|  |  |  |
| --- | --- | --- |
| itu_logo | **Unión Internacional de Telecomunicaciones****Oficina de Normalización de las Telecomunicaciones** |  |

 Ginebra, 8 de junio de 2018

|  |  |  |
| --- | --- | --- |
| Ref.: | **Circular TSB 97**TSB Events/XY | – A las Administraciones de los Estados Miembros de la Unión;– A los Miembros de Sector del UIT‑T;– A los Asociados del UIT‑T;– A las Instituciones Académicas de la UIT |
| Contacto | **Xiaoya YANG** |
| Tel.: | +41 22 730 6206 |
| Fax: | +41 22 730 5853 |
| Correo-e: | tsbevents@itu.int | **Copia**:- A los Presidentes y Vicepresidentes de las Comisiones de Estudio del UIT-T;- Al Director de la Oficina de Desarrollo de las Telecomunicaciones;– Al Director de la Oficina de Radiocomunicaciones |

|  |  |
| --- | --- |
| Asunto: | **Taller de la UIT sobre ataques de ciberseguridad avanzados y programas de secuestro Ginebra (Suiza), 28 de agosto de 2018** |

Muy Señora mía/Muy Señor mío:

1 Deseo informarle que **el Taller de la UIT sobre ataques de ciberseguridad avanzados y programas de secuestro** tendrá lugar en la Sede de la UIT (Ginebra) el día 28 de agosto de 2018.

El Taller tendrá lugar durante la próxima reunión de la Comisión de Estudio 17 del UIT-T, que se celebrará del 29 de agosto al 7 de septiembre de 2018, en el mismo lugar de celebración.

Puede obtener más detalles de la reunión de la CE 17 del UIT-T en la dirección <http://itu.int/go/tsg17>.

La inscripción de los participantes para este Taller comenzará a las 08.30 horas en la entrada de Montbrillant. En las pantallas situadas en las puertas de entrada de la Sede de la UIT se dará información detallada sobre la sala de reunión.

2 El Taller se celebrará únicamente en inglés.

3 La participación en el Taller está abierta a los Estados Miembros, a los Miembros de Sector, a los Asociados y a las Instituciones Académicas de la UIT, y a cualquier persona de un país que sea miembro de la UIT y desee contribuir a los trabajos. Esto incluye a las personas que también sean miembros de organizaciones nacionales, regionales e internacionales. La participación en el Taller es gratuita, pero no se otorgarán becas para el Taller.

4 Los ataques de ciberseguridad avanzados se refiere a todas las modalidades de ataque sofisticadas, en especial los ataques dirigidos a objetivos concretos y los programas de secuestro (ransomware) que son algo más que un mero ciberdelito. Los ataques dirigidos a objetivos concretos (también llamados amenazas persistentes avanzadas (APA)) son ataques dirigidos a un blanco específico, a diferencia de las campañas indiscriminadas a gran escala. Aunque se sospecha que la mayoría de los ataques dirigidos a un objetivo concreto están patrocinados por estados, un número más reducido de casos son perpetrados por grupos de ataque privados. Su razón de ser es en la mayoría de los casos la recopilación de información sensible, la perturbación, el sabotaje o las ganancias financieras. Los programas de secuestro son un tipo de programas informáticos malignos (malware) que amenazan con divulgar los datos de la víctima o bloquear perpetuamente el acceso a los mismos salvo que se pague un rescate a los secuestradores. Los programas de secuestro son uno de los principales retos para la ciberseguridad en los últimos años. Hay más de 50 programas de secuestro diferentes, y cada uno de ellos presenta múltiples variantes. Quienes perpetran ataques con programas de secuestro suelen buscar únicamente dinero, a diferencia de otros programas malignos que básicamente roban su información u obtienen acceso no autorizado.

Los objetivos de este Taller son, entre otros:

• lograr un mejor conocimiento del panorama de los ataques de ciberseguridad avanzados y de los programas de secuestro;

• analizar la manera en que se llevan a cabo de los ataques de ciberseguridad avanzados y con los programas de secuestro;

• entender los riesgos de los ataques de ciberseguridad avanzados y de los programas de secuestro a los sistemas social, cultural y económico;

• identificar qué capacidades de seguridad organizativas o técnicas pueden evitar/combatir estos ataques;

• compartir entre los grupos e industrias pertinentes las actividades en curso destinadas a prevenir dichos ataques;

• determinar la manera en que las normas internacionales podrían ayudar a las organizaciones a adoptar las medidas necesarias; y

• discutir el camino que debería seguir la CE 17 para definir contramedidas para dichos ataques.

5 La información relativa a este Taller, incluido el proyecto de programa, estará disponible en el sitio web del evento, en la dirección: <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx>. Este sitio web se actualizará periódicamente a medida que se disponga de información nueva o modificada. Se ruega a los participantes que consulten regularmente el sitio web.

6 Los delegados disponen de instalaciones de red de área local inalámbrica en las zonas aledañas a las principales salas de conferencias de la UIT. En el sitio web del UIT-T figura información más detallada (<http://www.itu.int/ITU-T/edh/faqs-support.html>).

7 Varios hoteles de Ginebra ofrecen precios especiales para los delegados que asisten a reuniones de la UIT, y regalan un abono gratuito para los transportes públicos de la ciudad. Puede consultar una lista de esos hoteles, e información sobre cómo solicitar los descuentos, en la dirección: <http://www.itu.int/travel/>.

8 Para que la TSB pueda tomar las disposiciones necesarias sobre la organización del Taller, le agradecería que se inscribiese a la mayor brevedad posible a través del formulario en línea en la dirección <http://itu.int/reg/tmisc/3001087>, y **a más tardar el 22 de agosto de 2018**.**Le ruego que tenga presente que la preinscripción de los participantes en los talleres es obligatoria y se lleva a cabo** **exclusivamente *en línea*. El Taller es gratuito y está abierto a todos los interesados**.

9 Le recuerdo que los ciudadanos de algunos países necesitan un visado para poder entrar y efectuar una estadía en Suiza. **El visado debe solicitarse al menos cuatro (4) semanas antes de la fecha de inicio del Taller**, y obtenerse en la oficina (Embajada o Consulado) que representa a Suiza en su país, o, si no existiera dicha oficina en su país, en la que sea más cercana al país de salida.

Si un **Estado Miembro**, un **Miembro de Sector**, un **Asociado** o una **Institución Académica** **de la UIT** tropieza con problemas, y previa solicitud oficial de su parte a la TSB, la Unión puede intervenir ante las autoridades suizas competentes para facilitar la expedición de ese visado pero solamente durante el periodo mencionado de **cuatro** semanas. Toda solicitud al respecto debe formularse marcando la casilla correspondiente en el formulario a más tardar cuatro semanas antes del evento. Las preguntas deben remitirse a la Sección de Viajes de la UIT (travel@itu.int) con la mención "**Apoyo para el visado**".

Atentamente,

*(firmado)*

Chaesub Lee
Director de la Oficina de Normalización
de las Telecomunicaciones