@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. 67/2021

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.

08/01/2021

- Errores en Firefox, Chrome y Edge permiten el pirateo remoto del sistema. Actualizados.
  https://threatpost.com/firefox-chrome-edge-bugs-system-hijacking/162873/
  https://www.welivesecurity.com/2021/01/08/chrome-firefox-updates-fix-severe-security-bugs/

- Hackers norcoreanos atacan a Corea del Sur con el troyano RokRat (más en el boletín 66).
  https://thehackernews.com/2021/01/alert-north-korean-hackers-targeting.html
  https://threatpost.com/nvidia-windows-gamers-graphics-driver-flaws/162857/

- **Signal corrige los retrasos de verificación causados por el éxodo masivo desde WhatsApp.**
  https://www.bleepingcomputer.com/news/software/signal-fixes-verification-delays-caused-by-whatsapp-mass-exodus/

- British Airways pagará 3.000 millones de libras como compensación por una fuga de datos.
  https://www.ehackingnews.com/2021/01/british-airways-to-pay-3bn-pound-as.html

09/01/2021

- La Fuerza Espacial (Space Force) se une a la Comunidad de Inteligencia de los Estados Unidos para asegurar el espacio exterior.
  https://www.bleepingcomputer.com/news/security/space-force-joins-us-intelligence-community-to-secure-outer-space/
  https://www.defenseone.com/technology/2021/01/us-space-force-becomes-18th-member-us-intelligence-community/171285/

- Apple retiró a Parler de la App Store por incitar a la violencia.
  https://www.bleepingcomputer.com/news/apple/apple-removed-parler-from-the-app-store-for-inciting-violence/

- Dassault Falcon Jet impactado por la banda de rescate de Ragnar Locker.
  https://securityaffairs.co/wordpress/113216/data-breach/dassault-falcon-data-breach.html

10/01/2021

- El Banco de la Reserva de Nueva Zelanda sufre una filtración de datos a través de un pirateo a socio que le provee de almacenamiento.
  https://securityaffairs.co/wordpress/113242/data-breach/new-zealand-central-bank-hacked.html
  https://www.theguardian.com/world/2021/jan/11/new-zealands-central-bank-says-its-systems-have-been-hacked

11/01/2021

- SANS Daily Network Security Podcast (Stormcast) para el lunes 11 de enero de 2021.
  https://isc.sans.edu/podcastdetail.html?id=7322

- Una brecha en los datos de las Naciones Unidas expuso más de 100.000 registros del personal del Programa de las Naciones Unidas para el Medio Ambiente.
https://www.infosecurity-magazine.com/news/100000-un-employee-records/

- Parler al borde de la expulsión permanente.
https://www.ehackingnews.com/2021/01/parler-on-verge-of-permanent-expulsion.html

- Los investigadores encuentran vínculos entre el Sunburst y el malware Kazuar ruso.
https://thehackernews.com/2021/01/researchers-find-links-between-sunburst.html

- Se publicó hoy una nueva herramienta por la empresa de seguridad rumana Bitdefender que permite a las víctimas del ransomware Darkside recuperar sus archivos sin tener que pagar.
https://www.zdnet.com/article/free-decrypter-released-for-victims-of-darkside-ransomware/

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

- Investigación sobre amenazas: Detalles técnicos adicionales de SUNBURST.
https://www.fireeye.de/blog/threat-research/2020/12/sunburst-additional-technical-details.html

- El nuevo ataque de canal lateral puede obtener las claves de cifrado de las llaves de seguridad Google Titan.
https://www.zdnet.com/article/new-side-channel-attack-can-recover-encryption-keys-from-google-titan-security-keys/
- Las claves de seguridad de Google Titan hackeadas por investigadores franceses.
https://nakedsecurity.sophos.com/2021/01/11/google-titan-security-keys-hacked-by-french-researchers/

NOTAS DE INTERÉS

- Las 10 habilidades de ciberseguridad de mayor crecimiento a aprender en 2021.
https://www.techrepublic.com/article/10-fastest-growing-cybersecurity-skills-to-learn-in-2021/

- Emotet encabeza las listas de malware en diciembre.
https://www.infosecurity-magazine.com/news/emotet-tops-malware-charts/

- El ataque a SolarWinds de Rusia y la seguridad del software.
https://www.schneier.com/blog/archives/2021/01/russias-solarwinds-attack-and-software-security.html

- El Departamento de Estado de EE.UU. aprueba la nueva Oficina de Seguridad del Ciberespacio.
https://securityaffairs.co/wordpress/113179/security/us-creates-cset.html

- Los registros judiciales de los EE.UU. fueron expuestos en la brecha de SolarWinds.
https://krebsonsecurity.com/2021/01/sealed-u-s-court-records-exposed-in-solarwinds-breach/

ACTUALIZACIONES DE SEGURIDAD

- La vulnerabilidad de día cero, PsExec Windows, consigue un micro parche gratuito.
https://www.bleepingcomputer.com/news/security/windows-psexec-zero-day-vulnerability-gets-a-free-micropatch/

- Nvidia publica una actualización de seguridad para las vulnerabilidades de alta severidad de sus controladores de gráficos.
https://www.zdnet.com/article/nvidia-releases-security-update-for-high-severity-graphics-driver-vulnerabilities/