OAC Boletín de octubre 2022

"Lección aprendida #2: Conozca el terreno político. La correspondencia pública estratégica, declaraciones, discursos, etc., pueden tener implicancias operacionales y tácticas para el Combatiente. Para evitar la sorpresa operacional, manténgase informado sobre ellos."

Percepciones son realidad
Brandon, Kitches y Yandura

Tabla de Contenidos

El **Observatorio Argentino del Ciberespacio** (**OAC**), **es un micro-sitio de la Escuela Superior de Guerra Conjunta, editado y publicado por el Instituto de Ciberdefensa de las Fuerzas Armadas**
URL: http://www.esgcffaa.edu.ar/esp/oac-boletines.php.
Esta publicación mensual se encuentra inserta en el **Nodo 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 ambiente operacional, aportando novedades reportes e informes que permitan a la comunidad educativa y a la sociedad en general conocer más acerca del mismo

ESTRATEGIA

El aumento del uso del ciberespacio como vector de ataque en conflictos

Un documento de interés escrito por Christian Dietrich y presentado por la IEEE, de España acerca de cómo el ciberespacio se ha convertido en un lugar común, determinante en cualquier conflicto bélico. Georgia en 2008 y toda la literatura referente a la guerra híbrida parecen hacer honor a esta argumentación. Así pues, ¿estamos ante un cambio de paradigma en el que el ciberespacio será el dominio más determinante en los conflictos actuales y futuros?. El documento ofrece una visión general de los diferentes vectores de ataque en el ciberespacio, la situación global de los ataques patrocinados por el Estado en la última década y los retos a los que se enfrentan atacantes y defensores en el ciberespacio.

https://www.ieee.es/publicaciones-new/documentos-de-opinion/2022/DIEEEO83_2022_CHRDIE_Ciberespacio.html

CIBERSEGURIDAD

La seguridad de los datos en las Operaciones Cibernéticas

El artículo de George Jueves da una mirada de cerca a los enclaves de la Doctrina de Operaciones Ciberespaciales (DCO), que se adjunta en el presente Boletín y cómo las organizaciones pueden apoyar sus misiones de DCO garantizando el intercambio seguro de información a través de redes de lado alto (clasificado) y lado bajo (no clasificado).
https://www.c4isrnet.com/cyber/2022/09/26/defensive-cyber-operation-enclaves-can-support-secure-sharing-of-data/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch
Cyberspace Operations
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-06-19-092120-930

CIBERDEFENSA

Software de código abierto como arma

Un grupo con vínculos con Corea del Norte ha estado desarrollando software de código abierto en sus campañas de ingeniería social dirigidas a empresas de todo el mundo desde junio de 2022.
Los equipos de inteligencia de amenazas de Microsoft, junto con LinkedIn Threat Prevention and Defense, atribuyeron las intrusiones a Zinc, un grupo de amenazas aliado a Lazarus que también se lo encuentra bajo el nombre de Labyrinth Chollima.
Los ataques se dirigieron a empleados de organizaciones de múltiples industrias, incluidos los medios de comunicación, la defensa y la industria aeroespacial, y los servicios de TI en los Estados Unidos, el Reino Unido, la India y Rusia.
https://thehackernews.com/2022/09/north-korean-hackers-weaponizing-open.html

https://www.ciberseguridadlatam.com/2021/02/01/microsoft-la-apt-zinc-vinculada-a-corea-del-norte-tiene-como-objetivo-a-los-expertos-en-seguridad/

https://www.ciberseguridadlatam.com/2021/02/01/microsoft-la-apt-zinc-vinculada-a-corea-del-norte-tiene-como-objetivo-a-los-expertos-en-seguridad/

La botnet Mirai ataca el servidor de Minecraft de Wynncraft con un ataque DDoS de 2,5 TBps

La empresa de seguridad e infraestructura web Cloudflare ha revelado esta semana que ha detenido un ataque de denegación de servicio distribuido (**DDoS**) de **2,5 TBps** lanzado por la ***botnet*** **Mirai.**
La botnet Mirai ataca el servidor de Minecraft de Wynncraft con un ataque DDoS de 2,5 TBps - Una al Día (hispasec.com)

