@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. 103 – 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.

26/05/2021

- El malware Data Wiper, disfrazado de ransomware, se enfoca en entidades israelíes.
https://thehackernews.com/2021/05/data-wiper-malware-disguised-as.html
- Una banda de ciberdelincuentes ataca el sistema de desempleados de Texas.
https://www.infosecurity-magazine.com/news/scattered-canary-targets-texas/
- VMware hace sonar la alarma del ransomware por un fallo de gravedad crítica.
https://threatpost.com/vmware-ransomware-alarm-critical-bug/166501/
- El Ministerio del Interior belga sufrió un "sofisticado" ataque de ciberespionaje.
https://securityaffairs.co/wordpress/118275/breaking-news/belgium-interior-ministry-cyber-attack.html
https://www.cyberscoop.com/belgium-cyber-espionage-china-microsoft-exchange/

27/05/2021

- Las agencias gubernamentales japonesas sufren filtraciones de datos tras el hackeo a Fujitsu.
https://www.bleepingcomputer.com/news/security/japanese-government-agencies-suffer-data-breaches-after-fujitsu-hack/
- "*Hackers*" utilizan fundaciones falsas para atacar a la minoría uigur en China.
https://thehackernews.com/2021/05/hackers-using-fake-foundations-to.html
- El instalador de AnyDesk distribuyó una campaña de publicidad maliciosa en Google.
https://thehackernews.com/2021/05/malvertising-campaign-on-google.html
- La NASA identificó 1.785 incidentes cibernéticos en 2020.
https://securityaffairs.co/wordpress/118323/reports/nasa-cyber-attacks.html
- Violación de datos en el principal operador postal de Canadá
https://www.infosecurity-magazine.com/news/data-breach-at-canada-post/

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

- Los investigadores de Google descubren una nueva variante del ataque Rowhammer.
https://thehackernews.com/2021/05/google-researchers-discover-new-variant.html
https://www.zdnet.com/article/this-weird-memory-chip-vulnerability-is-even-worse-than-we-realised/
- BazaLoader se hace pasar por un servicio de streaming de películas. Este ataque de phishing utiliza un "call center" para engañar a la gente y que instale un malware en su PC con Windows.
https://threatpost.com/bazaloader-fake-movie-streaming-service/166489/
https://www.zdnet.com/article/this-phishing-attack-is-using-a-call-centre-to-trick-people-into-installing-malware-on-their-windows-pc/
- Vulnerabilidad "no parcheable" en el nuevo chip de la Mac de Apple,
https://nakedsecurity.sophos.com/2021/05/27/unpatchable-vuln-in-apples-new-mac-chip-what-you-need-to-know/

- **Vectores potenciales de amenaza a la infraestructura 5G.**
https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF

NOTAS DE INTERÉS

- Apple acaba de solucionar una falla de seguridad que permitía a un malware realizar capturas de pantalla en los Mac.
https://www.zdnet.com/article/apple-just-fixed-a-security-flaw-that-allowed-malware-to-take-screenshots-on-macs/
- Los "corsarios" aparecen en la ciénaga de la ciberdelincuencia.
https://threatpost.com/privateer-threat-actors-emerge/166483/
- Los PDF certificados pueden ser manipulados en forma secreta durante el proceso de firma.
https://www.theregister.com/2021/05/26/pdf_certificate_flaw/
https://threatpost.com/pdf-certified-widely-vulnerable-to-attack/166505/
- Los fallos de Bluetooth abren la puerta a que los atacantes suplanten la identidad de los dispositivos.
https://www.zdnet.com/article/bluetooth-bugs-open-the-door-for-attackers-to-impersonate-devices/
- La policía británica sufrió miles de vulneraciones de datos en 2020.
https://www.infosecurity-magazine.com/news/uk-police-suffered-thousands-data/
- **Presidente de Microsoft: "1984" de Orwell podría ocurrir en 2024.**
https://www.bbc.com/news/technology-57122120
- Los *bugs* recién descubiertos en las extensiones de VSCode podrían dar lugar a ataques a la cadena de suministro.
https://thehackernews.com/2021/05/newly-discovered-bugs-in-vscode.html
- El ataque "*scam*" con criptomonedas en Twitter le recuerda a los usuarios que deben comprobar las conexiones de sus aplicaciones.
https://www.tripwire.com/state-of-security/featured/cryptocurrency-scam-attack-twitter-check-app-connections/
- Estados Unidos anuncia nuevas directivas de seguridad para los oleoductos tras el *hackeo*.
https://www.reuters.com/technology/us-announces-new-security-directives-pipelines-after-hack-2021-05-27/

ACTUALIZACIONES DE SEGURIDAD

- Chrome 91 presenta 32 correcciones de seguridad y mejoras para Linux.
https://www.scmagazine.com/home/security-news/cloud-security/chrome-91-features-32-security-fixes-enhancements-for-linux/
- El equipo de Kali Linux lanza Kaboxer, una herramienta para gestionar aplicaciones en contenedores.
https://www.helpnetsecurity.com/2021/05/27/kali-linux-team-releases-kaboxer/
- HP Enterprises corrige una vulnerabilidad crítica de "día-cero" divulgada en diciembre.
https://www.bleepingcomputer.com/news/security/hpe-fixes-critical-zero-day-vulnerability-disclosed-in-december/