@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. 175 – 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 08/07/22 y el 14/07/22

- El ataque del ransomware Quantum afecta a 657 organizaciones sanitarias.
https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-affects-657-healthcare-orgs/
- **Ciberdelincuentes pro rusos realizan un breve ataque DDoS al sitio del Congreso de EE.UU.**
https://www.cyberscoop.com/killnet-congress-ddos-russia-hacktivist/
- Un ataque de ransomware afecta a una empresa de telecomunicaciones francesa.
https://www.infosecurity-magazine.com/news/ransomware-french-telecomes/
- El Banco Central Europeo fue objeto de un intento de hackeo, pero no comprometió información.
https://www.securityweek.com/european-central-bank-head-targeted-hacking-attempt

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

- Detallan las técnicas que utiliza el ransomware LockBit para infectar a sus objetivos.
https://thehackernews.com/2022/07/researchers-detail-techniques-lockbit.html
- Los hackers aprovechan el fallo Follina para introducir el backdoor Rozena.
https://thehackernews.com/2022/07/hackers-exploiting-follina-bug-to.html
- **Método para detectar cámaras y micrófonos ocultos.**
https://www.kaspersky.com/blog/how-to-find-spy-cameras-and-other-iot-devices/44833/
- Empresa energética lituana afectada por un ataque DDOS.
https://www.infosecurity-magazine.com/news/lithuanian-energy-ddos-attack/
- Los atacantes utilizan los sitios de phishing AiTM como punto de entrada para continuar con el fraude financiero.
https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/
- **Los nuevos fallos de firmware UEFI afectan a más de 70 modelos de portátiles de Lenovo.**
https://www.bleepingcomputer.com/news/security/new-uefi-firmware-flaws-impact-over-70-lenovo-laptop-models/
- El ransomware Lilith ha aparecido con un sitio de extorsión y una lista de sus primeras víctimas.
https://www.bleepingcomputer.com/news/security/new-lilith-ransomware-emerges-with-extortion-site-lists-first-victim/
- Actor de la amenaza norcoreano apunta a pequeñas y medianas empresas con el ransomware H0lyGh0st.
https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

NOTAS DE INTERÉS

- China sufre una enorme brecha de ciberseguridad que afecta a más de mil millones de personas.
https://www.techrepublic.com/article/china-suffers-massive-cybersecurity-breach-affecting-over-1-billion-people/

- **Por qué el modo Lockdown de Apple es una de las ideas de seguridad más interesantes.**
https://arstechnica.com/information-technology/2022/07/introducing-lockdown-from-apple-the-coolest-defense-youll-probably-never-use/
- Los grupos de ciberespionaje chinos se centran cada vez más en Rusia.
https://www.infosecurity-magazine.com/news/chinese-cyber-espionage-russia/
- Se publica un descifrador gratuito para las víctimas del ransomware AstraLocker y Yashma.
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-astralocker-yashma-ransomware-victims/
- Acusan a Facebook de guardar datos “borrados” de Messenger y compartirlos con la policía.
https://news.sky.com/story/facebook-accused-of-saving-deleted-messenger-data-and-sharing-it-with-police-12648081
- ¿Quiénes son los hackers que dicen haber provocado un incendio en Irán?
https://www.bbc.com/news/technology-62072480
- Una campaña phishing a gran escala usa la red Anubis y afecta a Brasil y Portugal desde marzo de 2022.
https://securityaffairs.co/wordpress/133115/hacking/anubis-networks-new-c2.html
- **El repositorio PyPI hace obligatoria la seguridad 2FA para los proyectos críticos de Python.**
https://thehackernews.com/2022/07/pypi-repository-makes-2af-security.html
- El ransomware BlackCat (o ALPHV) aumenta las exigencias hasta 2,5 millones de dólares.
https://www.helpnetsecurity.com/2022/07/11/blackcat-alphv-ransomware/
- La nube Akamai Linode ofrece actualmente instalaciones de Kali Linux.
https://www.zdnet.com/article/akamai-linode-now-offers-kali-linux-instances/
- Hackers afirman que pueden desbloquear y arrancar los coches Honda a distancia.
https://www.vice.com/en/article/z34xnw/hackers-say-they-can-unlock-and-start-honda-cars-remotely
- Un fondo amparado por la Casa Blanca promete acelerar los avances de la "tecnología profunda" en ciberseguridad.
https://www.cyberscoop.com/white-house-backed-fund-deep-tech/
- **Los proyectos de seguridad IIoT/OT de infraestructuras críticas sufren altas tasas de fallos.**
https://www.techrepublic.com/article/critical-infrastructure-iiot-ot-security-projects-suffer-high-rates-of-failure/
- La Agencia Cibernética de Ucrania informa del aumento de ciberataques en el segundo trimestre.
https://www.infosecurity-magazine.com/news/ukraine-cyber-agency-cyber-attack/
- El ataque “Retbleed“, de ejecución especulativa, afecta a las CPUs de AMD e Intel.
https://thehackernews.com/2022/07/new-retbleed-speculative-execution.html
- Grupo APT patrocinado por un Estado tienen como objetivo a periodistas
https://www.cyberscoop.com/china-iran-north-korea-turkey-hackers-journalists-media-malware-phishing/

ACTUALIZACIONES DE SEGURIDAD

- Parche del Martes de Microsoft, julio de 2022 - Reglas de Snort y vulnerabilidades destacadas.
https://blog.talosintelligence.com/2022/07/microsoft-patch-tuesday-for-july-2022.html
- Martes de parches de Adobe: Fallos críticos en Acrobat, Reader y Photoshop.
https://www.securityweek.com/adobe-patch-tuesday-critical-flaws-acrobat-reader-photoshop
- **VMware parchea el fallo de vCenter Server divulgado en noviembre.**
https://www.bleepingcomputer.com/news/security/vmware-patches-vcenter-server-flaw-disclosed-in-november/