@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. 133 – 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 17/09/21 y el 23/09/21

- La multinacional TTEC sufre un ataque de ransomware que dificulta el trabajo de sus principales clientes.
https://www.zdnet.com/article/ttec-hit-with-ransomware-attack-hampering-work-for-major-clients/
- Los servicios telefónicos de VoIP.ms son interrumpidos por un ataque DDoS extorsivo.
https://www.bleepingcomputer.com/news/security/voipms-phone-services-disrupted-by-ddos-extortion-attack/
- La filtración de datos de Epik, empresa de hosting, afecta a 15 millones de usuarios, incluidos los que no son clientes.
https://arstechnica.com/information-technology/2021/09/epik-data-breach-impacts-15-million-users-including-non-customers/
- Los datos de los 100 millones de turistas de Tailandia se publican en Internet.
https://www.securityweek.com/details-100m-visitors-thailand-exposed-online-research-firm
- **La filtración de datos de una agencia inmobiliaria colombiana expone los registros de más de 100.000 compradores.**
https://thehackernews.com/2021/09/colombian-real-estate-agency-leak.html
- Error de MS Exchange deja al descubierto unas 100.000 credenciales de dominios de Windows.
https://thehackernews.com/2021/09/microsoft-exchange-bug-exposes-100000.html

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

- Alerta CISA: Actores APT se aprovechan de la vulnerabilidad recientemente identificada en ManageEngine ADSelfService Plus.
https://us-cert.cisa.gov/ncas/alerts/aa21-259a
- Investigadores recopilan una lista de vulnerabilidades utilizadas por las bandas de ransomware.
https://www.bleepingcomputer.com/news/security/researchers-compile-list-of-vulnerabilities-abused-by-ransomware-gangs/
- **Guía para combatir el ransomware de origen humano: Parte 1.**
https://www.microsoft.com/security/blog/2021/09/20/a-guide-to-combatting-human-operated-ransomware-part-1/
- Apache OpenOffice está actualmente afectado por un defecto de ejecución remota de código.
https://securityaffairs.co/wordpress/122426/security/apache-openoffice-rce-cve-2021-33035.html
- iOS 15 incluye una solución a Face ID utilizada para saltar la seguridad usando falsas caras.
https://nakedsecurity.sophos.com/2021/09/21/ios-15-includes-face-id-fix-for-security-bypass-using-3d-models/
- Microsoft: Análisis de una operación de phishing como sistema a gran escala.

https://www.microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/

- **Los nuevos *bugs* detectados n el software Nagios podrían permitir a los hackers tomar el control de las infraestructuras informáticas.**
https://thehackernews.com/2021/09/new-nagios-software-bugs-could-let.html
https://exchange.xforce.ibmcloud.com/collection/7e23d2950e3110b700c5f51240172455

NOTAS DE INTERÉS

- Se descubre ataque de malware al sector de la aviación tras pasar desapercibido durante 2 años.
https://thehackernews.com/2021/09/malware-attack-on-aviation-sector.html
- Este troyano bancario se aprovecha de YouTube para administrar la configuración remota.
https://www.zdnet.com/article/this-banking-trojan-abuses-youtube-to-manage-remote-settings/
- **Telegram se convierte en la nueva web oscura para los ciberdelincuentes.**
https://www.ft.com/content/cc3e3854-5f76-4422-a970-9010c3bc732b
https://arstechnica.com/information-technology/2021/09/telegram-emerges-as-new-dark-web-for-cyber-criminals/
- Una nueva aplicación ayuda a los iraníes a ocultar mensajes públicos.
https://arstechnica.com/information-technology/2021/09/a-new-app-helps-iranians-hide-messages-in-plain-sight/
- **Elimina tu contraseña de Windows 10 ahora: Microsoft emite repentinamente una actualización de seguridad para millones de personas.**
https://www.forbes.com/sites/daveywinder/2021/09/18/delete-your-windows-10-password-now-microsoft-suddenly-issues-security-advisory-for-millions/
- Australia emprende una ciberestrategia de cinco años.
https://www.zdnet.com/article/victoria-launches-five-year-au50-million-cyber-strategy/
- **Una nueva ola de ataques de malware dirigidos a organizaciones en Sudamérica.**
https://thehackernews.com/2021/09/a-new-wave-of-malware-attack-targeting.html
- Servidores de correo electrónico de la Asociación de Gobernadores Republicanos de EE.UU. fueron vulnerados por hackers de un Estado.
https://www.bleepingcomputer.com/news/security/republican-governors-association-email-server-breached-by-state-hackers/
- Se utiliza el Autodiscover de Microsoft para recopilar peticiones web y credenciales.
https://www.zdnet.com/article/design-flaw-in-microsoft-autodiscover-abused-to-leak-windows-domain-credentials/
- **100 millones de dispositivos IoT están expuestos a un *bug* de día cero.**
https://threatpost.com/100m-iot-devices-zero-day-bug/174963/
- El gobierno brasileño emprende una campaña de protección de datos.
https://www.zdnet.com/article/brazilian-government-launches-data-protection-campaign/

ACTUALIZACIONES DE SEGURIDAD

- Apple libera actualizaciones de seguridad para varios productos.
https://us-cert.cisa.gov/ncas/current-activity/2021/09/21/apple-releases-security-updates-multiple-products
- **VMware informa un error crítico en las instalaciones por defecto de vCenter Server: actualizar.**
https://thehackernews.com/2021/09/vmware-warns-of-critical-file-upload.html