordpress-releases-security-update
- Zoom presenta nuevas funciones de seguridad. https://www.zdnet.com/article/zoom-unveils-new-security-features-including-end-to-end-encryption-for-zoom-phone-verified-identities-and-more/
- **Apple soluciona la vulnerabilidad NSO Zero-Click Zero Day. Actualizar urgente.** https://exchange.xforce.ibmcloud.com/collection/195fcf30f42ebe5cb9837dfcc150adc3
- **Actualizar Google Chrome para resolver dos nuevos fallos de día cero bajo ataque.** https://thehackernews.com/2021/09/update-google-chrome-to-patch-2-new.html
- **Kali Linux 2021.3 ya está disponible.** https://www.kali.org/blog/kali-linux-2021-3-release/
- Microsoft, “Martes de parches”, septiembre de 2021: Se han corregido varios fallos. https://www.zdnet.com/article/microsoft-september-2021-patch-tuesday-remote-code-execution-flaws-in-mshtml-open-management-fixed/
- Adobe elimina errores críticos en Acrobat y Experience Manager. https://threatpost.com/adobe-bugs-acrobat-experience-manager/169467/