@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. 87/2021

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.

26/03/2021

- El Parlamento alemán vuelve a ser objetivo de los hackers estatales rusos.
  https://www.cyberscoop.com/bundestag-germany-hackers-ghostwriter/
  https://securityaffairs.co/wordpress/116001/apt/german-parliament-bundestag-russia-hackers.html
- Un proveedor de servicios de salud que ha sido objeto de phishing emprende acciones legales contra Amazon.
  https://www.infosecurity-magazine.com/news/saluscare-takes-legal-action/
- Un nuevo malware para Android espía mientras se hace pasar por una actualización del sistema.
  https://www.bleepingcomputer.com/news/security/new-android-malware-spies-on-you-while-posing-as-a-system-update/
  https://arstechnica.com/gadgets/2021/03/new-android-malware-with-full-range-of-spying-capabilities-has-been-found/

27/03/2021

- Los operadores del ransomware Hades están a la caza de grandes empresas en Estados Unidos.
  https://www.zdnet.com/article/hades-ransomware-operators-are-hunting-big-game-in-the-us/
  https://www.ehackingnews.com/2021/03/hades-ransomware-attacks-us-big-game.html
- Un atacante tiene como blanco a Guns.com y vuelca información sensible en la Dark Web.
  https://www.ehackingnews.com/2021/03/threat-actor-targets-gunscom-spills.html

28/03/2021

- Channel Nine, de Australia, sufre un "sofisticado y selectivo" ataque de piratería informática.
  https://www.dailymail.co.uk/news/article-9411131/Channel-Nine-falls-victim-targeted-cyber-attack.html
  https://securityaffairs.co/wordpress/116053/breaking-news/channel-nine-cyber-attack.html
- Una propuesta de orden ejecutiva de la administración Biden de EE.UU. obligaría a revelar las violaciones de seguridad que afecten a los usuarios del Gobierno.
  https://securityaffairs.co/wordpress/116033/security/executive-order-data-breach.html
- La conocida biblioteca *npm netmask* tiene una vulnerabilidad de red crítica.
  https://www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/

29/03/2021

- El servidor Git de PHP ha sido hackeado para introducir una puerta trasera secreta en su código fuente.
  https://thehackernews.com/2021/03/phps-git-server-hacked-to-insert-secret.html
- Presuntos piratas informáticos rusos accedieron a correos electrónicos de la seguridad nacional de Estados Unidos.

https://www.theguardian.com/us-news/2021/mar/29/solarwinds-suspected-russian-hackers-email-access-dhs

- Los defectos en las RTU Ovarro TBox podrían abrir los sistemas industriales a ataques remotos. https://thehackernews.com/2021/03/flaws-in-ovarro-tbox-rtus-could-open.html

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

- Un nuevo defecto del 5G expone a redes principales a la localización y otros ataques. https://thehackernews.com/2021/03/new-5g-flaw-exposes-priority-networks.html
- El FBI expone la debilidad del ransomware Mamba o DiskCryptor. https://www.bleepingcomputer.com/news/security/fbi-exposes-weakness-in-mamba-ransomware-diskcryptor/
- Kaspersky observa un aumento de los ataques de ransomware contra dispositivos ICS (Industrial Control System) en los países en desarrollo, entre ellos Argentina. https://www.securityweek.com/kaspersky-sees-rise-ransomware-attacks-ics-devices-developed-countries
- Análisis de malware con "*elastic-agent*" y Microsoft Sandbox. https://isc.sans.edu/diary/rss/27248
- No he *hackeado* su servidor MS Exchange. https://krebsonsecurity.com/2021/03/no-i-did-not-hack-your-ms-exchange-server/

NOTAS DE INTERÉS

- Se descubre otro fallo crítico de RCE en la plataforma Orion de SolarWinds. https://thehackernews.com/2021/03/solarwinds-orion-vulnerability.htmll https://www.bleepingcomputer.com/news/security/solarwinds-patches-critical-code-execution-bug-in-orion-platform/
- La sofisticada campaña de *hackeo* a Windows, Android e iOS fue en realidad obra de "operativos gubernamentales occidentales". https://gizmodo.com/turns-out-this-sophisticated-hacker-campaign-was-actual-1846561206
- El CIO de las Fuerzas Aéreas de EE.UU. trabajan en actividades fundamentales de confianza cero. https://www.nextgov.com/cybersecurity/2021/03/air-force-working-foundational-zero-trust-activities-cio-says/172955/
- El cable submarino de Facebook impulsará el Internet del sudeste asiático. https://www.bbc.com/news/technology-56565348

ACTUALIZACIONES DE SEGURIDAD

- Avisos de seguridad de Cisco 24 de marzo de 2021. https://exchange.xforce.ibmcloud.com/collection/67884a00c72311f9f97bb576d3cd51ba https://us-cert.cisa.gov/ncas/current-activity/2021/03/25/cisco-releases-security-updates
- OpenSSL publica parches para dos vulnerabilidades de seguridad de alta gravedad. https://thehackernews.com/2021/03/openssl-releases-patches-for-2-high.html
- iOS 14.4.2: Aviso emitido de nueva actualización a todos los usuarios de iPhone. https://support.apple.com/en-us/HT212256 https://www.zdnet.com/article/apple-releases-emergency-update-for-iphones-ipads-and-apple-watch/ https://securityaffairs.co/wordpress/116007/security/apple-zero%E2%80%91day.html