@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. 191 – 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 4/11/22 y el 10/11/22

- ALMA, en Chile, el observatorio más caro del mundo sufre un ciberataque.
  https://www.infosecurity-magazine.com/news/worlds-most-expensive-observatory/
- Un ciberataque bloqueó los trenes en Dinamarca.
  https://securityaffairs.co/wordpress/138127/cyber-crime/cyberattack-blocked-trains-denmark.html
- Los hackers de "Justice Blade" atacan a Arabia Saudita.
  https://securityaffairs.co/wordpress/138213/hacking/justice-blade-targets-saudi-arabia.html
- Medibank confirma que los datos robados en la filtración ya están disponibles en la red.
  https://www.infosecurity-magazine.com/news/medibank-confirms-data-stolen-now/

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

- La red de bots Emotet vuelve a difundir malware tras una pausa de 4 meses.
  https://www.bleepingcomputer.com/news/security/emotet-botnet-starts-blasting-malware-again-after-4-month-break/
- Detallan una nueva campaña de malware dirigida a los empleados del gobierno y defensa indio.
  https://www.infosecurity-magazine.com/news/android-rat-targets-india-defence/
- Campaña de carga software espía VPN en los dispositivos Android, mediante las redes sociales.
  https://www.csoonline.com/article/3678851/espionage-campaign-loads-vpn-spyware-on-android-devices-via-social-media.html
- Seis maneras de reducir la superficie de ataque del IoT.
  https://www.techrepublic.com/article/reduce-iot-attack-surface/
- Descubren que el escáner de seguridad URLScan filtra inadvertidamente URLs y datos sensibles
  https://thehackernews.com/2022/11/experts-find-urlscan-security-scanner.html

NOTAS DE INTERÉS

- **Ghidra: un conjunto de herramientas de ingeniería inversa de software (SRE) desarrollado por la NSA en apoyo de las misiónes de Ciberseguridad.**
  https://ghidra-sre.org/
- Los ataques de ransomware Black Basta están relacionados con el actor de la amenaza FIN7.
  https://www.infosecurity-magazine.com/news/black-basta-linked-to-fin7-threat/
- El gobierno británico está escaneando todos los dispositivos de Internet alojados en el Reino Unido.
  https://www.bleepingcomputer.com/news/security/british-govt-is-scanning-all-internet-devices-hosted-in-uk/
- TikTok admite que su personal en China puede acceder a los datos de los europeos.
  https://www.wired.com/story/tiktok-eu-privacy-policy-security-roundup/

- LinkedIn añade correos electrónicos verificados y fechas de creación de perfiles.
https://krebsonsecurity.com/2022/11/linkedin-adds-verified-emails-profile-creation-dates/
- Se detectan 29 paquetes maliciosos de PyPI que distribuyen el W4SP Stealer.
https://securityaffairs.co/wordpress/138113/hacking/pypi-packages-delivers-w4sp-stealer.html
- Es probable que China esté recopilando y luego utilizando vulnerabilidades.
https://www.theregister.com/2022/11/07/china_stockpiles_vulnerabilities_microsoft_asserts/
- Japón se une oficialmente al centro de ciberdefensa de la OTAN.
https://www.theregister.com/2022/11/07/japan_joins_nato_cyber_defence/
- Un hacker intentó ocultar 3.360 millones de dólares en bitcoins robados, pero el FBI lo encontró.
https://arstechnica.com/information-technology/2022/11/feds-seize-3-36-billion-in-bitcoin-stolen-10-years-ago-in-hack-of-silk-road/
- El troyano bancario para Android, Vultur, llegó a más de 100.000 descargas en Google Play Store.
https://www.infosecurity-magazine.com/news/vultur-android-banking-trojan/
- El malware Laplas Clipper orientado a los usuarios de criptomonedas a través de SmokeLoader.
https://thehackernews.com/2022/11/new-laplas-clipper-malware-targeting.html
- Se detecta que el bot Amadey implanta el ransomware LockBit 3.0 en máquinas hackeadas.
https://thehackernews.com/2022/11/amadey-bot-spotted-deploying-lockbit-30.html
- Los afiliados de Conti, Black Basta y BlackByte, siguen atacando las infraestructuras críticas.
https://www.infosecurity-magazine.com/news/black-basta-blackbyte-attack-eu/
- **Las 15 mayores filtraciones de datos del siglo XXI.**
https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
- El RAT avanzado "AgentTesla" es el malware más propagado en octubre.
https://www.infosecurity-magazine.com/news/advanced-rat-agenttesla-malware/
- APT29 usa característica de Windows para comprometer red de entidades diplomáticas europeas.
https://thehackernews.com/2022/11/apt29-exploited-windows-feature-to.html
- Informaron de que un grupo de vigilancia utiliza tres exploits de día cero para teléfonos Samsung.
https://securityaffairs.co/wordpress/138302/hacking/surveillance-vendor-exploited-samsung-phone-zero-days.html
- **IBM supera los 400 qubits con un nuevo procesador.**
https://arstechnica.com/science/2022/11/ibm-pushes-qubit-count-over-400-with-new-processor/
- Lenovo advierte sobre los bugs que pueden utilizarse para eludir las funciones de seguridad.
https://securityaffairs.co/wordpress/138312/security/lenovo-bypass-security-features.html

ACTUALIZACIONES DE SEGURIDAD

- Google soluciona las vulnerabilidades de escalada de privilegios de alta gravedad en Android.
https://www.securityweek.com/google-patches-high-severity-privilege-escalation-vulnerabilities-android
- **Martes de parches de Microsoft de noviembre de 2022.**
https://isc.sans.edu/diary/rss/29230
- VMware corrige tres fallos críticos en Workspae ONE Assist.
https://securityaffairs.co/wordpress/138283/security/vmware-workspace-one-assist-critical-bugs.html
- Solución de emergencia para la inyección de código de Apple.
https://nakedsecurity.sophos.com/2022/11/10/emergency-code-execution-patch-from-apple-but-not-an-0-day/
- **Cisco difunde actualizaciones de seguridad para varios productos**
https://www.cisa.gov/uscert/ncas/current-activity/2022/11/10/cisco-releases-security-updates-multiple-products