@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. 182 – 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 05/08/22 y el 08/09/22

- El segundo mayor distrito escolar de EE.UU. fue atacado por un ransomware.
  https://www.zdnet.com/article/the-second-biggest-school-district-in-the-us-was-hit-with-ransomware/
- El ciberataque de InterContinental Hotels Group afecta a los sistemas de reserva.
  https://www.bleepingcomputer.com/news/security/intercontinental-hotels-group-cyberattack-disrupts-booking-systems/
- El grupo "DangerousSavanna" atacó instituciones financieras en África durante dos años.
  https://www.infosecurity-magazine.com/news/hackers-targeted-financial/
- Los sitios web del gobierno de Japón son objeto de ciberataques, se sospecha de Killnet.
  https://www.infosecurity-magazine.com/news/japan-govt-websites-killnet/
- **Un ciberataque al gobierno portugués habría filtrado "cientos" de documentos clasificados de la OTAN.**
  https://www.itpro.co.uk/security/data-breaches/369022/portugal-government-cyber-attack-allegedly-leaks-hundreds-of

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

- Falsos antivirus y aplicaciones de limpieza instalan el troyano bancario SharkBot para Android.
  https://thehackernews.com/2022/09/fake-antivirus-and-cleaner-apps-caught.html
- QNAP parchea el día cero utilizado en los ataques del ransomware Deadbolt.
  https://arstechnica.com/information-technology/2022/09/new-wave-of-data-destroying-ransomware-attacks-hits-qnap-nas-devices/
- El nuevo servicio EvilProxy permite a los hackers utilizar tácticas avanzadas para eludir seguridad avanzada.
  https://thehackernews.com/2022/09/new-evilproxy-phishing-service-allowing.html
- Utilizan el panel TeslaGun para gestionar los ataques de backdoor de ServHelper.
  https://thehackernews.com/2022/09/ta505-hackers-using-teslagun-panel-to.html
- **Un nuevo malware para Linux apodado Shikitega aprovecha una cadena de infección de varias etapas para dirigirse a puntos finales y dispositivos IoT.**
- https://www.bleepingcomputer.com/news/security/new-linux-malware-evades-detection-using-multi-stage-deployment/
  https://securityaffairs.co/wordpress/135437/malware/shikitega-linux-malware.html
- Internet Storm Center: detalles del ISC Stormcast para el jueves 8 de septiembre de 2022.
  https://isc.sans.edu/podcastdetail/?id=8164
- Microsot analiza a “PHOSPHORUS”, subgrupo del ransomware iraní conocido como DEV-0270.
  https://www.microsoft.com/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/

- Los hackers norcoreanos de Lazarus atacan a los proveedores de energía de Estados Unidos.
https://www.bleepingcomputer.com/news/security/north-korean-lazarus-hackers-take-aim-at-us-energy-providers/
- Cómo las pruebas de penetración pueden ayudar a prevenir los ataques de ransomware.
https://www.tripwire.com/state-of-security/controls/penetration-testing-prevent-ransomware-attacks/
- El malware Bumblebee incluye una herramienta de postexplotación para infecciones furtivas.
https://www.bleepingcomputer.com/news/security/bumblebee-malware-adds-post-exploitation-tool-for-stealthy-infections/

NOTAS DE INTERÉS

- **China acusa a Estados Unidos de "decenas de miles" de ciberataques.**
https://www.securityweek.com/china-accuses-us-tens-thousands-cyberattacks
- TikTok niega los informes de que ha sido hackeado.
https://www.theverge.com/2022/9/5/23338051/tiktok-denies-reports-hacked-data-breach
- La OTAN investiga después de que unos ladrones afirman estar vendiendo los planos de misiles robados.
https://www.theregister.com/2022/09/05/in-brief-secuirty/
- Los ciberataques aumentan contra Linux en medio de la migración a la nube.
https://www.darkreading.com/application-security/defenders-prepared-cyberattacks-linux-cloud-migration
- Grupo de ciberespionaje Worok tiene como objetivo gobiernos y empresas de alto nivel.
https://www.bleepingcomputer.com/news/security/new-worok-cyber-espionage-group-targets-governments-high-profile-firms/
- EE.UU. incauta el mercado WT1SHOP que vende tarjetas de crédito, credenciales y documentos de identidad.
https://www.bleepingcomputer.com/news/security/us-seizes-wt1shop-market-selling-credit-cards-credentials-and-ids/
- Google afirma que los ex miembros del ransomware Conti atacan a Ucrania.
https://securityaffairs.co/wordpress/135447/cyber-crime/conti-ransomware-members-target-ukraine.html
- **La NSA publica los requisitos de los futuros algoritmos de robustez cuántica (QR) para los sistemas de seguridad nacional de EE.UU.**
https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/
- La red de bots Moobot se dirige a los routers D-Link sin parches.
https://www.bleepingcomputer.com/news/security/moobot-botnet-is-coming-for-your-unpatched-d-link-router/
- El Grupo Lazarus desplegó el malware MagicRAT para afectar a los proveedores de energía.
https://www.theregister.com/2022/09/08/lazarus_group_energy_firms_trade_secrets/
https://thehackernews.com/2022/09/north-korean-lazarus-hackers-targeting.html
- Hackers chinos se centran en funcionarios gubernamentales de Europa, Sudamérica y Oriente Medio con el malware PlugX.
https://thehackernews.com/2022/09/chinese-hackers-target-government.html
- Advertencia sobre la banda de ransomware Vice Society tras ataques a colegios de EE.UU.
https://www.tripwire.com/state-of-security/security-data-protection/warning-issued-vice-society-ransomware-gang/

ACTUALIZACIONES DE SEGURIDAD

- Cisco publica parches de seguridad para nuevas vulnerabilidades que afectan a varios productos.
https://thehackernews.com/2022/09/cisco-releases-security-patches-for-new.html