@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. 123 – 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.

03/08/2021

- Un ciberataque mantiene fuera de servicio el portal italiano de registro de vacunas.
  https://www.cyberscoop.com/italy-lazio-covid-19-vaccine-registration-system/
  https://www.bleepingcomputer.com/news/security/ransomexx-ransomware-hits-italys-lazio-region-affects-covid-19-site/
- Los hackers éticos colaboran con Defensa en el Reino Unido para reforzar la ciberseguridad.
  https://www.gov.uk/government/news/ethical-hackers-collaborate-with-defence-to-strengthen-cyber-security

04/08/2021

- **El grupo de ciberespionaje chino APT31 comienza a atacar a Rusia.**
  https://www.securityweek.com/chinese-cyberspy-group-apt31-starts-targeting-russia
- Se ha detectado un malware en películas de Marvel.
  https://www.infosecurity-magazine.com/news/marvel-movie-malware-detected/

05/08/2021

- La empresa energética italiana ERG se ve afectada por el ransomware LockBit 2.0.
  https://securityaffairs.co/wordpress/120841/cyber-crime/erg-lockbit-2-0-ransomware.html
- Un afiliado del ransomware Angry Conti filtra el libro de estrategias de ataque de la banda.
  https://news-block.com/angry-conti-affiliate-ransomware-leaks-gang-attack-playbook/

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

- **DeadRinger: Descubriendo a los ciberdelincuentes chinos que atacan a las grandes empresas de telecomunicaciones**
  https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
  https://thehackernews.com/2021/08/chinese-hackers-target-major-southeast.html
- Los 10 pasos en materia de ciberseguridad.
  https://www.ncsc.gov.uk/collection/10-steps
- La NSA y el CISA publican una guía de fortalecimiento de Kubernetes.
  https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2716980/nsa-cisa-release-kubernetes-hardening-guidance/
- Errores críticos afectan la pila TCP/IP embebida, ampliamente utilizada en dispositivos de control industrial.
  https://thehackernews.com/2021/08/critical-flaws-affect-embedded-tcpip.html
- Un nuevo programa espía chino se utiliza en ataques de ciberespionaje generalizados.
  https://thehackernews.com/2021/08/new-chinese-spyware-being-used-in.html

- Los fallos de seguridad de INFRA:HALT afectan a dispositivos de control industrial críticos. https://www.bleepingcomputer.com/news/security/infra-halt-security-bugs-impact-critical-industrial-control-devices/
- Varias familias de malware dirigidas a servidores web IIS con módulos maliciosos. https://thehackernews.com/2021/08/several-malware-families-targeting-iis.html
- Error de Telegram para Mac permite guardar para siempre los mensajes que se autodestruyen. https://threatpost.com/macos-flaw-in-telegram-retrieves-deleted-messages/168412/

NOTAS DE INTERÉS

- El 92% de las empresas farmacéuticas tienen al menos una base de datos visible. https://www.helpnetsecurity.com/2021/08/03/pharmaceutical-companies-exposed-database/
- **Lista de filtraciones y ciberataques en julio de 2021: 34 millones de registros afectados.** https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-july-2021-34-million-records-breached
- **Paragon: Otro fabricante de armas cibernéticas.** https://www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/
- Google Play Protect no supera la prueba de detección de malware de AV-TEST. https://www.ehackingnews.com/2021/08/google-play-protect-fails-malware.html
- Un proyecto busca detener errores del motor JavaScript de Chrome que da lugar a exploits. https://www.zdnet.com/article/bugs-in-chromes-javascript-engine-can-lead-to-powerful-exploits-this-project-aims-to-stop-them/
- Se estima que los ataques a la cadena de suministro se multipliquen por 4 en 2021. https://www.helpnetsecurity.com/2021/08/04/supply-chain-attacks-multiply/
- Están utilizando técnicas CAPTCHA para estafar a los usuarios de correo electrónico. https://www.cyberscoop.com/captcha-email-hack-scam-proofpoint/
- One Tap de Google permite iniciar sesión en sitios web y aplicaciones sin necesidad de contraseña.
- https://www.zdnet.com/article/googles-one-tap-lets-you-sign-into-websites-and-apps-without-a-password/
- El Pentágono asegura que su nueva IA puede ver los acontecimientos "con días de antelación". https://www.zdnet.com/article/the-pentagon-says-its-new-ai-can-see-events-days-in-advance/
- Los ciberdelincuentes están manipulando la realidad para modificar el escenario de las amenazas actuales. https://www.helpnetsecurity.com/2021/08/05/cybercriminals-manipulating-reality/

ACTUALIZACIONES DE SEGURIDAD

- Cisco corrige errores críticos de alta gravedad en los routers VPN. https://thehackernews.com/2021/08/cisco-issues-critical-security-patches.html
- VMware anuncia actualizaciones de seguridad para varios productos. https://us-cert.cisa.gov/ncas/current-activity/2021/08/05/vmware-releases-security-updates-multiple-products