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° 32
Marzo 2021

OAC Boletín de Marzo 2021

"Durante el desarrollo dinámico de la cultura moderna, que se basa en el desarrollo explosivo de la tecnología moderna, nos enfrentamos cada vez más con el hecho de la cooperación multidisciplinaria ".

E. Shulman en …la era de la ciencia y el futuro de la humanidad.

Tabla de Contenidos

El Observatorio 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 la **Antena Territorial de Defensa y Seguridad** de la Secretaría de Ciencia y Tecnología de la Nación y es administrado por el **Centro de Estudios de Prospectiva Tecnológica Militar "Gral. 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

ESTRATEGIA

La ciberseguridad se vuelve holística

En este artículo de Robert K. Ackerman (Periodista y Editor en Jefe de la revista Signal durante 20 años), analiza y reflexiona sobre las palabras del General de Brigada Matteo Martemucci, USAF, J-2 para el Comando Cibernético de los Estados Unidos. El citado Jefe dice "Existe absolutamente un papel para que los ciudadanos privados y las corporaciones se asocien con un enfoque de toda la nación". Se debería explorar si los papeles jugados en la defensa cibernética permanecen como están o cambian.

Pero el debate es necesario para evitar una brecha de expectativas donde el público en general piensa incorrectamente que los militares defenderán todos los aspectos del ciberespacio.

https://www.afcea.org/content/cybersecurity-turns-holistic?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=9BiR7#

CIBERSEGURIDAD

DARPA espera proteger la internet de las cosas en 5G

El programa, conocido como OPS-5G desarrollado por la Agencia del Proyecto de Investigación Avanzada de Defensa (DARPA), permitirá que la tecnología segura de código abierto prolifere a medida que las tecnologías de la llamada Internet de las cosas se vuelvan más omnipresentes. Para ello está desarrollando una pila de red portátil que cumple con los estándares para comunicaciones móviles de quinta generación (5G) que es de código abierto y seguro por diseño, el programa busca crear software y sistemas de código abierto que permitan 5G seguro y redes móviles posteriores como 6G.

https://www.afcea.org/content/darpa-hopes-mobile-carrier-will-adopt-secure-5g?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=8BiR7#

CIBERDEFENSA

Documento de Interés

Informe Anual del sector de las TIC, los medios y los servicios audiovisuales 2020

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) ha elaborado la edición en 2020 del informe anual del sector de las TIC en España, los medios y servicios audiovisuales. El informe muestra las principales características estructurales del sector, su desarrollo en 2019 y su evolución en los últimos 6 años. Para ello analiza diversos indicadores clave como el número de empresas que lo componen, la cifra de negocio y el empleo generado, así como las inversiones realizadas. Estos indicadores clave se complementan con otros de carácter económico como el valor añadido que genera el sector, el comercio exterior, la inversión extranjera directa en el sector y la inversión realizada por empresas españolas del sector en el extranjero.

https://www.ontsi.red.es/index.php/es/estudios-e-informes/informe-anual-del-sector-tic-2020?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-e366821fe56e46d1af72eb1ec4f2af48&esid=f1c5df16-597b-eb11-a812-000d3abf9124

CIBERGUERRA

El fenómeno de las operaciones de influencia

La mayor parte de la atención relacionada con las tecnologías digitales y los conflictos se ha centrado en las operaciones cibernéticas o de información entre estados, las operaciones de influencia en el contexto de los conflictos interestatales. Sin embargo, son los conflictos civiles los que han aumentado en número y se han prolongado durante la última década debido a una serie de factores, incluido su carácter cada vez más internacionalizado.

https://www.iss.europa.eu/content/digital-technologies-and-civil-conflicts?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-e366821fe56e46d1af72eb1ec4f2af48&esid=f1c5df16-597b-eb11-a812-000d3abf9124

CIBERCONFIANZA

El navegador Brave expone el historial en TOR

El navegador Brave incorpora una función de navegación privada a través de la red Tor, permitiendo a los usuarios acceder a sitios de la dark-web (dominios .onion), así como navegar por la web normal ocultando la dirección IP pública. Debido a un bug en la implementación del filtrado de publicidad, las peticiones DNS realizadas por el navegador, incluyendo las nativas de la red Tor (.onion), eran enviadas a los

servidores DNS configurados en el equipo. Es decir, tanto el proveedor de acceso a Internet como los gestores de los servidores DNS, podían detectar la visita de sitios de la dark-web.

https://thehackernews.com/2021/02/privacy-bug-in-brave-browser-exposes.html

Google ha reforzado su seguridad

Anunciada este 2 de marzo, la nueva actualización de Google Chrome viene con 47 parches de seguridad, la mayoría de ellos relacionados con un problema en el ciclo de vida de los objetos de audio.

https://unaaldia.hispasec.com/2021/03/nuevo-0-day-en-google-chrome.html

CIBERFORENSIA

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 de 15 de febrero: https://us-cert.cisa.gov/ncas/bulletins/sb21-053

Semana de 22 de febrero: https://us-cert.cisa.gov/ncas/bulletins/sb21-060

Informe Análisis de Malware:

1. https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048f (AppleJeus: Dorusio)
2. https://us-cert.cisa.gov/ncas/alerts/aa21-042a (Compromiso de la planta de tratamiento de agua)

CIBERDELITO

El Haker Hakeado

Maza, originalmente conocido como Mazafaka, es una comunidad de hacking elitista de habla rusa a la que sólo se podía acceder mediante enlace de invitación, hecho que no impidió a unos atacantes desconocidos acceder por otras vías, obteniendo en el proceso los datos de sus usuarios y realizando un ataque de tipo *'defacement'* al portal del sitio web.

https://www.flashpoint-intel.com/blog/breelite-cybercrime-forum-maza-breached-by-unknown-attacker/

Empresa de ciberseguridad afirma que hackers chinos atacaron instituto sérico, Bharat Biotech

El Ministerio de Relaciones Exteriores de China desestimó las acusaciones, describiendo las acusaciones de Cyfirmia como "especulaciones infundadas".

China rechazó el martes una acusación de una firma de inteligencia cibernética de que un grupo de hackers respaldado por el Estado se dirigió a los sistemas informáticos de dos fabricantes indios de vacunas contra el coronavirus.

Cyfirma dijo a Reuters que el grupo de hackers APT10, conocido como Stone Panda, había identificado lagunas y vulnerabilidades en la infraestructura de TI y el software de la cadena de suministro de Bharat Biotech y el Instituto Sérico de la India (SII), el mayor fabricante de vacunas del mundo.

"Sin mostrar ninguna evidencia, la parte pertinente hizo especulaciones infundadas, datos distorsionados y inventados, para desacreditar a una parte específica", dijo el ministerio de Relaciones Exteriores de China a Reuters.

"Este comportamiento es irresponsable y tiene un motivo oculto. China se opone firmemente", agregó en una respuesta escrita a las preguntas sobre las acusaciones de Cyfirma.

Cybersecurity Firm Claims Chinese Hackers Targeted Serum Institute, Bharat Biotech (thewire.in)

"Flotan "en internet 180.000 archivos de PEMEX sustraídos por delincuentes informáticos

Entre los documentos sustraídos mediante ataques cibernéticos hay información altamente sensible como manuales de operación vía remota de la refinería de Tula, listas de usuarios de trabajadores y contraseñas, revela una investigación de ONEA México.

https://www.eleconomista.com.mx/empresas/Flota-en-internet-informacion-sensible-de-Pemex-sustraida-por-hackers-20210216-0103.html