ISSN: 2718-6245

OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Edición: Bib Alejandra Castillo

ISSN: 2718-6245
http://www.esgcffaa.edu.ar/esp/oac-boletines.php

AÑO 4 N° 37
Agosto 2021

OAC Boletín de Agosto de 2021

"Debido a que el dominio cibernético no conoce fronteras ni límites, la futura doctrina militar y los límites jurisdiccionales deben evolucionar y converger para proporcionar una estrategia holística y coordinada para mantenerse competitivo con las amenazas"

Samuel J. Richman

Tabla de Contenidos

El **Observatorio de Argentino del Ciberespacio** (OAC), micro-sitio de la **Escuela Superior de Guerra Conjunta**
URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php.
Es un esfuerzo posible por el financiamiento que el observatorio recibe de la **Universidad de la Defensa Nacional**, a través de los programas UNDEFI y se encuentra inserto en el **Nodo Territorial de Defensa y Seguridad** del Ministerio de Ciencia, Tecnología e Innovación de la Nación y es administrado por el **Centro de Estudios de Prospectiva Tecnológica Militar "Grl Mosconi" de la Facultad de Ingeniería del Ejército Argentino**
Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial distintas perspectivas de este nuevo ámbito operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

Hemos incluido a partir de este número la sección PARA TENER EN CUENTA

ESTRATEGIA

La Constelación GPS III y la capacidad interferencias

La Fuerza Espacial de EE. UU. Anunció que tomó el control operativo del quinto satélite GPS III, completando la constelación de referencia necesaria para la cobertura mundial con una señal de posición, navegación y sincronización más confiable. El satélite más nuevo de la última generación de sistemas, se encuentra entre un grupo más grande de 24 cargas de GPS en órbita que son capaces de utilizar una nueva señal PNT militar, código M. El empelo del código M requiere un adiestramiento adicional para ser empleado con regularidad.

https://www.gps.gov/systems/gps/space/

https://www.defensenews.com/battlefield-tech/space/2021/06/18/space-force-launches-fifth-gps-iii-satellite/

https://www.c4isrnet.com/battlefield-tech/space/2021/07/15/space-force-declares-operational-acceptance-of-fifth-anti-jamming-gps-iii-satellite/

GPS II US Air Force Modernization, https://www.youtube.com/watch?v=MDfVdi26QMc .https://www.afcea.org/content/stavridis-warns-russia-and-china-cyber-attacks?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=DkwX6

CIBERSEGURIDAD

EE.UU. mantendría una fuerte ventaja en ciberseguridad en relación a sus adversarios

Los puntos fuertes de China como potencia cibernética se ven debilitados por la escasa seguridad y los débiles análisis de inteligencia, según un nuevo estudio que predice que Beijing será incapaz de igualar las capacidades cibernéticas de Estados Unidos durante al menos una década.

El estudio, publicado por el Instituto Internacional de Estudios Estratégicos, (IISS por sus siglas en inglés) se produce en un momento en que una serie de campañas de piratería informática han puesto de manifiesto la creciente amenaza del espionaje online por parte de Estados hostiles.

https://www.cronista.com/financial-times/el-poder-digital-de-china-esta-10-anos-atras-respecto-al-de-estados-unidos-segun-un-estudio/

España lanza un "ObserCiber"

El Instituto Nacional de Ciberseguridad y el Observatorio Nacional de Tecnología y Sociedad han lanzado conjuntamente 'ObservaCiber', el primer observatorio público especializado en ciberseguridad, cuyo objetivo es 'Estudio sobre percepción y nivel de confianza en España, acerca de cómo se protege la ciudadanía ante los ciberriesgo. 'ObservaCiber' nace para unificar y promover bajo un observatorio común, con una marca unificada, los estudios de ciberseguridad desarrollados por ONTSI e INCIBE. Con el fin de abordar el impulso y la divulgación de la importancia de la cultura de la ciberseguridad

https://revistabyte.es/ciberseguridad/observaciber/

¿SE PUEDE ESTABLECER UN ENTORNO CIBERSEGURO?

Lo que antes eran casos puntuales ahora se han vuelto cotidianos. Basta darse una vuelta por cualquier periódico no especializado de todo el mundo para descubrir que grandes empresas, multinacionales y organismos públicos supuestamente diseñados a prueba de cualquier ciberataque como el Pentágono, están sufriendo constantes amenazas.
(Ingreso mediante suscripción gratuita a la revista) https://revistabyte.es/ciberseguridad/

https://revistabyte.es/tema-de-portada-byte-ti/est-entorno-ciberseguro /

CIBERDEFENSA

NUEVAS ASOCIACIONES TECNOLÓGICAS PARA CONTRARRESTAR AMENAZAS

En un evento organizado por la Comisión de Seguridad Nacional sobre Inteligencia Artificial, altos líderes que abarcan desde la OTAN hasta el Pentágono y el Indo-Pacífico advirtieron sobre la amenaza que representa para los derechos humanos y la seguridad el ascenso tecnológico de China y la ambición de convertirse en el líder mundial en inteligencia artificial. y dar forma a la forma en que se utilizan las tecnologías emergentes al influir en los organismos que establecen estándares globales

https://www.c4isrnet.com/artificial-intelligence/2021/07/13/global-leaders-seek-new-technology-partnerships-to-counter-threat-posed-by-china/

