|  |  |  |
| --- | --- | --- |
| itu_logo | **Union internationale des télécommunications**  **Bureau de la Normalisation des Télécommunications** |  |

Genève, le 8 juin 2018

|  |  |  |  |
| --- | --- | --- | --- |
| Réf.:  Contact:  Tél.: Fax: E-mail: | **Circulaire TSB 97**  Manifestations du TSB/XY  **Xiaoya Yang**  +41 22 730 6206 +41 22 730 5853 [tsbevents@itu.int](mailto:tsbevents@itu.int) | - Aux administrations des Etats Membres de l'Union;  - Aux Membres du Secteur de l'UIT-T;  - Aux Associés de l'UIT-T;  - Aux établissements universitaires participant aux travaux de l'UIT | |
|  |  | **Copie**:  - Aux Présidents et Vice-Présidents des Commissions d'études de l'UIT-T;  - Au Directeur du Bureau de développement des télécommunications;  - Au Directeur du Bureau des radiocommunications | |
| Objet: | **Atelier de l'UIT sur les attaques de cybersécurité avancées et sur les rançongiciels  (Genève (Suisse), 28 août 2018)** | |

Madame, Monsieur,

1 J'ai l'honneur de vous informer que **l'atelier de l'UIT sur les attaques de cybersécurité avancées et sur les rançongiciels** aura lieu à Genève, au siège de l'UIT, le 28 août 2018.

Cet atelier se déroulera pendant la prochaine réunion de la Commission d'études 17 de l'UIT-T, qui se tiendra du 29 août au 7 septembre 2018, au même endroit.

Pour plus de renseignements concernant la réunion de la CE 17 de l'UIT-T, veuillez consulter la page suivante: <http://itu.int/go/tsg17>.

L'enregistrement des participants à l'atelier débutera à 8 h 30 à l'entrée Montbrillant le jour de la manifestation. Les précisions relatives à la salle de réunion seront affichées sur les écrans placés aux entrées du siège de l'UIT.

2 Cet atelier aura lieu en anglais seulement.

3 La participation à l'atelier est ouverte aux Etats Membres, aux Membres de Secteur, aux Associés de l'UIT et aux établissements universitaires participant aux travaux de l'UIT, ainsi qu'à toute personne issue d'un pays Membre de l'UIT qui souhaite contribuer aux travaux. Il peut s'agir de personnes qui sont aussi membres d'organisations internationales, régionales ou nationales. La participation à l'atelier est gratuite mais aucune bourse ne sera accordée pour l'atelier.

4 Les attaques de cybersécurité avancées renvoient à toutes les formes d'attaques élaborées, en particulier les attaques ciblées, ainsi qu'aux rançongiciels, qui dépassent le simple cadre de la cybercriminalité. Les attaques ciblées (aussi connues sous le nom de menaces persistantes avancées) visent une cible précise, au contraire des campagnes diffusées à grande échelle et à l'aveugle. Si la plupart des attaques ciblées sont soupçonnées d'être lancées avec l'aide des Etats, quelques cas sont l'oeuvre de groupes de cyberattaquants privés qui agissent principalement pour les motifs suivants: collecte de renseignements, perturbation, sabotage ou obtention de sommes d'argent. Le rançongiciel est un type de logiciel malveillant, c'est-à-dire un logiciel qui menace de publier les données concernant la victime, ou de bloquer l'accès à ces données de manière permanente jusqu'au versement d'une rançon aux attaquants. Depuis quelques années, les rançongiciels constituent l'un des principaux défis à relever en matière de cybersécurité. Il en existe plus de 50 différents, et chacun d'entre eux possède de multiples variantes. En règle générale, le but du rançongiciel est seulement de faire gagner de l'argent à son auteur, au contraire d'autres logiciels malveillants, qui visent principalement à voler vos renseignements ou à y accéder sans autorisation.

Les objectifs de cet atelier sont, sans que cette liste soit exhaustive, les suivants:

• mieux comprendre les attaques de cybersécurité avancées et la situation en matière de rançongiciels;

• analyser la manière dont les attaques de cybersécurité et les attaques par rançongiciel sont menées;

• comprendre les risques que posent les attaques de cybersécurité avancées et les attaques par rançongiciel pour les systèmes sociaux, culturels et économiques;

• identifier les capacités de sécurité organisationnelles ou techniques pour prévenir/combattre ces attaques;

• échanger au sujet des activités actuellement menées par les groupes et les secteurs d'activité concernés afin de prévenir de telles attaques;

• déterminer comment les normes internationales pourraient aider les organisations à prendre les mesures nécessaires; et

• examiner les activités que la CE 17 devrait entreprendre pour identifier les mesures de protection contre de telles attaques.

5 Des informations relatives à l'atelier, et notamment le projet de programme, seront disponibles sur le site web de la manifestation à l'adresse suivante: <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx>. Ce site web sera actualisé à mesure que parviendront des informations nouvelles ou modifiées. Les participants sont priés de consulter régulièrement le site pour prendre connaissance des dernières informations.

6 Des équipements de réseau local sans fil sont à la disposition des délégués dans les principaux espaces de conférence de l'UIT. Des informations détaillées sont disponibles sur le site web de l'UIT-T (<http://www.itu.int/ITU-T/edh/faqs-support.html>).

7 Un certain nombre d'hôtels à Genève offrent des tarifs préférentiels aux délégués assistant aux réunions de l'UIT et leur fournissent une carte permettant d'emprunter gratuitement les transports publics à Genève. Vous trouverez la liste des hôtels participants, et les modalités à suivre pour obtenir un tarif réduit, à l'adresse: [http://itu.int/travel/](https://www.itu.int/net4/travel/index-fr.aspx).

8 Afin de permettre au TSB de prendre les dispositions nécessaires concernant l'organisation de l'atelier, je vous saurais gré de bien vouloir vous inscrire au moyen du formulaire en ligne disponible à l'adresse: <http://itu.int/reg/tmisc/3001087> dès que possible et **au plus tard le 22 août 2018.** **Veuillez noter que l'inscription préalable des participants aux ateliers est obligatoire et se fait exclusivement en ligne. Cet atelier est gratuit et ouvert à tous.**

9 Nous vous rappelons que, pour les ressortissants de certains pays, l'entrée et le séjour, quelle qu'en soit la durée, sur le territoire de la Suisse sont soumis à l'obtention d'un visa. **Ce visa doit être demandé au moins quatre (4) semaines avant la date de début de l'atelier** et obtenu auprès de la représentation de la Suisse (ambassade ou consulat) dans votre pays ou, à défaut, dans le pays le plus proche de votre pays de départ.

En cas de problème pour des Etats **Membres, des Membres de Secteur et des Associés de l'UIT ou des établissements universitaires participant aux travaux de l'UIT**, et sur demande officielle de leur part au TSB, l'Union peut intervenir auprès des autorités suisses compétentes pour faciliter l'émission du visa, mais uniquement pendant la période de quatre semaines susmentionnée. Les demandes doivent être effectuées en cochant la case correspondante du formulaire d'inscription, au plus tard **quatre** semaines avant la date de la manifestation. Elles doivent être envoyées à la Section des voyages de l'UIT ([travel@itu.int](mailto:travel@itu.int)), avec la mention "**assistance pour le visa**".

Veuillez agréer, Madame, Monsieur, l'assurance de ma considération distinguée.

(*signé*)

Chaesub Lee  
Directeur du Bureau de la  
normalisation des télécommunications