@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. 183 – 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 09/09/22 y el 15/09/22

- El FBI recupera 30 millones de dólares en criptodivisas robadas por hackers norcoreanos.
https://www.schneier.com/blog/archives/2022/09/fbi-seizes-stolen-cryptocurrencies.html
- **China acusa a la unidad TAO de la NSA de hackear su Universidad de investigación militar.**
https://thehackernews.com/2022/09/china-accuses-nsas-tao-unit-of-hacking.html
- Montenegro y sus aliados están trabajando para recuperarse del ciberataque masivo.
https://securityaffairs.co/wordpress/135667/hacking/montenegro-massive-cyber-attack.html
- **Un ciberataque de piratas informáticos rusos interrumpió 20 sitios web del gobierno japonés.**
https://www.cpomagazine.com/cyber-security/cyber-attack-by-russian-hackers-disrupted-20-japanese-government-websites/
- El ransomware Hive reivindica el ciberataque a la filial de Bell Canada.
https://www.bleepingcomputer.com/news/security/hive-ransomware-claims-cyberattack-on-bell-canada-subsidiary/

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

- La mayoría de los sitios web comparten las consultas de búsqueda en el sitio con terceros.
https://www.helpnetsecurity.com/2022/09/09/search-terms-leaked/
- El malware Lampion vuelve en los ataques de phishing haciendo uso indebido de WeTransfer.
https://www.bleepingcomputer.com/news/security/lampion-malware-returns-in-phishing-attacks-abusing-wetransfer/
- Por qué los puertos corren el riesgo de sufrir ciberataques.
https://www.darkreading.com/attacks-breaches/why-ports-are-at-risk-of-cyberattacks
- **Las bandas de ransomware cambian a una nueva táctica de cifrado intermitente.**
https://www.bleepingcomputer.com/news/security/ransomware-gangs-switching-to-new-intermittent-encryption-tactic/
- Resumen de vulnerabilidades de la primera semana de septiembre.
https://www.cisa.gov/uscert/ncas/bulletins/sb22-255
- Errores de firmware en muchos modelos de ordenadores HP llevan más de un año sin corregirse.
https://thehackernews.com/2022/09/high-severity-firmware-security-flaws.html
- Ciberespías lanzan un malware de robo de información en las redes gubernamentales de Asia.
https://www.bleepingcomputer.com/news/security/cyberspies-drop-new-infostealer-malware-on-govt-networks-in-asia/
- **Ataques al navegador: ¡cuidado con las ventanas que no son! (Browser-in-the-browser).**
https://nakedsecurity.sophos.com/2022/09/13/serious-security-browser-in-the-browser-attacks-watch-out-for-windows-that-arent/

- Inyección de procesos fácil dentro de Python.
  https://isc.sans.edu/diary/Easy+Process+Injection+within+Python/29048
- El grupo APT SparklingGoblin utilizan una nueva variante de Linux del backdoor SideWalk.
  https://thehackernews.com/2022/09/sparklinggoblin-apt-hackers-using-new.html
- El grupo de ciberespionaje norcoreano Lazarus se centra en proveedores de energía de EE.UU., Canadá y Japón con un nuevo programa malicioso.
  https://www.techrepublic.com/article/lazarus-targets-energy-providers/
- Un nuevo paquete de malware se autodifunde a través de vídeos de juegos de YouTube.
  https://www.bleepingcomputer.com/news/security/new-malware-bundle-self-spreads-through-youtube-gaming-videos/

NOTAS DE INTERÉS

- Monti, el nuevo Conti: la banda de ransomware utiliza código reciclado.
  https://www.darkreading.com/vulnerabilities-threats/monti-conti-ransomware-recycled-code
- Se desconoce el impacto de la última filtración de datos de Samsung.
  https://www.techrepublic.com/article/samsung-data-breach/
- La APT42 iraní lanzó más de 30 ataques de espionaje contra activistas y disidentes.
  https://thehackernews.com/2022/09/iranian-apt42-launched-over-30.html
- Un nuevo ataque puede desbloquear y arrancar un Tesla Model Y en segundos, según investigadores.
  https://www.theverge.com/2022/9/12/23348765/tesla-model-y-unlock-drive-car-thief-nfc-relay-attack
- **El grupo pro-palestino GhostSec hackeó los PLC Berghof utilizados en Israel.**
  https://securityaffairs.co/wordpress/135656/hacktivism/ghostsec-hacked-berghof-plcs-israel.html
- Defecto tipo gusano y días 0 lideran el martes de parche de septiembre de 2022.
  https://krebsonsecurity.com/2022/09/wormable-flaw-0days-lead-sept-2022-patch-tuesday/
- Los hackers de Webworm utilizan RATs modificados en los últimos ataques de ciberespionaje.
  https://thehackernews.com/2022/09/webworm-hackers-using-modified-rats-in.html
- Microsoft Teams almacena tokens de autentificación en texto plano y no se podrá parchear rápidamente.
  https://arstechnica.com/information-technology/2022/09/microsoft-teams-stores-cleartext-auth-tokens-wont-be-quickly-patched/

ACTUALIZACIONES DE SEGURIDAD

- Apple libera actualizaciones de seguridad para múltiples productos.
  https://securityaffairs.co/wordpress/135647/security/apple-fixes-eighth-zero-day.html
- **El parche del martes de septiembre de 2022 de Microsoft corrige un día cero utilizado en ataques y 63 fallos.**
  https://thehackernews.com/2022/09/microsofts-latest-security-update-fixes.html
- Adobe publica actualizaciones de seguridad para varios productos.
  https://www.cisa.gov/uscert/ncas/current-activity/2022/09/13/adobe-releases-security-updates-multiple-products
- Nuevas actualizaciones de la BIOS de Lenovo corrigen errores de seguridad en cientos de modelos.
  https://www.bleepingcomputer.com/news/security/new-lenovo-bios-updates-fix-security-bugs-in-hundreds-of-models/