@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. 125 – 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.

10/08/2021

- La variante del ransomware eCh0raix se concentra en los dispositivos NAS de QNAP y Synology.
  https://threatpost.com/ech0raix-ransomware-variant-qnap-synology-nas-devices/168516/
- Crytek confirma el ataque del ransomware Egregor y el robo de datos de clientes.
  https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/
- Piratas informáticos chinos se hicieron pasar por iraníes para vulnerar objetivos israelíes.
  https://www.cyberscoop.com/china-israel-iran-fireeye-hacking/

11/08/2021

- Norton y Avast se fusionan en un imperio antivirus de 8.000 millones de dólares.
  https://www.theverge.com/2021/8/11/22619667/nortonlifelock-avast-merger-deal-anti-virus-cyber-security-software
- **La venta de tarjetas de vacunación COVID falsas se incrementa en la Dark Web.**
  https://www.techrepublic.com/article/fake-covid-vaccine-card-sales-ramp-up-on-dark-web/
- Filtración de datos en el sistema de salud de Georgia
  https://www.infosecurity-magazine.com/news/data-breach-at-georgia-health/
- Accenture afirma que el ataque del ransomware Lockbit no causó "ningún impacto".
  https://www.zdnet.com/article/accenture-says-lockbit-ransomware-attack-caused-no-impact-on-operations-or-clients/

12/08/2021

- **El gigante informático Accenture se ve afectado por el ransomware LockBit y los hackers amenazan con filtrar datos.**
  https://thehackernews.com/2021/08/it-giant-accenture-hit-by-lockbit.html
  https://www.infosecurity-magazine.com/news/accenture-tied-up-in-50m-ransom/
- **Después del parche del martes, Microsoft advierte de otra vulnerabilidad RCE del Print Spooler de Windows sin parchear.**
  https://thehackernews.com/2021/08/microsoft-security-bulletin-warns-of.html

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

- Los piratas informáticos explotan un nuevo fallo de anulación de autenticidad que afecta a millones de routers Arcadyan.
  https://thehackernews.com/2021/08/hackers-exploiting-new-auth-bypass-bug.html
- Los expertos creen que los hackers chinos están detrás de varios ataques dirigidos a Israel.
  https://thehackernews.com/2021/08/experts-believe-chinese-hackers-are.html

- El malware Chaos camina por la línea entre el ransomware y el borrador.
https://threatpost.com/chaos-malware-ransomware-wiper/168520/
- **CISA: Guía para la formación del personal de ciberseguridad.**
https://www.cisa.gov/publication/cybersecurity-workforce-training-guide
- La clave universal de descifrado de REvil de Kaseya se ha filtrado en un foro de hacking
https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/
- TA551 (Shathak) sigue impulsando a BazarLoader y las infecciones dirigen a Cobalt Strike.
https://isc.sans.edu/diary/rss/27738
- En la Universidad de Cornell descubren un ataque de "contaminación de códigos".
https://www.zdnet.com/article/cornell-university-researchers-discover-code-poisoning-attack/

NOTAS DE INTERÉS

- El ataque de " Glowworm " convierte los destellos de luz en audio.
https://threatpost.com/glowworm-attack-light-flickers-audio/168501/
- Una mala configuración de Salesforce puede exponer datos sensibles.
https://betanews.com/2021/08/10/salesforce-misconfiguration-expose-sensitive-data/
- Los piratas informáticos obtienen una media de casi 10.000 dólares por lo robado a la red.
https://www.zdnet.com/article/hackers-netting-average-of-nearly-10000-for-stolen-network-access/
- **Más de 600 millones de dólares supuestamente robados en el hackeo de criptodivisas.**
https://www.bleepingcomputer.com/news/security/over-600-million-reportedly-stolen-in-cryptocurrency-hack/
- Una nueva variante del malware AdLoad se cuela entre las defensas XProtect de Apple.
https://www.bleepingcomputer.com/news/apple/new-adload-malware-variant-slips-through-apples-xprotect-defenses/

ACTUALIZACIONES DE SEGURIDAD

- Firefox añade una limpieza de cookies mejorada y HTTPS por defecto en la navegación privada.
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/mozilla-releases-security-updates-firefox
- **Parches de Microsoft de agosto de 2021.**
https://blog.talosintelligence.com/2021/08/microsoft-patch-tuesday-for-august-2021.html
https://www.tripwire.com/state-of-security/vert/vert-threat-alert-august-2021-patch-tuesday-analysis/
- Citrix publica una actualización de seguridad.
https://us-cert.cisa.gov/ncas/current-activity/2021/08/10/citrix-releases-security-update-sharefile-storage-zones-controller
- Adobe soluciona vulnerabilidades críticas de preauth en Magento.
https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-preauth-vulnerabilities-in-magento/
- **Nueva versión: Navegador Tor 10.5.4 (Windows, macOS, Linux).**
https://blog.torproject.org/new-release-tor-browser-1054
- Nueve vulnerabilidades críticas y de alta gravedad han sido corregidas en productos SAP.
https://www.securityweek.com/nine-critical-and-high-severity-vulnerabilities-patched-sap-products
- **Apple publica una misteriosa actualización masiva de corrección de errores para los Mac.**
https://www.zdnet.com/article/apple-releases-massive-mystery-bug-fix-update-for-macs/