@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. 69/2021

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.

15/01/2021

- Xiaomi se agregó a la lista estadounidense de posibles empresas militares comunistas de China. https://www.zdnet.com/article/xiaomi-added-to-us-list-of-alleged-communist-chinese-military-companies/
- La vulnerabilidad, no publicada, del Apache Velocity XSS afecta a los sitios ".gov". https://www.bleepingcomputer.com/news/security/undisclosed-apache-velocity-xss-vulnerability-impacts-gov-sites/
- Signal se cae después de que ha sido "inundado" con nuevos usuarios. https://www.bleepingcomputer.com/news/software/signal-down-after-getting-flooded-with-new-users/
- **Un fallo grave de Windows 10 podría corromper el disco duro al abrir una carpeta.** https://betanews.com/2021/01/15/windows-10-ntfs-flaw-corrupt-hard-drive/
- WhatsApp retrasa la polémica actualización de la política de privacidad de 'Data-Sharing' por 3 meses. https://thehackernews.com/2021/01/whatsapp-delays-controversial-data.html

16/01/2021

- La "empresa" de tarjetas de crédito robadas, Joker's Stash, cierra después de hacer una fortuna. https://www.bleepingcomputer.com/news/security/stolen-credit-card-shop-jokers-stash-closes-after-making-a-fortune/
- Piratas informáticos 'manipularon' documentos de vacunas robados según una agencia de la *UE.* https://www.securityweek.com/eu-regulator-hackers-´manipulated´-stolen-vaccine-documents
- Dos niños encontraron como *puentear* el salvapantallas de Linux Mint con dos teclas. https://securityaffairs.co/wordpress/113518/hacking/screensaver-bypass-linux-mint.html

17/01/2021

- Hackers penetran en los ordenadores de la Oficina de Asuntos Exteriores en un ciberataque a un puesto de campo del Gobierno del RU. https://www.dailymail.co.uk/news/article-9153165/Hackers-breach-Foreign-Office-computers-cyber-attack-Government-countryside-outpost.html

18/01/2021

- Thales y TT Electronics se asocian para realizar investigaciones de ciberseguridad en OT. https://www.infosecurity-magazine.com/news/thales-tt-electronics-partner/
- El Ente Escocés de Regulación Ambiental sufre un impacto ransomware. https://www.infosecurity-magazine.com/news/environmental-regulator-suffers/
- El FBI advierte de ataques "*vishing*" (phishing) para robar cuentas corporativas.

https://www.bleepingcomputer.com/news/security/fbi-warns-of-vishing-attacks-stealing-corporate-accounts/

- Rob Joyce es el nuevo Director Cibernético de la NSA.
https://securityaffairs.co/wordpress/113568/security/rob-joyce-nsa-cyber-director.html

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

- Analizando dinámicamente un archivo malicioso de macros de Excel 4 fuertemente ofuscado.
https://isc.sans.edu/forums/diary/Dynamically+analyzing+a+heavily+obfuscated+Excel+4+macro+malicious+file/26986/
- Privacidad de la ubicación del teléfono móvil.
https://www.schneier.com/blog/archives/2021/01/cell-phone-location-privacy.html
- NSA: El DNS sobre HTTPS proporciona una "falsa sensación de seguridad".
https://www.infosecurity-magazine.com/news/nsa-dns-over-https-provides-false/
https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF
- Center for Internet Security: tablas comparativas (*benchmarks*).
https://www.cisecurity.org/cis-benchmarks/

NOTAS DE INTERÉS

- Se divulga el malware chino indocumentado utilizado en los últimos ataques.
https://thehackernews.com/2021/01/researchers-disclose-undocumented.html
- RAT Rogue: Un malware para Android que da a los hackers control total sobre un teléfono.
https://www.ehackingnews.com/2021/01/rogue-android-malware-that-gives.html
- #CES2021: La IA y las tecnologías cuánticas se preparan para trastornar la industria de la ciberseguridad.
https://www.infosecurity-magazine.com/news/ai-quantum-disrupt-cybersecurity/
- Guía sobre cómo las organizaciones pueden protegerse en el ciberespacio.
https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/common-cyber-attacks-reducing-the-impact
-

ACTUALIZACIONES DE SEGURIDAD

- Vulnerabilidades y actualizaciones para equipos Cisco.
https://tools.cisco.com/security/center/publicationListing.x
- Microsoft publica la actualización KB4598479 para corregir el error "Reiniciar este PC" en Windows 10.
https://betanews.com/2021/01/16/microsoft-releases-kb4598479-update-to-fix-reset-this-pc-bug-in-windows-10/
- Apple elimina la característica de MacOS que permitía a las aplicaciones eludir la seguridad del firewall.
https://thehackernews.com/2021/01/apple-removes-macos-feature-that.html