@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. 178 – 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 01/08/22 y el 07/08/22

- La banda de ransomware BlackCat informa que atacó al proveedor de energía de Luxemburgo.
https://www.darkreading.com/risk/european-energy-supplier-encevo-breached-in-attack
- El fabricante de misiles europeo MBDA niega haber sido “pirateado” pero admite pérdida de datos.
https://cybernews.com/news/missile-maker-mbda-denies-being-hacked-admits-to-data-loss/
- El fabricante alemán de semiconductores Semikron sufre un ataque de ransomware en LV.
https://www.bleepingcomputer.com/news/security/semiconductor-manufacturer-semikron-hit-by-lv-ransomware-attack/
- Sitios del gobierno taiwanés sufren ataques DDoS antes de la visita de Pelosi.
https://www.cyberscoop.com/taiwan-china-ddos-pelosi-visit/
- La agencia de investigación y desarrollo española se sigue recuperando tras el ataque ransomware.
https://www.bleepingcomputer.com/news/security/spanish-research-agency-still-recovering-after-ransomware-attack/
- Las Cámaras de Industria y Comercio alemanas sufren un ciberataque "masivo".
https://www.bleepingcomputer.com/news/security/german-chambers-of-industry-and-commerce-hit-by-massive-cyberattack/

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

- Hackers chinos utilizan el nuevo marco de hacking Manjusaka, similar a Cobalt Strike.
https://thehackernews.com/2022/08/chinese-hackers-using-new-manjusaka.html
- Lobo con piel de cordero: cómo el malware engaña a los usuarios y a los antivirus.
https://www.bleepingcomputer.com/news/security/wolf-in-sheep-s-clothing-how-malware-tricks-users-and-antivirus/
- **Una CPU de un solo núcleo descifra un algoritmo candidato a la encriptación poscuántica en sólo una hora.**
https://nakedsecurity.sophos.com/2022/08/03/post-quantum-cryptography-new-algorithm-gone-in-60-minutes/
- GitHub fue afectado por un "investigador" que creó miles de proyectos fraudulentos.
https://nakedsecurity.sophos.com/2022/08/04/github-blighted-by-researcher-who-created-thousands-of-malicious-projects/
- Un nuevo malware para Linux que por fuerza bruta penetra redes desde los servidores SSH.
https://www.bleepingcomputer.com/news/security/new-linux-malware-brute-forces-ssh-servers-to-breach-networks/
- **CISA añade la vulnerabilidad del e-mail Zimbra a su catálogo de vulnerabilidades explotadas..**
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- Hackers emplean nuevo ransomware en ataques a los sitios web del gobierno de Albania.
https://www.cyberscoop.com/iran-hack-albania-ransomware-mek/
- El nuevo ransomware GwisinLocker encripta servidores Windows y Linux ESXi.
https://www.bleepingcomputer.com/news/security/new-gwisinlocker-ransomware-encrypts-windows-and-linux-esxi-servers/

NOTAS DE INTERÉS

- El cargador de Gootkit reaparece con una táctica nueva que compromete computadoras objetivo.
https://thehackernews.com/2022/07/gootkit-loader-resurfaces-with-updated.html
- Según Akamai Technologies, esta firma anuló el mayor ataque DDoS de la historia en Europa.
https://www.theregister.com/2022/08/01/ddos_europe_akamai/
- El nuevo rootkit CosmicStrand se centra en las placas base Gigabyte y ASUS.
https://www.techrepublic.com/article/new-cosmicstrand-rootkit-targets-gigabyte-and-asus-motherboards/
- Hackers norcoreanos utilizan una extensión del navegador para espiar las cuentas de Gmail y AOL.
https://www.infosecurity-magazine.com/news/north-korean-hackers-use-browser/
- La vulnerabilidad "ParseThru" permite el acceso no autorizado a las aplicaciones nativas en la nube.
https://www.helpnetsecurity.com/2022/08/02/parsethru-vulnerability/
- Microsoft anunció un nuevo producto de seguridad que permite al equipo de ciberseguridad detectar los recursos expuestos a Internet.
https://www.bleepingcomputer.com/news/microsoft/microsoft-announces-new-external-attack-surface-audit-tool/
- Organizaciones rusas son atacadas con el malware Woody RAT.
https://www.bleepingcomputer.com/news/security/russian-organizations-attacked-with-new-woody-rat-malware/
- Las agencias de ciberseguridad revelan las principales variedades de malware del año pasado.
https://www.bleepingcomputer.com/news/security/cybersecurity-agencies-reveal-last-year-s-top-malware-strains/
- El misterioso grupo TAC-040 utilizó el Backdoor Ljl, no detectado anteriormente.
https://securityaffairs.co/wordpress/134033/hacking/tac-040-ljl-backdoor.html
- Crece el número de ataques de malware que aprovechan las utilidades oscuras "C2-as-a-Service".
https://thehackernews.com/2022/08/a-growing-number-of-malware-attacks.html
- Twitter confirma el uso de un día cero para exponer los datos de 5,4 millones de cuentas.
https://www.bleepingcomputer.com/news/security/twitter-confirms-zero-day-used-to-expose-data-of-54-million-accounts/
- Es probable grupos iraníes estén detrás de ciberataques graves contra el gobierno de Albania.
https://thehackernews.com/2022/08/iranian-hackers-likely-behind.html

ACTUALIZACIONES DE SEGURIDAD

- VMware libera parches para varios fallos que afectan a sus productos y vulnerabilidades críticas.
https://thehackernews.com/2022/08/vmware-releases-patches-for-several-new.html
- Google soluciona un fallo crítico de Bluetooth en Android en el boletín de seguridad de agosto.
https://www.infosecurity-magazine.com/news/google-patches-critical-android/
- Cisco corrige un fallo crítico de ejecución remota de código en los routers VPN.
https://exchange.xforce.ibmcloud.com/collection/15a81b717045ff9fc29427ffddef74b4