@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. 139 – Año 2021

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 28/10/21 y el 3/11/21

- Datos sensibles de 400.000 estudiantes alemanes quedan expuestos por un error de Scoolio. https://www.bleepingcomputer.com/news/security/sensitive-data-of-400-000-german-students-exposed-by-api-flaw/
- Filtración de datos en la Universidad de Colorado. https://www.infosecurity-magazine.com/news/data-breach-university-colorado/
- Red de salud de Massachusetts fue hackeada y la información de los pacientes publicada. https://www.securityweek.com/massachusetts-health-network-hacked-patient-info-exposed
- Hackers, aparentemente vinculados a Irán, penetran en una empresa israelí de Internet. https://www.securityweek.com/apparent-iran-linked-hackers-breach-israeli-internet-firm
- El ransomware afecta al sistema de transporte de Toronto, interrumpiendo algunos servicios. https://www.cyberscoop.com/toronto-transit-commission-ann-arbor-theride-ransomware/
- Estados Unidos sanciona a NSO Group de Israel y a otras tres empresas por la venta de programas espía y exploits. https://www.bleepingcomputer.com/news/security/us-sanctions-nso-group-and-three-others-for-spyware-and-exploit-sales/
- El grupo pirata BlackShadow vulnera una empresa de hosting israelí y extorsiona a sus clientes. https://www.bleepingcomputer.com/news/security/blackshadow-hackers-breach-israeli-hosting-firm-and-extort-customers/
- El troyano bancario Mekotio resurge con un código modificado y una campaña sigilosa. https://threatpost.com/mekotio-banking-trojan-campaign/175981/

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

- Mediante el acelerómetro, varias apps de iPhone pueden informar muchas cosas sobre usted. https://www.mysk.blog/2021/10/24/accelerometer-ios/
- El nuevo malware AbstractEmu afecta a los dispositivos Android y evita su detección. https://thehackernews.com/2021/10/this-new-android-malware-can-gain-root.html
- La NSA y la CISA comparten orientaciones sobre la seguridad de la infraestructura de la nube 5G. https://securityaffairs.co/wordpress/123910/reports/5g-networks-prevent-lateral-movement.html
- Campaña de espionaje de Nobelium. https://exchange.xforce.ibmcloud.com/collection/cf77b924454eebd52e099b1e6bce37b6
- MITRE y CISA anuncian la lista de 2021 de los puntos débiles más comunes del hardware. https://www.securityweek.com/mitre-cisa-announce-2021-list-most-common-hardware-weaknesses
- ESET ha encontrado una variante del ransomware Hive que cifra Linux y FreeBSD.

https://securityaffairs.co/wordpress/123931/malware/hive-ransomware-linux-freebsd.html

- El bug "Trojan Source" amenaza la seguridad de todos los códigos.
https://krebsonsecurity.com/2021/11/trojan-source-bug-threatens-the-security-of-all-code/

NOTAS DE INTERÉS

- Las principales amenazas de ciberseguridad a las que se enfrentarán las empresas en 2022.
https://www.helpnetsecurity.com/2021/10/28/cybersecurity-threats-enterprises-2022/
- Microsoft Edge finalmente entra en Linux. La versión "oficial" se encuentra en los repositorios.
https://nakedsecurity.sophos.com/2021/10/29/microsoft-edge-finally-arrives-on-linux-official-build-lands-in-repos/
- Los ciberdelincuentes atentan contra la infraestructura de los coches enlazados a las redes.
https://www.darkreading.com/attacks-breaches/cybercriminals-take-aim-at-connected-car-infrastructure
- Resumen semanal de ataques ransomware.
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-29th-2021-making-arrests/
- Irán sospecha que Israel y EE.UU. están detrás del ciberataque al suministro de combustible.
https://www.securityweek.com/iran-suspects-israel-and-us-behind-fuel-cyber-attack
- Descubren el malware de bots "Pink" que infectó a más de 1,6 millones de dispositivos.
https://thehackernews.com/2021/11/researchers-uncover-pink-botnet-malware.html
- Facebook da al gobierno de Kazajistán acceso directo al sistema de notificación de contenidos.
https://www.zdnet.com/article/facebook-gives-kazakhstan-government-direct-access-to-content-reporting-system/
- Hackers aprovechan el fallo RCE no autenticado de GitLab.
https://thehackernews.com/2021/11/alert-hackers-exploiting-gitlab.html
- La mayoría de los compiladores de código son vulnerables a nuevos ataques.
https://www.infosecurity-magazine.com/news/computer-code-compilers-attacks/
- Facebook informa que “elimina” su sistema de reconocimiento facial, alegando " problemas sociales" y normas inciertas de los entes reguladores.
https://www.cyberscoop.com/facebook-kills-its-facial-recognition-system-citing-societal-concerns-uncertain-rules-from-regulators/
- AV-Comparatives publica lista de programas antivirus que funcionan bajo Windows 11.
- https://www.av-comparatives.org/av-comparatives-releases-list-of-working-consumer-av-programs-for-windows-11/

ACTUALIZACIONES DE SEGURIDAD

- Google corrige dos fallos de día cero de alta gravedad en Chrome.
https://www.zdnet.com/article/google-fixes-two-high-severity-zero-day-flaws-in-chrome/
- Apple corrige la omisión de funciones de seguridad en macOS (CVE-2021-30892).
https://www.helpnetsecurity.com/2021/10/29/cve-2021-30892/
- Android soluciona un fallo del kernel de día cero que es explotado de forma activa.
https://threatpost.com/android-patches-exploited-kernel-bug/175931/