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° 22
Abril 2020

OAC Boletín de Abril 2020

"Un avance en nuestro pensamiento puede abrir el dominio del reino de las armas. Tal como lo vemos, una sola caída del mercado de valores, una invasión de virus informáticos o un rumor o escándalo que resulte en una fluctuación en las tasas de cambio del país enemigo o expone a los líderes de un país enemigo en Internet. Todos se pueden incluir en las filas de las armas del nuevo concepto."

La Guerra Irrestricta
Cnel Qiao Liang y Cnel Wang Xiangsui

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

El trabajo Digital post COVID 19

La crisis del coronavirus ha estimulado el crecimiento del trabajo en línea. María Mexi en este artículo nos dice: "*El genio no volverá a la botella y debemos planear un futuro de 'digiwork decente*". Covid-19 obliga a las empresas y organizaciones a imponer políticas obligatorias de trabajo desde el hogar en un mundo cada vez más "sin contacto". El cambio repentino al trabajo digital remoto, de la noche a la mañana y en masa, tiene el potencial de acelerar los cambios en la forma en que se realiza el trabajo y la forma en que pensamos sobre los arreglos del mismo.

Mirando la imagen más amplia, Covid-19 puede ser un punto de inflexión importante para la transformación digital del lugar de trabajo. Parece casi imposible volver a poner ese genio digital en la botella, una vez que termina la emergencia de salud.

https://www.socialeurope.eu/the-future-of-work-in-the-post-covid-19-digital-era?utm_source=sfmc&utm_medium=email&utm_term=&utm_content=41946&utm_id=50180981-ce02-45c4-9b2c-2c4934dc3ff8&sfmc_id=358830394&sfmc_activityid=47f7ceea-864a-44b2-af60-3eaa0c56aadc&utm_source=sfmc&utm_medium=email&utm_campaign=2715323_StrategicIntelligenceWeekly&utm_term=&emailType=Strategic%20Intelligence%20Newsletter

Las oportunidades de la Inteligencia Artificial

La inteligencia artificial (IA) tiene el potencial de transformar el crecimiento económico y el comercio, afectando los tipos de trabajos disponibles y las habilidades que se necesitan. Estados Unidos, China, Japón, Alemania, el Reino Unido, Francia y otros han reconocido la oportunidad y están apoyando la investigación y el desarrollo de IA, y preparando a su fuerza Laboral.

Para que la AI se desarrolle también se requiere un entorno propicio que incluya una nueva regulación en áreas como la ética de AI, el acceso a datos y la revisión de las leyes y regulaciones existentes en áreas como los derechos de privacidad y propiedad intelectual (IP).

https://www.brookings.edu/research/artificial-intelligence-primer-what-is-needed-to-maximize-ais-economic-social-and-trade-opportunities/

Cerebro Sociedad y Defensa. Escenario mundial de la guerra híbrida

En el escenario actual de los conflictos ciber, donde no es nada nueva la formación de "trolls" para crear tendencias en redes sociales como parte una batalla cultural. El Prof. Dr. Mario Kamelman Director del Proyecto de Investigación sobre Neurociencias y Defensa de la Escuela Superior de Guerra Conjunta - Universidad de la Defensa de la República Argentina, analiza desde un punto de vista sistémico a la sociedad globalizada describiendo el impacto de las neurociencias y las TICs en los escenarios de la comunicación político-social y de guerra psicológica. Se describen los mecanismos cerebrales del miedo y las emociones, así como los mecanismos de adaptación y stress social. Se destaca la importancia de las emociones frente al raciocinio en el marco de los conflictos híbridos y la manipulación del cerebro del miedo en la Guerra Psicológica frente a deseos y satisfactores

http://www.cefadigital.edu.ar/bitstream/1847939/1428/1/OAC%20I05%20KAMELMAN.pdf

Las Neurociencias y la Guerra Híbrida

El advenimiento de la post-verdad. Un neologismo que describe la distorsión deliberada de la realidad con el fin de crear y modelar la opinión pública e influir en las actitudes sociales en donde los hechos objetivos se desdibujan frente a la manipulación de las emociones y las creencias personales a través de medios tecnológicos.

