ISSN: 2718-6245

OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Editora: Bib Alejandra Castillo

ISSN: 2718-6245
http://www.esgcffaa.edu.ar/esp/oac-boletines.php

AÑO 3 N° 28
Octubre 2020

OAC Boletín de octubre 2020

" En tiempo de guerra, la verdad es tan preciosa que deberá estar siempre vigilada por un guardaespaldas de mentiras".

–Winston S. Churchill.

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

La lucha contra la desinformación; cambio de Modelo

Felix Arteaga expone este artículo en Ciber Elcano, acerca de la cuestión de la desinformación como una enfermedad de la sociedad que aprovecha los instrumentos diseñados para la comunicación, el bienestar y la libertad de la sociedad para suscitar dudas, generar tensiones, cuestionar identidades y desarticular comunidades. La desinformación es un desorden de la globalización que fomentan deliberadamente agentes totalitarios, populistas, supremacistas o sectarios que no sólo buscan notoriedad o dinero, sino capacidad de control sobre el cuerpo social.

http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-la-lucha-contra-la-desinformacion-cambio-de-modelo?utm_source=CIBERelcano&utm_medium=email&utm_campaign=58-sep2020&_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-a5e4c470e59de911a97d000d3a233b72-85b55db62d5640f583bcbe6b4cce2915&esid=0256e27f-62f7-ea11-a815-000d3aab18bd

CIBERDEFENSA

Documento de Interés

El futuro Digital de Europa

La disponibilidad de servicios digitales de suficiente calidad ha sido decisiva para desarrollar actividades de forma no presencial durante el confinamiento provocado por la COVID-19, y se ha puesto en evidencia que es posible realizar muchas de estas tareas de forma más eficiente y sostenible, por lo que existe una oportunidad histórica para promover la evolución hacia una nueva normalidad más digital. Los planes para superar la crisis deben facilitar el avance hacia nuevos modelos de desarrollo que utilicen todo el potencial de las tecnologías digitales y faciliten el liderazgo de Europa en el contexto internacional.

http://www.realinstitutoelcano.org/wps/wcm/connect/9eec583e-af76-4261-bec7-2e699a3e4c22/El-futuro-digital-de-Europa.pdf?MOD=AJPERES&CACHEID=9eec583e-af76-4261-bec7-2e699a3e4c22

CIBERGUERRA

La 'guerra híbrida' y la vigilancia masiva

Se filtró una base de datos de 2,4 millones de personas, incluidos más de 35.000 australianos, de la empresa Zhenhua Data de Shenzhen. La información recopilada incluye fechas de nacimiento, direcciones, estado civil, junto con fotografías, asociaciones políticas, familiares e identificaciones de redes sociales, recopila cuentas de Twitter, Facebook, LinkedIn, Instagram e incluso TikTok, así como noticias, antecedentes penales y delitos corporativos

https://www.abc.net.au/news/2020-09-14/chinese-data-leak-linked-to-military-names-australians/12656668

CIBERCONFIANZA

Ciberataques en el sistema sanitario en Barcelona

El Hospital Moisès Broggi de Sant Joan Despí (Barcelona) ha sufrido un ciberataque de ransomware que ha inutilizado parte de sus servidores desde, al menos, el pasado domingo. Los atacantes, presumiblemente rusos, han pedido un rescate por liberar las máquinas que el centro se ha negado a pagar.

https://www-genbeta-com.cdn.ampproject.org/c/s/www.genbeta.com/seguridad/hospital-moises-broggi-barcelona-sufre-ciberataque-se-apunta-a-hackers-rusos-como-responsables-ransomware/amp

CIBERSEGURIDAD

Denuncia de amenaza de ciberseguridad

Según una acusación formal reciente del Departamento de Justicia de EEUU, dos piratas informáticos han sido acusados de piratería a los sistemas informáticos de cientos de empresas, gobiernos y organizaciones no gubernamentales, clérigos y activistas democráticos y de derechos humanos en los Estados Unidos, Australia, Bélgica, Alemania, Japón, Lituania, Paises Bajos, España, Corea del Sur, Suecia y Reino Unido en una campaña que duró más de diez años. Los actores habrían trabajado para el Departamento de Seguridad del Estado de Guangdong (GSSD) del Ministerio de Seguridad del Estado (MSS), encargados de la campaña global de intrusión informática dirigida en especial a la propiedad intelectual y la información comercial confidencial, incluida las investigaciones sobre COVID 19,

Estos piratas informáticos habrían actuado tanto para su beneficio personal como para el MSS.

https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

https://us-cert.cisa.gov/ncas/alerts/aa20-258a

CIBERFORENSIA

Informes de la Agencia de Ciberseguridad e Infraestructuras de los EE.UU

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 07 de septiembre https://us-cert.cisa.gov/ncas/bulletins/sb20-258

Semana de 14 de septiembre: https://us-cert.cisa.gov/ncas/bulletins/sb20-265

Semana de 21 de septiembre: https://us-cert.cisa.gov/ncas/bulletins/sb20-272

Semana de 28 de septiembre: https://us-cert.cisa.gov/ncas/bulletins/sb20-279

Malware LokiBot las amenazas a las vulnerabilidades de las VPN

CISA ha observado un aumento notable en el uso de malware LokiBot por parte de ciberatacantes desde julio de 2020. A lo largo de este período, el sistema de detección de intrusiones EINSTEIN de CISA, que protege las redes del poder ejecutivo civil federal, ha detectado actividad maliciosa persistente de LokiBot.

LokiBot utiliza un malware de robo de información y credenciales, a menudo enviado como un archivo adjunto malicioso y conocido por ser simple pero efectivo, lo que lo convierte en una herramienta atractiva para una amplia gama de actores cibernéticos en una amplia variedad de casos de uso de compromiso de datos. Se ha observado que explota varias vulnerabilidades y exposiciones comunes (CVE) públicas que se ocupan de la red privada virtual (VPN) Pulse Secure, Citrix NetScaler y vulnerabilidades F5.Los detalles técnicos en:

https://us-cert.cisa.gov/ncas/alerts/aa20-266a

https://us-cert.cisa.gov/ncas/alerts/aa20-259a

AGENDA de INTERÉS

Cursos y Seminarios en Línea

1. **Kaspersky Seguridad adaptable para su transformación digital** Mié., 14 de Oct. de 2020 12:00 - 13:00 ART

   https://register.gotowebinar.com/register/2347199349766829071?mkt_tok=eyJpIjoiWWpRek5HRXlOV1kxWWpFNSIsInQiOiI1amU1NTlwWDFicWJ6KzZwRE5XZUFlcFMxQ2VCZmlzVGw2Y0NFR2pCWlk3U01TcXBCdlp6ZnRZczZ0STRSY0xxY3NWT2VKZ0hZRUp1WWR3cWlHbHhrSXdLZEluYlBnazRPVVdOOUwxUWpiTkl5NXZ3Qm12S1lIMUEwdGozOHhTMSs5Q0IwRitnblNvbGx5MlhyME5pSGc9PSJ9