@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. 114 – 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.

02/07/2021

- Bandas ransomware están atacando a los sistemas de control industrial de "objetivos blandos". https://www.zdnet.com/article/ransomware-gangs-are-taking-aim-at-soft-target-industrial-control-systems/
- La autoridad de certificación de Mongolia fue hackeada para distribuir software “backdoor”. https://thehackernews.com/2021/07/mongolian-certificate-authority-hacked.html
- La empresa estadounidense AJG informa una filtración de datos tras un ataque de ransomware. https://www.bleepingcomputer.com/news/security/us-insurance-giant-ajg-reports-data-breach-after-ransomware-attack/
- La APT28, rusa, es culpable de una campaña de fuerza bruta que utiliza Kubernetes. https://www.infosecurity-magazine.com/news/russias-apt-28-blamed-brute-force/

03/07/2021

- **El ataque a la cadena de suministro de Kaseya afecta a cientos de proveedores de servicios y compañias con el ransomware REvil. Enorme ciberataque.**
  https://thehackernews.com/2021/07/kaseya-revil-ransomware-attack.html
  https://www.theverge.com/2021/7/2/22561252/revil-ransomware-attacks-systems-using-kaseyas-remote-it-management-software
  https://www.bbc.com/news/world-us-canada-57703836
- Un distribuidor químico estadounidense comparte información sobre como fue el robo de datos del ransomware DarkSide. https://www.bleepingcomputer.com/news/security/us-chemical-distributor-shares-info-on-darkside-ransomware-data-theft/
- Aplicaciones de Android con 5,8 millones de instalaciones son descubiertas robando las contraseñas de Facebook de los usuarios. https://thehackernews.com/2021/07/android-apps-with-58-million-installs.html

04/07/2021

- **Kaseya estaba arreglando el día cero justo cuando el ransomware REvil lanzó su ataque.** https://www.bleepingcomputer.com/news/security/kaseya-was-fixing-zero-day-just-as-revil-ransomware-sprung-their-attack/#.YOHgsk0lirI.twitter

05/07/2021

- Ataque ransomware de Kaseya: Estados Unidos inicia una investigación mientras la banda exige el pago de 70 millones de dólares en Bitcoins. https://www.zdnet.com/article/kaseya-ransomware-attack-us-launches-investigation-as-gang-demands-giant-70-million-payment/
  https://news.sky.com/story/russian-speaking-hackers-claim-major-ransomware-attack-which-has-hit-hundreds-of-us-companies-12349018

- **CISA y el FBI comparten orientaciones para las víctimas del ataque de ransomware a Kaseya.**
https://www.bleepingcomputer.com/news/security/cisa-fbi-share-guidance-for-victims-of-kaseya-ransomware-attack/
https://threatpost.com/kaseya-attack-fallout/167541/

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

- La nueva herramienta de Google Scorecards analiza software de código abierto en busca de riesgos de seguridad.
https://thehackernews.com/2021/07/new-google-scorecards-tool-scans-open.html
- El ransomware REvil afecta a 200 empresas en un ataque a la cadena de suministro de MSP.
https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-200-companies-in-msp-supply-chain-attack/
- **CISA ofrece una nueva solución para el error PrintNightmare.**
https://threatpost.com/cisa-mitigation-printnightmare-bug/167515/
- Lista de filtraciones de datos y ciberataques, junio de 2021, 9,8 millones de registros vulnerados.
https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-june-2021-9-8-million-records-breached
- **Ataque a la cadena de suministro de Kaseya: Lo que sabemos hasta ahora.**
https://www.welivesecurity.com/2021/07/03/kaseya-supply-chain-attack-what-we-know-so-far/

NOTAS DE INTERÉS

- **Investigadores de seguridad detectan accidentalmente la vulnerabilidad de ejecución remota PrintNightmare en el spooler de impresión de Windows.**
https://thehackernews.com/2021/07/microsoft-warns-of-critical.html
https://www.zdnet.com/article/microsoft-adds-second-cve-for-printnightmare-remote-code-execution/
- La NSA y el FBI divulgan los métodos de pirateo utilizados por los hackers militares rusos.
https://thehackernews.com/2021/07/nsa-fbi-reveal-hacking-methods-used-by.html
- Aparece el ransomware Diavol en el ámbito de las amenazas. ¿Obra de la banda Wizard Spider?
https://securityaffairs.co/wordpress/119637/malware/diavol-ransomware-wizard-spider-gang.html
- Un nuevo botnet inspirado en Mirai podría estar utilizando sus DVRs KGUARD en ciberataques.
https://thehackernews.com/2021/07/new-mirai-inspired-botnet-could-be.html
- TrickBot moderniza su troyano bancario.
https://threatpost.com/trickbot-banking-trojan-module/167521/
- Las conexiones inalámbricas mundiales de 5G llegan a 298 millones en el primer cuarto de 2021.
https://www.helpnetsecurity.com/2021/07/05/worldwide-wireless-5g-connections/

ACTUALIZACIONES DE SEGURIDAD

- Microsoft insta a los usuarios de Azure y de PowerShell a que se actualicen.
https://securityaffairs.co/wordpress/119629/security/microsoft-azure-powershell-rce-flaw.html
https://betanews.com/2021/07/03/microsoft-urges-powershelll-users-to-upgrade-to-protect-against-critical-vulnerability/
- QNAP corrige error crítico en la aplicación de copia de seguridad y recuperación de desastres del NAS.
https://www.bleepingcomputer.com/news/security/qnap-fixes-critical-bug-in-nas-backup-disaster-recovery-app/