@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. 187 – 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 7/10/22 y el 13/10/22

- Un hacker roba criptomonedas por valor de 566 millones de dólares en Binance.
https://www.bleepingcomputer.com/news/security/hacker-steals-566-million-worth-of-crypto-from-binance-bridge/
- Piratas informáticos interrumpen al líder supremo iraní en la televisión estatal con un mensaje contra el régimen.
https://www.timesofisrael.com/hackers-disrupt-iranian-supreme-leader-on-state-tv-with-anti-regime-message/
- Los sitios web de aeropuertos de EE.UU. caen en ataques DDoS por parte de hackers prorrusos.
https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet
- Toyota revela la filtración de datos tras exponer la clave de acceso en GitHub.
https://www.bleepingcomputer.com/news/security/toyota-discloses-data-leak-after-access-key-exposed-on-github/

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

- El grupo LofyGang construyó una empresa para el robo de credenciales en Discord y NPM.
https://www.bleepingcomputer.com/news/security/lofygang-hackers-built-a-credential-stealing-enterprise-on-discord-npm/
- **Se aprovechan de un fallo RCE sin parche en Zimbra Collaboration Suite.**
https://www.bleepingcomputer.com/news/security/hackers-exploiting-unpatched-rce-bug-in-zimbra-collaboration-suite/
- Advertencia de la NSA y el FBI: Cuidado con estas 20 fallas de los programas de software más usadas por los hackers.
https://www.zdnet.com/article/nsa-fbi-warning-beware-these-20-software-flaws-most-used-by-hackers/
- La apropiación de credenciales es la principal amenaza del sector minorista.
https://www.darkreading.com/edge-threat-monitor/credential-harvesting-is-retail-industry-s-top-threat
- **La lucha por cortar la criptofinanciación de la invasión rusa de Ucrania.**
https://arstechnica.com/tech-policy/2022/10/the-fight-to-cut-off-the-crypto-funding-russias-invasion-of-ukraine/
- Nuevo informe revela las técnicas de entrega y evasión de Emotet usadas en los últimos ataques.
https://thehackernews.com/2022/10/new-report-uncovers-emotets-delivery.html
- **Fortinet indica que un fallo crítico de autentificación está siendo explotado en los ataques.**
https://www.bleepingcomputer.com/news/security/fortinet-says-critical-auth-bypass-bug-is-exploited-in-attacks/
- 'Ataque térmico' puede leer la contraseña a partir del calor que dejan las yemas de sus dedos.
https://www.zdnet.com/article/this-thermal-attack-can-read-your-password-from-the-heat-your-fingertips-leave-behind/
- POLONIUM se centra en Israel con el malware Creepy, una familia de herramientas de hacking.
https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/
https://thehackernews.com/2022/10/researchers-uncover-custom-backdoors.html

- Listado de vulnerabilidades a octubre de 2022.
https://www.cisa.gov/uscert/ncas/bulletins/sb22-284
- Un fallo crítico de VM2, librería de Java que se obtiene del repositorio NPM, permite a los atacantes ejecutar código "fuera de la caja de arena".
https://www.bleepingcomputer.com/news/security/critical-vm2-flaw-lets-attackers-run-code-outside-the-sandbox/
- Error crítico en los PLC SIMATIC de Siemens permite a los atacantes robar claves criptográficas.
https://thehackernews.com/2022/10/critical-bug-in-siemens-simatic-plcs.html
- El nuevo marco de ataque Alchimist se centra en Windows, macOS y Linux .
https://www.bleepingcomputer.com/news/security/new-alchimist-attack-framework-targets-windows-macos-linux/

NOTAS DE INTERÉS

- El Gobierno australiano estudia la posibilidad de centralizar la verificación del DNI digital en myGov tras la filtración de Optus.
https://www.theguardian.com/technology/2022/oct/07/government-considers-centralising-digital-id-verification-on-mygov-in-wake-of-optus-breach
- Microsoft: Windows 11 22H2 causa un impacto en el rendimiento de la copia de archivos.
https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-11-22h2-causes-file-copy-performance-hit/
- **Bug sin parches en Zimbra permite a los hackers entrar por la puerta trasera en los servidores.**
https://arstechnica.com/information-technology/2022/10/ongoing-0-day-attacks-backdoor-zimbra-servers-by-sending-a-malicious-email/
- Intel confirma que el código fuente de la BIOS de Alder Lake filtrado es auténtico.
https://www.bleepingcomputer.com/news/security/intel-confirms-leaked-alder-lake-bios-source-code-is-authentic/
- Detallan las herramientas maliciosas utilizadas por el grupo de ciberespionaje Earth Aughisky.
https://thehackernews.com/2022/10/researchers-detail-malicious-tools-used.html
- El fallo de VMware vCenter Server comunicado el año pasado aún no ha sido parcheado.
https://www.bleepingcomputer.com/news/security/vmware-vcenter-server-bug-disclosed-last-year-still-not-patched/
- El metaverso está llegando, y las amenazas a la seguridad ya han llegado.
https://www.zdnet.com/article/the-metaverse-is-coming-and-the-security-threats-have-already-arrived/
- Budworm resurge con nuevos ataques de espionaje dirigidos a organizaciones estadounidenses.
https://www.infosecurity-magazine.com/news/budworm-espionage-group-targets-us/
- Los ataques QAKBOT se agudizan en medio de alarmantes colaboraciones de cibercriminales.
https://www.darkreading.com/attacks-breaches/qakbot-attacks-spike-cybercriminal-collaborations

ACTUALIZACIONES DE SEGURIDAD

- **Instalar un parche ya: Fortinet FortiGate y FortiProxy contienen una vulnerabilidad crítica.**
https://www.darkreading.com/vulnerabilities-threats/patch-now-fortinet-fortigate-and-fortiproxy-contain-critical-vuln
- **El martes de parches de Microsoft de octubre de 2022 no corrige los fallos de Exchange Server.**
https://securityaffairs.co/wordpress/136987/security/microsoft-patch-tuesday-oct-2022.html
https://msrc.microsoft.com/update-guide/releaseNote/2022-Oct
- Adobe publica actualizaciones de seguridad para varios productos.
https://www.cisa.gov/uscert/ncas/current-activity/2022/10/11/adobe-releases-security-updates-multiple-products