@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. 147 – 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 22/12/21 y el 28/12/21

- Un incidente de phishing provoca filtración de datos en hospitales de Virginia Occidental, EE.UU.
  https://www.zdnet.com/article/phishing-incident-causes-data-breach-at-west-virginia-hospitals/
- **El proveedor francés de servicios informáticos Inetum sufre un ataque de ransomware.**
  https://securityaffairs.co/wordpress/126022/cyber-crime/inetum-hit-by-blackcat-ransomware.html
- El Primer Ministro de Albania pide disculpas por la filtración de datos.
  https://www.infosecurity-magazine.com/news/albanias-prime-minister-issues/
- Los servicios de Shutterfly, de fotografía, se interrumpieron por el ataque del ransomware Conti.
  https://www.bleepingcomputer.com/news/security/shutterfly-services-disrupted-by-conti-ransomware-attack/
- La multinacional de la logística D.W. Morgan expuso 100 GB de datos de clientes, incluidos los de Fortune 500.
  https://securityaffairs.co/wordpress/126086/data-breach/d-w-morgan-data-leak.html

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

- Mitigación de Log4Shell y otras vulnerabilidades relacionadas con Log4j.
  https://www.cisa.gov/uscert/ncas/current-activity/2021/12/22/mitigating-log4shell-and-other-log4j-related-vulnerabilities
- **Un experimento de *honeypot* revela que quieren los hackers de los dispositivos IoT.**
  https://www.bleepingcomputer.com/news/security/honeypot-experiment-reveals-what-hackers-want-from-iot-devices/
- Un fallo de hace 4 años en Azure App Service expuso cientos de repositorios de código fuente.
  https://thehackernews.com/2021/12/4-year-old-bug-in-azure-app-service.html
- Cómo implementar "*machine learning*" con privacidad diferencial.
  https://www.nist.gov/blogs/cybersecurity-insights/how-deploy-machine-learning-differential-privacy
- El ransomware AvosLocker se reinicia en modo seguro para evitar las medidas de seguridad.
  https://www.bleepingcomputer.com/news/security/avoslocker-ransomware-reboots-in-safe-mode-to-bypass-security-tools/
- Nuevo malware para Android enfocado en los clientes del banco Itaú Unibanco de Brasil.
  https://thehackernews.com/2021/12/new-android-malware-targeting-brazils_27.html
- SANS Daily Network Security Podcast (28/12/2021.
  https://isc.sans.edu/podcastdetail.html?id=7812
- **Las 5 historias de amenazas informáticas más populares de 2021.**
  https://threatpost.com/5-top-threatpost-stories-2021/177278/
- El malware RedLine muestra por qué no se deben guardar las contraseñas en los navegadores.
  https://www.bleepingcomputer.com/news/security/redline-malware-shows-why-passwords-shouldnt-be-saved-in-browsers/

NOTAS DE INTERÉS

- Un nuevo fallo de Log4J completa un año de implacables crisis de ciberseguridad.
https://www.wsj.com/articles/new-log4j-flaw-caps-year-of-relentless-cybersecurity-crises-11640178004
- **NVIDIA divulga las aplicaciones afectadas por la vulnerabilidad de Log4j.**
https://www.bleepingcomputer.com/news/security/nvidia-discloses-applications-impacted-by-log4j-vulnerability/
- El ransomware Conti se aprovecha de la vulnerabilidad Log4Shell para recaudar millones.
https://www.techrepublic.com/article/conti-ransomware-is-exploiting-the-log4shell-vulnerability-to-the-tune-of-millions/
- PCI SSC actualiza su norma de seguridad de dispositivos para los HSM.
https://www.helpnetsecurity.com/2021/12/23/pci-ssc-hsms/
- Investigadores revelan vulnerabilidades sin parches en el software de Microsoft Teams.
https://thehackernews.com/2021/12/researchers-disclose-unpatched.html
- **El organismo regulador de telecomunicaciones de China puso en pausa su asociación con Alibaba.**
https://www.bbc.com/news/technology-59760486
https://www.infosecurity-magazine.com/news/alibaba-suffers-governmen
- Uso abusivo de Telegram para robar credenciales de criptocarteras.
https://threatpost.com/telegram-steal-crypto-wallet-credentials/177266/
- El soft espía NSO fue utilizado para *hackear* a políticos polacos, la esposa de Khashoggi y a otros.
https://www.zdnet.com/article/nso-spyware-used-to-hack-polish-politicians-wife-of-khashoggi-un-war-crimes-investigator-and-more/
- El sigiloso malware BLISTER se cuela inadvertidamente en los sistemas Windows.
https://thehackernews.com/2021/12/new-blister-malware-using-code-signing.html
- **El motor de búsqueda basado en la privacidad DuckDuckGo creció un 46% en 2021.**
https://www.bleepingcomputer.com/news/technology/privacy-focused-search-engine-duckduckgo-grew-by-46-percent-in-2021/
- Las descargas piratas de 'Spider-Man: No Way Home' contienen malware de minería de criptomonedas.
https://thehackernews.com/2021/12/spider-man-no-way-home-pirated.html
- **Los detectores de metales Garrett Walk-Through pueden ser *hackeados* a distancia.**
https://thehackernews.com/2021/12/garrett-walk-through-metal-detectors.html
- Seis innovaciones tecnológicas en materia de seguridad que nos entusiasma ver en 2022.
https://www.darkreading.com/dr-tech/6-security-tech-innovations-we-re-excited-to-see-in-2022
- Nueva ola de ataques ransomware **ech0raix** tiene como objetivo los dispositivos NAS de QNAP.
https://securityaffairs.co/wordpress/126081/malware/ech0raix-ransomware-targeting-qnap-nas.html
- Apps de streaming, de alto riesgo, para Android se encuentran en la tienda Galaxy de Samsung.
https://www.bleepingcomputer.com/news/security/riskware-android-streaming-apps-found-on-samsungs-galaxy-store/#.YctYCe-GRCs.twitter
- Ese juguete que le regalaron por Navidad podría estar espiándole.
https://threatpost.com/toy-christmas-spying/177288/

ACTUALIZACIONES DE SEGURIDAD

- La nueva actualización de seguridad de Apache para el servidor HTTP corrige dos fallos.
https://www.zdnet.com/article/apaches-new-security-update-for-http-server-fixes-two-flaws/