@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. 121 – 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.

27/07/2021

- Las terminales portuarias de Sudáfrica siguen afectadas días después del ciberataque.
https://www.securityweek.com/safricas-port-terminals-still-disrupted-days-after-cyber-attack
- DIVD revela tres nuevos días cero sin parchear de Kaseya Unitrends.
https://securityaffairs.co/wordpress/120591/security/kaseya-unitrends-zero-days.html
- Se encontró una vulnerabilidad crítica en el producto de vigilancia aérea Sunhillo.
https://www.securityweek.com/critical-vulnerability-found-sunhillo-aerial-surveillance-product
- UC San Diego Health informa de una filtración de datos tras un ataque *phishing*.
https://www.bleepingcomputer.com/news/security/uc-san-diego-health-discloses-data-breach-after-phishing-attack/

28/07/2021

- Ciberataques en los Juegos Olímpicos de Tokio al comienzo de los mismos.
https://www.ehackingnews.com/2021/07/cyberattacks-zero-in-tokyo-olympics-as.html
- **Irlanda del Norte suspende el sistema de pases de vacunas tras la filtración de datos.**
https://www.bleepingcomputer.com/news/security/northern-ireland-suspends-vaccine-passport-system-after-data-leak/

29/07/2021

- Surgen nuevas bandas de ransomware, Haron y BlackMatter, en los foros de ciberdelincuencia.
https://thehackernews.com/2021/07/new-ransomware-gangs-haron-and.html
- Agencias gubernamentales israelíes visitan las oficinas de NSO Group.
https://threatpost.com/government-nso-offices/168241/
https://www.theregister.com/2021/07/29/israel_probes_nso_group/
- Usan error del browser de Microsoft para implantar malware VBA en ordenadores objetivo.
https://thehackernews.com/2021/07/hackers-exploit-microsoft-browser-bug.html
- Nuevo wiper malware destructivo, Meteor, fue utilizado en el ataque a los ferrocarriles iraníes.
https://www.bleepingcomputer.com/news/security/new-destructive-meteor-wiper-malware-used-in-iranian-railway-attack/

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

- Se encontraron fallas en 3 programas informáticos de código abierto utilizados en empresas.
https://thehackernews.com/2021/07/several-bugs-found-in-3-open-source.html
- HP concluye que el 75% de las amenazas fueron enviadas por correo electrónico en los primeros seis meses de 2021
https://www.zdnet.com/article/hp-finds-75-of-threats-were-delivered-by-email-in-first-six-months-of-2021/

- **Seis scripts maliciosos de Linux Shell utilizados para evadir las defensas y cómo detenerlos.**
https://threatpost.com/six-malicious-linux-shell-scripts-how-to-stop-them/168127/

- **Principales vulnerabilidades que actualmente se aprovechan de forma rutinaria.**
https://us-cert.cisa.gov/ncas/alerts/aa21-209a

- El costo de filtración de datos alcanza récords durante la pandemia.
https://securityaffairs.co/wordpress/120627/data-breach/cost-of-data-breach-2021.html
https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

- Ciberdelincuentes aprovechan el error del navegador de Microsoft para implantar el malware VBA en los ordenadores objetivo.
https://thehackernews.com/2021/07/hackers-exploit-microsoft-browser-bug.html

- **Informe de tendencias de APT del segundo trimestre de 2021.**
https://securelist.com/apt-trends-report-q2-2021/103517/

NOTAS DE INTERÉS

- La protección contra phishing de Defender para Office 365 "Safe Links" ya está disponible para todos los usuarios de Teams.
https://www.zdnet.com/article/microsoft-teams-just-got-this-new-protection-against-phishing-attacks/

- **Un nuevo bug podría permitir a los atacantes apropiarse del servidor Zimbra mediante el envío de correos electrónicos maliciosos**
https://thehackernews.com/2021/07/new-bug-could-let-attackers-hijack.html
https://threatpost.com/zimbra-server-bugs-email-plundering/168188/

- El tráfico de ataques a la API crece más del 300%.
https://betanews.com/2021/07/28/api-attack-traffic-grows-300-percent/

- El grupo "Praying Mantis" ataca con malware a servidores Windows dedicados a Internet.
https://www.zdnet.com/article/praying-mantis-threat-actor-targeting-windows-internet-facing-servers-with-malware/

- **No More Ransom** reúne *descifradores* para que víctimas de ransomware no tengan que pagar.
https://threatpost.com/no-more-ransom-saves-victims-e1-5-years/168192/

- La Casa Blanca le pide a la CISA y al NIST que establezcan objetivos de rendimiento de ciberseguridad para los operadores de infraestructuras críticas.
https://www.defenseone.com/policy/2021/07/white-house-asks-cisa-nist-set-cybersecurity-performance-goals-critical-infrastructure-operators/184104/
https://www.zdnet.com/article/biden-signs-memo-ordering-cisa-and-nist-to-develop-cybersecurity-performance-goals-for-critical-infrastructure/

- Piratas informáticos iraníes se hicieron pasar por una chica llamada Marcy para tentar a trabajadores de los sectores de defensa y aeroespacial.
https://www.theregister.com/2021/07/28/flirty_scouse_fitness_instructor_actually_iranian_spy/

- La falta de gente calificada en ciberseguridad afecta a más de la mitad de las organizaciones.
https://betanews.com/2021/07/28/cybersecurity-skills-crisis-impacts-organizations/

ACTUALIZACIONES DE SEGURIDAD

- **La NSA comparte sus consejos sobre cómo proteger sus dispositivos inalámbricos.**
https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2711968/nsa-issues-guidance-on-securing-wireless-devices-in-public-settings/