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 2 N° 18
Noviembre 2019

OAC Boletín de Noviembre 2019

"LA PRÓXIMA GUERRA MUNDIAL SE LLEVARÁ A CABO CON PIEDRAS"

Albert Einstein

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

Resolución 1380/2019 Redefine conceptos de Ciberdefensa

El MinDef ha publicado esta resolución, mediante la cual se llevan adelante varias acciones relacionadas con el campo de la estrategia en ciberdefensa, entre ellas: (1) Redefine el concepto de ciberdefensa, (2) crea Centro de Respuesta ante Emergencias Informáticas (CSIRT de DEFENSA), Centro Inteligente de Operaciones de Seguridad (iSOC) y el Laboratorio de Análisis Cibernético (CyberLab). (3) define las cuatro líneas de acción en ciberdefensa y los 3 ejes políticos de acción (4) crea un comité consultivo en la materia. Como novedad interesante, la defensa se puso los pantalones largos y la resolución posee anexos caracterizado como secretos

https://www.boletinoficial.gob.ar/detalleAviso/primera/219968/20191029

Alemania crea su Comando de Ciberdefensa e Información

Con la creación del Comando de Ciberdefensa e Información (CIR), especializado en seguridad cibernética, el Ejército de Alemania procura blindar sus sistemas de información y proteger al país contra el creciente número de ataques digitales extranjeros.

https://www.dw.com/es/ciberdefensa-el-bundeswehr-y-sus-desaf%C3%ADos/a-44989489

CIBERSEGURIDAD

Malware para interceptar tráfico SMS de suscriptores Internacionales

Los investigadores han descubierto un nuevo malware para espionaje utilizado por el grupo relacionado con APT41. **El malware intercepta el tráfico del servidor SMS de telecomunicaciones y detecta ciertos números de teléfono y mensajes SMS**, especialmente aquellos con palabras clave relacionadas con disidentes políticos chinos.

https://threatpost.com/china-hackers-spy-texts-messagetap-malware/149761/

INFOBAE cuenta como se ha robado datos de las FFSS

Infobae a través de Federico Fahsbender presenta una nota que guarda relación con el pirata informático Argentino y el ataque de Julio de 2019 a las FFSS de nuestro país

https://www.infobae.com/sociedad/policiales/2019/10/31/la-gorra-leaks-como-es-el-insolito-y-sencillo-truco-que-uso-un-hacker-para-robar-los-datos-privados-de-la-policia-federal/

CIBERDEFENSA

Documento de Interés

Presentación del libro de Mariano Oscar Gomez "En busca de un modelo de resiliencia cibernética basado en las experiencias de la OTAN y su posible transferencia a América del Sur

El autor presenta un trabajo de investigación basado en gran cantidad de fuentes bibliográficas, normativas y tratados que conforman una muy completa descripción del estado del arte motivo del estudio. Sintetizando el trabajo, el autor plantea una interesante metodología de análisis de riesgo y una serie de interrogantes a tener en cuenta para la aplicación práctica de la teoría en el contexto de la transferencia de políticas de la OTAN a América del Sur

www.cefadigital.edu.ar/bitstream/1847939/1299/1/Resiliencia%20Cibernética%20-%20Mariano%20Gomez%20-%20PDF.pdf

Interesante trabajo presentado por el Real Instituto Elcano (autor Félix Arteaga) donde se plantea a la disuasión como alternativa defensiva en el ciberespacio.

La protección del ciberespacio se ha volcado en medidas defensivas para proteger las infraestructuras críticas de los países o los despliegues de sus fuerzas en teatros de operaciones. De las primeras se han venido ocupando las Administraciones Públicas y el sector privado corresponsables de la ciberseguridad, mientras que de las segundas se han encargado los mandos y fuerzas de ciberdefensa.

www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari92-2019-arteaga-capacidades-ofensivas-disuasion-y-ciberdefensa

CIBERGUERRA

Como la IoT y los multidominios impactan en la estrategia de Guerra

Expertos explican como a medida que aumenta el número de dispositivos electrónicos conectados a Internet, también lo hace el riesgo de seguridad y la posibilidad de que los adversarios extraigan datos. El uso de dispositivos de Internet de las cosas por parte de los ciberatacantes hace que los militares sean cada vez más vulnerables

https://www.afcea.org/content/internet-things-invasion?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email#

Las operaciones multidominio, prevén que las guerras futuras se ejecuten extremadamente rápido e incorporen una gran cantidad de automatización y redes para conectar sensores a los participantes en todos

los dominios: terrestre, aéreo, marítimo, espacial y cibernético. Esta estrategia da origen a las Operaciones Multidominio (MDO) que se basan en un grado de sincronización sin precedentes entre los servicios armados y los aliados de la coalición.

