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° 35
Junio 2021

OAC Boletín de Junio 2021

"Occidente necesita aprender a luchar en las sombras sin perder su alma, o seguirá siendo golpeado por las autocracias"

Sean Mc Fate
Las nuevas reglas de Guerra Victoria en la era del desorden permanente (Pag 165)

Tabla de Contenidos

ESTRATEGIA 2
¿Debería EEUU firmar un acuerdo "sin espías" con Alemania y otros socios de la UE? 2
Estados Unidos y Reino Unido acuerdan colaborar en 6G 3
CIBERSEGURIDAD 3
Ciberincidentes importantes de 2006 a mayo de 2021 (informe del CSIS) 3
La ciberseguridad de la cadena de suministro en defensa y ante la adopción del multidominio 3
CIBERDEFENSA 3
La revista de ciberdefensa 3
CIBERGUERRA 4
Se necesita un enfoque complejo para ganar la Ciberguerra 4
Northrop entrega el 1er bloque SEWIP 3 Jammer a la Marina 4
CIBERCONFIANZA 4
Informes Semanales 4
Parche de seguridad para Adobe 5
CIBERFORENSIA 5
Las agencias de inteligencia de EEUU advierten sobre las debilidades de la red 5G 5
Puntos débiles de la tecnología 5G 5
CIBERDELITO 5

Vulnerabilidad permite el seguimiento del usuario entre la mayoría de navegadores 5

NOVEDADES 6

Telefónica se une a un consorcio español de IA 6

El **Observatorio Argentino del Ciberespacio** (**OAC**), **micro-sitio de la Escuela Superior de Guerra Conjunta de la Facultad Militar 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

Hemos incluido a partir del número de marzo de este año, la sección NOTICIAS, una serie de posibilidades de participación en webinars y seminarios, especialmente destinados a la actualización sobre 5G.

ESTRATEGIA

¿Debería Estados Unidos firmar un acuerdo "sin espías" con Alemania y otros socios de la UE?

El autor del artículo *James Andrew Lewis es vicepresidente senior y director del Programa de Tecnologías Estratégicas en el Centro de Estudios Estratégicos e Internacionales en Washington, DC.*

La tecnología digital puede ser un punto focal para reconstruir la relación transatlántica, pero hay problemas difíciles de abordar relacionados con los flujos de datos, el contenido digital, la competitividad, los impuestos y la privacidad. Un elemento central de estos problemas es la creencia generalizada en Europa de que Estados Unidos realiza una vigilancia masiva contra sus ciudadanos. Las revelaciones de Snowden (y la respuesta moderada de Estados Unidos a ellas) ayudaron a motivar a Europa a propiciar la "soberanía digital" y reducir la dependencia de la tecnología estadounidense y las plataformas en línea.

Mientras que una Europa económicamente fuerte sigue siendo lo mejor para los intereses de Estados Unidos, la soberanía digital europea no. Las acusaciones de vigilancia estadounidense obstaculizan la capacidad de Estados Unidos para avanzar en temas como la privacidad y el comercio digital. Muchos europeos creen que EE. UU. Toman acciones que violan sus derechos de privacidad al exponerlos a una vigilancia masiva e indiscriminada, acusación que impulsa las disputas observadas en el caso Max Schrems (NOYB – Centro Europeo de Derechos Digitales) , cuyo resultado ha sido invalidar acuerdos entre Estados Unidos y Europa que permiten el flujo de datos transatlánticos.

https://www.csis.org/analysis/should-united-states-enter-no-spy-agreement-germany-and-other-eu-partners

Estados Unidos y Reino Unido acuerdan colaborar en 6G

El acuerdo se ha anunciado en el curso de la visita al Reino Unido de Joe Biden, presidente de Estados Unidos, con motivo de la cumbre anual del G7. Plantean concentrarse en áreas tales como la solidez y seguridad de cadenas de suministros claves, las tecnologías de baterías y la IA, y el trabajo para mejorar la accesibilidad y el flujo de datos como apoyo al crecimiento económico, la seguridad y el progreso científico y tecnológico. Los implicados en el sector prevén que el lanzamiento comercial de la 6G tendrá lugar en 2030.

https://www.mobileworldlive.com/spanish/estados-unidos-y-reino-unido-acuerdan-colaborar-en-6g?ID=a6g69000000lk9LAAQ&JobID=785429&utm_source=sfmc&utm_medium=email&utm_campaign=MWL_ES_20210616&utm_content=https%3a%2f%2fwww.mobileworldlive.com%2fspanish%2festados-unidos-y-reino-unido-acuerdan-colaborar-en-6g

CIBERSEGURIDAD

Ciberincidentes importantes de 2006 a mayo de 2021

Interesante documento publicado por el CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, el mismo resume práticamente todos y cada uno de los ciberataques ocurridos en este período.

