@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. 76/2021

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.

09/02/2021

- El desarrollador de Cyberpunk 2077, una compañía polaca, sufre un ciberataque ramsonware. https://www.infosecurity-magazine.com/news/cyberpunk-developer-hit-cyber/
- Se filtran en la *Dark Web* los historiales médicos de dos hospitales de Estados Unidos. https://www.ehackingnews.com/2021/02/medical-records-of-two-us-based.html
- Microsoft advierte de la escalada de privilegios de Windows Win32k. https://us-cert.cisa.gov/ncas/current-activity/2021/02/09/microsoft-warns-windows-win32k-privilege-escalation
- El nuevo malware APT BendyBear se vincula a un grupo de hackers chino. https://www.bleepingcomputer.com/news/security/new-bendybear-apt-malware-gets-linked-to-chinese-hacking-group/
- Un escáner de códigos de barras con 10 millones de descargas es retirado del mercado de Google Play tras posibilitar un aluvión de anuncios en los teléfonos. https://threatpost.com/google-boots-barcode-scanner-app-ad-explosion/163803/
- Rusia adoptará los estándares estatales OpenRAN para el desarrollo de la 5G. https://www.ehackingnews.com/2021/02/russia-will-adopt-state-openran.html

10/02/2021

- Una antigua vulnerabilidad dejó a millones de dispositivos del IoT sensibles a ataques. https://www.zdnet.com/article/this-old-security-vulnerability-left-millions-of-internet-of-things-devices-vulnerable-to-attacks/
- El malware LodaRAT para Windows ahora también se centra en los dispositivos Android. https://thehackernews.com/2021/02/lodarat-windows-malware-now-also.html
- Un fallo de seguridad crítico de SAP Commerce permite el RCE. https://threatpost.com/sap-commerce-critical-security-bug/163822/

11/02/2021

- Singtel (telco de Singapur) sufre una filtración de datos de sus clientes debido a un fallo de seguridad de un proveedor externo. https://www.zdnet.com/article/singtel-hit-by-third-party-vendors-security-breach-customer-data-may-be-leaked/
- PayPal corrige la vulnerabilidad XSS detectada en el convertidor de divisas del monedero del usuario. https://www.zdnet.com/article/paypal-fixes-reflected-xss-vulnerability-in-business-wallet/

- **Entidades militares y nucleares están en la mira de un nuevo malware para Android.** https://threatpost.com/military-nuclear-entities-under-target-by-novel-android-malware/163830/
- Se publica un descifrador gratuito para las víctimas del ransomware Avaddon pero los ciberdelincuentes modifican el código rápidamente. https://www.zdnet.com/article/free-decrypter-released-for-avaddon-ransomware-victims-aaand-its-gone/

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

- Cuidado con los "expertos" técnicos que te bombardean con informes de errores. https://nakedsecurity.sophos.com/2021/02/09/beware-of-technical-experts-bombarding-you-with-bug-reports/
- Un equipo de diferentes orígenes, géneros, etnias y capacidades neurológicas están mejor equipados para afrontar los retos actuales de seguridad. https://www.darkreading.com/careers-and-people/how-neurodiversity-can-strengthen-cybersecurity-defense/a/d-id/1340078
- Análisis de phishing recibido en la casilla de correo electrónico de los administradores de ISC. https://isc.sans.edu/diary/rss/27082

NOTAS DE INTERÉS

- Buenas prácticas en las redes sociales para el Día de la Internet Segura (9 de febrero). https://www.tripwire.com/state-of-security/security-data-protection/social-media-best-practices-or-safer-internet-day
- Ignorar el pedido del ransomware y restaure desde la copia de seguridad, bueno... si fuera tan fácil. https://www.theregister.com/2021/02/09/ignore_that_ransomware_demand/
- Expertos de la ONU: Corea del Norte utiliza los ciberataques para actualizar sus armas nucleares. https://www.securityweek.com/un-experts-north-korea-using-cyber-attacks-update-nukes
- Ex funcionarios instan a EE.UU. a tomar medidas para evitar otro *hackeo* al estilo de SolarWinds. https://www.cyberscoop.com/solarwinds-chris-krebs-russian-hack/
- Un bug de Windows Defender de hace 12 años da a los hackers privilegios de administrador. https://www.bleepingcomputer.com/news/security/12-year-old-windows-defender-bug-gives-hackers-admin-rights/

ACTUALIZACIONES DE SEGURIDAD

- Parches de los martes, febrero de 2021: Microsoft y Adobe solucionan los días cero y otros problemas de seguridad. https://www.helpnetsecurity.com/2021/02/09/february-2021-patch-tuesday/ https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-10-bug-letting-attackers-trigger-bsod-crashes/
- Apple publica actualizaciones de seguridad. https://us-cert.cisa.gov/ncas/current-activity/2021/02/09/apple-releases-security-updates
- La vulnerabilidad de día cero de Internet Explorer 11 recibe un microparche no oficial. https://www.bleepingcomputer.com/news/security/internet-explorer-11-zero-day-vulnerability-gets-unofficial-micropatch/