@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. 115 – 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.

06/07/2021

- Cerca de 16.000 datos de trabajadores de Washington expuestos tras un ataque ransomware.
https://www.ehackingnews.com/2021/07/16000-washington-workers-data-exposed.html
- La Interpol detiene a un hacker marroquí implicado en actividades cibernéticas delictivas.
https://thehackernews.com/2021/07/interpol-arrests-hacker-in-morocco-who.html
- **Kaseya: Alrededor de 1.500 empresas afectadas por el ataque del ransomware REvil.**
https://securityaffairs.co/wordpress/119759/cyber-crime/kaseya-attack-impacted-1500-businesses.html
- Ataque DDoS a medios de comunicación filipinos vinculados al gobierno y al ejército.
https://www.ehackingnews.com/2021/07/ddos-attack-on-filipino-media-outlets.html
- La aplicación oficial de la Fórmula 1 fue hackeada.
https://www.infosecurity-magazine.com/news/official-formula-1-app-hacked/

07/07/2021

- Decenas de miles de personas fueron estafadas con falsas aplicaciones de minería de criptomonedas para Android.
https://www.bleepingcomputer.com/news/security/tens-of-thousands-scammed-using-fake-android-cryptomining-apps/
https://threatpost.com/cloud-cryptomining-swindle-google-play/167581/
- WildPressure APT aparece con un nuevo malware enfocado en Windows y macOS.
https://thehackernews.com/2021/07/wildpressure-apt-emerges-with-new.html
- Los ciberdelincuentes de SideCopy utilizan nuevos troyanos personalizados en ataques contra el ejército de la India.
https://www.zdnet.com/article/sidecopy-cybercriminals-use-custom-trojans-in-india-attacks/

08/07/2021

- El Comité Nacional Republicano de EE.UU. niega que hackers rusos hayan accedido a sus datos.
https://www.theguardian.com/us-news/2021/jul/06/republican-national-committee-denies-hack-synnex
- **Se descubren ataques de malware dirigidos a redes corporativas de América Latina.**
https://thehackernews.com/2021/07/experts-uncover-malware-attacks.html
- Morgan Stanley divulga una filtración de datos resultante de los hackeos de Accellion FTA.
https://arstechnica.com/gadgets/2021/07/morgan-stanley-discloses-data-breach-that-resulted-from-accellion-fta-hacks/

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

- Armagedón IoT/ICS: hackear dispositivos como si no hubiera un mañana (parte 1).
https://www.redtimmy.com/iot-ics-armageddon-hacking-devices-like-theres-no-tomorrow-part-1/

- Los usuarios de Western Digital se enfrentan a otro RCE.
https://krebsonsecurity.com/2021/07/another-0-day-looms-for-many-western-digital-users/#more-56182
https://threatpost.com/rce-0-day-western-digital-users/167547/

- **Ataque de ransomware a Kaseya.**
https://exchange.xforce.ibmcloud.com/collection/bdccc1803f827075771ab4350873cdd2

- Falsa actualización de seguridad de Kaseya VSA con Cobalt Strike.
https://www.bleepingcomputer.com/news/security/fake-kaseya-vsa-security-update-backdoors-networks-with-cobalt-strike/

- Decenas de paquetes NuGet vulnerables permiten a los atacantes atacar la plataforma .NET
https://thehackernews.com/2021/07/dozens-of-vulnerable-nuget-packages.html

- El parche publicado por Microsoft no soluciona totalmente la vulnerabilidad *PrintNightmare*.
https://thehackernews.com/2021/07/microsofts-emergency-patch-fails-to.html

NOTAS DE INTERÉS

- Japón reforzará la defensa de la ciberseguridad nacional con 800 nuevas contrataciones.
https://www.zdnet.com/article/japan-to-bolster-national-cybersecurity-defence-with-800-new-hires-report/

- Distribución cuántica de claves: ¿Es tan segura como se dice y qué puede ofrecer a la empresa?
https://www.theregister.com/2021/07/06/quantum_key_distribution/

- Fallos críticos en el servicio Print spooler de Windows podrían permitir ataques remotos.
https://www.techrepublic.com/article/critical-flaws-in-windows-print-spooler-service-could-allow-for-remote-attacks/
https://isc.sans.edu/diary/rss/27610

- Cisco anuncia Webex para Defensa, diseñado específicamente para el Pentágono.
https://www.zdnet.com/article/cisco-announces-webex-for-defense-built-specifically-for-the-pentagon/

- Los hackers rusos habrían atacado los sistemas informáticos del Partido Republicano de EE.UU.
https://www.theverge.com/2021/7/6/22565779/rnc-breach-russian-hackers-cozy-bear

- **Una oficina del Pentágono dejó los diseños de chalecos antibalas y de equipos de los vehículos al alcance de los piratas informáticos, según un organismo de control.**
https://www.cyberscoop.com/pentagon-cyber-vulnerabilities-printers-hack/

- Las filtraciones de datos pueden costar a las empresas hasta un 20 por ciento de sus ingresos.
https://betanews.com/2021/07/07/insider-data-breaches-cost-20-percent-revenue/

- La ciberdelincuencia le cuesta a las organizaciones casi 1,79 millones de dólares por minuto.
https://www.infosecurity-magazine.com/news/cybercrime-costs-orgs-per-minute/

ACTUALIZACIONES DE SEGURIDAD

- Las actualizaciones de julio de Microsoft Office solucionan los errores de Outlook y los problemas de rendimiento.
https://www.bleepingcomputer.com/news/microsoft/microsoft-office-july-updates-fix-outlook-crashes-performance-issues/

- El browser Tor agrega una nueva función contra la censura.
https://www.bleepingcomputer.com/news/security/tor-browser-adds-new-anti-censorship-feature-v2-onion-warnings/