@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. 92/2021

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.

16/04/2021

- El malware BazarLoader se aprovecha de las nubes de Slack y BaseCamp.
  https://threatpost.com/bazarloader-malware-slack-basecamp/165455/
- El bitcoin cae después de que Turquía prohíba los pagos con criptomonedas, por sus riesgos.
  https://www.reuters.com/technology/turkey-bans-use-cryptocurrencies-payments-sends-bitcoin-down-2021-04-16/
- Resumen semanal de ransomware.
  https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-16th-2021-the-houston-rockets/
- La Universidad de Swinburne, en Melbourne, Australia, confirma que más de 5.000 personas se han visto afectadas por una filtración de datos.
  https://www.zdnet.com/article/swinburne-university-confirms-over-5000-individuals-affected-in-data-breach/

17/04/2021

- Una importante intrusión en BGP interrumpe a miles de redes en todo el mundo.
  https://www.bleepingcomputer.com/news/security/major-bgp-leak-disrupts-thousands-of-networks-globally/
- Twitter está sufriendo en el día de hoy otra interrupción mundial.
  https://www.bleepingcomputer.com/news/technology/twitter-is-suffering-from-another-worldwide-outage-today/
- La enseñanza en línea de la Universidad de Hertfordshire se ve interrumpida por un grave ciberataque.
  https://www.ehackingnews.com/2021/04/online-learning-of-university-of.html

18/04/2021

- La empresa de pruebas de código CodeCov sufre una filtración de datos que no fue detectada durante meses.
  https://www.ehackingnews.com/2021/04/the-code-testing-company-codecov.html
  https://www.theverge.com/2021/4/18/22390379/federal-investigators-breach-software-codecov-solarwinds

19/04/2021

- La OTAN pone a prueba su defensa contra los ataques combinados de ciber desinformación.
  https://www.cyberscoop.com/nato-blended-cyber-disinformation-defense-locked-shields-article-v/
- El proveedor de seguros de automóviles Geico ha sufrido una intrusión de sus datos.
  https://www.bleepingcomputer.com/news/security/geico-data-breach-exposed-customers-drivers-license-numbers/

- Los hackers de "Gamaredon" atacan a funcionarios ucranianos en medio de las crecientes tensiones con Rusia.
https://www.cyberscoop.com/gamaredon-russia-ukraine-border-primitive-bear/
- Ahora el grupo APT Lazarus utiliza imágenes BMP para ocultar malware RAT.
https://thehackernews.com/2021/04/lazarus-apt-hackers-are-now-using-bmp.html

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

- El malware HackBoss se hace pasar por herramientas para hackers en Telegram para robar monedas digitales.
https://www.bleepingcomputer.com/news/security/hackboss-malware-poses-as-hacker-tools-on-telegram-to-steal-digital-coins/
- Se informa de la existencia de graves fallas en la pila EtherNet/IP de sistemas industriales.
https://thehackernews.com/2021/04/severe-bugs-reported-in-ethernetip.html
- El juego infantil Morph para iOS se convierte en un criptocasino clandestino.
https://threatpost.com/ios-kids-game-crypto-casino/165450/
- La acción del ransomware Ryuk actualiza las técnicas de hacking.
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-operation-updates-hacking-techniques/
- Aplicaciones Android maliciosas enfocadas a los usuarios de JIO Telecom en la India.
https://exchange.xforce.ibmcloud.com/collection/990a238dc4fe1037c65c1abfac553dc8
https://www.zscaler.com/blogs/security-research/android-apps-targeting-jio-users-india
- Se descubren vulnerabilidades de ejecución remota de código (RCE) en una freidora por aire inteligente (Smart air fryer, sin aceite).
https://www.zdnet.com/article/remote-code-execution-vulnerabilities-uncovered-in-smart-air-fryer/

NOTAS DE INTERÉS

- **La primera red cuántica de varios nodos prepara el camino para la Internet cuántica.**
https://www.zdnet.com/article/first-multi-node-quantum-network-pavis-the-way-for-the-quantum-internet/
- NSA: 5 errores de seguridad bajo el ciberataque activo de un estado nacional.
https://threatpost.com/nsa-security-bugs-active-nation-state-cyberattack/165446/
- La actualización del ransomware REvil cambia las contraseñas de Windows para que el cifrado de archivos se realice de forma automática a través del modo seguro.
https://www.techrepublic.com/article/update-to-revil-ransomware-changes-windows-passwords-to-automate-file-encryption-via-safe-mode/
- Actualmente el malware XCSSET se centra en macOS 11 y en los Mac basados en M1.
https://securityaffairs.co/wordpress/116983/malware/xcsset-malware-apple-m1.html

ACTUALIZACIONES DE SEGURIDAD

- Microsoft corrige el error de Windows 10 que puede corromper las unidades NTFS.
https://www.bleepingcomputer.com/news/security/microsoft-fixes-windows-10-bug-that-can-corrupt-ntfs-drives/