@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. 91/2021

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.

13/04/2021

- Millones de dispositivos IoT en peligro por los bugs del DNS NAME:WRECK.
  https://www.computerweekly.com/news/252499233/Millions-of-devices-at-risk-from-NAMEWRECK-DNS-bugs
  https://securityaffairs.co/wordpress/116734/reports/namewreck-flaws.html
- Alrededor de 500.000 dispositivos Huawei son afectados por el malware Joker.
  https://www.ehackingnews.com/2021/04/500000-huawei-devices-hit-by-joker.html
- Nuevo malware para Linux y macOS oculto en un falso paquete NPM de Browserify.
  https://www.bleepingcomputer.com/news/security/new-linux-macos-malware-hidden-in-fake-browserify-npm-package/
- La NSA indica que ha encontrado nuevas vulnerabilidades críticas en Microsoft Exchange Server.
  https://www.cyberscoop.com/nsa-microsoft-exchange-server-vulnerabilities/
  https://us-cert.cisa.gov/ncas/alerts/aa21-062a

14/04/2021

- **El FBI *hackea* cientos de servidores del gobierno de EE.UU. infectados (y los desinfecta).**
  https://nakedsecurity.sophos.com/2021/04/14/fbi-hacks-into-hundreds-of-infected-us-servers-and-disinfects-them/
  https://www.cyberscoop.com/fbi-court-order-microsoft-exchange-server-web-shells/
  https://www.theverge.com/2021/4/13/22382821/fbi-doj-hafnium-remote-access-removal-hack
- Los bugs de WhatsApp podrían haber habilitado a los atacantes *hackear* tu teléfono de manera remota.
  https://thehackernews.com/2021/04/new-whatsapp-bug-couldve-let-attackers.html
- Se utilizan 100.000 sitios de Google para instalar el RAT de SolarMarket.
  https://threatpost.com/google-sites-solarmarket-rat/165396/
- El segundo exploit de día cero de Google Chrome apareció en Twitter esta semana.
  https://www.bleepingcomputer.com/news/security/second-google-chrome-zero-day-exploit-dropped-on-twitter-this-week/

15/04/2021

- **Estados Unidos impone sanciones a Rusia por los ciberataques a SolarWinds.**
  https://news.sky.com/story/us-set-to-impose-new-russia-sanctions-and-expel-officials-over-huge-solarwinds-hacking-attack-12275798
  https://www.cyberscoop.com/nsa-fbi-dhs-russian-hacking-svr-solarwinds-apt29-cozy-bear/
  https://www.theverge.com/2021/4/15/22385371/russia-sanctions-solarwinds-biden-white-house-putin-hack
  https://securityaffairs.co/wordpress/116866/cyber-warfare-2/us-sanctions-russia-solarwinds.html
- La Universidad de Hertfordshire sufre un ciberataque que hace caer toda su red informática.

https://www.infosecurity-magazine.com/news/uni-hertfordshire-cyber-attack-it/

- La red de bots Gafgyt utiliza los trucos DDoS de Mirai.
https://threatpost.com/gafgyt-botnet-ddos-mirai/165424/
- El popular mercado NFT Rarible es blanco de estafadores y malware.
https://www.bleepingcomputer.com/news/microsoft/popular-nft-marketplace-rarible-targeted-by-scammers-and-malware/

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

- Podcast diario de seguridad de redes de SANS (Stormcast) del martes 13 de abril de 2021.
https://isc.sans.edu/podcastdetail.html?id=7454
- El malware BRATA se hace pasar por un escáner de seguridad para Android en Google Play Store.
https://thehackernews.com/2021/04/brata-malware-poses-as-android-security.html
- Las vulnerabilidades del DNS NAME:WRECK afectan a más de 100 millones de dispositivos.
https://www.bleepingcomputer.com/news/security/name-wreck-dns-vulnerabilities-affect-over-100-million-devices/
https://www.zdnet.com/article/these-new-vulnerabilities-millions-of-iot-devives-at-risk-so-patch-now/
- Detección del "próximo" ciberataque al estilo de SolarWinds.
https://thehackernews.com/2021/04/detecting-next-solarwinds-attack.html

NOTAS DE INTERÉS

- El navegador Brave desactiva el sistema de seguimiento FLoC de Google.
https://www.zdnet.com/article/brave-browser-disables-googles-floc-tracking-system/
- FireEye: en 2020 se rastrearon 650 nuevos grupos de piratas informáticos peligrosos.
https://securityaffairs.co/wordpress/116813/cyber-crime/fireeye-report-650-new-threat-groups.html
- La ciberseguridad en un mundo post-pandémico.
https://cybernews.com/security/cybersecurity-in-a-post-pandemic-world/
- Ahora un nuevo exploit de JavaScript permite realizar ataques al DDR4 Rowhammer.
https://thehackernews.com/2021/04/new-javascript-exploit-can-now-carry.html
- Un ataque ransomware provoca escasez de queso en Holanda.
https://threatpost.com/ransomware-cheese-shortages-netherlands/165407/

ACTUALIZACIONES DE SEGURIDAD

- Adobe resuelve vulnerabilidades críticas en Photoshop y Digital Editions.
https://us-cert.cisa.gov/ncas/current-activity/2021/04/13/adobe-releases-security-updates
- **Microsoft tiene un agitado martes de “parches” con Zero-Days y correcciones para Exchange.**
https://threatpost.com/microsoft-april-patch-tuesday-zero-days/165393/
- Google Chrome 90 se publicó con HTTPS como protocolo por defecto.
https://www.bleepingcomputer.com/news/google/google-chrome-90-released-with-https-as-the-default-protocol/
- SAP ha publicado sus parches de seguridad de abril de 2021 para diversos productos.
https://exchange.xforce.ibmcloud.com/collection/38f143609a480056e9ea1f44478d99bc