El Prof. Dr. Mario Kamelman continúa su interesante análisis al que se enfrenta el líder en el conflicto moderno donde amigos y enemigos, izquierda y derecha son bombardeados en el ambiente Ciber por la comunicación profesional de base cognitiva, cuyo objetivo es el manejo de la percepción y las creencias de las poblaciones segmentadas a través de técnicas de microtargeting. El modelado de la “realidad” es ecualizado por “voces influyentes” en la multimedia que determina rankings en las redes sociales y carga los motores de búsqueda que posicionan posturas que no necesariamente obedecen a los hechos reales sino a los ecualizados por los poderes políticos.

http://www.cefadigital.edu.ar/bitstream/1847939/1429/1/OAC%20I06%20KAMELMAN.pdf

CIBERSEGURIDAD

Resumen de Vulnerabilidades

El Boletín de Vulnerabilidad del Departamento de Seguridad Nacional de los EE.UU. la semana del 23 de marzo, proporcionó un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad del Instituto Nacional de Estándares y Tecnología (NIST).

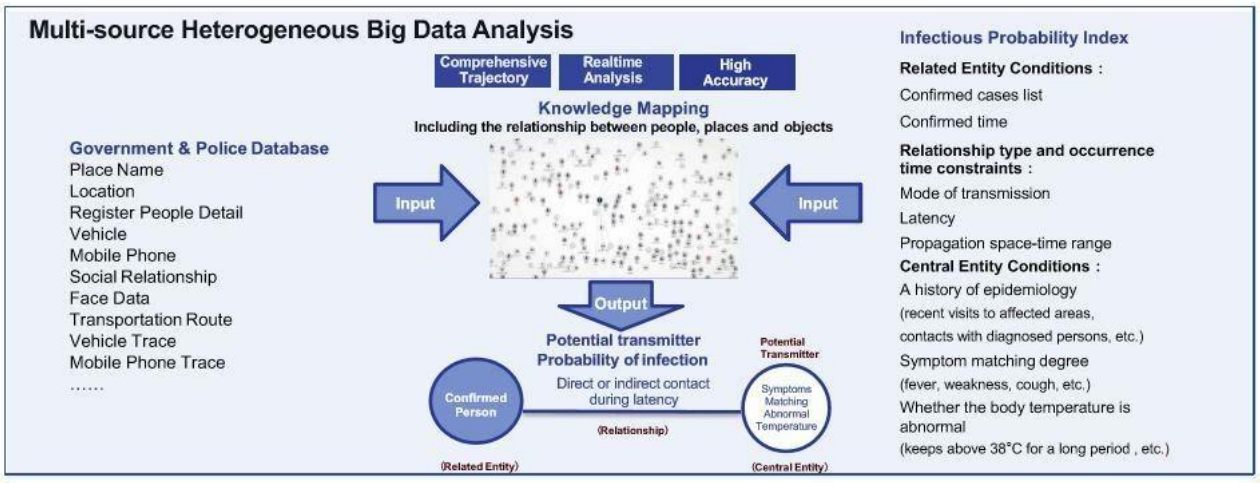
Tenga en cuenta que parte de la información del boletín se compila a partir de informes externos de código abierto y no es un resultado directo del análisis de CISA (Cybersecurity and Infrastructure Security Agency).

https://www.us-cert.gov/ncas/bulletins/sb20-090

CIBERDEFENSA

El impacto de COVID 19 en las Infraestructuras de la Información

El foro económico mundial informa acerca de cómo la Infraestructura digital ayuda en la emergencia del COVID 19, los mapas del mundo muestran cómo la disminución en el transporte de personas ha reducido drásticamente las emisiones de carbono en diferentes países, pero ¿cuál es el caso de las emisiones de las tecnologías digitales? ¿El volumen de personas que trabajan desde casa o usan dispositivos digitales en cuarentena provocará un aumento en las emisiones de otras fuentes? ¿Qué están haciendo los grandes proveedores de la nube para abordar el problema de capacidad?



Las ciudades de todo el mundo han hecho de la innovación de infraestructuras una prioridad para salvaguardar sus sistemas físicos para que puedan mantenerse robustos durante desastres naturales como terremotos, tsunamis y huracanes. Pero las pandemias han demostrado que estos métodos no son suficientes para garantizar la conectividad y el acceso a nuestra sociedad durante los desastres biológicos.

https://www.weforum.org/agenda/2020/04/digital-infrastructure-public-health-crisis-covid-19/?utm_source=sfmc&utm_medium=email&utm_term=&utm_content=41946&utm_id=50180981-ce02-45c4-9b2c-2c4934dc3ff8&sfmc_id=358830394&sfmc_activityid=47f7ceea-864a-44b2-af60-3eaa0c56aadc&utm_source=sfmc&utm_medium=email&utm_campaign=2715323_StrategicIntelligenceWeekly&utm_term=&emailType=Strategic%20Intelligence%20Newsletter

CIBERCONFIANZA

Informe sobre el sistema de Video Conferencias ZOOM

Situación

Zoom es una plataforma popular de reuniones y videoconferencias en línea conocida por sus capacidades de seminarios web para eventos virtuales en vivo y transmisión, fundada por el chino- estadounidense Eric Yuan. Cuenta con video y audio HD, herramientas de colaboración, funcionalidad de chat y un sistema de teléfono en la nube.

