@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. 94/2021

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.

2304/2021

- ToxicEye: Este troyano utiliza la plataforma Telegram para robar datos.
  https://www.zdnet.com/article/toxiceye-trojan-abuses-telegram-platform-to-steal-your-data/
- Las autoridades de Taiwán investigan el hackeo a proveedores de Apple.
  https://www.bbc.com/news/technology-56846361
- Twitter alarma a los usuarios con mensajes que se asemejan a correos electrónicos de phishing.
  https://www.cyberscoop.com/twitter-phishing-confirm-email-mistake/
- Informe semanal sobre amenazas 23 de abril de 2021 del NSCS de Gran Bretaña.
  https://www.ncsc.gov.uk/report/weekly-threat-report-23rd-april-2021
- EE.UU. alerta a Irlanda que es un objetivo para los ciberdelincuentes.
  https://www.infosecurity-magazine.com/news/ireland-target-cyber-criminals/#.YIMYRAene78.twitter

24/04/2021

- Se ha encontrado un error RCE crítico en el gestor de paquetes Homebrew para macOS y Linux.
  https://thehackernews.com/2021/04/critical-rce-bug-found-in-homebrew.html
- La actualización del gestor de contraseñas australiano Passwordstate ha sido pirateada, instalando un *backdoor* en miles de ordenadores.
  https://thehackernews.com/2021/04/passwordstate-password-manager-update.html

25/04/2021

- El malware Emotet del grupo TA542 ha sido removido hoy a la fuerza, por la policía alemana.
  https://www.bleepingcomputer.com/news/security/emotet-malware-forcibly-removed-today-by-german-police-update/
- Hackers tienen como objetivo los servidores dedicados a compartir archivos de Soliton FileZen.
  https://securityaffairs.co/wordpress/117208/hacking/soliton-filezen-file-sharing-servers.html

26/04/2021

- El CEO de la bolsa de criptomonedas Thodex se fuga con 2.000 millones de dólares en fondos de clientes. La bolsa afirma que tales informes son "infundados".
  https://www.zdnet.com/article/thodex-cryptocurrency-exchange-founder-allegedly-goes-on-the-run-with-2bn-in-client-funds/
- Se filtraron 3.200 millones de contraseñas con 1,5 millones de registros con correos electrónicos de distintos gobiernos.
  https://thehackernews.com/2021/04/32-billion-leaked-passwords-contain-15.html
- La policía de Washington DC, EE.UU., confirma un ciberataque tras la filtración de datos por parte de una banda de ransomware.

https://www.bleepingcomputer.com/news/security/dc-police-confirms-cyberattack-after-ransomware-gang-leaks-data/

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

- Un nuevo malware de criptominería construye un ejército de bots para Windows y Linux.
https://www.bleepingcomputer.com/news/security/new-cryptomining-malware-builds-an-army-of-windows-linux-bots/
- La red de bots Prometei podría desencadenar ataques del estilo APT.
https://threatpost.com/prometei-botnet-apt-attacks/165574/
https://thehackernews.com/2021/04/prometei-botnet-exploiting-unpatched.html
- AirDrop de Apple tiene una "importante vulnerabilidad", según investigadores alemanes.
https://nakedsecurity.sophos.com/2021/04/23/apple-airdrop-has-significant-privacy-leak-say-german-researchers/
https://www.cyberscoop.com/apple-air-drop-security-hackers/
https://arstechnica.com/gadgets/2021/04/apples-airdrop-leaks-users-pii-and-theres-not-much-they-can-do-about-it/
- **Evil Maid Attack - Armado de una inofensiva aspiradora, esconde en su interior un pequeño dispositivo en una Raspberry Pi.**
https://securityaffairs.co/wordpress/117139/hacking/evil-maid-attack-vacuum-hack.html
-

NOTAS DE INTERÉS

- El Pentágono habría dado a una pequeña empresa el control de sus direcciones IP para encontrar problemas de seguridad.
https://www.theverge.com/2021/4/24/22401339/pentagon-ip-addresses-security-department-defense
- China podría "controlar el sistema operativo global" tecnológico, advierte el jefe de espionaje del Reino Unido.
https://www.zdnet.com/article/china-could-control-the-global-operating-system-of-tech-warns-uk-spy-chief/
- El ransomware está creciendo a un ritmo alarmante, advierte el jefe del GCHQ.
https://www.zdnet.com/article/ransomware-is-growing-at-an-alarming-rate-warns-gchq-chief/
- Una nueva cepa de ransomware llamada "Qlocker" tiene como objetivo los dispositivos de almacenamiento en red (NAS) de QNAP.
https://thehackernews.com/2021/04/new-qnap-nas-flaws-exploited-in-recent.html
- Adobe presenta una "ventanilla única" de código abierto para la detección de amenazas de seguridad y anomalías en los datos.
https://www.zdnet.com/article/adobe-releases-open-source-one-stop-shop-for-security-threat-data-anomaly-detection/

ACTUALIZACIONES DE SEGURIDAD

- iOS 14.5: Aviso de actualización para todos los usuarios de iPhone.
https://www.forbes.com/sites/kateoflahertyuk/2021/04/26/ios-145-update-now-warning-issued-to-all-iphone-users/