@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. 155 – 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 21/2/22 y el 25/2/22

- La emisora estatal iraní IRIB afectada por el destructivo malware Wiper.
  https://thehackernews.com/2022/02/iranian-state-broadcaster-irib-hits-by_21.html
- Los usuarios de OpenSea pierden 2 millones de dólares en NFT en un ataque de *phishing*.
  https://www.bleepingcomputer.com/news/security/opensea-users-lose-2-million-worth-of-nfts-in-phishing-attack/
- Ucrania: Los bancos "sufren ciberataques" y las páginas web del gobierno son "inaccesibles".
  https://news.sky.com/story/ukraine-crisis-banks-hit-by-cyber-attacks-as-government-website-home-pages-inaccessible-12549660
  https://www.theregister.com/2022/02/23/ukraine_ddos_russia_malware/
- Los sitios web del gobierno ruso están actualmente inactivos (24feb2022).
  https://www.vice.com/en/article/bvnpnv/russian-government-websites-are-currently-down

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

- **ENISA y CERT-EU publican un conjunto de buenas prácticas de ciberseguridad para organizaciones públicas y privadas.**
  https://www.helpnetsecurity.com/2022/02/21/eu-cybersecurity-best-practices/
- Los hackers utilizan dispositivos Android infectados para registrar cuentas desechables.
  https://thehackernews.com/2022/02/hackers-exploit-bug-in-sms-verification.html
- APT china atenta contra el sector financiero de Taiwán con un ataque a la cadena de suministro.
  https://thehackernews.com/2022/02/chinese-hackers-target-taiwans.html
- **Documento CISA: Comprensión y mitigación de las ciberamenazas patrocinadas por el Estado ruso a las infraestructuras críticas de Estados Unidos.**
  https://media.defense.gov/2022/Jan/11/2002919950/-1/-1/1/JOINT_CSA_UNDERSTANDING_MITIGATING_RUSSIAN_CYBER_THREATS_TO_US_CRITICAL_INFRASTRUCTURE_20220111.PDF
- **Se detectaron casi 100.000 nuevas variantes de troyanos bancarios para móviles, en 2021.**
  https://www.zdnet.com/article/almost-100000-new-mobile-banking-trojans-detected-in-2021/
- Servidores Microsoft SQL Server vulnerables afectados con Cobalt Strike.
  https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/
- La máquina contraataca: La IA que lucha contra las ciberamenazas en nombre de los humanos.
  https://www.theregister.com/2022/02/22/darktrace_aiutonomous_response/
- **Investigadores chinos detallan la puerta trasera de Linux del grupo Equation vinculado a la NSA.**
  https://www.securityweek.com/chinese-researchers-detail-linux-backdoor-nsa-linked-equation-group
  https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group.en.pdf
- Contratistas de defensa de EE.UU. son afectados por la puerta trasera de Windows SockDetour.

https://www.bleepingcomputer.com/news/security/us-defense-contractors-hit-by-stealthy-sockdetour-windows-backdoor/

NOTAS DE INTERÉS

- **Rusia " pre-posiciona" ciber-ataques para una potencial invasión.**
https://www.infosecurity-magazine.com/news/russia-prepositioning-attacks/
- **El troyano bancario Xenomorph para Android se distribuye a través de Google Play Store.**
https://securityaffairs.co/wordpress/128253/malware/xenomorph-android-banking-trojan.html
- El 40% de los correos electrónicos entrantes son amenazas potenciales.
https://betanews.com/2022/02/21/40-percent-of-incoming-emails-are-potential-threats/
- Los creadores de malware se enfrentan a sus rivales con paquetes *npm* maliciosos.
https://www.zdnet.com/article/malware-authors-target-rivals-with-malicious-npm-packages/
- El ransomware Entropy está vinculado al downloader de malware Dridex.
https://www.bleepingcomputer.com/news/security/entropy-ransomware-linked-to-dridex-malware-downloader/
- **Palo Alto Networks presenta la plataforma de seguridad autónoma basada en IA, Cortex XSIAM.**
https://thehackernews.com/2022/02/9-year-old-unpatched-email-hacking-bug.html
- Se descubre un fallo de piratería de correo electrónico, sin parches, de 9 años de antigüedad en el software de correo web Horde.
https://thehackernews.com/2022/02/9-year-old-unpatched-email-hacking-bug.html
- Aumenta el número de grupos de amenazas que tienen como objetivo los sistemas OT en Norteamérica.
https://www.securityweek.com/increasing-number-threat-groups-targeting-ot-systems-north-america
- **Samsung distribuyó "100 millones" de teléfonos con un cifrado defectuoso.**
https://www.theregister.com/2022/02/23/samsung_encryption_phones/
- Revelaron un nuevo malware “que borra” datos, Wiper, y que ha sido utilizado en ataques contra cientos de computadoras en Ucrania.
https://securityaffairs.co/wordpress/128349/malware/wiper-malware-hermeticwipe-ukrain.html
- El *phishing* que utiliza falsas solicitudes Citibank atrae a los clientes con alertas de suspensión.
https://www.bleepingcomputer.com/news/security/citibank-phishing-baits-customers-with-fake-suspension-alerts/
- Servidores de Microsoft Exchange hackeados para distribuir el ransomware Cuba.
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/
- Putin advierte a las infraestructuras críticas rusas que se preparen para posibles ciberataques.
https://thehackernews.com/2022/02/putin-warns-russian-critical.html

ACTUALIZACIONES DE SEGURIDAD

- Microsoft actualiza las aplicaciones de seguridad para entornos *multicloud*.
https://www.csoonline.com/article/3651110/microsoft-updates-security-applications-for-multicloud-environments.html
- Ubuntu aplica correcciones de seguridad para todas las versiones hasta la 14.04.
https://www.theregister.com/2022/02/23/ubuntu_kernel_updates/
- Cisco libera parches para 4 vulnerabilidades en sus S.O. de red FXOS y NX-OS.
https://www.securityweek.com/nsa-informs-cisco-vulnerability-exposing-nexus-switches-dos-attacks