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

La ciberseguridad de la cadena de suministro en defensa y ante la adopción del multidominio

Un ataque TI clásico a un proveedor (fallo en la ciberseguridad de la industria) se puede convertir en una ventaja táctica muy relevante en el campo de batalla, y ser utilizado por una potencia enemiga. En este sentido, un buen ejemplo sería la captura de un dron RQ-170 norteamericano por parte de Irán en diciembre de 2011, en donde, la teoría más extendida y aceptada se basa en el robo de las claves de autenticación del dron a uno de los proveedores de la cadena de suministro norteamericana.

https://www.thiber.org/wp-content/uploads/2021/05/Comentario.pdf

https://www.militaryaerospace.com/computers/article/16715072/iranus-rq170-incident-has-defense-industry-saying-never-again-to-unmanned-vehicle-hacking

CIBERDEFENSA

La revista de ciberdefensa

Cyber Defense Magazine (CDM), es una revista de seguridad de la información electrónica líder en la industria que trata acerca de las implicaciones internacionales para la ciberseguridad.

Durante la pandemia se han intensificado por los impactos ampliamente divergentes del COVID-19 y sus variantes en nuestras naciones y organizaciones internacionales. Cada vez más, vemos vectores en conflicto que nos empujan en diferentes direcciones a desafiar nuestra capacidad para mantener una coordinación saludable entre intereses nacionales y respuestas internacionales, incluso globales, a la disrupción de negocios y la llamada "nueva normalidad".

https://www.cyberdefensemagazine.com/newsletters/may-2021/CDM-CYBER-DEFENSE-eMAGAZINE-May-2021.pdf
https://www.cyberdefensemagazine.com/

CIBERGUERRA

Se necesita un enfoque complejo para ganar la Ciberguerra

El ciberataque masivo en los Estados Unidos a través del proveedor de tecnología de la información SolarWinds continúa enviando ondas de choque a través de los departamentos de Defensa, Estado y Seguridad Nacional, así como otras agencias. Las evaluaciones de daños están en curso. Si el gobierno de EE. UU. En general y el Departamento de Defensa en particular quieren defenderse con éxito de los ataques de enemigos bien financiados, pacientes y muy motivados, deberán cambiar su enfoque para defender sus redes y sistemas.

Desde sus incursiones modestas pero exitosas en este espacio en Estonia, Georgia y Ucrania a principios de la década de 2000, Rusia ha reforzado significativamente sus capacidades ofensivas, aumentando su personal y capacidades con operaciones cibernéticas realizadas por varias agencias de la comunidad rusa de defensa e inteligencia.

https://www.afcea.org/content/complex-approach-needed-win-cyber-wars?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=pIIVg1&_zl=Tp1c7#

Northrop entrega el 1er bloque SEWIP 3 Jammer a la Marina

Después de años de desarrollo, Northrop Grumman ha entregado oficialmente el primer modelo funcional completo del Bloque III del Programa de Mejora de Guerra Electrónica de Superficie (SEWIP) de la Armada para pruebas en tierra.

Dijo Bryan Clark, un comandante de la Marina retirado y experto en EW en el Hudson Institute. “Lo más importante es que podrá operar en un rango de frecuencia más amplio para contrarrestar nuevas amenazas de misiles y utilizar procesamiento digital que podría permitir nuevas técnicas de interferencia o engaño, incluidos los algoritmos cognitivos de la Guerra Electrónica, habilitados por la Inteligencia Artificial”.

https://breakingdefense.com/2021/06/northrop-delivers-1st-sewip-block-3-jammer-to-navy/

CIBERCONFIANZA

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 24 de mayo https://us-cert.cisa.gov/ncas/bulletins/sb21-151

