@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. 90/2021

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.

09/04/2021

- Un adware se propaga a través de una falsa aplicación de TikTok y de ofertas de ordenadores portátiles.
  https://threatpost.com/adware-tiktok-laptop-offers/165318/
- El grupo de cosméticos Pierre Fabre sufre un ataque de ransomware de 25 millones de dólares.
  https://www.bleepingcomputer.com/news/security/leading-cosmetics-group-pierre-fabre-hit-with-25-million-ransomware-attack/
- Alerta - Hay un nuevo malware, *"Saint Bot"*, que roba las contraseñas de los usuarios.
  https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html
- La mayor asociación de patólogos del mundo revela un incidente con una tarjeta de crédito.
  https://www.bleepingcomputer.com/news/security/worlds-largest-pathologists-association-discloses-credit-card-incident/
- Se venden en la *dark web* 330.000 tarjetas de pago y 895.000 tarjetas de regalo robadas.
  https://securityaffairs.co/wordpress/116558/deep-web/gift-cards-sold-dark-web.html
- Hackers manipularon la *tienda* APKPure para distribuir apps con malware.
  https://thehackernews.com/2021/04/hackers-tampered-with-apkpure-store-to.html

10/04/2021

- El malware Joker infecta más de 500.000 dispositivos Android de Huawei.
  https://www.bleepingcomputer.com/news/security/joker-malware-infects-over-500-000-huawei-android-devices/
- El FBI ha detenido a un hombre por planear un supuesto atentado contra Amazon Web Services (AWS) para acabar con cerca del 70% de la red Internet.
  https://securityaffairs.co/wordpress/116612/cyber-crime/plot-bomb-attack-aws.html

11/04/2021

- El CEO de Clubhouse asegura que los datos de los usuarios no se filtraron.
  https://www.theverge.com/2021/4/11/22378302/personal-information-1-million-clubhouse-users-leaked-privacy-security
- Se produjo un "accidente" en la red de distribución de electricidad de la instalación nuclear iraní de Natanz y los expertos especulan que fue causado por un ciberataque.
  https://securityaffairs.co/wordpress/116668/cyber-warfare-2/iran-accident-natanz-cyberattack.html

12/04/2021

- Windows, Ubuntu, Zoom, Safari y MS Exchange fueron hackeados en el concurso Pwn2Own 2021.
  https://thehackernews.com/2021/04/windows-ubuntu-zoom-safari-ms-exchange.html

- **Irán califica el corte de energía de la planta atómica de Natanz de "terrorismo nuclear".**
https://www.securityweek.com/iran-calls-natanz-atomic-site-blackout-nuclear-terrorism
https://www.ehackingnews.com/2021/04/iran-natanz-nuclear-facility-struck-by.html

- Apple y Google bloquean la actualización oficial de la aplicación COVID-19 del Reino Unido.
https://nakedsecurity.sophos.com/2021/04/12/apple-and-google-block-official-uk-covid-19-app-update/

- IcedID circula a través de formularios web y URLs de Google
https://threatpost.com/icedid-web-forms-google-urls/165347/

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

- CISA publica un nuevo panel de detección de amenazas (*"Aviary"*).
https://www.darkreading.com/analytics/cisa-launches-new-threat-detection-dashboard/d/d-id/1340638
https://us-cert.cisa.gov/ncas/current-activity/2021/04/08/using-aviary-to-analyze-post-compromise-threat-activity

- Fallo de seguridad de Zoom: A la espera el parche los hackers pueden tomar el control de tu PC.
- https://www.ehackingnews.com/2021/04/zoom-security-flaw-now-hackers-can-take.html

NOTAS DE INTERÉS

- Vídeo: Un mono utiliza el Neuralink de Elon Musk para jugar al Pong con su mente.
https://www.bleepingcomputer.com/news/technology/watch-monkey-uses-elon-musks-neuralink-to-play-pong-with-its-mind/

- Estados Unidos incluye en la lista negra a siete grupos de superordenadores chinos.
https://www.bbc.com/news/business-56685136

- Un informe de los servicios de inteligencia de EE.UU. advierte del aumento de ciberataques y de la desinformación en todo el mundo.
https://www.cyberscoop.com/us-intelligence-report-warns-of-increased-offensive-cyber-disinformation-around-the-world/

- LifeLabs presenta un programa de divulgación de vulnerabilidades.
https://www.infosecurity-magazine.com/news/lifelabs-launches-vulnerability/

- Q Link Wireless hizo accesible la información privada de los clientes con sólo un número de teléfono.
https://www.theverge.com/2021/4/9/22376452/q-link-wireless-hello-mobile-customer-data-unlocked-no-password-phone-number

- Linux podría funcionar en los chips M1 de Apple en pocos meses.
https://betanews.com/2021/04/11/linux-could-run-on-apple-m1-chips-in-just-a-few-months/

ACTUALIZACIONES DE SEGURIDAD

- Boletín de seguridad de Android - Abril 2021.
https://exchange.xforce.ibmcloud.com/collection/8fc189529860972561d0fd3e55c249ad
https://source.android.com/security/bulletin/2021-04-01

- Índice de parches prioritarios, según Tripwire, para marzo de 2021.
https://www.tripwire.com/state-of-security/vert/tripwire-patch-priority-index-for-march-2021/

- Actualizaciones sobre las vulnerabilidades de Microsoft Exchange Server.
https://us-cert.cisa.gov/ncas/current-activity/2021/04/12/updates-microsoft-exchange-server-vulnerabilities