AUMENTA EL RANSOMWARE DIRIGIDO A LOS SISTEMAS DE CONTROL INDUSTRIAL

"Los sistemas de **control industrial** son increíblemente difíciles de proteger, ya que dejan muchas brechas de seguridad que los actores de amenazas están explotando claramente con creciente determinación", comenta Ryan Flores, director senior del equipo *forward-looking threat research de Trend Micro.*

https://revistabyte.es/ciberseguridad/ataq-sistemas-de-control-industrial/

https://us-cert.cisa.gov/ncas/alerts/aa21-200a

CIBERGUERRA

El éxito de la guerra cibernética significa examinar el software

Estados Unidos se encuentra en la cúspide de un futuro definido por competencias de grandes potencias que sin duda se caracterizarán por estrategias y tácticas de guerra cibernética amplias, profundas y sutiles. La nación debe tomar una decisión deliberada para defender la superficie de ataque humano digital de manera efectiva al difuminar las líneas de batalla tradicionales y crear un espacio de batalla combinado de la patria y el exterior.

Una ciber Guerra Fría que domina la realidad moderna se libra todos los días, tanto en el exterior como en suelo estadounidense, deliberadamente mantenida por debajo del umbral del conflicto armado. A medida que los mundos civil y militar se definen cada vez más por software, se enfrentan al desafío continuo de mantenerse al día con los nuevos frentes de batalla emergentes. El futuro de la guerra cibernética bien puede consistir, en su mayor parte, en subsumir todos los demás dominios de la guerra. Y debido a que el dominio cibernético no conoce fronteras ni límites, la futura doctrina militar y los límites jurisdiccionales deben evolucionar y converger para proporcionar una estrategia holística y coordinada para mantenerse competitivo con las amenazas.

https://www.afcea.org/content/defending-digital-human-network?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIlVg1&_zl=v2Kk7#

OPERACIONES CIBERNÉTICAS PATROCINADAS POR EL ESTADO CHINO: TTP OBSERVADOS

La Agencia de Seguridad Nacional, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y la Oficina Federal de Investigaciones (FBI) evalúan que la actividad cibernética maliciosa patrocinada por el estado de la República Popular China es una amenaza importante para los activos ciberespaciales de Estados Unidos y los Aliados. Los actores cibernéticos patrocinados por el estado chino apuntan agresivamente al personal y las organizaciones políticas, económicas, militares, educativas y de infraestructura crítica (CI) de los EE. UU y sus aliados para robar datos confidenciales, tecnologías clave críticas y emergentes, propiedad intelectual e información de identificación personal

https://us-cert.cisa.gov/ncas/alerts/aa21-200b

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS DE LOS APT40 acusados como asociados con el Departamento de Seguridad del Estado de Hainan del MSS de China

APT40, también conocido como *BRONZE MOHAWK, FEVERDREAM, G0065, Gadolinium, GreenCrash, Hellsing, Kryptonite Panda, Leviathan, MUDCARP, Periscope, Temp.Periscope y Temp.Jumper*, se encuentra en Haikou, provincia de Hainan, República Popular de China (PRC), y ha estado activo desde al menos 2009. APT40 se ha dirigido a organizaciones gubernamentales, empresas y universidades en una amplia gama de industrias, incluida la investigación biomédica, robótica y marítima, en los Estados Unidos, Canadá, Europa, el Medio Oriente y el Área del Mar de China Meridional, así como industrias incluidas en la Iniciativa de la Franja y la Ruta de China.

https://us-cert.cisa.gov/ncas/alerts/aa21-200a

CIBERCONFIANZA

Alemania bloque Paginas WEB de Pornografía

En los últimos años, algunos países de Europa han intentadoe limitar el acceso de menores a páginas web pornográficas, se ha visto cómo Reino Unido ponía en marcha toda una regulación para ello, que acabó en saco roto. Alemania es la siguiente en intentarlo, en esta ocasión de forma bastante más agresiva
https://tech.slashdot.org/story/20/10/27/2238221/german-regulators-look-to-block-teens-from-porn-sites
https://www.dw.com/en/germany-cracks-down-on-child-porn-sites-but-critics-want-more-action/a-4126813
https://www.elespanol.com/omicrono/tecnologia/20210716/alemania-va-bloquear-paginas-porno-populares/596940949_0.html

Informes Semanales

En esta área hemos incorporado los informes semanales que proporciona la CISA (*Cybersecurity & Infrastructure Security Agency*) de los EEUU, estos boletines proporcionan un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad (NVD) del Instituto Nacional de Estándares y Tecnología (NIST)

