OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya

ISSN: en trámite
http://www.esgcffaa.edu.ar/obsciber/

AÑO 3 N° 21
Marzo 2020

OAC Boletín de Marzo 2020

"En vano los hombres se empeñan en arrastrar a su opinión a los demás, cuando ella no está cimentada en la razón."

Manuel Belgrano

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 “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

ESTRATEGIA

Manipulación de Tecnología con fines de Inteligencia

Un dossier de servicio secreto de 280 páginas de la CIA y el Servicio Federal de Inteligencia (BND) de Alemania demuestra cómo durante décadas, ha habido espionaje a través de dispositivos de cifrado manipulados de la compañía suiza Crypto AG. Un dispositivo que posee más de 100 países usuarios de la compañía con sede en Zug, que bajo la apariencia de neutralidad suiza pertenecía a la CIA y al BND.

https://www.swissinfo.ch/eng/politics/crypto-spying-affair_how-manipulated-swiss-tech-shaped-world-politics/45554828

https://www.bbc.com/news/world-europe-51487856

http://periodicoeltiempo.mx/suiza-investiga-espionaje-de-la-cia-a-120-paises-a-traves-de-la-empresa-crypto-ag/

CIBERSEGURIDAD

Un modelo seguro para Internet de las cosas Industriales (IIoT)

La seguridad del modelo Purdue fue una separación OT-IT (Operation Technology e Information Technology) que divide a la estructura de la empresa en capas o niveles, cada una haciendo lo propio y enviando datos a la capa siguiente. Esta división es en función de las necesidades corporativas, pero también de los controles de seguridad básicos y cerrados que tradicionalmente se han utilizado para mantener los sistemas OT separados y seguros de las redes más expuestas o no confiables (incluido

Internet). Pero en el IIoT, la separación OT-IT ya no es válida, y la conectividad a Internet y a la nube son elementos básicos.

https://owlcyberdefense.com/blog/a-new-model-for-secure-iiot-connectivity/

https://oasys-sw.com/diferencias-entre-it-y-ot/ (acerca de las diferencias entre OT e IT)

CIBERDEFENSA

EE.UU. ante la amenaza cibernética de sus posibles adversarios

Estados Unidos está lamentablemente mal preparado para proteger el ciberespacio contra los peores escenarios que amenazan al país, dice el ex comandante supremo aliado de la OTAN. El almirante James Stavridis, USN (Ret.), Ejecutivo operativo del Grupo Carlyle, advierte que las soluciones a largo plazo deben combinarse con acciones a corto plazo para evitar que una serie de amenazas cibernéticas paralicen a los Estados Unidos militar y económicamente

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#

CIBERGUERRA

Los funcionarios estadounidenses están repensando cómo disuadir los ataques cibernéticos

QUINTO DOMINIO- En una demostración coordinada de fuerza el mes de febrero de 2020, el Departamento de Estado y el Departamento de Defensa de los Estados Unidos se unieron a más de otras 20 naciones para atribuir y condenar el ataque cibernético de 2019 a Georgia por parte del área de inteligencia militar de Rusia.
Durante la citada reunión se sentaron distintas opiniones respecto de conceptos de CIBERDISUACIÓN.

https://www.fifthdomain.com/show-reporters/rsa/2020/03/06/whats-the-next-step-us-officials-are-rethinking-how-to-dissuade-cyberattacks/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2003.09.20&utm_term=Editorial%20-%20Early%20Bird%20Brief

CIBERCONFIANZA

Las políticas públicas en la era digital pueden y deben basarse en datos

La limitada disponibilidad de datos cuantitativos responde, por un lado, a la relativa inmadurez del sector para conocer la relación entre inversiones e impacto y elaborar métricas que permitan evaluar la progresión hacia los objetivos que se señalan".

Según expresa Félix Arteaga (investigador principal de Seguridad y Defensa del Real Instituto Elcano):

"Las políticas públicas en la era digital pueden y deben basarse en datos."

http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-ciberseguridad-espana-pasar-de-filosofia-a-matematicas?utm_source=CIBERelcano&utm_medium=email&utm_campaign=53-marzo2020&_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-40393088398848ee9d29da118acc3516&esid=67ecd0fc-6168-ea11-a811-000d3a44a2a9

CIBERFORENSIA

Vulnerabilidades detectadas en los EE.UU. Alerta (AA20-049A)

La Agencia de Seguridad, Ciberseguridad e Infraestructura (CISA) respondió a un ataque cibernético que afecta los activos de control y comunicación en la red de tecnología operativa (OT) de una instalación de compresión de gas natural

https://www.us-cert.gov/ncas/alerts/aa20-049a

«Vicious Panda»: una campaña de malware que utiliza el Coronavirus como vector de infección