Semana de 31 de mayo https://us-cert.cisa.gov/ncas/bulletins/sb21-158

Semana del 07 de junio https://us-cert.cisa.gov/ncas/bulletins/sb21-165

Semana del 14 de junio https://us-cert.cisa.gov/ncas/bulletins/sb21-172

Informe Cadena de suministro: Los temas de CISA para cada semana incluyen:

- Semana 1: Fortalecimiento de la resiliencia de la cadena de suministro colectiva
- Semana 2: Evaluación de la confiabilidad de las TIC
- Semana 3: Comprensión de las amenazas de la cadena de suministro
- Semana 4: Conociendo lo esencial

Parche de seguridad para Adobe

Adobe ha publicado actualizaciones de seguridad para Adobe Acrobat y Reader para Windows y macOS. Estas actualizaciones abordan múltiples vulnerabilidades críticas e importantes . La explotación exitosa podría conducir a la ejecución de código arbitrario en el contexto del usuario actual. Adobe ha recibido un informe de que CVE-2021-28550 ha sido explotado en forma salvaje en ataques limitados dirigidos a usuarios de Adobe Reader en Windows.

https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

CIBERFORENSIA

Las agencias de inteligencia de EE. UU. Advierten sobre las debilidades de la red 5G

La implementación inadecuada de los estándares de telecomunicaciones, las amenazas a la cadena de suministro y las debilidades en la arquitectura de los sistemas podrían plantear importantes riesgos de ciberseguridad para las redes 5G, lo que podría convertirlas en un objetivo lucrativo para que los ciberdelincuentes y los adversarios de los estados nacionales los exploten en busca de inteligencia valiosa.

https://thehackernews.com/2021/05/us-intelligence-agencies-warn-about-5g.html

Puntos débiles de la tecnología 5G

La NSA, junto a otras instituciones gubernamentales estadounidense, publicó un estudio sobre los principales riesgos y vulnerabilidades de las redes 5G.

Este nuevo estudio, publicado por la NSA, el DHS y la CISA, señala que los principales riesgos y vulnerabilidades se producen a consecuencia de:

- Las políticas y estándares que regulan la tecnología 5G.
- La cadena de abastecimiento.
- La arquitectura de los sistemas 5G.

https://unaaldia.hispasec.com/2021/05/puntos-debiles-de-la-tecnologia-5g.html

CIBERDELITO

Vulnerabilidad permite el seguimiento del usuario entre la mayoría de navegadores

El fallo permite identificar al usuario gracias al listado de aplicaciones instaladas en el equipo, creando una huella ineludible aunque se cambie de navegador, afectando a la mayoría de exploradores incluyendo Tor. Según han podido comprobar investigadores de FingerprintJS, la mayoría de los navegadores de

escritorio **permiten enumerar las aplicaciones instaladas en el sistema** que hacen uso de **urls personalizadas** en el navegador, como pueden ser *'slack:///'*, *'tg:///'*, etc. Esta huella puede utilizarse para **identificar al usuario aunque utilice otro navegador** u otras medidas de seguridad como pueden ser un proxy o una VPN.
https://fingerprintjs.com/blog/external-protocol-flooding/

NOVEDADES

WEBINARS Y SEMINARIOS

Telefónica se une a un consorcio español de IA

El operador se ha unido a Microsoft, la energética Repsol, la empresa Gestamp de ingeniería de automoción, la constructora naval Navantia y la ingeniería Tecnicas Reunidas para constituir el grupo IndesAI, que busca promover el uso de los datos y la IA entre las empresas industriales españolas.

https://www.mobileworldlive.com/spanish/telefonica-se-une-a-un-consorcio-espanol-de-ia?ID=a6g69000000lk9LAAQ&JobID=787083&utm_source=sfmc&utm_medium=email&utm_campaign=MWL_ES_20210618&utm_content=https%3a%2f%2fwww.mobileworldlive.com%2fspanish%2ftelefonica-se-une-a-un-consorcio-espanol-de-ia

Sitio web:
http://www.esgcffaa.edu.ar/esp/oac-boletines.php
Nuestra dirección postal es:
* | Luis María Campos 480 - CABA - República Argentina |
* Nuestro correo electrónico:
*|observatorioargentinodelciberespacio@conjunta.undef.edu.ar | *