@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. 153 – 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 4/2/22 y el 11/2/22

- Un ataque del ransomware a Swissport retrasa los vuelos e interrumpe las operaciones.
https://securityaffairs.co/wordpress/127655/cyber-crime/swissport-international-ransomware-attack.html
- El ransomware Conti cifró el 80% de los sistemas informáticos del servicio de salud irlandés.
https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/
- Morley Companies informó de más de 500 mil personas se vieron afectadas por una filtración de datos derivada de un ataque de ransomware.
https://www.zdnet.com/article/fortune-500-service-provider-says-ransomware-attack-led-to-leak-of-more-than-500k-ssns-more/
- News Corp (Dow Jones, Daily Telegraph, NY Post, Fox, etc.), informa de un ciberataque.
https://www.infosecurity-magazine.com/news/news-corp-discloses-cyberattack/
- El *Foreign Office* de Gran Bretaña es objeto de un "grave incidente cibernético".
https://www.bbc.com/news/technology-60309335
- Los servicios 4G y 5G de Vodafone Portugal caen tras un ciberataque.
https://www.bleepingcomputer.com/news/security/vodafone-portugal-4g-and-5g-services-down-after-cyberattack/

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

- **Los hackers explotaron una vulnerabilidad de día 0 en la plataforma de correo electrónico Zimbra para espiar a los usuarios.**
https://thehackernews.com/2022/02/hackers-exploited-0-day-vulnerability.html
- Las 3 causas más comunes de los ataques a los datos en 2021.
https://www.darkreading.com/edge-threat-monitor/most-common-cause-of-data-breach-in-2021-phishing-smishing-bec
- **Se descubren vulnerabilidades críticas de Samba.**
https://exchange.xforce.ibmcloud.com/collection/684490b9f673f05c9af43409bf16fd48
- Amenazas adaptativas altamente evasivas (HEAT) que eluden las defensas de seguridad tradicionales.
https://www.helpnetsecurity.com/2022/02/08/cyberthreats-bypass-security-defenses/
- Qbot sólo necesita 30 minutos para robar sus credenciales y correos electrónicos.
https://www.bleepingcomputer.com/news/security/qbot-needs-only-30-minutes-to-steal-your-credentials-emails/
- Falsos instaladores de la actualización de Windows 11 infectan con el malware RedLine.
https://www.bleepingcomputer.com/news/security/fake-windows-11-upgrade-installers-infect-you-with-redline-malware/

- El desarrollador del ransomware Egregor y Maze publica las claves de desencriptación maestras. https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/
- El grupo de piratas informáticos "ModifiedElephant" no fue descubierto durante una década. https://www.bleepingcomputer.com/news/security/hacking-group-modifiedelephant-evaded-discovery-for-a-decade/

NOTAS DE INTERÉS

- El mercado de seguridad de bases de datos alcanzará los 16.273,8 millones de dólares en 2028. https://www.helpnetsecurity.com/2022/02/04/2028-database-security-market/
- Microsoft desactiva el controlador de protocolo MSIX que se ha utilizado en los ataques Emotet. https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-msix-protocol-handler-abused-in-emotet-attacks/
- Microsoft revela nuevos detalles de la campaña de piratería informática rusa dirigida a Ucrania. https://thehackernews.com/2022/02/microsoft-uncovers-new-details-of.html
- APT china ataca instituciones financieras taiwanesas con una nueva puerta trasera furtiva. https://thehackernews.com/2022/02/chinese-hackers-target-taiwanese.html
- La APT rusa Gamaredon tiene como objetivo Ucrania desde octubre. https://securityaffairs.co/wordpress/127729/apt/actinium-gamaredon-ukraine.html
- El malware CapraRAT para Android tiene como objetivo al gobierno indio y su personal militar. https://thehackernews.com/2022/02/new-caprarat-android-malware-targets.html
- El bug Win32k de Microsoft se añade a la lista de CISA de vulnerabilidades explotables. https://www.zdnet.com/article/microsoft-win32k-bug-added-to-cisas-exploited-vulnerabilities-list/
- Microsoft bloquea macros que se descargan en las versiones de Office que se remontan a 2013. https://arstechnica.com/gadgets/2022/02/microsoft-will-block-downloaded-macros-in-office-versions-going-back-to-2013/
- Google ha registrado automáticamente a 150 millones de usuarios en la verificación en dos pasos. https://www.zdnet.com/article/google-has-auto-enrolled-150-million-users-in-2-step-verification/
- Hackers afines a Palestina utilizan el nuevo implante *NimbleMamba* en sus recientes ataques. https://thehackernews.com/2022/02/palestinian-hackers-using-new.html
- **Los ataques de malware a Linux están aumentando y las empresas no están preparadas.** https://www.zdnet.com/article/linux-malware-attacks-are-on-the-rise-and-businesses-arent-ready-for-it/
- La red de bots P2P FritzFrog ataca sectores de sanidad, la educación y la administración pública. https://thehackernews.com/2022/02/fritzfrog-p2p-botnet-attacking.html
- Los errores de PHP Everywhere ponen en riesgo de RCE a más de 30.000 sitios de WordPress. https://threatpost.com/php-everywhere-bugs-wordpress-rce/178338/
- Gobierno de EE.UU.: otros 15 bugs de seguridad que están siendo atacados en este momento. https://www.theregister.com/2022/02/11/cisa_database/

ACTUALIZACIONES DE SEGURIDAD

- Las grandes empresas de software publican las actualizaciones de parches de febrero de 2022. **https://thehackernews.com/2022/02/microsoft-and-other-major-software.html**
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D
  https://threatpost.com/sap-patches-severe-icmad-bugs/178344/
  https://thehackernews.com/2022/02/apple-releases-ios-ipados-macos-updates.html