@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. 149 – 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 5/1/22 y el 11/1/22

- Kosovo prohíbe la minería de *criptomonedas* tras los apagones.
  https://www.bbc.com/news/world-europe-59879760
- La empresa química Element Solutions revela un incidente de ciberseguridad.
  https://www.securityweek.com/chemicals-company-element-solutions-discloses-cybersecurity-incident
- **Hackers norcoreanos comienzan el año con ataques al Ministerio de Asuntos Exteriores ruso.**
  https://thehackernews.com/2022/01/north-korean-hackers-start-new-year.html

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

- Script malicioso en Python que tiene como objetivo a los chinos.
  https://isc.sans.edu/forums/diary/Malicious+Python+Script+Targeting+Chinese+People/28220/
- La técnica de persistencia NoReboot simula el apagado del iPhone.
  https://securityaffairs.co/wordpress/126358/hacking/noreboot-persistence-iphone.html
- **El ejército suizo prohíbe todas las aplicaciones de chat excepto Threema, de desarrollo local.**
  https://www.bleepingcomputer.com/news/security/swiss-army-bans-all-chat-apps-but-locally-developed-threema/
- Norton 360 ahora incluye un programa de minería de *criptomonedas*.
  https://krebsonsecurity.com/2022/01/norton-360-now-comes-with-a-cryptominer/
  https://community.norton.com/en/forums/faq-norton-crypto
- Night Sky es el último ransomware enfocado a las redes corporativas.
  https://securityaffairs.co/wordpress/126400/malware/night-sky-ransomware-operation.html
- Generador de RAT personalizado, en Python.
  https://isc.sans.edu/forums/diary/Custom+Python+RAT+Builder/28224/
- Encuentran fallos en más de una docena de bibliotecas de análisis de URL muy utilizadas.
  https://thehackernews.com/2022/01/researchers-find-bugs-in-over-dozen.html

NOTAS DE INTERÉS

- Los cibercriminales se centran en las webs inmobiliarias con un skimmer en el último ataque a la cadena de suministro.
  https://thehackernews.com/2022/01/hackers-target-real-estate-websites.html
- Investigadores de ciberseguridad demuestran cómo utilizar las emanaciones de los campos electromagnéticos de dispositivos IoT para detectar malware.
  https://securityaffairs.co/wordpress/126312/malware/electromagnetic-signals-iot-malware-classification.html
- Los proveedores de Sistemas de Control Industrial reaccionan ante las vulnerabilidades de Log4j.
  https://www.securityweek.com/ics-vendors-respond-log4j-vulnerabilities

- **Un artículo de la Escuela de Guerra del Ejército de EE.UU. sugiere que Taiwán debería amenazar con destruir su industria de semiconductores si es invadida por China.**
https://www.theregister.com/2022/01/05/taiwan_should_destory_tsmc_paper/
- Consideraciones clave para la próxima estrategia nacional de ciberseguridad de Canadá
https://www.tripwire.com/state-of-security/government/key-considerations-for-canadas-forthcoming-national-cyber-security-strategy/
- Grupo de piratas informáticos se enfoca en antiguas aplicaciones Java para entrar en las redes.
https://www.zdnet.com/article/this-sneaky-hacking-group-targets-old-java-applications-to-break-into-networks/
- Líder polaco admite que su país compró un potente programa espía israelí.
https://www.securityweek.com/polish-leader-admits-country-bought-powerful-israeli-spyware
- Siete predicciones sobre la ciberseguridad energética mundial en 2022.
https://www.darkreading.com/vulnerabilities-threats/7-predictions-for-global-energy-cybersecurity-in-2022
- Un grupo se centra en los servidores de VMware Horizon, utilizando exploits de Log4Shell.
https://securityaffairs.co/wordpress/126421/hacking/log4shell-nhs-attacks.html
- La contrainteligencia estadounidense comparte consejos para bloquear los ataques de spyware.
https://www.bleepingcomputer.com/news/security/us-counterintelligence-shares-tips-to-block-spyware-attacks/
- FBI: Los hackers utilizan BadUSB para atacar a las empresas de defensa con ransomware.
https://securityaffairs.co/wordpress/126439/breaking-news/fin7-badusb-attacks.html
- **Ciberespías indios exponen su operación tras infectarse con RAT.**
https://www.securityweek.com/indian-cyberspies-expose-their-operation-after-infecting-themselves-rat
- Las organizaciones sufren 925 ataques semanales, el máximo histórico.
https://threatpost.com/cyber-spike-attacks-high-log4j/177481/
- Los ciberataques semanales se dispararon un 50% en 2021.
https://www.techrepublic.com/article/weekly-cyberattacks-jumped-by-50-in-2021-with-a-peak-in-december-due-largely-to-the-log4j-exploit/
- El director general de Signal dimite y el cofundador de WhatsApp toma el relevo como director general interino.
https://thehackernews.com/2022/01/signal-ceo-resigns-whatsapp-co-founder.html
- CISA, el FBI y la NSA publican un aviso sobre las ciberamenazas rusas a las infraestructuras críticas de Estados Unidos.
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/cisa-fbi-and-nsa-release-cybersecurity-advisory-russian-cyber

ACTUALIZACIONES DE SEGURIDAD

- Google corrige 48 vulnerabilidades con la primera serie de actualizaciones de Android de 2022.
https://www.securityweek.com/google-patches-48-vulnerabilities-first-set-2022-android-updates
- Chrome 97 parchea 37 vulnerabilidades.
https://www.securityweek.com/chrome-97-patches-37-vulnerabilities
- VMware soluciona agujeros de seguridad en Workstation, Fusion y ESXi.
https://www.securityweek.com/vmware-plugs-security-holes-workstation-fusion-and-esxi
- **Microsoft publica las actualizaciones de seguridad de enero de 2022.**
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/microsoft-releases-january-2022-security-updates