# BOLETIN OAC JULIO 2018


**En el futuro los soldados usan botas de combate y uniformes de camuflaje, funcionan sistemas de armas complejos, pero todos irremediablemente tienen encorvados sobre sus teclados.**

---

## Ciberdefensa

### HACIA LA SUPERIORIDAD EN LAS OPERACIONES CIBERESPACIALES

**El Departamento de Defensa de los EE. UU está priorizando sus capacidades en el equipamiento de sus fuerzas cibernéticas con una plataforma unificada de guerra para lograr, mantener y defender la superioridad del campo.**

**La Plataforma Unida (UP) tiene como objetivo fundamental la capacidad del comando para responder con la velocidad, agilidad y precisión que requiere para contrarrestar las amenazas, permitir la sincronización, integración y ejecución global de variadas misiones y funciones. Esta plataforma unificada permitirá a CMF [Fuerzas de la Misión Cibernética] llevar a cabo operaciones de ciber en apoyo de los requerimientos nacionales.**

**A multas de marzo de 2018, el Comando Cibernético dio a conocer su orientación bajo el título "Lograr y mantener la superioridad de las esferas", lo que denotaba un**

**perfil más agresivo orientado hacia el futuro que los adversarios estaban ejecutando las operaciones cibernéticas directas y continuas contra los Estados Unidos y sus aliados.**

**En este artículo, se hace especial hincapié en aumentar la resiliencia reaccionando lo más rápidamente de hecho el ataque. El objetivo es lograr la superioridad en el ámbito privado Involucrar y desafiar implacablemente a los adversarios por debajo del nivel del conflicto armado salvo que el mismo exista. La plataforma permitirá a los miembros nacionales y regionales de los equipos cibernéticos trabajar con unidad de criterios.**

**El recurso humano de CMF está conformado para el servicio activo, el personal de reserva y el personal civil de cada rama de la FFAA y la Guardia Costera de los EE. UU. UU. Los 6.200 miembros de esta fuerza de élite están organizados en 133 equipos distribuidos de la siguiente manera:**

**El documento está disponible en:**

https://www.afcea.org/content/unified-platform-unifies-cyber-warfighting?utm_source=Informz&utm_medium = Correo electrónico y utm_campaign = Informz%20Email

## Análisis

### EL CIBERESPACIO, UN ASPECTO A TENER EN CUENTA EN EL PLANEAMIENTO MILITAR

**Cuando una militar investiga las implicancias que las nuevas tecnologías (y en particular las tecnologías de la información y las comunicaciones) tienen en las operaciones militares, puede observar que la ejecución de las mismas en el país se está materializando por parte del potencial atacante Para muchos conductores y / o planificadores el ciberespacio sigue siendo un ámbito de conflictos para un futuro lejano.**

**El documento está disponible en:**

http://www.cefadigital.edu.ar/bitstream/123456789/1026/1/EL%20CIBERESPACIO%2c%20UN%20ASPECTO%20A%20TENER%20EN%20CUENTA%20EN%20EL%20PLANEAMIENTO% 20% 20MILITAR.pdf

Ciberguerra

## SE PUEDE AFECTAR DISCOS DUROS, MEDIANTE SEÑALES INAUDIBLES DE ULTRASONIDO

Los investigadores han visto cómo las señales sónicas y ultrasónicas (inaudibles para los humanos) pueden ser utilizados para causar daño físico a las discos duros simplemente reproduciendo sonidos ultrasónicos a través del propio teléfono incorporado de la computadora objetivo o explotando un altavoz cerca del dispositivo objetivo.
Una investigación similar fue realizada el año pasado por un grupo de investigadores de la Universidad de Princeton y Purdue, quienes demostraron un ataque de denegación de servicio contra las discotecas duros mediante la explotación de un fenómeno físico llamado resonancia acústica.
Dado que las unidades de disco duro están expuestas a vibraciones externas, los investigadores demostraron que, en última instancia, a la falla en los sistemas que dependen de ellos, vibraciones significativas en los componentes internos de las unidades de disco duro la unidad de disco duro.
El documento está disponible en:
http://www.princeton.edu/~liweis/Publications/Acoustic_Attacks_on_HDDs.pdf

## LA RESILIENCIA, UN PROBLEMA A RESOLVER TAMBIÉN EN LOS SISTEMAS DE ARMAS AEROESPACIALES

La Fuerza Aérea de los EE. UU. Está estudiando una metodología para evaluar la resistencia a la cibernética de los sistemas de armas y examinar cómo estandarizar esa metodología en todo el servicio. Podrían mejorar la seguridad de los sistemas de armas, incluidos los aviones de reabastecimiento de combustible, los aviones de combate y los sistemas de navegación inercial.
El documento está disponible en:
https://www.afcea.org/content/cyber-resiliency-feather-crows-flight-cap?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email

