@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. 166 – 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 6/5/22 y el 12/5/22

- Secuestraron un subdominio de Ferrari para promocionar una falsa colección de NFT de Ferrari.
https://www.bleepingcomputer.com/news/security/ferrari-subdomain-hijacked-to-push-fake-ferrari-nft-collection/
- El fabricante de maquinaria agrícola estadounidense AGCO sufre un ataque de ransomware.
https://www.theregister.com/2022/05/09/farm_machinery_giant_agco_hit/
- **Costa Rica declara la emergencia nacional tras los ataques del ransomware Conti.**
https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
- El ransomware Conti afirma haber hackeado el Ministerio de Finanzas de Perú y la Dirección General de Inteligencia (DIGIMIN).
https://securityaffairs.co/wordpress/131093/cyber-crime/conti-ransomware-peru-direccion-general-de-inteligencia.html
- Dan la voz de alarma sobre la venta del backdoor DarkCrystalRat en los foros de hacking rusos.
https://thehackernews.com/2022/05/experts-sound-alarm-on-dcrat-backdoor.html
- **La empresa de reconocimiento facial Clearview AI aceptó la prohibición que le impedirá vender su BD de reconocimiento facial de más de 20.000 millones de personas a empresas privadas.**
https://www.cyberscoop.com/clearview-ai-aclu-facial-recognition/
- Atacantes informáticos sustituyen la programación de la televisión rusa durante el "Día de la Victoria" por mensajes contra la guerra.
https://www.infosecurity-magazine.com/news/hackers-russian-tv-schedules/

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

- El nuevo gusano Raspberry Robin utiliza el instalador de Windows para introducir malware.
https://redcanary.com/blog/raspberry-robin/
- Un nuevo malware, sin archivos, oculta *shellcode* en los registros de eventos de Windows.
https://thehackernews.com/2022/05/this-new-fileless-malware-hides.html
- El backdoor Octopus ha vuelto con un nuevo archivo "bat", ofuscado e insertado.
https://isc.sans.edu/diary/rss/28628
- **¿Cuál es el malware más sencillo del mundo?**
https://isc.sans.edu/forums/diary/What+is+the+simplest+malware+in+the+world/28620/
- **Cómo eliminar, paso a paso, los resultados de una búsqueda en Internet y ocultar su identidad.**
https://www.zdnet.com/article/how-to-erase-your-digital-footprint-and-make-google-forget-you/
- Los ciberespías de la APT Bitter afectan a los gobiernos del sur de Asia con un nuevo malware.
https://www.bleepingcomputer.com/news/security/bitter-cyberspies-target-south-asian-govts-with-new-malware/

- Miles de sitios de WordPress hackeados para redirigir a los visitantes a sitios de estafa.
https://thehackernews.com/2022/05/thousands-of-wordpress-sites-hacked-to.html
- BPFdoor: Un malware sigiloso para Linux que salta los cortafuegos para acceder de forma remota
https://www.bleepingcomputer.com/news/security/bpfdoor-stealthy-linux-malware-bypasses-firewalls-for-remote-access/

NOTAS DE INTERÉS

- Descubren nuevos ataques de espionaje por parte de los hackers chinos "Mustang Panda".
https://securityaffairs.co/wordpress/131083/apt/mustang-panda-q1-attacks.html
- Los reguladores de criptodivisas se afanan por atrapar a los piratas informáticos que están robando miles de millones.
https://www.cyberscoop.com/cryptocurrency-sec-cybersecurity-bitcoin-regulation-enforcement/
- **La criptografía poscuántica sustituirá a RSA y ECC.**
https://www.darkreading.com/tech-trends/post-quantum-cryptography-set-to-replace-rsa-aes-ecc
- Un grupo de hackers rusos ha amenazado con desconectar los respiradores de los hospitales británicos.
https://www.dailymail.co.uk/news/article-10787595/Sinister-Russian-hacking-group-threatens-shut-hospital-ventilators-Britain.html
- El gobierno británico publica una herramienta gratuita para comprobar los riesgos de ciberseguridad del correo electrónico.
https://www.bleepingcomputer.com/news/security/uk-govt-releases-free-tool-to-check-for-email-cybersecurity-risks/
- El malware FluBot para Android se concentra en Finlandia con nuevas campañas de SMS.
https://www.bleepingcomputer.com/news/security/flubot-android-malware-targets-finland-in-new-sms-campaigns/
- El nuevo troyano "Nerbian" utiliza métodos avanzados de anti detección.
https://threatpost.com/nerbian-rat-advanced-trick/179600/
- Hackers iraníes aprovechan BitLocker y DiskCryptor en ataques de ransomware.
https://thehackernews.com/2022/05/iranian-hackers-leveraging-bitlocker.html

ACTUALIZACIONES DE SEGURIDAD

- Google publica una actualización de Android para corregir una vulnerabilidad que es explotada de manera activa.
https://thehackernews.com/2022/05/google-releases-android-update-to-patch.html
- QNAP corrige la vulnerabilidad crítica de ejecución de comandos remotos de QVR.
https://www.qnap.com/de-de/security-advisory/qsa-22-07
- Se han desarrollado exploits para el fallo crítico de F5 BIG-IP. Se debe instalar el parche.
https://securityaffairs.co/wordpress/131102/hacking/f5-big-ip-exploit-code.html
- Microsoft publicará la corrección por un "defecto de código" en la actualización KB5012599 para Windows 10.
https://betanews.com/2022/05/09/microsoft-to-release-fix-for-code-defect-in-kb5012599-update-for-windows-10/
- Se ha corregido un error en la cadena de suministro del lenguaje de programación Ruby.
https://nakedsecurity.sophos.com/2022/05/09/rubygems-supply-chain-rip-and-replace-bug-fixed-check-your-logs/
- **Microsoft publica las actualizaciones del “martes de parches” de mayo de 2022.**
https://thehackernews.com/2022/05/microsoft-releases-fix-for-new-zero-day.html