Semana del 5 de julio:	https://us-cert.cisa.gov/ncas/bulletins/sb21-193
Semana del 12 de julio:	https://us-cert.cisa.gov/ncas/bulletins/sb21-200
Semana del 19 de Julio:	https://us-cert.cisa.gov/ncas/bulletins/sb21-207
Semana del 26 de Julio:	https://us-cert.cisa.gov/ncas/bulletins/sb21-214

Preparando la vuelta al Cole

En el artículo que nos ocupa, dirigido a la educación familiar, debemos abstraernos sobre los pilares formativos en ciberseguridad que aplicaríamos a futuros profesionales. En este caso interesa aprender, como mínimo, qué recursos tenemos disponibles para afrontar el reto de iniciarnos en ciberseguridad como padres, y, además, hacerlo con relativo poco esfuerzo, en los escasos huecos que tenemos.

https://unaaldia.hispasec.com/2021/07/preparando-la-vuelta-al-cole-asignatura-pendiente-ciberseguridad.html

CIBERFORENSIA

Microsoft publica parches para 117 vulnerabilidades, 8 de ellas de día cero

Microsoft publicó su esperado martes de parches, en esta ocasión con actualizaciones de seguridad para ciento diecisiete vulnerabilidades, incluidas ocho de día cero que están siendo explotadas actualmente. Entre estas vulnerabilidades, **trece se han clasificado como críticas** y **ciento tres como importantes** por su gravedad e impacto, **seis de los fallos ya se conocían públicamente en el momento del lanzamiento del parch**e. Cuatro de estas vulnerabilidades de día cero reportadas **están siendo explotadas activamente**.

https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul

https://windowsreport.com/patch-tuesday-july-2021/

https://unaaldia.hispasec.com/2021/07/microsoft-publica-parches-para-117-vulnerabilidades-8-de-ellas-de-dia-cero.html

CIBERDELITO

Facebook contra los Hackers

Facebook ha eliminado hasta 200 cuentas falsas que pertenecían a una campaña iraní de espionaje. Los ciberdelincuentes tenían como objetivo perfiles militares de Estados Unidos y Europa, después de haber pasado un año centrados en otro objetivos de Medio Oriente, ellos emplearon las redes sociales para acercarse a sus víctimas y ganarse su confianza con la intención de dirigirles a webs fraudulentas desde las que descargar el malware con el que controlar sus dispositivos en remoto.

https://edition.cnn.com/2021/07/15/tech/facebook-iran-hackers/index.html

https://www.reuters.com/technology/facebook-says-iran-based-hackers-used-site-target-us-military-personnel-2021-07-15/

https://www.nbcnews.com/tech/tech-news/facebook-says-iranian-hackers-used-lure-defense-company-employees-rcna1433

https://www.elespanol.com/omicrono/tecnologia/20210716/facebook-paro-campana-hackers-iranies-militares-eeuu/596940686_0.html

NOVEDADES

PARA TENER EN CUENTA

Los ciberataques aumentan un 300% debido al teletrabajo

https://revistabyte.es/ciberseguridad/los-ciberataques-teletrabajo/

TELEFÓNICA ADJUDICA A ERICSSON Y A NOKIA LA INFRAESTRUCTURA DE SU RED 5G EN ESPAÑA

Telefónica ha adjudicado la radio de su red 5G SA (*Stand Alone*) en España a los proveedores Ericsson y Nokia en un porcentaje del 50% a cada uno hasta el año 2026.

El despliegue de Nokia y Ericsson se realizará sobre las bandas de 3,5 GHz y de 700 MHz, dedicando la primera a altas prestaciones y capacidad y la segunda, cuya subasta comenzará antes del 21 de julio, para dar continuidad a la cobertura 5G.

https://revistabyte.es/actualidad-it/telefonica-5g-en-espana/https://www2.deloitte.com/us/en/pages/public-sector/articles/cybersecurity-capture-the-flag-training.html

CURSO DE HOMOLOGACIÓN DE COMPETENCIAS EN CIBERDEFENSA

El Jefe del Estado Mayor Conjunto de las Fuerzas Armadas, General de División Juan Martín Paleo, junto al Secretario de Estrategia y Asuntos Militares, Sergio Rossi, el Secretario de Ciberdefensa, Oscar Niss y el Comandante Conjunto de Ciberdefensa, General de Brigada Aníbal Luis Intini, participaron de la ceremonia de inicio del ciclo lectivo del **Instituto de Ciberdefensa de las Fuerzas Armadas** en el Aula Magna de la Escuela Superior de Guerra Conjunta.

El mismo brindará el primer curso Conjunto de Homologación de competencias en Ciberdefensa impartido por el instituto que tiene como objetivo principal, el perfeccionamiento Conjunto del personal militar y civil específico del área.

https://www.fuerzas-armadas.mil.ar/Noticia-2021-08-13-curso-homologacion-ciberdefensa.aspx