## ATAQUES CIBERNÉTICOS CONTRA LA INFRAESTRUCTURA DEL AGUA

Investigadores de ciberseguridad han descubierto una campaña para realizar ataques de pozo de agua. Se cree que la campaña está activa, fue detectada por los investigadores de Kaspersky Labs, quienes atribuyeron al grupo de actores LuckyMouse.
LuckyMouse, también conocido como Iron Tiger, Emissary Panda, APT 27 y Threat Group-3390, es el mismo grupo de piratas informáticos chinos que se descubrió atacando a los países asiáticos con malware de minería de Bitcoin a principios de este año.
El documento está disponible en:
https://thehackernews.com/2018/06/chinese-watering-hole-attack.html

---

Ciberseguridad

## LA MINERÍA DE DATOS UN CONCEPTO ESENCIAL EN LA SEGURIDAD DE HOY

El tráfico en las redes ópticas de transporte está creciendo exponencialmente, dejando las agencias de inteligencia cibernéticamente a cargo de monitorear estas redes con la menor envidiable tarea de tratar con cantidades cada vez mayores de datos para obtener las amenazas cibernéticas.
A medida que las velocidades de transmisión se multiplican por el volumen de tráfico se expanden de manera exponencial, las exigencias de las herramientas son compatibles con el tiempo real y todos los canales de datos de la red de transporte.
El documento está disponible en:
https://www.afcea.org/content/finding-cyber-threats-big-data-analytics?utm_source=Informz&utm_medium=Email&utm_campaign=Informz%20Email

## MALWARE EN TELEGRAM

Telegram es como se ha bautizado a este malware que se detectó por primera vez el 4 de abril de 2018, y surgió una segunda variante el 10 de abril del presente año. Mientras que la primera versión solo robaba las credenciales y las cookies del navegador, junto con todos los archivos de texto que puedan estar en el sistema, la segunda variante agregó la capacidad de recopilar la información del cliente y las claves de esta famosa aplicación de mensajería , así como otro tipo de información. Un ataque de este tipo podría acarrear que se pueda secuestrar las sesiones de Telegram.
El documento está disponible en:
https://blog.talosintelligence.com/2018/05/telegrab.html

## CIBERAMENAZAS Y TENDENCIAS DEL CCN-CERT

El Centro Criptológico Nacional de España ha publicado su informe de ciberamenazas y tendencias edición 2018.

Entre los datos de interés se encuentra un aumento del 26,55% respecto a la contabilidad del año 2016. Destaca el continuo ascenso en el protagonismo de las acciones ejecutadas por grupos estatales y, por otro lado, la de los omnipresentes grupos criminales. Expone temas acerca de Ciberincidentes. Amenazas y vulnerabilidades, métodos de ataque y tendencias

El documento está disponible en:

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18 - ciberamenzas-y-tendencias-edicion-2018-1 / file.html

### LA CONECTIVIDAD DE LA INTERNET DE LA COSAS EN JAQUE

Unos 100 millones de dispositivos IoT expuestos por una vulnerabilidad en el protocolo Z-Wave. La onda Z es un uso-utilizado principalmente en domótica. Este protocolo permite el control inalámbrico de electrodomésticos y otros dispositivos, está destinado a la automatización del hogar y / o la oficina, permite una conexión a través de Internet para controlarlo.

El documento está disponible en:

https://thehackernews.com/2018/05/z-wave-wireless-hacking.html

---

## DOCUMENTO DE INTERÉS

### PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS EN LATINOAMÉRICA Y EL CARIBE 2018

Los avances en la tecnología digital revolucionan la forma en que las personas, empresas y estados interactúan. El flujo general de bienes y servicios, se ha transformado debido a la mayor conexión a Internet y el advenimiento del comercio electrónico. Sin embargo, las nuevas tecnologías se han convertido en desafíos y gustos propios. La adopción de nuevas tecnologías digitales es más eficiente en términos de escala, tiempo y distancia, pero también introduce nuevas vulnerabilidades que hacen que la protección de la información crítica de Infraestructuras una tarea importante.

