@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. 78/2021

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.

19/02/2021

- Se encontró un misterioso malware denominado Silver Sparrow en 30 mil Macs.
  https://threatpost.com/silver-sparrow-malware-30k-macs/164121/
  https://arstechnica.com/information-technology/2021/02/new-malware-found-on-30000-macs-has-security-pros-stumped/
- El gigante de la certificación Underwriters Laboratories (UL) es víctima de un ransomware.
  https://www.bleepingcomputer.com/news/security/underwriters-laboratories-ul-certification-giant-hit-by-ransomware/

20/02/2021

- En Brasil la empresa Experian sufre una fuga masiva de datos.
  https://www.zdnet.com/article/experian-challenged-over-massive-data-leak-in-brazil/
- Una falla de seguridad del navegador Brave expone el historial de sus usuarios en la *dark web*.
  https://thehackernews.com/2021/02/privacy-bug-in-brave-browser-exposes.html

21/02/2021

- Sequoia Capital informó a los inversores que había sido hackeada.
  https://www.ehackingnews.com/2021/02/sequoia-capital-told-investors-it-was.html
- La Universidad de Lakehead cierra la red del campus tras un ciberataque.
  https://www.bleepingcomputer.com/news/security/lakehead-university-shuts-down-campus-network-after-cyberattack/

22/02/2021

- Hackers chinos clonaron una herramienta de ataque perteneciente al grupo Equation de la NSA.
  https://www.zdnet.com/article/chinese-hackers-cloned-attack-tools-belonging-to-nsas-equation-group/
  https://thehackernews.com/2021/02/chinese-hackers-had-access-to-us.html
- Ucrania acusa a las redes rusas de nuevos ciberataques masivos.
  https://www.reuters.com/article/us-ukraine-cyber/ukraine-accuses-russian-networks-of-new-massive-cyber-attacks-idUSKBN2AM1VF

23/02/2021

- Una nueva clase de ciberdelincuentes se infiltra en las organizaciones y luego vende el acceso.
  https://betanews.com/2021/02/23/new-cybercriminal-breaches-organizations-sells-access/
- Agencias de salud y transporte australianas afectadas por el hacking de Accellion. Se publican datos del fabricante de aviones Bombardier afectados por el mismo ataque.
  https://www.securityweek.com/australian-health-and-transport-agencies-hit-accellion-hack
  https://www.zdnet.com/article/airplane-maker-bombardier-data-posted-on-ransomware-leak-site-following-fta-hack/

24/02/2021

- La NASA y la FAA también fueron vulneradas por los atacantes de SolarWinds.
https://www.bleepingcomputer.com/news/security/nasa-and-the-faa-were-also-breached-by-the-solarwinds-hackers/

25/02/2021

- Ciberespías chinos atacaron a tibetanos con un complemento malicioso instalado en Firefox.
https://www.zdnet.com/article/chinese-cyberspies-targeted-tibetans-with-a-malicious-firefox-add-on/

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

- Se descubre un nuevo programa espía en Android vinculado al conflicto entre India y Pakistán.
https://blog.lookout.com/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict
- Informe de análisis de malware NCAS AR21-048D - AppleJeus: Kupay Wallet.
https://exchange.xforce.ibmcloud.com/collection/05a1ba7a3c289a30daf278249a6e9aee
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048d
- Estados Unidos enfrenta un problema con el GPS.
https://www.schneier.com/blog/archives/2021/02/gps-vulnerabilities.html
https://www.nytimes.com/2021/01/23/opinion/gps-vulnerable-alternatives-navigation-critical-infrastructure.html
- CrowdStrike elaboró una lista de conexiones y cómo ciberdelincuentes cooperan entre sí.
https://www.zdnet.com/article/this-chart-shows-the-connections-between-cybercrime-groups/

NOTAS DE INTERÉS

- Cómo minimizar las consecuencias de un ataque de ransomware corporativo.
https://usa.kaspersky.com/blog/ransomware-attack-what-to-do/24259/
- Podcast diario de seguridad de redes de SANS (Stormcast) del lunes 22 de febrero de 2021.
https://isc.sans.edu/podcastdetail.html?id=7382
- WhatsApp desactivará los mensajes de todos los usuarios que rechacen las nuevas condiciones.
https://www.bbc.com/news/technology-56154543
- Ataques “shadow” permiten a los agresores sustituir el contenido de PDF firmados digitalmente.
https://thehackernews.com/2021/02/shadow-attacks-let-attackers-replace.html
- Twitter borra cuentas vinculadas a operaciones de propaganda rusas e iraníes.
https://www.cyberscoop.com/russia-iran-influence-operations-takedowns-twitter/

ACTUALIZACIONES DE SEGURIDAD

- Actualizaciones de Chrome.
https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html
- La actualización de Telegram para Windows 10 trae una nueva función de privacidad.
https://www.bleepingcomputer.com/news/software/telegram-for-windows-10-update-brings-a-new-privacy-feature/
- VMware corrige un error crítico de RCE en todas las instalaciones por defecto del vCenter.
https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-all-default-vcenter-installs/