@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. 165 – 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 29/4/22 y el 5/5/22

- Un ciberataque al sistema de reservas de un hotel finlandés de lujo, ha dejado al descubierto los datos personales de miles de clientes.
  https://www.infosecurity-magazine.com/news/finnish-hotels-data-compromised/
- El enorme grupo de alquiler de coches Sixt, se enfrenta a interrupciones debido a un ciberataque.
  https://www.bleepingcomputer.com/news/security/car-rental-giant-sixt-facing-disruptions-due-to-a-cyberattack/
- **Se encuentra un software espía, Pegasus, en el teléfono del primer ministro español.**
  https://www.infosecurity-magazine.com/news/spyware-found-on-spanish-pms-phone/

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

- GitHub publica un informe final sobre las intrusiones en el código fuente de la cadena de suministro.
  https://nakedsecurity.sophos.com/2022/04/29/github-issues-final-report-on-supply-chain-source-code-intrusions/
- Las falsas actualizaciones de Windows 10 lo infectan con el ransomware Magniber.
  https://www.bleepingcomputer.com/news/security/fake-windows-10-updates-infect-you-with-magniber-ransomware/
- Herramienta de código abierto 'Package Analysis': encuentra paquetes maliciosos de npm y PyPI.
  https://www.bleepingcomputer.com/news/security/open-source-package-analysis-tool-finds-malicious-npm-pypi-packages/
- La APT china ShadowPad es sorprendida usando productos antivirus populares para atacar el sector de las telecomunicaciones.
  https://thehackernews.com/2022/05/chinese-hackers-caught-exploiting.html
- El grupo de hackers chino conocido como 'Winnti' robó datos sin ser detectado de organizaciones de EEUU y Europa desde 2019.
  https://www.darkreading.com/attacks-breaches/china-winnti-apt-trade-secrets-us
- El proyecto Tor mejora el rendimiento de la velocidad de la red con un nuevo sistema.
  https://www.bleepingcomputer.com/news/security/tor-project-upgrades-network-speed-performance-with-new-system/
- **Documento del NIST: Riesgo de la cadena de suministro de ciberseguridad. Prácticas de gestión de riesgos en la cadena de suministro para sistemas y organizaciones.**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

NOTAS DE INTERÉS

- La APT conocida como TA410, que maneja la sofisticada RAT FlowCloud, cuenta con tres subgrupos que operan a nivel mundial.
  https://threatpost.com/apt-id-3-separate-actors/179435/

- Sina Weibo, el análogo chino de Twitter, revela la ubicación y la dirección IP de los usuarios.
https://www.theregister.com/2022/04/29/weibo_location_services_default/
- **"Hacktivistas" rusos lanzan ataques DDoS contra sitios del gobierno rumano.**
https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/
- La India da un tiempo de 60 días a los técnicos locales para que cumplan el plazo de 6 horas para informar sobre incidentes de infoseguridad.
https://www.theregister.com/2022/04/29/cert_in_directive/
- La APT china "Override Panda" reaparecen con nuevos ataques de espionaje.
https://thehackernews.com/2022/05/chinese-override-panda-hackers.html
- Abuso del servicio de retransmisión SMTP de Google para el envío de e-mail de phishing.
https://www.bleepingcomputer.com/news/security/google-smtp-relay-service-abused-for-sending-phishing-emails/
- **Nuevo proyecto permite Incorporar scripts de Python en HTML con PyScript.**
https://www.bleepingcomputer.com/news/technology/embed-python-scripts-in-html-with-pyscript/
- Vulnerabilidad relacionada con el DNS sin parches afecta a una amplia gama de dispositivos IoT.
https://thehackernews.com/2022/05/unpatched-dns-related-vulnerability.html
- Nuevas variantes de ransomware vinculadas a hackers del gobierno norcoreano.
https://www.darkreading.com/threat-intelligence/new-ransomware-variant-linked-to-north-korean-cyber-army
- Google TAG señala que el grupo del EPL de China persigue a varios contratistas de defensa rusos.
https://www.zdnet.com/article/google-tag-sees-china-pla-group-go-after-multiple-russian-defence-contractors/
- Un número cada vez mayor de actores de amenazas están utilizando la actual guerra ruso-ucraniana como señuelo en diversas campañas de phishing y malware
https://thehackernews.com/2022/05/ukraine-war-themed-files-become-lure-of.html
- GitHub lanza nuevos requisitos de 2FA para los desarrolladores de código y los colaboradores.
https://www.zdnet.com/article/github-launches-new-two-factor-authentication-mandates-for-code-developers/
- **Corea del Sur es admitida en el Centro de Ciberdefensa de la OTAN.**
https://www.infosecurity-magazine.com/news/south-korea-admitted-to-nato-cyber/
- El ransomware VHD está vinculado al grupo Lazarus de Corea del Norte.
https://threatpost.com/vhd-ransomware-lazarus-group/179507/
- UNC3524: La amenaza de ciberespionaje casi invisible que se encuentra en los dispositivos de red.
https://www.techrepublic.com/article/unc3524-invisible-threat-network-appliances/

ACTUALIZACIONES DE SEGURIDAD

- Microsoft está incorporando una VPN gratuita a su navegador Edge.
https://www.theverge.com/2022/4/29/23049015/microsoft-free-built-in-vpn-edge-browser-edge-secure-network
- Microsoft publica la Build 22610 de Windows 11 con nuevas políticas de grupo y un gran número de correcciones.
https://betanews.com/2022/04/29/windows-11-build-22610/
- La distribución Linux Tails 5.0, centrada en la privacidad, ya está disponible.
https://betanews.com/2022/05/03/linux-distro-tails-5-released/
- Microsoft advierte que la autentificación básica de Exchange Online se desactivará.
https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-exchange-online-basic-auth-will-be-disabled/
- Cisco corrige los errores de NFVIS que ayudan a obtener root y apropiarse de los hosts.
https://securityaffairs.co/wordpress/130952/security/cisco-nfvis-software-bugs.html