@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. 167 – 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 13/5/22 y el 19/5/22

- La empresa brasileña de e-commerce Americanas registra pérdidas multimillonarias tras un ciberataque.
  https://www.zdnet.com/article/brazilian-e-commerce-firm-americanas-reports-multimillion-dollar-loss-following-cyberattack/
- **La APT "Space Pirates" de china, hackean a las empresas aeroespaciales rusas.**
  https://securityaffairs.co/wordpress/131440/apt/space-pirates-targets-space-industry.html
- El banco nacional de Zambia fue afectado por el ransomware.
  https://www.bleepingcomputer.com/news/security/national-bank-hit-by-ransomware-trolls-hackers-with-dick-pics
- La unidad asiática del grupo mediático Nikkei sufre un ataque de ransomware.
  https://www.bleepingcomputer.com/news/security/media-giant-nikkei-s-asian-unit-hit-by-ransomware-attack/

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

- Los falsos bots de Binance NFT Mystery Box roban las criptocarteras de las víctimas.
  https://www.bleepingcomputer.com/news/security/fake-binance-nft-mystery-box-bots-steal-victims-crypto-wallets/
- Encuentran una forma potencial de ejecutar malware en el iPhone incluso cuando está apagado.
  https://thehackernews.com/2022/05/researchers-find-way-to-run-malware-on.html
- **Las agencias de ciberseguridad revelan los principales vectores de ataque de acceso inicial.**
  https://www.bleepingcomputer.com/news/security/cybersecurity-agencies-reveal-top-initial-access-attack-vectors/
- Vulnerabilidades halladas en Bluetooth LE permiten a hackers acceder a numerosos dispositivos.
  https://arstechnica.com/information-technology/2022/05/new-bluetooth-hack-can-unlock-your-tesla-and-all-kinds-of-other-devices/
- Actores de amenazas comprometen las páginas de pago en línea, de las empresas estadounidenses, para robar la información de las tarjetas de crédito.
  https://www.techrepublic.com/article/threat-actors-compromising-us-business-online-checkout-pages-to-steal-credit-card-information/
- Presidente de Microsoft: El ciberespacio se ha convertido en el nuevo dominio de la guerra.
  https://www.infosecurity-magazine.com/news/microsoft-cyberspace-domain-warfare/
- **Informe de tendencias de seguridad de las API.**
  https://salt.security/api-security-trends

NOTAS DE INTERÉS

- Saitama, nueva puerta trasera, afecta a funcionario del Ministerio de Asuntos Exteriores de Jordania.
  https://thehackernews.com/2022/05/new-saitama-backdoor-targeted-official.html
- Actores de la amenaza utilizan Telegram para difundir el malware como servicio "Eternity".
  https://threatpost.com/telegram-spread-eternity-maas/179623/

- **La UE acuerda una nueva legislación sobre ciberseguridad para las organizaciones de servicios críticos.**
  https://www.infosecurity-magazine.com/news/eu-cybersecurity-legislation/
- Microsoft: La red de bots Sysrv se centra en servidores Windows y Linux con nuevos exploits.
  https://www.bleepingcomputer.com/news/security/microsoft-sysrv-botnet-targets-windows-linux-servers-with-new-exploits/
- La Casa Blanca se une a la OpenSSF y la Fundación Linux para asegurar el software de código abierto.
  https://www.zdnet.com/article/white-house-joins-openssf-and-the-linux-foundation-in-securing-open-source-software/
- CERT italiano: Los *hacktivistas* atacan sitios gubernamentales en ataques DDoS "Slow HTTP".
  https://www.bleepingcomputer.com/news/security/italian-cert-hacktivists-hit-govt-sites-in-slow-http-ddos-attacks/
- Ataque de *phishing* se enfoca en los usuarios de MetaMask que visitan sitios de criptografía.
  https://www.theverge.com/2022/5/13/23071786/etherscan-coingecko-crypto-phishing-ad-popup-coinzilla-metamask
- **Algunos de los 100.000 sitios web más importantes recopilan todo lo que escribes, antes de que pulses "enviar".**
  https://arstechnica.com/information-technology/2022/05/some-top-100000-websites-collect-everything-you-type-before-you-hit-submit/
- EE.UU. vincula el ransomware Thanos y Jigsaw con un médico de 55 años.
  https://thehackernews.com/2022/05/us-charges-venezuelan-doctor-for-using.html
- La banda rusa Conti Ransomware amenaza con derrocar al nuevo gobierno de Costa Rica,
  https://thehackernews.com/2022/05/russian-conti-ransomware-gang-threatens.html
- Microsoft advierte de la existencia de un malware de robo de información "Cryware" dirigido a las criptocarteras.
  https://thehackernews.com/2022/05/microsoft-warns-of-cryware-info.html

ACTUALIZACIONES DE SEGURIDAD

- Zyxel publica parche para una vulnerabilidad crítica de inyección de comandos en el sistema operativo del firewall.
  https://www.helpnetsecurity.com/2022/05/13/cve-2022-30525/
- Kali Linux 2022.2 se presenta con 10 nuevas herramientas, mejoras en WSL y más.
  https://www.kali.org/blog/kali-linux-2022-2-release/
- **CISA advierte que no se deben instalar las actualizaciones de Windows de mayo en los controladores de dominio.**
  https://www.bleepingcomputer.com/news/security/cisa-warns-not-to-install-may-windows-updates-on-domain-controllers/
- Red Hat Enterprise Linux 8.6: mejor seguridad, más opciones.
  https://www.zdnet.com/article/red-hat-enterprise-linux-8-6-better-security-more-options/
- La actualización de emergencia de Apple corrige el día cero utilizado para hackear Macs.
  https://nakedsecurity.sophos.com/2022/05/17/apple-patches-zero-day-kernel-hole-and-much-more-update-now/
- NVIDIA corrige diez vulnerabilidades en los controladores de pantalla de la GPU de Windows.
  https://www.bleepingcomputer.com/news/security/nvidia-fixes-ten-vulnerabilities-in-windows-gpu-display-drivers/
- VMware parchea un fallo crítico de derivación de autenticidad en varios productos.
  https://securityaffairs.co/wordpress/131429/security/vmware-critical-auth-bypass-issue.html