CIBERDELITO

"URUGUAY, El ciberdelito se comporta como la pandemia"

El pronóstico de que en el futuro la guerra puede liberarse en el campo de batalla informático parece aún lejano, pero lo que tenemos día a día es un creciente número de incidentes que nos afectan individualmente y como sociedad. A pesar de los esfuerzos locales de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), para educar a los ciudadanos respecto a las amenazas de la ciberdelincuencia, sigue siendo un flanco débil para personas y organizaciones. A esto se suma que, como se dice por parte de las autoridades de AGESIC, Uruguay sigue teniendo una situación crítica a nivel de recursos, con un notorio déficit en personal especializado en ciberseguridad, donde según algunas estimaciones, faltan más de 200 profesionales capacitados.

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/

https://carve850.com.uy/2022/09/24/mariano-jacquet-el-ciberdelito-se-comporta-como-la-pandemia/

Hackean agencia de criptomonedas y pierde 160 M de dolares

El creador de mercados de criptomonedas Wintermute ha sido víctima del más reciente ataque al mundo de las finanzas descentralizadas (DeFi), cuyo atacante consiguió robar activos digitales por un valor de 160 millones de dólares**.** El ataque consistió en la realización de una serie de transacciones no autorizadas que transferían dinero a la cartera del atacante en 70 criptodivisas diferentes, incluyendo USD Coin, Binance USD y Tether USD.

https://unaaldia.hispasec.com/2022/09/wintermute-hackeada-pierde-160m.html

https://es.cointelegraph.com/news/the-impact-of-the-wintermute-hack-could-have-been-worse-than-3ac-voyager-and-celsius-here-is-why

CIBERCONFIANZA

La OEA organizó con pleno éxito *Cyberwomen Challenge*

"La seguridad cibernética es ya uno de los principales desafíos a los que se enfrentan los países del hemisferio. El carácter transnacional de las amenazas que enfrenta la ciberseguridad la convierte en un elemento fundamental de la agenda global de los países. Al mismo tiempo, la ciberseguridad incorpora retos que están presentes en otros ámbitos profesionales, como es la inclusión y diversidad. Hoy las mujeres representan una pequeña parte de este sector, y es responsabilidad de todos dar la vuelta a esta situación. Colaboraciones como las que desde la OEA desarrollamos con Trend Micro para impulsar el papel de la mujer en la ciberseguridad, sin duda, contribuyen a reducir esta brecha género," afirmó Claudia Paz y Paz, Secretaria de Seguridad Multidimensional.

https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-035/18

https://www.argentina.gob.ar/jefatura/innovacion-publica/centro-gt/cyberwomen-challenge-argentina-2022

https://resources.trendmicro.com/CyberwomenChallenge_LAR_2021

TECNOLOGÍA

Tecnología de reconocimiento facial: Hacia una ley modelo

Muchos de nosotros habremos experimentado el reconocimiento facial desbloqueando un teléfono inteligente, organizando fotos de amigos y familiares, en los sistemas de seguridad del hogar, en el control de pasaportes y en el monitoreo y la vigilancia por parte de los empleadores y las fuerzas del orden. Si bien el reconocimiento facial se usa principalmente para identificar a una persona o para verificar que es quien dice ser, también se usa cada vez más para evaluar características, como la edad, el género o incluso las emociones de una persona. Por ello el Instituto de Tecnología Humana de Australia, ha publicado un informe liderando la cuestión a en el nivel planetario. Describe una Ley Modelo para el reconocimiento facial. Este informe responde a los crecientes llamados a la reforma de las principales voces de la sociedad civil, el sector privado, el gobierno y expertos académicos. La ley debe proteger contra los usos dañinos del reconocimiento facial, al mismo tiempo que fomenta la innovación para el beneficio público.

https://www.uts.edu.au/human-technology-institute/explore-our-work/facial-recognition-technology-towards-model-law

