“Cuanto más se abre un dispositivo o sistema más se expone a que esa misma funcionalidad retorne como una fresca y sonora bofetada en la cara”

David García

CIBERDEFENSA

Exposición del Dr Gral (R) Ben Israel en la Maestría de Ciberdefensa y Ciberseguridad de la UBA

Como mencionáramos en nuestro boletín anterior, en su paso por Buenos Aires en el mes de julio de este año, el Mayor Gen. (Res.) Prof. Isaac Ben-Israel – Director of the Blavatnik Interdisciplinary Cyber Research Center (ICRC), dictó una clase magistral para nuestros maestrandos.

En el citado evento desarrolló el proceso de evolución del área en cuestión en su país destacando que “no hay transferencia de tecnología. Solo es posible la transferencia de tecnólogos”.

Es de destacar que el mencionado Centro se estableció en la Universidad de Tel Aviv como una iniciativa conjunta con la Oficina Nacional de Cibernética, dependiente en forma directa del Primer Ministro de Israel.

https://drive.google.com/open?id=1UaUvHURCeeaA4VdIqb5PLBggICLVkhm9

CIBERGUERRA

Guerras híbridas: El fusil y la ciberarma. Despliegue operacional de las FFAA Ecuatorianas en la frontera Ecuador y Colombia

Carl Von Clausewitz sostuvo que cada era tiene su propia concepción de los conflictos armados. De esta forma, a partir del ataque a las Torres Gemelas del 9/11, militares y

Transformación de la Guerra", sostiene que los conflictos han evolucionado hasta un punto en que, en un futuro no tan lejano, las bases militares serán reemplazadas por escondites y depósitos, y el control de la población se efectuará mediante una mezcla de propaganda y terror. Estas afirmaciones aportaron sustento intelectual a lo que Lind había denominado pocos años antes las "Guerras de Cuarta Generación" (en adelante, 4GW). Van Creveld también previó la desaparición de los principales sistemas de combate tradicionales y su conversión en conflictos de baja intensidad, también llamados "Guerras Asimétricas".
El siguiente trabajo final de la materia Tecnologías de la Información, fue desarrollado por un grupo multidisciplinario de siete maestrandos que cursan la maestría en Ciberdefensa y Ciberseguridad que se dicta en de la Universidad de Buenos Aires. Los hechos y las operaciones descritas son meramente ficticios.

https://drive.google.com/open?id=1UaUvHURCeeaA4VdIqb5PLBgglCLVkhm9

CIBERSEGURIDAD

Prohíben el uso de dispositivos con servicio GPS en el pentágono

Las funciones de geolocalización, estas características de geolocalización pueden ayudar a Patrick Shanahan a proteger el contenido del Departamento de Defensa. exponer información personal, ubicaciones, rutinas y números de personal del Departamento de Defensa ", dijo, lo que puede crear" consecuencias de seguridad importantes y un mayor riesgo para la fuerza y la misión conjunta ".

https://www.nextgov.com/policy/2018/08/pentagon-prohibits-personnel-using-gps-services-all-operational-areas/150304/

– – –

Recompensas por la detección de errores claves para la seguridad en la Red

Dado que la seguridad depende realmente de la comunicación colaborativa de las identidades y los datos de identidad dentro de los dominios, las identidades digitales de los clientes suelen ser la clave para acceder a los servicios e interactuar a través de Internet.
La piratería de redes y el robo de datos se han vuelto comunes y más fáciles de usar, pero no todos los datos tienen el mismo valor comercial o conllevan el mismo riesgo.
Microsoft lanzó hoy un nuevo programa de recompensas de errores para los cazadores de errores y los investigadores que encontraron vulnerabilidades de seguridad en sus servicios de identidad.

https://thehackernews.com/2018/07/microsoft-bug-bounty.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-Security+Blog%29&_m=3n.009a.1788.po0ao0di5a.13d8

– – –

Cisco Talos tiene una campaña dirigida contra iPhone que parece radicada en la India. La reproducción podría hacerse a través del acceso físico a los dispositivos, o muy probablemente mediante el uso de ingeniería social para atraer a un usuario a registrarse. En los ataques de ingeniería social, haga clic en la opción para aceptar para acceder al físico al atacante a un dispositivo. Esta campaña es notable ya que el malware ha hecho todo lo posible para reemplazar aplicaciones móviles por interceptación de datos.

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

– – –

Criptografía basada en hardware

Si bien el tratar de ocultar la información es algo tan viejo como la humanidad, la criptografía ahora juega un papel fundamental en la protección de datos, ella proporciona confidencialidad, integridad, autenticación y acceso a la información que se encuentra almacenada en cualquier medio electrónico, que viaja a través de una red de datos o que está siendo usado en tiempo real.
Ocultar la información a unos y hacerla visible a otros, evadiendo a los atacantes que analizan los métodos y los algoritmos matemáticos en busca de la clave que permiten tener acceso a los datos para obtener beneficio.

https://revista.seguridad.unam.mx/print/2199

– – –

Una solución para evitar la Guerra de la Información a través de Redes Sociales

El 16 de julio, el parlamento egipcio aprobó una nueva ley que clasifica una cuenta personal de redes sociales, blog o sitio web con más de 5,000 seguidores como medios de comunicación, lo que permite al estado una cuenta de redes sociales y penalizar a periodistas por publicar noticias falsas. Si bien las redes sociales son un modo poderoso y rápido de compartir ideas e información, no siempre se hace con la verdad o buenas intenciones.

https://thehackernews.com/2018/07/social-media-fake-news-law.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1791.po0ao0di5a.13fr

CIBERCONFIANZA

Google incrementa su seguridad y da la confianza a los usuarios

Los usuarios de Google Chrome son notificados de que un sitio no era seguro. A veces porque el responsable de la web olvidó actualizar el certificado HTTPS (tienen caducidad), otras veces porque la página web envía por cifrar contraseñas o información de la tarjeta de crédito ... La cuestión es que te salta un aviso, a veces es difícil de esquivar, informándote que la página no es segura.
HTTP es el protocolo clásico para servir páginas web (que son especialmente contenido HTML) en Internet, pero HTTP no permite saber si quien utiliza la web es quién dice ser, y la información viaja sin cifrar entre el navegador y el servidor. Esta

que sirvan su contenido utilizando HTTP en vez de su versión autenticada y cifrada HTTPS, como parte del esfuerzo de Google de hacer Internet más segura.

https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

CIBERCRIMEN
Documento de Interés

Informe de delitos en Internet (IC3) 2107

El IC3 (Internet Crime Complaint Centre) del Internet.
Previene sobre los avances en ciberdelincuencia y cómo hacer frente a las ciberamenazas persistentes y cambiantes que enfrentamos.
El informe sobre crímenes en Internet de 2017 enfatiza los esfuerzos del IC3 para monitorear estafas vía Business email compromise (BEC), Ransomware, Fraude de soporte técnico y extorsión.
El informe presenta historias de éxito a partir de IC3 y la Iniciativa Operación Wellspring (OWS) investigación cibernética mediante la utilización de una Fuerza de Trabajo Cibernética, fortaleciendo así la colaboración de las fuerzas del orden público a nivel estatal y local.

https://pdf.ic3.gov/2017_ic3report.pdf