@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. 193 – 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 18/11/22 y el 24/11/22

- La banda de ransomware Daixin roba 5 millones de datos de pasajeros y empleados de AirAsia.
  https://thehackernews.com/2022/11/daixin-ransomware-gang-steals-5-million.html
- El Parlamento Europeo declara a Rusia patrocinadora del terrorismo, y luego, su sitio se cae.
  https://arstechnica.com/information-technology/2022/11/european-parliament-ddosed-after-declaring-russia-a-sponsor-of-terrorism/

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

- **Evolución de las amenazas informáticas en el tercer trimestre de 2022.**
  https://securelist.com/it-threat-evolution-q3-2022/107957/
- La caza de amenazas con MITRE ATT&CK y Wazuh.
  https://thehackernews.com/2022/11/threat-hunting-with-mitre-att-and-wazuh.html
- **Red Federal de Estados Unidos fue hackeada por APT que obtuvo acceso al controlador de dominio.**
  https://cybersecuritynews.com/u-s-federal-network-hacked/
- Los investigadores ayudaron en secreto a desencriptar el ransomware Zeppelin durante 2 años.
  https://www.bleepingcomputer.com/news/security/researchers-secretly-helped-decrypt-zeppelin-ransomware-for-2-years/
- **Ciberamenazas financieras y de software delictivo en 2023.**
  https://securelist.com/crimeware-financial-cyberthreats-2023/108005/
- Advierten que los ciberdelincuentes utilizan el malware Aurora Stealer basado en Go.
  https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/
- 5 Vulnerabilidades de la API que son explotadas por los delincuentes.
  https://securityaffairs.co/wordpress/138879/security/5-api-vulnerabilities.html
- **CISA actualiza las directrices para aumentar la resiliencia de la planificación de infraestructuras.**
  https://www.infosecurity-magazine.com/news/cisa-resilience-infrastructure/
- Hackers modifican la popular aplicación OpenVPN para Android para incluir software espía.
  https://www.bleepingcomputer.com/news/security/hackers-modify-popular-openvpn-android-app-to-include-spyware/

NOTAS DE INTERÉS

- Israel coloca torretas robóticas de seguimiento de objetivos en Cisjordania.
  https://www.theregister.com/2022/11/18/israel_sets_robotic_targettracking_turrets/
- La minería sigue siendo una grave amenaza para la infraestructura de la nube.
  https://www.kaspersky.com/blog/miners-threaten-cloud-infrastructure/46275/

- El ataque a la cadena de suministro se dirige a los desarrolladores de Python con WASP Stealer.
https://securityaffairs.co/wordpress/138692/cyber-crime/wasp-stealer-supply-chain-attack.html
- **El actor de amenazas DEV-0569 amplía su kit de herramientas para distribuir el ransomware Royal.**
https://www.infosecurity-magazine.com/news/dev0569-expands-toolkit-royal/
- El malware LodaRAT resurge con nuevas variantes empleando funcionalidades actualizadas.
https://thehackernews.com/2022/11/lodarat-malware-resurfaces-with-new.html
- **Octocrypt, Alice y AXLocker Ransomware, nuevas amenazas en la red.**
https://securityaffairs.co/wordpress/138783/malware/octocrypt-alice-axlocker-ransomware.html
- Las instalaciones de gas y petróleo en alta mar de Estados Unidos corren un riesgo "creciente" de sufrir un ciberataque.
https://www.theregister.com/2022/11/21/us_oil_gas_cyber_threats/
- El grupo de ransomware ALPHV incluye a la aerolínea tailandesa Nok como víctima.
https://thecyberexpress.com/alphv-ransomware-group-lists-thailands-nok-air-airline-as-victim/
- Los vehículos autónomos se suman a la lista de amenazas para la seguridad nacional de Estados Unidos.
https://www.wired.com/story/autonomous-vehicles-china-us-national-security/
- ViperSoftX: Este malware instala extensiones de navegador maliciosas para robar las contraseñas y criptomonedas de los usuarios.
https://thehackernews.com/2022/11/this-malware-installs-malicious-browser.html
- Investigadores de Meta crean una IA que domina la Diplomacia, engañando a jugadores humanos.
https://arstechnica.com/information-technology/2022/11/meta-researchers-create-ai-that-masters-diplomacy-tricking-human-players/
- Los ciberdelincuentes rusos han robado más de 50 millones de contraseñas este año.
https://www.bleepingcomputer.com/news/security/russian-cybergangs-stole-over-50-million-passwords-this-year/
- **Aplicación de gestión de archivos de Android infectó miles de dispositivos con el malware SharkBot.**
https://thehackernews.com/2022/11/this-android-file-manager-app-infected.html
- Una agresiva campaña de malware se centra en empresas con sede en Estados Unidos con Qakbot para distribuir el ransomware Black Basta.
https://securityaffairs.co/wordpress/138924/cyber-crime/qakbot-campaign-black-basta-ransomware.html
- El ransomware RansomExx se actualiza al lenguaje de programación Rust.
https://securityaffairs.co/wordpress/138933/malware/ransomexx-ransomware-rust-language.html
- El Reino Unido prohíbe las cámaras de videovigilancia chinas en lugares "sensibles" del gobierno.
https://www.theregister.com/2022/11/25/uk_government_china_cctv_ban_/

ACTUALIZACIONES DE SEGURIDAD

- Samba parchea una vulnerabilidad que puede conducir a un DoS y a la ejecución remota de código.
https://www.securityweek.com/samba-patches-vulnerability-can-lead-dos-remote-code-execution
- Microsoft publica una actualización fuera de banda para solucionar los problemas de autentificación de Kerberos causados por un parche para CVE-2022-37966.
https://securityaffairs.co/wordpress/138869/security/out-of-band-fix-kerberos-issues.html