@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. 176 – 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 15/07/22 y el 21/07/22

- El fabricante de videojuegos Bandai Namco confirma ciberataque.
https://www.computerweekly.com/news/252522744/Videogame-maker-Bandai-Namco-confirms-cyber-attack
- Bélgica afirma que hackers chinos atacaron su Ministerio de Defensa.
https://www.bleepingcomputer.com/news/security/belgium-says-chinese-hackers-attacked-its-ministry-of-defense/
- La filtración de Neopets expone los datos personales de 69 millones de miembros.
https://www.bleepingcomputer.com/news/security/neopets-data-breach-exposes-personal-data-of-69-million-members/

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

- **El Navegador Tor ahora evita la censura de Internet automáticamente.**
https://www.bleepingcomputer.com/news/security/tor-browser-now-bypasses-internet-censorship-automatically/
- El APT Sandworm, que opera para el GRU de Rusia, se burlar de los investigadores cuando se da cuenta de que está siendo vigilado.
https://www.darkreading.com/threat-intelligence/sandworm-apt-trolls-researchers-on-its-trail-while-it-targets-ukraine
- Un nuevo ataque al canal lateral de la caché puede anonimizar a los usuarios en línea afectados.
https://thehackernews.com/2022/07/new-cache-side-channel-attack-can-de.html
- Los piratas informáticos están atacando los sistemas industriales con malware.
https://arstechnica.com/information-technology/2022/07/malware-circulating-online-wrangles-industrial-systems-into-a-botnet/
- Un investigador descubrió un malware de aplicación en Google Play que roba su dinero.
https://thenextweb.com/news/researcher-discovered-new-app-malware-that-steals-your-money
- El reciente malware CloudMensis abre las puertas de los Mac para robar los datos de las víctimas.
https://www.bleepingcomputer.com/news/security/new-cloudmensis-malware-backdoors-macs-to-steal-victims-data/
- Cinco consejos para asegurar SSH en sus servidores Linux.
https://www.techrepublic.com/article/tips-securing-ssh-linux-servers/
- Hackers rusos utilizan DropBox y Google Drive para introducir archivos peligrosos.
https://thehackernews.com/2022/07/russian-hackers-using-dropbox-and.html
- Luna y Black Basta - nuevos ransomware para Windows, Linux y ESXi.
https://securelist.com/luna-black-basta-ransomware/106950/
- Errores de GPS sin “parchear” permiten a los atacantes interceptar vehículos en forma remota.
https://thehackernews.com/2022/07/unpatched-gps-tracker-bugs-could-let.html

- El nuevo malware para Linux "Lightning Framework" instala rootkits y puertas traseras.
https://securityaffairs.co/wordpress/133506/malware/lightning-framework-linux-malware.html
- Google bloquea el sitio de la mayor sociedad informática, ACM, por ser "perjudicial".
https://www.bleepingcomputer.com/news/security/google-blocks-site-of-largest-computing-society-for-being-harmful-/
- Actores de la amenaza atacaron una gran empresa de desarrollo de software en Ucrania utilizando el backdoor GoMet.
https://securityaffairs.co/wordpress/133520/malware/attackers-target-software-firm-ukraine-gomet.html

NOTAS DE INTERÉS

- La botnet Mantis está detrás del mayor ataque DDoS HTTPS dirigido a clientes de Cloudflare.
https://thehackernews.com/2022/07/mantis-botnet-behind-largest-https-ddos.html
- Las empresas financieras no solucionan los fallos de autenticación.
https://www.infosecurity-magazine.com/news/financial-firms-authentication/
- Los hackers atacan los servidores de VoIP explotando el software telefónico de Digium.
https://thehackernews.com/2022/07/hackers-targeting-voip-servers-by.html
- La red de mensajería descentralizada Matrix ya cuenta con más de 60 millones de usuarios.
https://www.bleepingcomputer.com/news/security/the-matrix-messaging-network-now-counts-more-than-60-million-users/
- Se solucionó el problema del ataque Retbleed del kernel de Linux y se ha retrasado el parche.
https://www.darkreading.com/application-security/retbleed-fixed-in-linux-kernel-patch-delayed
- La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de EE.UU. abrirá una oficina en Londres.
https://www.infosecurity-magazine.com/news/cisa-set-to-open-london-office/
- Los servidores en la nube de Google y Oracle se derriten por la ola de calor en el Reino Unido y dejan de funcionar.
https://www.theregister.com/2022/07/19/google_oracle_cloud/
- Google retira las aplicaciones infectadas con malware en su tienda.
https://www.theregister.com/2022/07/19/google_malware_apps/
- El grupo '8220' hace crecer la red de bots en la nube a más de 30.000 hosts.
https://www.bleepingcomputer.com/news/security/hacking-group-8220-grows-cloud-botnet-to-more-than-30-000-hosts/
- El Cibercomando de EE.UU. revela malware dirigido a entidades ucranianas.
https://www.theregister.com/2022/07/21/us_cyber_command_malware_ukraine/

ACTUALIZACIONES DE SEGURIDAD

- Aviso de actualización de parches críticos de Oracle, julio de 2022.
https://www.oracle.com/security-alerts/cpujul2022.html
- Google presenta actualizaciones de seguridad para Chrome.
https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html
- Cisco repara vulnerabilidades graves en el tablero Nexus.
https://www.securityweek.com/cisco-patches-severe-vulnerabilities-nexus-dashboard
- Apple libera parches de seguridad que corrigen decenas de vulnerabilidades.
https://thehackernews.com/2022/07/apple-releases-security-patches-for-all.html