@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. 150 – Año 2022

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 12/1/22 y el 18/1/22

- Electronic Arts confirma que docenas de cuentas de FIFA de alto nivel han sido hackeadas.
https://www.zdnet.com/article/ea-confirms-dozens-of-high-profile-fifa-accounts-hacked-blame-customer-experience-employees/
- **Un hacker adolescente consigue controlar remotamente a más de 20 automóviles Tesla.**
https://www.techspot.com/news/92971-teen-hacker-gains-remote-control-over-20-teslas.html
- Un ataque "masivo" de ciberdelincuentes ha afectado a los sitios web del gobierno de Ucrania.
https://www.zdnet.com/article/a-massive-hacking-attack-has-hit-government-websites-in-ukraine/
- El gobierno ruso detiene a los miembros de la banda de ransomware REvil.
https://www.bleepingcomputer.com/news/security/russian-government-arrests-revil-ransomware-gang-members/
https://www.techrepublic.com/article/russia-arrests-revil-ransomware-gang-members-at-request-of-us-officials/
- **El contratista de defensa Hensoldt confirma el ataque del ransomware Lorenz.**
https://www.bleepingcomputer.com/news/security/defense-contractor-hensoldt-confirms-lorenz-ransomware-attack/
- Un malware destructivo destinado a entidades gubernamentales y empresariales ucranianas.
https://thehackernews.com/2022/01/a-new-destructive-malware-targeting.html
- Crypto.com interrumpe las extracciones y restablece el 2FA en caso de actividad sospechosa.
https://www.zdnet.com/article/crypto-com-pauses-withdrawals-and-resets-2fa-following-suspicious-activity/

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

- **Piratas informáticos se apoderan del e-mail de un diplomático y apuntan al viceministro ruso.**
https://www.bleepingcomputer.com/news/security/hackers-take-over-diplomats-email-target-russian-deputy-minister/
- Los hackers usan servicios en la nube para distribuir el malware Nanocore, Netwire y AsyncRAT.
https://thehackernews.com/2022/01/hackers-use-cloud-services-to.html
- El *ransomware* Magniber utiliza archivos APPX firmados para infectar los sistemas.
https://www.bleepingcomputer.com/news/security/magniber-ransomware-using-signed-appx-files-to-infect-systems/
- Los investigadores descifran las claves de registro encriptadas del troyano bancario Qakbot.
https://thehackernews.com/2022/01/researchers-decrypted-qakbot-banking.html
- **DHL destrona a Microsoft como la marca más imitada en los ataques de *phishing*.**
https://www.bleepingcomputer.com/news/security/dhl-dethrones-microsoft-as-most-imitated-brand-in-phishing-attacks/
- **El PCI SSC actualiza las normas de seguridad de las tarjetas para asegurar el proceso de producción de las mismas.**
https://www.helpnetsecurity.com/2022/01/18/pci-card-production-and-provisioning-security-requirements-3-0/

- Expertos evitan la autenticación multifactorial basada en SMS que protege las cuentas de Box.
https://thehackernews.com/2022/01/researchers-bypass-sms-based-multi.html
- Nuevo ransomware White Rabbit vinculado al grupo APT FIN8.
https://www.bleepingcomputer.com/news/security/new-white-rabbit-ransomware-linked-to-fin8-hacking-group/

NOTAS DE INTERÉS

- Los hackers están utilizando el fallo Log4j para ofrecer una nueva puerta trasera "modular".
https://www.zdnet.com/article/hackers-are-using-the-log4j-flaw-to-deliver-this-new-modular-backdoor/
- Nuevo malware de espionaje SysJoker que tiene como objetivo a los usuarios de Windows, macOS y Linux.
https://thehackernews.com/2022/01/new-sysjoker-espionage-malware.html
- **El Cibercomando de Estados Unidos vincula a MuddyWater con la inteligencia iraní.**
https://www.zdnet.com/article/us-cyber-command-links-muddywater-to-iranian-intelligence/
- Los principales grupos de piratas informáticos que atacan el sector financiero son Lazarus, Cobalt y FIN7.
https://www.zdnet.com/article/fingers-point-to-lazarus-cobalt-fin7-as-key-hacking-groups-focused-on-finance-industry/
- Grupos APT norcoreanos robaron una cantidad récord de criptodivisas el año pasado.
https://threatpost.com/north-korea-apts-stole-400m-cryptocurrency/177638/
- El Gobierno de EE.UU. y los gigantes tecnológicos discuten la seguridad del soft de código abierto.
https://www.securityweek.com/us-government-tech-giants-discuss-open-source-software-security
- Nuevo error del navegador Safari de Apple, sin parches, permite el rastreo cruzado de usuarios.
https://thehackernews.com/2022/01/new-unpatched-apple-safari-browser-bug.html
- Por seguridad, se debería pagar adecuadamente los proyectos de código abierto.
https://www.zdnet.com/article/for-security-alone-we-could-try-paying-open-source-projects-properly/
- Campaña de ciberespionaje se concentra en las empresas de energías renovables.
https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/
- Europol retira un servicio de VPN utilizado por *ciberdelincuentes* para distribuir ransomware.
https://www.zdnet.com/article/this-vpn-service-used-by-cyber-criminals-to-deliver-ransomware-has-just-been-taken-down-by-police/

ACTUALIZACIONES DE SEGURIDAD

- **El primer martes de parches de 2022 trae una solución para una vulnerabilidad crítica de Windows. La nota informa de actualizaciones de otros productos y proveedores.**
https://thehackernews.com/2022/01/first-patch-tuesday-of-2022-brings-fix.html
- Apple corrige el problema “doorLock” que puede inutilizar iPhones y iPads.
https://www.bleepingcomputer.com/news/security/apple-fixes-doorlock-bug-that-can-disable-iphones-and-ipads/
- AWS corrige los fallos de seguridad que exponían los datos de sus clientes.
https://www.bleepingcomputer.com/news/security/aws-fixes-security-flaws-that-exposed-aws-customer-data/
- Cisco libera un parche para un error crítico que afecta a Unified CCMP y Unified CCDM.
https://thehackernews.com/2022/01/cisco-releases-patch-for-critical-bug.html
- Zoho cierra otro agujero de seguridad crítico en Desktop Central.
https://www.bleepingcomputer.com/news/security/zoho-plugs-another-critical-security-hole-in-desktop-central/