Cada vez que existe una noticia de interés mundial, esta es usada por los ciberdelincuentes como cebo para inducir a sus víctimas a clickar en los enlaces que sirven como vectores de infección del malware. En este caso, como ya podéis deducir, el cebo ha sido Coronavirus

https://unaaldia.hispasec.com/2020/03/vicious-panda-una-campana-de-malware-que-utiliza-el-coronavirus-como-vector-de-infeccion.html

Troyano en Tor Browser: compradores en la Darknet ven cómo sus bitcoins son robados

Mediante el uso de una versión de Tor Browser infectada por un troyano, los cibercriminales detrás de esta campaña han tenido bastante éxito – hasta el momento sus cuentas de pastebin.com han tenido más de 500.000 visitas y **han podido robar más de US$40.000 en bitcoins**.

https://unaaldia.hispasec.com/2019/10/troyano-en-tor-browser-compradores-en-la-darknet-ven-como-sus-bitcoins-son-robados.html

CIBERDELITO

El Departamento de Justicia de EE. UU. anunció cargos contra cuatro piratas informáticos chinos

El Departamento de Justicia de EE. UU. Anunció cargos contra cuatro piratas informáticos chinos respaldados por el ejército en relación con la realización del ataque cibernético de 2017 contra Equifax, una agencia de informes de crédito al consumo. La intrusión condujo al mayor robo conocido de información de identificación personal jamás realizado por actores patrocinados por el estado.

https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

Documentos de Interés

Perspectivas de la Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA)

El presente es un informe y recomendaciones sobre el brote de rasomware en los próximos años elaborado por La Agencia de Seguridad, Ciberseguridad e Infraestructura (CISA)

https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf

Sesgo y percepción errónea en el ciberespacio por Miguel Alberto Gómez. ARI 25/2020 - 17/3 /

La necesidad de educar mejor a las élites no es una idea nueva, pero requiere mayor esfuerzo por la falta de experiencia en este ambiente sobre el uso de operaciones cibernéticas como un instrumento de política exterior debiera evitar disputas innecesarias que surgen por la percepción errónea y la visión sesgada

https://eur04.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.realinstitutoelcano.org%2Fwps%2Fportal%2Frielcano_en%2Fcontenido%3FWCM_GLOBAL_CONTEXT%3D%2Felcano%2Felcano_in%2Fzonas_in%2Fari25-2020-gomez-bias-and-misperception-in-cyberspace%3Futm_source%3DCIBERelcano%26utm_medium%3Demail%26utm_campaign%3D53-marzo2020%26_cldee%3DYW1vcmVzaTUxQGdtYWlsLmNvbQ%253d%253d%26recipientid%3Dcontact-a5e4c470e59de911a97d000d3a233b72-40393088398848ee9d29da118acc3516%26esid%3D67ecd0fc-6168-ea11-a811-000d3a44a2a9&data=02%7C01%7C%7C7b79d96516294ce29ee108d7cb41a4bc%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637201355097885911&sdata=8DtgFmpmUUYfIZGLOpdh1Ofnm%2BnwBid13EZW6WzVIjM%3D&reserved=0

Ciberseguridad en 5G Riesgos en su Gerenciamiento

James Sullivan y Rebecca Lucas

La principal prioridad política para los estados debería ser la implementación de medidas técnicas pragmáticas de gestión del riesgo cibernético que se protejan contra la mayoría de los riesgos para las redes 5G. En enero de 2020, el Consejo de Seguridad Nacional del Reino Unido tomó la decisión de excluir la tecnología Huawei de las partes más sensibles de la red 5G del Reino Unido, al tiempo que le permitía suministrar componentes periféricos como mástiles de teléfonos móviles y antenas. Desde una

perspectiva puramente técnica, esta fue una decisión práctica y realista que se adhiere a los principios de la gestión del riesgo cibernético y refleja la opinión experta del Centro Nacional de Seguridad Cibernética, autoridad técnica nacional del Reino Unido,.

https://rusi.org/sites/default/files/20200602_5g_cyber_security_final_web_copy.pdf?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-40393088398848ee9d29da118acc3516&esid=67ecd0fc-6168-ea11-a811-000d3a44a2a9

NOVEDADES

Competencias "Capture Flag"

El desafío de la captura cibernética de la bandera (CTF) está diseñado para ayudar a mejorar las habilidades de seguridad cibernética y proporcionar oportunidades prácticas de aprendizaje y creación de redes para los participantes. La dificultad de los desafíos se puede modificar para varios escenarios, desde ciencia, tecnología, ingeniería y matemáticas. Los desafíos ofrecen una oportunidad única de aprendizaje y capacitación en un ambiente divertido y competitivo.

https://www2.deloitte.com/us/en/pages/public-sector/articles/cybersecurity-capture-the-flag-training.html