@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. 174 – 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 01/07/22 y el 07/07/22

- Piratas informáticos iraníes filtran información de más de 300.000 israelíes de sitios turísticos.
  https://www.jpost.com/israel-news/article-710973
- **Las cuentas de YouTube y Twitter del ejército británico fueron hackeadas para promover estafas de criptomonedas.**
  https://www.theverge.com/2022/7/3/23193668/british-army-youtube-twitter-accounts-hacked-promote-crypto-scam-fraud
- **Un hacker afirma haber robado datos de 1.000 millones de ciudadanos chinos.**
  https://www.bleepingcomputer.com/news/security/hacker-claims-to-have-stolen-data-on-1-billion-chinese-citizens/
- Marriott confirma filtración, que expone información de huéspedes y empleados del hotel.
  https://www.cyberscoop.com/marriott-data-breach-baltimore/
- La agencia de noticias iraní Fars afirma que se ha producido un ciberataque contra una empresa que participa en la construcción del metro de Tel Aviv.
  https://securityaffairs.co/wordpress/132897/hacking/tel-aviv-metro-company-attacked.html
- La APT Bitter sigue atacando a las entidades militares de Bangladesh.
  https://thehackernews.com/2022/07/bitter-apt-hackers-continue-to-target.html
- El gigante de la IT, SHI, sufre un "ataque de malware profesional".
  https://www.bleepingcomputer.com/news/security/it-services-giant-shi-hit-by-professional-malware-attack/

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

- **Cómo una aplicación de Android puede vaciar su cuenta.**
  https://www.microsoft.com/security/blog/2022/06/30/toll-fraud-malware-how-an-android-application-can-drain-your-wallet/
- **Una amplia gama de routers está siendo atacada por un nuevo y sofisticado malware**
  https://arstechnica.com/information-technology/2022/06/a-wide-range-of-routers-are-under-attack-by-new-unusually-sophisticated-malware/
- El Informe de Amenazas Portugal Segundo Trimestre, recopila los datos obtenidos de las campañas maliciosas ocurridas entre marzo y junio de 2022 en ese país.
  https://securityaffairs.co/wordpress/132842/security/threat-report-portugal-q2-2022.html
- Investigadores comparten técnicas para descubrir sitios ransomware anónimos en la Dark Web.
  https://thehackernews.com/2022/07/researchers-share-techniques-to-uncover.html
- El nuevo ransomware RedAlert se enfoca en servidores VMware ESXi de Windows y Linux.
  https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/

NOTAS DE INTERÉS

- Nueva puerta trasera "SessionManager" enfocada en los servidores IIS de Microsoft.
https://thehackernews.com/2022/07/new-sessionmanager-backdoor-targeting.html
- El FBI y el CISA advierten: Un ransomware usa los defectos de RDP para entrar en las redes.
https://www.zdnet.com/article/fbi-and-cisa-warn-this-ransomware-is-using-rdp-flaws-to-break-into-networks/
- El soporte de Windows Server 2012 llega a su fin en octubre de 2023.
https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-server-2012-reaches-end-of-support-in-october-2023/
- DragonForce Malaysia difunde el exploit LPE y amenaza con el ransomware.
https://www.darkreading.com/vulnerabilities-threats/dragonforce-malaysia-releases-lpe-exploit-threatens-ransomware
- **Detectan una herramienta de malware de criptominería renovada que afecta a sistemas Linux.**
https://www.infosecurity-magazine.com/news/cryptomining-malware-linux-systems/
- Microsoft encuentra el gusano Raspberry Robin en cientos de redes Windows.
https://www.bleepingcomputer.com/news/security/microsoft-finds-raspberry-robin-worm-in-hundreds-of-windows-networks/
- **La OTAN desarrollará capacidades de ciber respuesta rápida.**
https://www.infosecurity-magazine.com/news/nato-rapid-cyber-response/
- Grupo pro chino utiliza la campaña Dragonbridge para atacar a empresas mineras de tierras raras.
https://thehackernews.com/2022/07/pro-china-group-uses-dragonbridge.html
- La guerra de Ucrania podría proporcionar un manual de ciberguerra para los generales chinos que tienen en la mira a Taiwán.
https://www.cyberscoop.com/china-taiwan-russia-ukraine-cyberspace/
- **El NIST presenta las cuatro primeras herramientas de cifrado resistentes a la tecnología cuántica.**
https://www.infosecurity-magazine.com/news/nist-quantum-resistant-encryption/
- El ransomware Hive se actualiza a Rust para obtener un método de cifrado más sofisticado.
https://thehackernews.com/2022/07/hive-ransomware-upgrades-to-rust-for.html
- Para evadir la detección en ataques utilizan la herramienta de penetración del equipo Red BRc4.
https://securityaffairs.co/wordpress/132922/hacking/brc4-used-in-attacks.html
- Advierten del nuevo malware OrBit Linux que se apodera del flujo de ejecución.
https://thehackernews.com/2022/07/researchers-warn-of-new-orbit-linux.html

ACTUALIZACIONES DE SEGURIDAD

- La actualización del gestor de contraseñas de Chrome permitirá añadir manualmente las credenciales en todas las plataformas.
https://www.theverge.com/2022/6/30/23189450/chrome-password-manager-updates-ios-android
- Google repara un bug de Chrome que se aprovecha muy activamente.
https://www.cisa.gov/uscert/ncas/current-activity/2022/07/05/google-releases-security-update-chrome
- OpenSSL corrige dos fallos criptográficos: que hay que saber.
https://nakedsecurity.sophos.com/2022/07/06/openssl-fixes-two-one-liner-crypto-bugs-what-you-need-to-know/
- **Cisco y Fortinet publican parches de seguridad para varios productos.**
https://thehackernews.com/2022/07/cisco-and-fortinet-release-security.html