C2 Superioridad en un área de competencia tecnológica

JADC2 solo se puede lograr con tecnologías revolucionarias. POR EL TENIENTE CHRIS BRITT, EL TENIENTE ANDRE LEON Y LA DRA. BRITTA HALE

Desde el fondo marino hasta el espacio, la aplicación de sistemas autónomos inteligentes (IAS) está evolucionando dentro de la arquitectura conjunta de comando y control de todos los dominios (JADC2).
A medida que madure la aplicación integrada de estos dispositivos heterogéneos, también lo harán las nuevas amenazas a la ciberseguridad de la futura flota interconectada de plataformas y sensores tripulados y no tripulados.

Dentro de la red de sensores de todos los dominios JADC2, los sistemas autónomos son una capacidad de servicio compartido que amplía el alcance y la capacidad de la fuerza conjunta, contribuyendo directamente a una toma de decisiones informada y más rápida por parte del comandante de la fuerza conjunta.
https://www.afcea.org/signal-media/cyber-edge/c2-superiority-era-technological-competition?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email&_zs=vBgDh1&_zl=Etpc8

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).

1. Vulnerabilidades semana 22 de agosto: https://www.cisa.gov/uscert/ncas/bulletins/sb22-241
2. Vulnerabilidades semana 29 de agosto: https://www.cisa.gov/uscert/ncas/bulletins/sb22-249
3. Vulnerabilidades semana 5 de septiembre: https://www.cisa.gov/uscert/ncas/bulletins/sb22-255
4. Vulnerabilidades semana 12 de septiembre: https://www.cisa.gov/uscert/ncas/bulletins/sb22-262
5. Vulnerabilidades semana 19 de septiembre: https://www.cisa.gov/uscert/ncas/bulletins/sb22-269
6. Vulnerabilidades semana 26 de septiembre: https://www.cisa.gov/uscert/ncas/bulletins/sb22-276
7. Vulnerabilidades semana 3 de octubre: https://www.cisa.gov/uscert/ncas/bulletins/sb22-284

Informes de interés:

1. **Mozilla lanza actualización de seguridad para Thunderbird:** https://www.cisa.gov/uscert/ncas/current-activity/2022/09/30/mozilla-releases-security-update-thunderbirdhttps://www.cisa.gov/uscert/ncas/current-activity/2022/09/30/mozilla-releases-security-update-thunderbird y https://www.mozilla.org/en-US/security/advisories/mfsa2022-43/

2. **Vulnerabilidades de día cero en Microsoft Exchange Server**: Microsoft ha publicado una guía para el cliente sobre vulnerabilidades de día cero notificadas en Microsoft Exchange Server. Según la publicación del blog, "Microsoft es consciente de los ataques dirigidos limitados que utilizan las dos vulnerabilidades para ingresar a los sistemas de los usuarios". Las dos vulnerabilidades son CVE-2022-41040 y CVE-2022-41082, que afectan a Microsoft Exchange Server 2013, 2016 y 2019 en las instalaciones.

   Nota: Microsoft Exchange Online no se ve afectado.
   Un atacante podría explotar estas vulnerabilidades para tomar el control de un sistema afectado.
   Guía para el cliente sobre vulnerabilidades de día cero notificadas en Microsoft Exchange Server.
   Análisis de ataques utilizando las vulnerabilidades de Exchange CVE-2022-41040 y CVE-2022-41082
   https://www.cisa.gov/uscert/ncas/current-activity/2022/09/30/microsoft-releases-guidance-zero-day-vulnerabilities-microsoft

Toyota afectada por una filtración de casi 300.000 clientes

Toyota ha anunciado tras pedir disculpas por las redes sociales que 296,019 cuentas de correo electrónico y varias credenciales de clientes podrían haber sido expuestas tras un ciberataque.

https://seguridadpy.info/2022/10/toyota-afectada-por-una-filtracion-de-casi-300-000-clientes/?utm_source=rss&utm_medium=rss&utm_campaign=toyota-afectada-por-una-filtracion-de-casi-300-000-clientes