@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. 170 – 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 3/6/22 y el 9/6/22

- **Apple bloqueó 1,6 millones de apps que defraudaban a los usuarios en 2021.**
https://www.tripwire.com/state-of-security/security-data-protection/apple-protected-app-store-users-from-fraud/
- La ciudad italiana de Palermo apaga todos los sistemas para defenderse de un ciberataque.
https://www.bleepingcomputer.com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/
- La filtración de datos de Shields Health Care Group afecta a 2 millones de pacientes.
https://www.bleepingcomputer.com/news/security/shields-health-care-group-data-breach-affects-2-million-patients/
- Tiendas de armas online en Estados Unidos fueron hackeadas para robar tarjetas de crédito.
https://www.bleepingcomputer.com/news/security/online-gun-shops-in-the-us-hacked-to-steal-credit-cards/
- Una campaña de phishing en Facebook permite obtener millones de dólares en identificaciones (ID) y dinero en efectivo.
https://www.theregister.com/2022/06/09/facebook_phishing_campaign/
- **El Ministerio de Defensa del Reino Unido adquiere el primer ordenador cuántico del gobierno.**
https://www.bbc.com/news/technology-61647134?

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

- El grupo chino LuoYu utiliza los ataques Man-on-the-Side para desplegar el *backdoor* WinDealer.
https://thehackernews.com/2022/06/chinese-luoyu-hackers-using-man-on-side.html
- **El grupo de hackers WatchDog lanza una nueva campaña denominada *cryptojacking* Docker.**
https://www.bleepingcomputer.com/news/security/watchdog-hacking-group-launches-new-docker-cryptojacking-campaign/
- **Agentes patrocinados por China se aprovechan de proveedores y dispositivos de redes.**
https://www.cisa.gov/uscert/ncas/alerts/aa22-158a
- La versión Linux del ransomware Black Basta se concentra en los servidores VMware ESXi.
https://www.bleepingcomputer.com/news/security/linux-version-of-black-basta-ransomware-targets-vmware-esxi-servers/
- El nuevo malware SVCReady se carga desde las propiedades del documento de Word.
https://www.bleepingcomputer.com/news/security/new-svcready-malware-loads-from-word-doc-properties/
- **Symbiote: Un malware de Linux casi indetectable afecta al sector financiero latinoamericano.**
https://www.zdnet.com/article/this-new-linux-malware-is-almost-impossible-to-detect/
- **Cómo la Inteligencia Artificial es útil, y en que no, para la ciberseguridad.**
https://www.darkreading.com/attacks-breaches/how-ai-is-useful-and-not-useful-for-cybersecurity

NOTAS DE INTERÉS

- Microsoft bloquea a los intrusos libaneses vinculados a Irán que atacan a empresas israelíes.
https://thehackernews.com/2022/06/microsoft-blocks-iran-linked-lebanese.html
- El dispositivo de videoconferencia Meeting Owl utilizado por gobiernos es un desastre de seguridad.
https://arstechnica.com/information-technology/2022/06/vulnerabilities-in-meeting-owl-videoconference-device-imperil-100k-users/
- Descubren un malware que controla miles de sitios de la red Parrot TDS.
https://thehackernews.com/2022/06/researchers-uncover-malware-controlling.html
- Microsoft desbarata la operación de spear-phishing de los hackers de Bohrium.
https://www.bleepingcomputer.com/news/security/microsoft-disrupts-bohrium-hackers-spear-phishing-operation/
- **Conti se reestructura en varios grupos más pequeños, ¿son ahora más peligrosos que nunca?**
https://www.techrepublic.com/article/conti-reforms-into-several-smaller-groups-are-they-now-more-dangerous-than-ever/
- Las pérdidas por estafas con criptomonedas superan los 1.000 millones de dólares, según la FTC.
https://www.cyberscoop.com/cryptocurrency-scams-ftc-romance/
- El ransomware YourCyanide se propaga con enlaces de PasteBin, Discord y Microsoft.
https://www.darkreading.com/threat-intelligence/yourcyanide-ransomware-pastebin-discord-microsoft-links
- **Miles de bases de datos Elasticsearch desprotegidas están siendo secuestradas.**
https://www.techrepublic.com/article/thousands-of-unprotected-elasticsearch-databases-are-being-ransomed/
- QBot ahora utiliza el ransomware Black Basta en ataques impulsados por bots.
https://www.bleepingcomputer.com/news/security/qbot-now-pushes-black-basta-ransomware-in-bot-powered-attacks/
- El grupo de hackers Evil Corp cambia las tácticas del ransomware para eludir las sanciones estadounidenses.
https://www.infosecurity-magazine.com/news/evil-corp-changes-ransomware/
- El ransomware Cuba vuelve a extorsionar a las víctimas con un *encriptador* actualizado.
https://www.bleepingcomputer.com/news/security/cuba-ransomware-returns-to-extorting-victims-with-updated-encryptor/
- Variante de Emotet roba información de las tarjetas de crédito de usuarios de Google Chrome.
https://thehackernews.com/2022/06/new-emotet-variant-stealing-users.html
- Una APT de habla china no documentada anteriormente, rastreada como Aoqin Dragon, afecta a entidades del sudeste asiático y Australia.
https://securityaffairs.co/wordpress/132099/apt/aoqin-dragon-targets-south-asia-australia.html

ACTUALIZACIONES DE SEGURIDAD

- La actualización de seguridad de GitLab corrige un fallo crítico de toma de control de cuentas.
https://www.bleepingcomputer.com/news/security/gitlab-security-update-fixes-critical-account-take-over-flaw/
- El día 0 crítico de Atlassian está bajo explotación activa. Se debe parchear.
https://arstechnica.com/information-technology/2022/06/hacker-free-for-all-hammers-servers-not-patched-against-atlassian-0-day/
- **Google publica boletín de seguridad mensual de Android, corrigiendo vulnerabilidades críticas.**
https://www.infosecurity-magazine.com/news/google-android-security-patches/