La aplicación de videoconferencia ha disfrutado de una explosión de popularidad a medida que las escuelas y oficinas cierran sus puertas y las familias intentan mantenerse conectadas, de acuerdo con

Clarín la compañía creció de 10 millones de usuarios a 200 Millones en la crisis COVID 19 (https://www.clarin.com/tecnologia/coronavirus-mitos-verdades-zoom-app-convirtio-boom-plena-pandemia_0_OccA84xu2.html).

Cada vez más personas recurren a herramientas de colaboración remota para el trabajo, la educación y mantenerse al día con amigos y familiares, creando una nueva dependencia de la videoconferencia y la colaboración.

Zoom fue una de las más elegidas y ello la convirtió en objeto de un escrutinio inmenso que detectó cuestiones como: (1) permitir a un atacante robar las credenciales de acceso de los usuarios que hacen clic en un enlace para unirse a una reunión, (2) utilizar una técnica "sombría" para instalar la aplicación de Mac sin interacción del usuario, (3) Intromisiones sin permiso a reuniones virtuales que se dieron a llamar "Zoombombing", (4) Alemania y Taiwán han impuesto restricciones sobre el uso de la aplicación, (5) una escuela en los EE. UU. Ha dejado de usarla después de que un "hombre adulto desnudo usando insultos raciales" se entrometió en una reunión protegida con contraseña.

Zoom se ha embarcado en un plan de 90 días para abordar los problemas de privacidad y seguridad, solicitando la ayuda de un ex jefe de seguridad de Facebook mientras intenta recuperar la credibilidad.

Nuestras Conclusiones

Siempre que habilitamos nuestra cámara y micrófono en nuestros dispositivos, incrementamos nuestra exposición a las vulnerabilidades de cualquier sistema operativo e incrementa la posibilidad de recibir amenazas cibernéticas, (virus de tipo, residentes en memoria, acción directa sobre-escritura, de arranque, Macro Virus, polimórfico, secuencias de comandos, ataque al disco rígido, ransomware, troyanos, gusanos, etc.). Con un crecimiento desmesurado como el que ha tenido esta aplicación resulta completamente lógico que haya sido objeto de escrutinio y oportunidad para el uso malicioso de la misma así comopa ala exploración de sus debilidades.

Probablemente se deba hacer un balance entre sus bondades, facilidad de uso y las falencias remanentes (dado que están saliendo parches de la misma) y definir la conveniencia o no de su empleo, siempre será más segura una herramienta propietaria y empleada dentro de una VPN o portal seguro, pero eso normalmente tiene un costo que debe asumirse, finalmente si quiere minimizar impactos negativos de Zoom aquí le damos algunas recomendaciones resumidos en principio en 14 items de fácil implementación cuando organice se reunión como anfitrión gentilmente aportadas por el Ingeniero Manrique Gonzalez Avellaneda (maestrando de la Maestría en Ciberdefensa de la Universidad de Buenos Aires y a la vez Perito Informático).

Léalos con atención.

http://www.cefadigital.edu.ar/bitstream/1847939/1427/1/OAC%20I04%20AVELLANEDA.pdf

CIBERFORENSIA

Maryan, una Herramienta sencilla para actividades de Inteligencia en Fuentes abiertas

Maryam Framework Tool es una herramienta OSINT (investigación de código abierto). Principalmente, se utiliza para pruebas de penetración de aplicaciones web para reconocer la información sobre la aplicación web. Esta herramienta Maryam está construida en el lenguaje de programación python. Es fácil de entender y cada probador de penetración puede usar esta herramienta para recopilar información sobre el objetivo.

https://www.securitynewspaper.com/2020/04/10/simple-to-use-osint-open-source-investigation-framework-maryam/

Reporte sobre Ransomware

La Agencia de Seguridad de la Ciberseguridad e Infraestructura (CISA) ha observado un aumento en los ataques de ransomware en todo el mundo: consulte los Informes de sensibilización de CISA sobre la lucha contra el ransomware, la declaración conjunta de ransomware y las estadísticas de CISA: brote de ransomware .

https://www.us-cert.gov/Ransomware