@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. 81/2021

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.

05/03/2021

- Hackeo a empresas de aviación: robo de cientos de miles de datos de pasajeros de Star Alliance.
  https://www.theguardian.com/world/2021/mar/05/airline-data-hack-hundreds-of-thousands-of-star-alliance-passengers-details-stolen
  https://www.bleepingcomputer.com/news/security/sita-data-breach-affects-millions-of-travelers-from-major-airlines/
- *Mazafaka* (un foro de élite de hacking y cibercrimen), *hackeado*!
  https://thehackernews.com/2021/03/mazafaka-elite-hacking-and-cybercrime.html
- Recursos de Docker Hub y Bitbucket pirateados para minería de criptomonedas.
  https://www.infosecurity-magazine.com/news/docker-hub-bitbucket-hijacked/
- *Hackers* obtienen datos sensibles sobre proyectos de ayuda del Reino Unido en el extranjero.
  https://www.theguardian.com/politics/2021/mar/05/hackers-obtain-sensitive-data-on-uk-aid-projects-overseas

06/03/2021

- Está prosperando un nuevo tipo de ataque a la cadena de suministro con graves consecuencias.
  https://arstechnica.com/gadgets/2021/03/more-top-tier-companies-targeted-by-new-type-of-potentially-serious-attack/
- Funcionarios checos han sido alcanzados por un ciberataque de gran escala.
  https://www.euronews.com/2021/03/05/czech-officials-in-prague-hit-by-massive-cyber-attack

07/03/2021

- Paquetes corruptos: Un usuario de "Supply Chain Risks" ataca a la comunidad Python con 4.000 módulos falsos.
  https://nakedsecurity.sophos.com/2021/03/07/poison-packages-supply-chain-risks-user-hits-python-community-with-4000-fake-modules/
- El creador del software antivirus de McAfee, acusado de conspiración.
  https://www.ehackingnews.com/2021/03/creator-of-mcafee-antivirus-software.html

08/03/2021

- Los datos de los clientes de Flagstar Bank han sido pirateados por Accellion.
  https://www.zdnet.com/article/flagstar-bank-customer-data-breached-through-accellion-hack/
- Los dispositivos QNAP sin parches están siendo hackeados para minar criptomonedas.
  https://www.bleepingcomputer.com/news/security/unpatched-qnap-devices-are-being-hacked-to-mine-cryptocurrency/
- CISA insta encarecidamente a todas las organizaciones de los EE.UU. a abordar inmediatamente las vulnerabilidades de Microsoft Exchange.

https://us-cert.cisa.gov/ncas/current-activity/2021/03/08/cisa-strongly-urges-all-organizations-immediately-address

- Ciberdelincuentes atacan a la Universidad de Texas.
https://www.infosecurity-magazine.com/news/hackers-target-texas-university/
- Podcast diario de seguridad de redes de SANS (Stormcast) del lunes 8 de marzo de 2021. Especialmente MSFT Exchange.
https://isc.sans.edu/podcastdetail.html?id=7402

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

- D-Link y dispositivos IoT son atacados por una variante de Gafgyt basada en Tor.
https://threatpost.com/d-link-iot-tor-gafgyt-variant/164529/
- El malware puede aprovecharse de un nuevo fallo en las CPU de Intel para lanzar ataques de canal lateral.
https://thehackernews.com/2021/03/malware-can-exploit-new-flaw-in-intel.html

NOTAS DE INTERÉS

- Surgen más víctimas de los "*días cero*" de Microsoft Exchange Server.
https://www.cyberscoop.com/microsoft-exchange-server-czech-republic-norway-hafnium-chinese-hackers/
- Miles de organizaciones estadounidenses comprometidas a través de un error de Microsoft.
https://www.reuters.com/article/us-usa-cyber-microsoft-idUSKBN2AX23U
https://www.zdnet.com/article/microsoft-exchange-zero-day-attacks-30000-servers-hit-already-says-report/
- El espionaje de China y Rusia tardará años en ser aclarado.
https://arstechnica.com/information-technology/2021/03/chinas-and-russias-spying-spree-will-take-years-to-unpack/
- Un falso ataque de phishing con reCAPTCHA de Google roba contraseñas de Office 365.
https://threatpost.com/google-recaptcha-phishing-office-365/164566/
- Las mujeres en la ciberseguridad: La brecha de género se reduce, pero no lo suficiente.
https://www.welivesecurity.com/2021/03/08/women-cybersecurity-gender-gap-narrows-but-not-enough/

ACTUALIZACIONES DE SEGURIDAD

- Supermicro y Pulse Secure publican correcciones para los ataques "TrickBoot".
https://www.bleepingcomputer.com/news/security/supermicro-pulse-secure-release-fixes-for-trickboot-attacks/
- Samsung corrige errores críticos de Android en las actualizaciones de marzo de 2021.
https://www.bleepingcomputer.com/news/security/samsung-fixes-critical-android-bugs-in-march-2021-updates/
- Microsoft publica una herramienta de detección de IOC para los errores de Microsoft Exchange Server.
https://securityaffairs.co/wordpress/115324/security/microsoft-exchange-server-audit-tool.html