@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. 164 – 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 25/4/22 y el 28/5/22

- Los hackers de Lapsus$ atacan a T-Mobile.
  https://threatpost.com/lapsus-hackers-target-t-mobile/179384/
- Grupo médico francés desconecta Internet tras robo de datos por parte de piratas informáticos.
  https://www.bleepingcomputer.com/news/security/french-hospital-group-disconnects-internet-after-hackers-steal-data/
- **Costa Rica se niega a pagar el rescate cibernético. También Perú se ve afectado.**
  https://www.infosecurity-magazine.com/news/costa-rica-refuses-to-pay-ransom/
  https://www.welivesecurity.com/la-es/2022/04/28/ransomware-conti-afecta-organismo-gubernamental-peru/
- Un hospital de Kansas divulga una filtración de datos.
  https://www.infosecurity-magazine.com/news/kansas-hospital-data-breach/
- Ladrón roba 1 millón de dólares en NFT del Club Náutico Bored Ape con un hackeo a Instagram.
  https://www.theverge.com/2022/4/25/23041415/bored-ape-yacht-club-nft-hack-instagram
- **Un atacante accedió a "docenas" de repositorios de GitHub utilizando tokens OAuth robados.**
  https://threatpost.com/github-repos-stolen-oauth-tokens/179427/

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

- **Análisis de ataques DDoS en el primer trimestre de 2022.**
  https://securelist.com/ddos-attacks-in-q1-2022/106358/
- Los expertos advierten de un aumento de los bugs de día cero observados y explotados en 2021.
  https://securityaffairs.co/wordpress/130569/apt/zero-day-discovered-exploited-2021.html
- **Reporte especial de DFIR sobre el ransomware Quantum.**
  https://thedfirreport.com/2022/04/25/quantum-ransomware/
- Microsoft encuentra un fallo en el escritorio de Linux que da acceso a la raíz a usuarios que no son de confianza..
  https://arstechnica.com/information-technology/2022/04/microsoft-finds-linux-desktop-flaw-that-gives-root-to-untrusted-users/
- Inyecciones de malware en el gestor de contraseñas KeePass
  https://unaaldia.hispasec.com/2022/04/inyecciones-de-malware-en-el-gestor-de-contrasenas-keepass.html
- En 2021 se divulgaron más de 20.000 vulnerabilidades y riesgos comunes (CVE)
  https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3011622/cisa-fbi-nsa-and-international-partners-warn-organizations-of-top-routinely-exp/
- El nuevo ransomware Black Basta entra en acción con una docena de infiltraciones.
  https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/

- **Informe de actividades de APT en el primer trimestre de 2022.**
  https://securelist.com/apt-trends-report-q1-2022/106351/
- La Agencia de Ciberseguridad de EE.UU. enumera las 15 vulnerabilidades de software más explotadas en 2021.
  https://securityaffairs.co/wordpress/130691/hacking/top-15-most-exploited-software-vulnerabilities.html
- Los expertos detallan 3 equipos de hackers que trabajan bajo el paraguas del grupo TA410.
  https://thehackernews.com/2022/04/experts-detail-3-hacking-teams-working.html

NOTAS DE INTERÉS

- Nueva variante del malware BotenaGo centrada en dispositivos DVR de cámaras de seguridad Lilin.
  https://thehackernews.com/2022/04/new-botenago-malware-variant-targeting.html
- Los ataques ransomware cuestan a las universidades de Gran Bretaña más de 2 millones de libras.
  https://www.infosecurity-magazine.com/news/ransomware-attacks-cost/
- Un fallo crítico en Everscale Wallet podría haber permitido a los atacantes robar criptomonedas.
  https://thehackernews.com/2022/04/critical-bug-in-everscale-wallet.html
- Hackers norcoreanos atacan a periodistas con un novedoso malware.
  https://www.bleepingcomputer.com/news/security/north-korean-hackers-targeting-journalists-with-novel-malware/
- Mastercard presenta la tecnología de identidad de próxima generación con Microsoft.
  https://www.darkreading.com/endpoint/mastercard-launches-next-generation-identity-technology-with-microsoft
- Analistas se apoderan de “sandbox” sin parches utilizadas por antivirus, a través de VirusTotal.
  https://thehackernews.com/2022/04/researchers-report-critical-rce.html
- La botnet Emotet prueba nuevas ideas de distribución después de que Microsoft deshabilitó las macros VBA por defecto.
  https://thehackernews.com/2022/04/emotet-testing-new-delivery-ideas-after.html
- Un grupo de amenaza, hasta ahora desconocido y con por motivos económicos, se hace pasar por un organismo ruso en una campaña de phishing dirigida a entidades de países de Europa del Este.
  https://www.bleepingcomputer.com/news/security/russian-govt-impersonators-target-telcos-in-phishing-attacks/
- **El ransomware Onyx destruye los archivos en lugar de cifrarlos.**
  https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/
- Fallo de Log4j: miles de aplicaciones siguen vulnerables, advierten investigadores de seguridad.
  https://www.zdnet.com/article/log4j-flaw-thousands-of-applications-are-still-vulnerable-warn-security-researchers/
- Cómo los ataques a los cables de fibra óptica franceses acentúan la vulnerabilidad de las infraestructuras críticas.
  https://www.cyberscoop.com/french-fiber-optic-cables-attack-critical-infrastructure/
- Cloudflare frena un enorme ataque DDoS a una plataforma de criptomonedas.
  https://www.theregister.com/2022/04/28/cloudflare-largest-ddos-attack-/

ACTUALIZACIONES DE SEGURIDAD

- QNAP advierte a los usuarios que desactiven AFP hasta que solucione los errores críticos.
  https://www.bleepingcomputer.com/news/security/qnap-warns-users-to-disable-afp-until-it-fixes-critical-bugs/
- Cisco repara 11 vulnerabilidades de alta gravedad en productos de seguridad.
  https://www.securityweek.com/cisco-patches-11-high-severity-vulnerabilities-security-products