@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. 161 – 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 1/4/22 y el 7/4/22

- American Express sufre una interrupción y los usuarios informan de problemas de acceso y pago en EE.UU., RU y Europa.
  https://www.bleepingcomputer.com/news/security/american-express-down-in-outage-users-report-login-and-payment-issues/
- Los clientes de Trezor son víctimas de *phishing* tras el ataque a MailChimp.
  https://www.infosecurity-magazine.com/news/trezor-customers-phished-mailchimp/
- **Fuga de datos de una *app* rusa de envíos muestra los hábitos alimenticios de la policía secreta.**
  https://www.theverge.com/2022/4/3/23008658/data-leak-russian-delivery-app-dining-habits-secret-police-yandex-food
- Alemania cierra el mercado ruso de la *dark web* Hydra y confisca 25 millones de u$s en Bitcoin.
  https://thehackernews.com/2022/04/germany-shuts-down-russian-hydra.html
  https://securityaffairs.co/wordpress/129866/cyber-crime/german-police-shut-down-hydra-market.html
- El sitio web del gigante petrolero ruso Gazprom Neft no está operativo tras un presunto pirateo.
  https://www.infosecurity-magazine.com/news/russian-oil-gazprom-neft-hack/

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

- Los fallos críticos del PLC de Rockwell podrían permitir a los hackers implantar código malicioso.
  https://thehackernews.com/2022/04/critical-bugs-in-rockwell-plc-could.html
- Una vulnerabilidad crítica de GitLab permite a los atacantes tomar el control de las cuentas.
  https://www.bleepingcomputer.com/news/security/critical-gitlab-vulnerability-lets-attackers-take-over-accounts/
- Hackers chinos se dirigen a servidores VMware Horizon con Log4Shell para implantar un *rootkit*.
  https://thehackernews.com/2022/04/chinese-hackers-target-vmware-horizon.html
- **Un nuevo malware para Android graba audios y rastrea tu ubicación.**
  https://www.bleepingcomputer.com/news/security/newly-found-android-malware-records-audio-tracks-your-location/
- Grupos norcoreanos distribuyen apps de billetera DeFi troyanizadas para robar criptomonedas.
  https://thehackernews.com/2022/04/north-korean-hackers-distributing.html
- La red de bots Beastmode aumenta el potencial de DDoS con nuevos exploits de routers.
  https://thehackernews.com/2022/04/beastmode-ddos-botnet-exploiting-new.html
- **El grupo FIN7 amplía su kit de herramientas y trabaja con múltiples bandas de ransomware.**
  https://thehackernews.com/2022/04/fin7-hackers-leveraging-password-reuse.html
- Descubren cómo el malware Colibri se mantiene “persistente” en los sistemas pirateados.
  https://thehackernews.com/2022/04/researchers-uncover-how-colibri-malware.html
- Lista de filtraciones de datos y ciberataques en marzo: 3,99 millones de registros vulnerados.

https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-march-2022-3-99-million-records-breached

NOTAS DE INTERÉS

- ¿Se acerca el fin del cifrado de extremo a extremo?
  https://www.theguardian.com/commentisfree/2022/apr/02/is-the-end-nigh-for-end-to-end-for-encryption-whatsapp
- **China es acusada de ciberataques a Ucrania antes de la invasión rusa.**
  https://www.theguardian.com/technology/2022/apr/01/china-accused-of-launching-cyber-attacks-on-ukraine-before-russian-invasion
- El nuevo malware de acceso remoto Borat no es cosa de risa.
  https://www.bleepingcomputer.com/news/security/new-borat-remote-access-malware-is-no-laughing-matter/
- Expertos arrojan luz sobre el malware BlackGuard Infostealer que se vende en los foros de hacking rusos.
  https://thehackernews.com/2022/04/experts-shed-light-on-blackguard.html
- **Nuevo impulso a la Internet rusa soberana tras la reacción de la guerra contra Ucrania.**
  https://arstechnica.com/tech-policy/2022/04/russia-inches-closer-to-its-splinternet-dream/
- Descubren un nuevo software espía para Android en servidor C2 vinculado a los hackers de Turla.
  https://thehackernews.com/2022/04/researchers-uncover-new-android-spyware.html
- Varios grupos de hackers aprovechan el conflicto de Ucrania para distribuir malware.
  https://thehackernews.com/2022/04/multiple-hacker-groups-capitalizing-on.html
- Rastrean ataques de espionaje generalizados y los atribuyen a los hackers chinos "Cicada".
  https://thehackernews.com/2022/04/researchers-trace-widespread-espionage.html
- EE.UU. desbarata la red de bots rusa Cyclops Blink antes de ser utilizada en ataques.
  https://www.securityweek.com/fbi-disables-cyclops-blink-botnet-controlled-russian-intelligence-agency
- El troyano bancario SharkBot reaparece en Google Play Store oculto tras 7 nuevas aplicaciones.
  https://thehackernews.com/2022/04/sharkbot-banking-trojan-resurfaces-on.html
- **Divulgaron la vulnerabilidad SSRF en una API ya integrada en muchos sistemas bancarios.**
  https://threatpost.com/ssrf-flaw-fintech-bank-accounts/179247/
- Se sospecha que hackers chinos tienen como objetivo la red eléctrica de la India.
  https://www.cyberscoop.com/chinese-hackers-india-power-grid-recorded-future-red-echo/

ACTUALIZACIONES DE SEGURIDAD

- Apple se apresura en sacar parches para días 0 en los sistemas operativos MacOS e iOS.
  https://threatpost.com/apple-rushes-out-patches-0-days-macos-ios/179222/
  https://arstechnica.com/information-technology/2022/03/apple-rushes-out-patches-for-two-zero-days-threatening-ios-and-macos-users/
- Trend Micro corrige un fallo de ejecución de código remoto ampliamente "*explotado*".
  https://www.bleepingcomputer.com/news/security/trend-micro-fixes-actively-exploited-remote-code-execution-bug/
- VMware parchea el fallo RCE de Spring4Shell en varios productos. Informa de vulnerabilidades.
  https://www.bleepingcomputer.com/news/security/vmware-patches-spring4shell-rce-flaw-in-multiple-products/
  https://www.bleepingcomputer.com/news/security/vmware-warns-of-critical-vulnerabilities-in-multiple-products/
- Microsoft anuncia nuevas funciones de seguridad y cifrado de Windows 11.
  https://www.bleepingcomputer.com/news/microsoft/microsoft-announces-new-windows-11-security-encryption-features/