@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. 71/2021

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.

22/01/2021

- Han rastreado el origen de una campaña -que infectaba servidores SQL para minar criptomonedas- hasta una empresa de software iraní.
https://threatpost.com/sql-server-malware-tied-to-iranian-software-firm-researchers-allege/163230/
- El sitio MyFreeCams es hackeado para robar información de 2 millones de usuarios.
https://www.bleepingcomputer.com/news/security/myfreecams-site-hacked-to-steal-info-of-2-million-paying-users/
- Atacantes ransomware publican 4K archivos privados de una agencia del gobierno escocés.
https://threatpost.com/attackers-publish-private-scottish-gov-files/163254/
- Los hackers robaron información de ganancias de Intel no publicadas del sitio corporativo.
https://www.bleepingcomputer.com/news/security/intel-hackers-stole-unpublished-earnings-info-from-corporate-site/
- Un técnico de ADT *hackea* las cámaras de seguridad de hogares para espiar a las mujeres.
https://threatpost.com/adt-hacks-home-security-cameras/163271/

23/01/2021

- El gobierno ruso advierte de los ciberataques de represalia de Estados Unidos.
https://www.bleepingcomputer.com/news/security/russian-government-warns-of-us-retaliatory-cyberattacks/
- SonicWall, empresa de seguridad, fue víctima de un "sofisticado" hackeo.
https://thehackernews.com/2021/01/exclusive-sonicwall-hacked-using-0-day.html
https://www.bloomberg.com/news/articles/2021-01-23/cyber-firm-sonicwall-says-it-was-victim-of-sophisticated-hack

24/01/2021

- Un hacker revela los datos de 2,28 millones de usuarios de sitios de citas.
https://www.zdnet.com/article/hacker-leaks-data-of-2-28-million-dating-site-users/
- Otro ransomware utiliza ahora ataques DDoS para obligar a las víctimas a pagar.
https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/
- **Cuidado: un nuevo malware para Android que se propaga a través de WhatsApp.**
https://thehackernews.com/2021/01/beware-new-wormable-android-malware.html

25/01/2021

- Intel: La filtración de los beneficios se debe a un error interno.
https://www.infosecurity-magazine.com/news/intel-earnings-leak-down-to/

- El gigante del embalaje WestRock informa que el ataque ransomware afectó sus sistemas OT.
https://www.securityweek.com/packaging-giant-westrock-says-ransomware-attack-impacted-ot-systems
- Se informa a empresas industriales sobre graves vulnerabilidades del producto Matrikon OPC.
https://www.securityweek.com/industrial-firms-informed-about-serious-vulnerabilities-matrikon-opc-product
- El regulador australiano de valores informa de un brecha en la seguridad.
https://www.bleepingcomputer.com/news/security/australian-securities-regulator-discloses-security-breach/
- Un bufete de abogados de San Francisco investiga la filtración de datos de PupBox.
https://www.infosecurity-magazine.com/news/law-firm-investigating-pupbox-data/

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

- Compartir un eBook con Kindle podría haber permitido a los ciberdelincuentes secuestrar su cuenta.
https://thehackernews.com/2021/01/sharing-ebook-with-your-kindle-could.html
- Presentado por el investigador de seguridad John Page, el nuevo sitio web **MalVuln** enumera los defectos de código de malware.
https://www.malvuln.com/
- Nuevas capacidades de detección de amenazas a nivel CPU de Intel orientadas al ransomware.
https://www.csoonline.com/article/3603522/new-intel-cpu-level-threat-detection-capabilities-target-ransomware.html
- Comparación de diferentes enfoques de IA para la seguridad del correo electrónico.
https://www.darkreading.com/edge/theedge/comparing-different-ai-approaches-to-email-security/b/d-id/1339965

NOTAS DE INTERÉS

- Así fue como los hackers de SolarWinds lograron que no sean detectados durante un tiempo suficiente.
https://thehackernews.com/2021/01/heres-how-solarwinds-hackers-stayed.html
- Los servidores de Escritorio Remoto de Windows se utilizan para amplificar los ataques DDoS.
https://www.bleepingcomputer.com/news/security/windows-remote-desktop-servers-now-used-to-amplify-ddos-attacks/
- Tendencias del la industria de los datos a las que prestar atención en 2021.
https://www.helpnetsecurity.com/2021/01/13/data-industry-trends-2021/
- Con la subida del precio del Bitcoin, las bandas extorsivas DDoS vuelven con fuerza.
https://www.zdnet.com/article/as-bitcoin-price-surges-ddos-extortion-gangs-return-in-force/

ACTUALIZACIONES DE SEGURIDAD

- Debian: Plugins actualizados recientemente.
https://www.tenable.com/plugins/updated
- El gestor de contenidos, Drupal, publica una corrección de una vulnerabilidad crítica.
https://www.bleepingcomputer.com/news/security/drupal-releases-fix-for-critical-vulnerability-with-known-exploits/