El documento está disponible en:

https://www.oas.org/es/sms/cicte/cipreport.pdf?_cldee=YW1vcmVzaTUxQGdtYWlsLmNvbQ%3d%3d&recipientid=contact-c72ddabb9af8e711812870106fa6f4a1-47d644d91b3e4f528fa621c1126ccba5&esid=336401db-e96e-e811-8141-70106faa5281&urlid=14

---

## Ciberconfianza

### MILLAS DE APLICACIONES MÓVILES EXPONEN SUS

## BASES DE DATOS SIN PROTECCIÓN

Investigadores de seguridad móvil descubrieron bases de datos de Firebase desprotegidas en aplicaciones móviles iOS y Android (el servicio Firebase de Google es una de las plataformas de desarrollo más populares para aplicaciones móviles y web).

Esta situación expone más de 100 millones de registros de datos, incluyendo contraseñas de texto plano, identificaciones de usuario, ubicación y, en algunos casos, registros financieros como transacciones bancarias y de criptomonedas.
El documento está disponible en:
https://thehackernews.com/2018/06/mobile-security-firebase-hosting.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog % 29 & _m = 3n.009a.1770.po0ao0di5a.12x2

## LA TENDENCIA AL ESCRITORIO VIRTUAL

La demanda, la demanda, la demanda, la demanda y el precio de la demanda total de la demanda. El documento está disponible en:
https://www.vmware.com/products/horizon.html

## PUBLICACIÓN DEL OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), presenta una nueva edición del "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles". El informe recoge muchos más datos de interés:
Medidas de seguridad, para el empleo de computadoras hogareñas, Redes de WiFi, para el empleo de dispositivos móviles y también los motivos para los que estas no son empleadas.
Hábitos de comportamiento en la navegación y usos de Internet: hábitos de uso de las redes inalámbricas Wi-Fi, dispositivos Android y altas en redes sociales. Las descargas en internet y el uso de la Banca en línea.
Incidentes de seguridad: tipos de malware, incidentes de seguridad en las redes inalámbricas Wi-Fi, tipos de malware detectados y peligrosidad del código malicioso. Riesgos malware vs. sistema operativo, malware vs. actualización del sistema, malware vs. Java en PC.
Consecuencias de los incidentes de seguridad y reacción de los usuarios: Intento de fraude en línea y manifestaciones, seguridad y fraude, cambios adoptados por incidente de seguridad. E-Confianza y limitaciones en la Sociedad de la Información, percepción de los usuarios sobre la evolución en seguridad, valoración de los peligros de Internet, responsabilidad en la seguridad de Internet.
El documento está disponible en:
http://www.ontsi.red.es/ontsi/sites/ontsi/files/Ciberseguridad%20y%20confianza%20en%20los%20hogares%20espa%C3%B1oles%20%28abril%202017%29.pdf

---

## VISITA DEL GENERAL DR. ISAAC BEN ISRAEL A LA MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA DICTADA EN LA UNIVERSIDAD DE BUENOS AIRES

Ciberdefensa y ciberseguridad constituyen dos áreas prioritarias de la gestión gubernamental. Se sabe

que internet es el ámbito de crecimiento más importante de la economía mundial y la herramienta que más ha influido en la comunicación global. Desafortunadamente, en internet también se llevan a cabo las agresiones más insidiosas entre Estados y las felonías más rentables del crimen organizado transnacional. Lobby destaca lo relevante de la estadística en la Argentina de quien se reconoce como el científico de mayor nivel en Israel en ciberdefensa y ciberseguridad, el doctor Isaac Ben Israel, director del Centro interdisciplinario de investigación cibernética Blavatnit de la Universidad de Tel Aviv.

En la fotografía: Prof. Dr. Tcnel OIM Roberto Uzal (Director de la Maestría en Ciberdefensa y Ciberseguridad de la Universidad de BsAs), Dr. General de la FA de Israel Isaac Ben Israel, Lic. Alejandro Salomon (Director de la Escuela Nacional de Inteligencia), Especialista Tcnel OIM Carlos F. Amaya (Subdirector de la Maestría en Ciberseguridad de la Universidad de BsAs), Coronel OIM Alejandro Echazu (Profesor)
En la reunión mantenida por el Dr. Ben Israel con profesores y alumnos de la Maestría en Ciberdefensa y Ciberseguridad de la UBA, abierta a la posibilidad de encarar investigaciones, en un esquema cooperativo, en temas variados como "Ingeniería reversa de ciberarmas" y "Derecho Internacional y ciberconflictos". Lo que se presenta es una posibilidad para que la habitación maestra se posicione globalmente con ventajas y posibilidades, nuestras áreas, las necesidades de nuestro país.
https://www.lanacion.com.ar/2151449-de-los-lectores-cartas-mails