@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. 146 – 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 15/12/21 y el 21/12/21

- Ataques de piratas informáticos vinculados a Irán contra objetivos israelíes.
https://www.securityweek.com/iran-linked-hackers-attack-israeli-targets-company
- Francia ordena a Clearview AI que borre los datos y deje de procesar ilegalmente imágenes.
https://www.infosecurity-magazine.com/news/france-orders-clearview-ai-delete/
- Las cervecerías McMenamins afectadas por un ataque de ransomware Conti.
https://www.bleepingcomputer.com/news/security/mcmenamins-breweries-hit-by-a-conti-ransomware-attack/
- **Intrusos aprovechan el fallo de Log4j para entrar en el Departamento de Defensa belga.**
https://www.cyberscoop.com/intruders-leverage-log4j-flaw-to-breach-belgian-defense-department/
- Un ciberataque afecta a empresas australianas.
https://www.infosecurity-magazine.com/news/cyberattack-impacts-aussie/

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

- La red de bots Phorpiex regresa con nuevos trucos que la hacen más difícil de desbaratar.
https://www.bleepingcomputer.com/news/security/phorpiex-botnet-returns-with-new-tricks-making-it-harder-to-disrupt/
https://www.darkreading.com/attacks-breaches/phorpiex-botnet-variant-spread-across-96-countries
- Se descubren nuevos ataques de coexistencia en los chips Wi-Fi y Bluetooth.
https://thehackernews.com/2021/12/researchers-uncover-new-coexistence.html
- **La NSA y CISA publican la parte final de la guía de seguridad de infraestructuras de la nube 5G.**
https://www.cisa.gov/uscert/ncas/current-activity/2021/12/16/nsa-and-cisa-release-final-part-iv-guidance-securing-5g-cloud
- Nuevas vulnerabilidades en las redes móviles afectan a todas las generaciones de celulares desde la 2G en adelante.
https://thehackernews.com/2021/12/new-mobile-network-vulnerabilities.html
- Campaña de espionaje masivo denominada "PseudoManuscrypt", afecta a 35.000 sistemas.
https://threatpost.com/pseudomanuscrypt-mass-spyware-campaign/177097/
- Descubren una puerta trasera desplegada en la red de una Agencia Federal de Estados Unidos.
https://thehackernews.com/2021/12/experts-discover-backdoor-deployed-on.html
- Microsoft advierte de la facilidad con la que se “toman” los dominios de Windows a través de los fallos de Active Directory.
https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-of-easy-windows-domain-takeover-via-active-directory-bugs/
- “2easy” se ha convertido en un importante mercado de datos robados en la web oscura.
https://www.bleepingcomputer.com/news/security/2easy-now-a-significant-dark-web-marketplace-for-stolen-data/

NOTAS DE INTERÉS

- **Los hackers ya explotan la segunda vulnerabilidad de Log4j mientras surge un tercer fallo.**
https://thehackernews.com/2021/12/hackers-begin-exploiting-second-log4j.html
- La segunda vulnerabilidad de Log4j conlleva una amenaza de denegación de servicio.
https://www.csoonline.com/article/3645132/second-log4j-vulnerability-carries-denial-of-service-threat-new-patch-available.html
- Owowa, un soft malicioso de IIS Server usado para robar credenciales de Microsoft Exchange.
https://securityaffairs.co/wordpress/125682/hacking/owowa-malicious-iis-server-module-used-to-steal-microsoft-exchange-credentials.html
- "Grupos de amenazas" trabajan supuestamente en el gusano Log4Shell.
https://www.securityweek.com/threat-groups-reportedly-working-log4shell-worm
- Las portátiles Lenovo son vulnerables a un error que permite obtener privilegios de administrador.
https://www.bleepingcomputer.com/news/security/lenovo-laptops-vulnerable-to-bug-allowing-admin-privileges/
- Google: NSO Pegasus Zero-Click es el "exploit técnicamente más sofisticado jamás visto".
https://www.securityweek.com/google-says-nso-pegasus-zero-click-most-technically-sophisticated-exploit-ever-seen
- Facebook bloquea 1.500 cuentas falsas utilizadas por empresas de ciberespionaje.
https://www.theregister.com/2021/12/17/cyber_spying_firms_facebook_meta/
- **No es demasiado pronto para empezar a hablar del 6G.**
https://securityintelligence.com/articles/its-not-too-soon-start-talking-about-6g/
- La RAF derriba un "dron terrorista" sobre una base de operaciones especiales de EE.UU. en Siria.
https://www.theregister.com/2021/12/17/raf_shoots_down_drone_syria/
- Brasil investiga uso de claves del personal en ciberataques contra organismos gubernamentales.
https://www.zdnet.com/article/brazil-investigates-use-of-staff-credentials-in-cyberattacks-against-government-bodies/
- **Más de 500 mil usuarios descargaron la aplicación de malware Joker, de Play Store.**
https://thehackernews.com/2021/12/over-500000-android-users-downloaded.html
- Meta toma medidas contra las estafas de phishing que utilizan sus marcas comerciales.
https://www.theverge.com/2021/12/20/22846952/meta-lawsuit-phishing-attacks
- El ransomware PYSA está detrás de la mayoría de los ataques extorsivos de noviembre.
https://www.bleepingcomputer.com/news/security/pysa-ransomware-behind-most-double-extortion-attacks-in-november/

ACTUALIZACIONES DE SEGURIDAD

- VMware parchea un fallo crítico en la consola UEM de Workspace ONE.
https://www.securityweek.com/vmware-patches-critical-flaw-workspace-one-uem-console
- OpenSSL corrige los fallos que provocan "confluencia de errores".
https://nakedsecurity.sophos.com/2021/12/17/serious-security-openssl-fixes-error-conflation-bugs-how-mixing-up-mistakes-can-lead-to-trouble/
- **Apache publica el tercer parche para solucionar un nuevo fallo de Log4j.**
https://securityaffairs.co/wordpress/125760/hacking/log4j-third-flaw.html
- Corregir 2 fallos de Active Directory para evitar la toma de control de los dominios de Windows.
https://securityaffairs.co/wordpress/125857/security/windows-active-directory-flaws.html