@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. 172 – 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 17/6/22 y el 23/6/22

- Flagstar Bank revela una filtración de datos que afecta a 1,5 millones de clientes.
https://www.bleepingcomputer.com/news/security/flagstar-bank-discloses-data-breach-impacting-15-million-customers/
- **Una interrupción de Cloudflare afectó a grandes franjas de Internet.**
https://www.theverge.com/2022/6/21/23176519/cloudflare-outage-june-2022-discord-shopify-fitbit-peleton
- La empresa de mensajería Yodel confirma que el ciberataque está interrumpiendo las entregas.
https://www.bleepingcomputer.com/news/security/yodel-parcel-company-confirms-cyberattack-is-disrupting-delivery/
- La policía europea desmantela una banda de phishing multimillonaria.
https://www.infosecurity-magazine.com/news/cops-dismantle-phishing-gang/
- **Lituania sufre un ciberataque tras prohibir el transporte de productos por trenes rusos.**
https://securityaffairs.co/wordpress/132518/hacktivism/lithuania-under-cyber-attack.html
- Nichirin, fabricante de partes de automóviles, es afectado por un ransomware.
https://www.helpnetsecurity.com/2022/06/23/nichirin-ransomware/

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

- Hackers chinos aprovecharon un error de día cero del firewall Sophos, para atacar a una entidad del sur de Asia.
https://thehackernews.com/2022/06/chinese-hackers-exploited-sophos.html
- El atacante de Capital One explotó bases de datos de AWS mal configuradas.
https://www.darkreading.com/attacks-breaches/capital-one-attacker-exploited-misconfigured-aws-databases
- **El ataque “NTLM relay”, permite a los atacantes tomar el control del dominio de Windows.**
https://thehackernews.com/2022/06/new-ntlm-relay-attack-lets-attackers.html
- Diez pasos para incrementar la ciberseguridad.
https://www.ncsc.gov.uk/collection/10-steps
- La APT ToddyCat, vinculada a China, es pionera en la creación de un nuevo software espía.
https://www.darkreading.com/attacks-breaches/china-linked-toddycat-apt-pioneers-novel-spyware
- 7-zip ahora es compatible con la función de seguridad "Mark-of-the-Web" de Windows.
https://www.bleepingcomputer.com/news/microsoft/7-zip-now-supports-windows-mark-of-the-web-security-feature/
- La infraestructura de Magecart, recién descubierta, revela la escala de la campaña en curso.
https://thehackernews.com/2022/06/newly-discovered-magecart.html

- **Mega, empresa de almacenamiento en la nube, asegura que no se pueden descifrar los archivos de los usuarios. El nuevo exploit POC demuestra lo contrario.**
https://arstechnica.com/information-technology/2022/06/mega-says-it-cant-decrypt-your-files-new-poc-exploit-shows-otherwise/
https://www.securityweek.com/top-cryptographers-flag-devastating-flaws-mega-cloud-storage

- Los ataques malintencionados 'LNK', a Windows, son más simples con el nuevo editor Quantum.
https://www.bleepingcomputer.com/news/security/malicious-windows-lnk-attacks-made-easy-with-new-quantum-builder/

NOTAS DE INTERÉS

- QNAP "investiga a fondo" los nuevos ataques del ransomware DeadBolt.
https://www.bleepingcomputer.com/news/security/qnap-thoroughly-investigating-new-deadbolt-ransomware-attacks/

- Autoridades de EE.UU. cierran la red de bots rusa RSOCKS que hackeó millones de dispositivos.
https://thehackernews.com/2022/06/authorities-shut-down-russian-rsocks.html

- Más de doce bugs se detectaron en el sistema de gestión de redes industriales de Siemens.
https://thehackernews.com/2022/06/over-dozen-flaws-found-in-siemens.html

- El malware BRATA para Android adquiere capacidades avanzadas de amenaza móvil.
https://thehackernews.com/2022/06/brata-android-malware-gains-advanced.html

- Funcionarios de ciberseguridad ucranianos revelan dos nuevas campañas de hacking.
https://www.cyberscoop.com/ukraine-russia-hacking-apt28-trickbot-follina/

- **La Fundación Linux anuncia el "Proyecto de Infraestructura Programable Abierta" para guiar los estándares para la nueva clase de infraestructura nativa de la nube.**
https://www.darkreading.com/cloud/linux-foundation-announces-open-programmable-infrastructure-project-to-drive-open-standards-for-new-class-of-cloud-native-infrastructure

- El buscador para Internet, Brave Search, centrado en la privacidad, creció un 5.000% en un año.
https://www.bleepingcomputer.com/news/software/privacy-focused-brave-search-grew-by-5-000-percent-in-a-year/

- Grupo chino dispara, armado con Nim Language y Bizarro AES.
https://research.checkpoint.com/2022/chinese-actor-takes-aim-armed-with-nim-language-and-bizarro-aes/

- Una investigación cuestiona las consecuencias potencialmente peligrosas del ejército informático de Ucrania.
https://www.cyberscoop.com/ukraine-it-army-fedorov-russia-ddos/

- Hackers chinos distribuyen una herramienta SMS Bomber con malware oculto.
https://thehackernews.com/2022/06/chinese-hackers-distributing-sms-bomber.html

- El grupo ransomware Avos actualiza su arsenal de ataque.
https://www.techrepublic.com/article/avos-ransomware-updates-attack/

- **El ransomware de Conti ha vulnerado más de 40 organizaciones en un mes,**
https://www.bleepingcomputer.com/news/security/conti-ransomware-hacking-spree-breaches-over-40-orgs-in-a-month/

ACTUALIZACIONES DE SEGURIDAD

- Cisco ha publicado un aviso que contiene un parche oficial para Secure Email y Web Manager.
https://exchange.xforce.ibmcloud.com/collection/5978be4e16816b62c609545877f6e1ac

- Google anuncia actualizaciones de seguridad para Chrome.
https://www.cisa.gov/uscert/ncas/current-activity/2022/06/22/google-releases-security-updates-chrome