@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. 173 – 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 24/6/22 y el 30/6/22

- Fast Shop, uno de los mayores minoristas de Brasil, sufrió un ciberataque ransomware extorsivo.
https://www.bleepingcomputer.com/news/security/fast-shop-brazilian-retailer-discloses-extortion-cyberattack/
- El proveedor de tejidos para automóviles TB Kawashima informa un ciberataque.
https://www.bleepingcomputer.com/news/security/automotive-fabric-supplier-tb-kawashima-announces-cyberattack/
- **El grupo de hackers pro rusos Killnet ataca sitios web gubernamentales críticos en Lituania.**
https://www.infosecurity-magazine.com/news/killnet-hacks-lithuania-government/
https://www.reuters.com/technology/lithuania-hit-by-cyber-attack-government-agency-2022-06-27/
- El gobierno de Lituania confirmó que ha sufrido un intenso ciberataque.
https://securityaffairs.co/wordpress/132676/cyber-warfare-2/lithuania-massive-ddos.html
- **Las instalaciones siderúrgicas iraníes sufren aparentes ciberataques.**
https://www.cyberscoop.com/iran-cyberattack-israel-hacktivist-steel-ics/
- **Un grupo de hackers rusos derriba los sitios del gobierno de Noruega en ataques DDoS.**
https://www.bleepingcomputer.com/news/security/russian-hacktivists-take-down-norway-govt-sites-in-ddos-attacks/

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

- Múltiples librerías de Python con respaldo descubiertas robando secretos y claves de AWS.
https://thehackernews.com/2022/06/multiple-backdoored-python-libraries.html
https://www.helpnetsecurity.com/2022/06/27/python-packages-malicious-code-aws-credentials-video/
- El ransomware Conti pone fin a la filtración de datos y a los sitios de negociación.
https://www.bleepingcomputer.com/news/security/conti-ransomware-finally-shuts-down-data-leak-negotiation-sites/
- **Detalle de ataques ransomware de la última semana.**
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-24th-2022-splinter-cells/
- Nuevo troyano, 'Revive' para Android, enfocado en usuarios de servicios financieros españoles.
https://thehackernews.com/2022/06/new-android-banking-trojan-revive.html
- Los chatbots de Messenger ahora se utilizan para robar cuentas de Facebook.
https://www.bleepingcomputer.com/news/security/messenger-chatbots-now-used-to-steal-facebook-accounts/
- El aprendizaje automático *adversario*: cómo los agresores afectan los sistemas de IA y ML.
https://www.csoonline.com/article/3664748/adversarial-machine-learning-explained-how-attackers-disrupt-ai-and-ml-systems.html
- Raccoon Stealer ha vuelto con una nueva versión para robar contraseñas.
https://www.bleepingcomputer.com/news/security/raccoon-stealer-is-back-with-a-new-version-to-steal-your-passwords/

- **MITRE comparte la lista de errores de software más peligrosos de este año.**
https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
- **Asegurar el Metaverso y la Web3.**
https://www.securityweek.com/securing-metaverse-and-web3
- Los routers SOHO se usan como punto inicial de compromiso en una campaña de ataque furtivo.
https://www.techrepublic.com/article/soho-routers-compromise-attack/

NOTAS DE INTERÉS

- Google revela una sofisticada campaña de spyware italiana dirigida a víctimas de Italia y Kazajistán.
https://www.cyberscoop.com/google-reveals-sophisticated-italian-spyware-campaign-targeting-victims-in-italy-kazakhstan/
- Log4Shell sigue siendo explotado para hackear servidores VMWare para extraer datos sensibles.
https://thehackernews.com/2022/06/log4shell-still-being-exploited-to-hack.html
- Según un reporte sólo el 3% de los fallos del software de código abierto son realmente atacables.
https://www.darkreading.com/application-security/open-source-software-bugs--attackability
- Las empresas corren el riesgo de sufrir "pérdidas financieras catastróficas" por los ciberataques, advierte un organismo de control estadounidense.
https://www.theverge.com/2022/6/23/23180115/gao-infrastructure-catastrophic-financial-loss-cyberattacks-insurance
- Los investigadores advierten de la campaña de malware "Matanbuchus".
https://thehackernews.com/2022/06/researchers-warn-of-matanbuchus-malware.html
- **Actores vinculados a Rusia podrían estar detrás de una explosión en una planta de gas natural licuado en Texas.**
https://securityaffairs.co/wordpress/132608/security/liquefied-natural-gas-plant-texas-explosion.html
- Hackers APT atacan los sistemas de control industrial con el backdoor ShadowPad.
https://thehackernews.com/2022/06/apt-hackers-targeting-industrial.html
- Un error del VoIP de Mitel es aprovechado en los ataques de ransomware.
https://threatpost.com/mitel-voip-bug-exploited/180079/
- Una base de datos cataloga las vulnerabilidades de la nube y los problemas de seguridad.
https://www.securityweek.com/new-database-catalogs-cloud-vulnerabilities-security-issues
- El malware ZuoRAT piratea los routers de tipo “home office” para espiar redes seleccionadas.
https://thehackernews.com/2022/06/zuorat-malware-hijacking-home-office.html
- **Nueva vulnerabilidad UnRAR, permite hackear los servidores de correo web de Zimbra.**
https://thehackernews.com/2022/06/new-unrar-vulnerability-could-let.html

ACTUALIZACIONES DE SEGURIDAD

- **Las actualizaciones opcionales de Windows publicadas corrigen problemas de VPN, RDP, RRAS y Wi-Fi.**
https://www.bleepingcomputer.com/news/microsoft/june-windows-preview-updates-fix-vpn-rdp-rras-and-wi-fi-issues/
- **OpenSSL publica una solución para un error previo.**
https://nakedsecurity.sophos.com/2022/06/24/openssl-issues-a-bugfix-for-the-previous-bugfix/