@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. 163 – Año 2022

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.

Noticias de ciberseguridad entre el 18/4/22 y el 24/4/22

- El sistema de financiación descentralizado y basado en créditos, *Beanstalk*, pierde 182 millones de dólares en un ataque "flash loan" (préstamos instantáneos).
  https://www.theverge.com/2022/4/18/23030754/beanstalk-cryptocurrency-hack-182-million-dao-voting
- Descubren ataques de spyware contra políticos y activistas catalanes.
  https://thehackernews.com/2022/04/experts-uncover-spyware-attacks-against.html
- El sitio web de la Autoridad Aeroportuaria de Israel es objeto de un presunto ciberataque por parte de piratas informáticos proiraníes.
  https://www.timesofisrael.com/airports-authority-website-targeted-by-pro-iranian-hackers-in-suspected-cyberattack/

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

- Que el phishing vuelva crecer. Los archivos *office* VSTO son la nueva pesadilla de las macros.
  https://medium.com/@airlockdigital/make-phishing-great-again-vsto-office-files-are-the-new-macro-nightmare-e09fcadef010
- Nueva variante del malware SolarMarker utiliza técnicas actualizadas para pasar desapercibido.
  https://thehackernews.com/2022/04/new-solarmarker-malware-variant-using.html
- Una reciente variante del malware BotenaGo se centra en los dispositivos DVR.
  https://www.bleepingcomputer.com/news/security/new-stealthy-botenago-malware-variant-targets-dvr-devices/
- Los hackers estatales rusos atacan a Ucrania con nuevas variantes de malware.
  https://www.bleepingcomputer.com/news/security/russian-state-hackers-hit-ukraine-with-new-malware-variants/
- **Servidores de Microsoft Exchange son hackeados para distribuir el ransomware Hive.**
  https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
- El grupo TeamTNT tiene como objetivo AWS y Alibaba.
  https://blog.talosintelligence.com/2022/04/teamtnt-targeting-aws-alibaba.html

NOTAS DE INTERÉS

- Citizen Lab ha descubierto un nuevo exploit "zero-click" de iMessage utilizado para instalar el software espía NSO Group en los iPhones.
  https://www.bleepingcomputer.com/news/security/newly-found-zero-click-iphone-exploit-used-in-nso-spyware-attacks/
- El FBI, el Tesoro de Estados Unidos y el CISA advierten de que los hackers norcoreanos atacan a las empresas de blockchain.
  https://thehackernews.com/2022/04/fbi-us-treasury-and-cisa-warns-of-north.html

- GitHub notifica a los propietarios de repositorios privados robados, mediante tokens OAuth. https://www.bleepingcomputer.com/news/security/github-notifies-owners-of-private-repos-stolen-using-oauth-tokens/
- MS desactiva por defecto el protocolo de intercambio de archivos SMB1 en Windows 11 Home. https://www.zdnet.com/article/microsoft-disables-smb1-file-sharing-protocol-by-default-in-windows-11-home/
- **Detallan un fallo que podría paralizar el sistema de detección de intrusiones Snort.** https://thehackernews.com/2022/04/researchers-detail-bug-that-could.html
- Okta: Sólo dos clientes fueron afectados por la brecha relacionada con Lapsus$. https://www.infosecurity-magazine.com/news/okta-just-two-customers-lapsus/
- EE.UU. y sus aliados advierten de la amenaza de hackeo ruso a las infraestructuras críticas. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
- **El ransomware BlackCat ha afectado al menos a 60 organizaciones de todo el mundo.** https://www.bleepingcomputer.com/news/security/fbi-blackcat-ransomware-breached-at-least-60-entities-worldwide/
- Los correos electrónicos de phishing dirigidos a las cuentas de LinkedIn están aumentando. https://www.zdnet.com/article/phishing-emails-targeting-linkedin-accounts-are-on-the-rise-heres-what-to-watch-out-for/
- Un bug crítico podría haber permitido a los hackers hacerse con millones de dispositivos Android. https://arstechnica.com/information-technology/2022/04/critical-bug-could-have-let-hackers-commandeer-millions-of-android-devices/
- La red de bots LemonDuck saquea instancias en la nube Docker, en una oleada de delitos contra criptomonedas. https://www.zdnet.com/article/lemonduck-botnet-plunders-docker-cloud-instances-in-cryptocurrency-crime-wave/
- **Los hackers rusos están buscando opciones alternativas para el blanqueo de dinero.** https://www.bleepingcomputer.com/news/security/russian-hackers-are-seeking-alternative-money-laundering-options/
- Grupos hackers están programando ataques de ransomware contra los agricultores durante la temporada de cosecha en EE.UU. https://www.pcmag.com/news/hackers-are-timing-ransomware-attacks-to-hit-farmers-during-harvest-season

ACTUALIZACIONES DE SEGURIDAD

- Lenovo parchea las vulnerabilidades del firmware UEFI que afectan a millones de usuarios en más de 100 modelos. https://arstechnica.com/information-technology/2022/04/bugs-in-100-lenovo-models-fixed-to-prevent-unremovable-infections/
- Google corrige el día cero de Chrome que está siendo utilizado en exploits. https://www.zdnet.com/article/google-fixes-chrome-zero-day-being-used-in-exploits-in-the-wild/
- La actualización trimestral de parches críticos de Oracle llega con 520 correcciones. https://www.zdnet.com/article/time-to-get-patching-oracles-quarterly-critical-patch-update-arrives-with-520-fixes/
- Parche a un error crítico de seguridad criptográfica de Java. https://nakedsecurity.sophos.com/2022/04/20/critical-cryptographic-java-security-blunder-patched-update-now/cada
- Cisco informó la publicación de parches para varias vulnerabilidades de alta gravedad en sus productos, entre las que se encuentra una denunciada por la NSA. https://www.securityweek.com/cisco-patches-virtual-conference-software-vulnerability-reported-nsa