@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. 181 – 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 26/08/22 y el 04/09/22

- Un hacker roba el código fuente de LastPass, según la empresa.
https://www.vice.com/en/article/k7b7xa/hacker-steals-lastpass-source-code-company-says
- **La infraestructura estatal de Montenegro sufre un ciberataque.**
https://www.securityweek.com/montenegro-reports-massive-russian-cyberattack-against-govt
- El grupo Everest afirma haber accedido a los servidores del gobierno brasileño.
https://www1.folha.uol.com.br/tec/2022/08/grupo-hacker-diz-ter-invadido-governo-brasileiro.shtml
- El ransomware Ragnar Locker reivindica el ataque a la aerolínea de bandera de Portugal.
https://securityaffairs.co/wordpress/135168/data-breach/ragnar-locker-ransomware-tap-air-portugal.html
- El ransomware BlackCat reivindica el ataque a la agencia energética italiana.
https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/
- Ciberpiratas provocaron un atasco masivo en Moscú utilizando una aplicación de servicio de taxis.
https://www.theverge.com/2022/9/3/23335694/hackers-traffic-jam-russia-moscow-ride-hailing-app-yandex-taxi

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

- El falso proyecto P2E "Cthulhu World" se utiliza para difundir un malware que roba información.
https://www.bleepingcomputer.com/news/security/fake-cthulhu-world-p2e-project-used-to-push-info-stealing-malware/
- CISA añade a su catálogo 10 nuevas vulnerabilidades conocidas y utilizadas activamente.
https://thehackernews.com/2022/08/cisa-adds-10-new-known-actively.html
- Hackers chinos atacan al gobierno australiano con el malware ScanBox.
https://www.bleepingcomputer.com/news/security/chinese-hackers-target-australian-govt-with-scanbox-malware/
- **Stuxnet en detalle: La primera ciber-arma conocida.**
https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html
- **NSA y CISA comparten consejos para asegurar la cadena de suministro de software (ver PDF).**
https://www.bleepingcomputer.com/news/security/nsa-and-cisa-share-tips-to-secure-the-software-supply-chain/

NOTAS DE INTERÉS

- Los grupos de ciberdelincuentes adoptan cada vez más el marco de mando y control de Sliver.
https://thehackernews.com/2022/08/cybercrime-groups-increasingly-adopting.html
- **La OTAN investiga la venta de datos de empresas de misiles por parte de hackers.**
https://www.bbc.com/news/technology-62672184
- La APT Mercury, asociada a iraníes, siguen explotando los bugs de Log4j contra Israel.
https://securityaffairs.co/wordpress/134876/apt/mercury-exploit-log4shell-flaw.html

- Descubrieron una campaña pro-estadounidense difundiendo propaganda en redes sociales.
https://www.theverge.com/2022/8/25/23322214/us-government-propaganda-campaign-twitter-facebook
- El número de empresas envueltas en el hackeo de Twilio sigue creciendo.
https://arstechnica.com/information-technology/2022/08/the-number-of-companies-caught-up-in-the-twilio-hack-keeps-growing/
- Se descubre una vulnerabilidad crítica en el servidor y centro de datos de Atlassian Bitbucket.
https://thehackernews.com/2022/08/critical-vulnerability-discovered-in.html
- Grupos de hackers hallaron una forma de acceder a los “inbox” de Gmail, Outlook y Yahoo.
https://www.digitaltrends.com/computing/hackers-found-way-to-access-gmail-outlook-yahoo-inbox/
- DuckDuckGo abre a todo el mundo su servicio de correo electrónico centrado en la privacidad.
https://www.bleepingcomputer.com/news/security/duckduckgo-opens-its-privacy-focused-email-service-to-everyone/
- **Documentos filtrados de una empresa de vigilancia muestran la compra de un exploit RCE de día cero para iOS por 8 millones de dólares.**
https://securityaffairs.co/wordpress/134962/malware/surveillance-firm-intellexa-offer.html
- Nitrokod Crypto Miner infectó a más de 111.000 usuarios
https://thehackernews.com/2022/08/nitrokod-crypto-miner-infected-over.html
- El gobierno de EE.UU. demanda a Kochava por vender datos de geolocalización sensibles.
https://securityaffairs.co/wordpress/135004/security/ftc-sued-data-broker-kochava.html
- La OTAN investiga la filtración en la web oscura de datos robados a un proveedor de misiles.
https://www.darkreading.com/vulnerabilities-threats/nato-investigates-leak-of-data-stolen-from-missile-vendor
- El ransomware "Agenda", basado en Go, ofrece ataques personalizados.
https://www.infosecurity-magazine.com/news/golang-ransomware-agenda/
- Los hackers utilizan ModernLoader infectando los sistemas para robar y realizar cripto minería.
https://thehackernews.com/2022/08/hackers-use-modernloader-to-infect.html
- Estados Unidos e Israel se unen para luchar contra el ransomware.
https://www.defenseone.com/policy/2022/08/us-and-israel-strengthen-cybersecurity-partnership/376481/
- El parche de seguridad del sistema Ubuntu Linux 18.04 quiebra el DNS en Microsoft Azure.
https://www.theregister.com/2022/08/30/ubuntu_systemd_dns_update/
- La plataforma rusa de streaming "START" confirma la vulneración de datos que afecta a 7,5 millones de usuarios.
https://www.bleepingcomputer.com/news/security/russian-streaming-platform-confirms-data-breach-affecting-75m-users/
- **Esconden malware en las impresionantes imágenes tomadas por el telescopio espacial Webb.**
https://thehackernews.com/2022/08/hackers-hide-malware-in-stunning-images.html

ACTUALIZACIONES DE SEGURIDAD

- Se ha anunciado la versión 1.40 de NetworkManager, que incluye 600 parches.
https://www.helpnetsecurity.com/2022/08/29/networkmanager-1-40-network-management-daemon/
- Chrome parchea 24 brechas de seguridad y activa el sistema de seguridad "Sanitizer".
https://nakedsecurity.sophos.com/2022/08/31/chrome-patches-24-security-holes-enables-sanitizer-safety-system/
- Apple publica una actualización del iOS para los iPhones más antiguos.
https://thehackernews.com/2022/09/apple-releases-ios-update-for-older.html