https://www.afcea.org/content/incoming-multidomain-operations-and-what-innovation-means-future-warfare?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email#

CIBERCONFIANZA

Facebook, sigue con problemas de filtración de datos después del caso Cambridge Analítica

Como parte de nuestra revisión en curso, recientemente descubrimos que algunas aplicaciones retuvieron el acceso a la información de los miembros del grupo, como nombres e imágenes de perfil en relación con la actividad del grupo, desde la API de Grupos, durante más tiempo del que pretendíamos. Desde entonces hemos eliminado su acceso. Hoy también estamos llegando a aproximadamente 100 socios que pueden haber accedido a esta información desde que anunciamos restricciones a la API de Grupos

https://developers.facebook.com/blog/post/2019/11/05/changes-groups-api-access/

El portero eléctrico con video de Amazon, permite a los atacantes robar la vclave de Wi-Fi

Los investigadores de seguridad de Bitdefender han descubierto una vulnerabilidad de seguridad de alta gravedad en los dispositivos Ring Video Doorbell Pro de Amazon que podría permitir a los atacantes cercanos robar su contraseña de WiFi y lanzar una variedad de ataques cibernéticos usando MitM contra otros dispositivos conectados a la misma red.

https://thehackernews.com/2019/11/ring-doorbell-wifi-password.html

Usan Citaciones Judiciales para robar información

Descubiertos por investigadores de la compañía de seguridad cibernética Cofense , los correos electrónicos de phishing tienen el tema 'Corte' y presentan logotipos del Ministerio de Justicia del Reino Unido . Afirman proporcionar información sobre 'Su Citación' y le piden a la víctima que haga clic en un enlace porque se les ordenó asistir a un tribunal de justicia y tienen 14 días para cumplir. No hay información sobre lo que supuestamente se relaciona con el caso judicial.

https://www.zdnet.com/article/phishing-campaign-delivers-data-stealing-malware-via-fake-court-summons-emails/

CIBERFORENSIA

Un exploits que puede complicar a algunos servidores

Si está ejecutando un sitio web basado en PHP en el servidor NGINX y tiene habilitada la función PHP-FPM para un mejor rendimiento, tenga cuidado con una vulnerabilidad recientemente revelada que podría permitir que atacantes no autorizados pirateen su servidor de sitio web de forma remota.
Esta vulnerabilidad (CVE-2019-11043) es una ejecución de código remoto en PHP7, la nueva rama en producción de PHP, uno de los lenguajes de programación más extendidos para sitios web, permite tomar

el control del servidor vulnerable ejecutando código remoto. El exploit publicado convierte esta hazaña en algo trivial, por lo que es muy posible que esté siendo aprovechada por atacantes

https://thehackernews.com/2019/10/nginx-php-fpm-hacking.html

CIBERTERRORISMO

La Diputación de Gipuzkoa ha puesto en marcha Ziur, el Centro de Ciberseguridad de Gipuzkoa

Asistimos a una muy interesante entrevista a su presidente Carlos Abad.

https://www.eitb.eus/es/radio/radio-euskadi/programas/cronica-fin-de-semana/detalle/6822130/reportaje-ziur-centro-ciberseguridad-gipuzkoa-noviembre-2019/

El futuro de la protesta está en las TICs

El empleo de las TICs, se ha convertido en una manera de congregar a protestas masivas, el año pasado, los escolares de todo el mundo se unieron a las huelgas de los Viernes para el Futuro , presenciando huelgas masivas de escuelas de todo el mundo. En Chile, las protestas coordinadas para evasión de tarifas en el transporte público, también dirigidas por alumnos escolares, ahora se han convertido en disturbios masivos contra el creciente costo de la vida. Durante las últimas dos semanas, las protestas han estallado en todo el Líbano en oposición al aumento de los impuestos, que involucran bloqueos de carreteras y una cadena humana en todo el país para ilustrar la unidad de la gente.

http://theconversation.com/the-future-of-protest-is-high-tech-just-look-at-the-catalan-independence-movement-125776

NOVEDADES

WEBINAR ¿Cómo enfrentar este nuevo dominio militar?

Los videos completos de la WEBINAR, pueden se visitados en las siguientes direcciones de Youtbe:

1. **Nivel Táctico**: https://www.youtube.com/watch?v=e554iMxXeOw&feature=youtu.be
2. **Nivel Operacional**: https://www.youtube.com/watch?v=AHMMHuiqqqY&feature=youtu.be
3. **Nivel Estratégico**: https://www.youtube.com/watch?v=g2RkcPKb0NM&feature=youtu.be
4. **Conclusiones**: https://www.youtube.com/watch?v=C0orDR8mpXc&feature=youtu.be