INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

COM 17 – LS 303 – E

English only

Original: English

Question(s): 6/17 Geneva, 20 February - 2 March 2012

Ref. : TD 2663 Rev.4

Source: ITU-T SG 17 (Geneva, 20 February - 2 March 2012)

Title: LS on the management of infected terminals in mobile networks

LIAISON STATEMENT

For action to: GSMA, IETF Security area

For comment to:

For information to:

Approval: Agreed to at ITU-T Study Group 17 meeting

Deadline: 20 August 2012

Contact: Yutaka Miyake
Associate rapporteur of Question 6/17
Tel: +81 49 278 7367
Fax: +81 49 278 7510
Email: yu-miyake@kddi.com

ITU-T Study Group 17 Question 6 on "Security aspects of ubiquitous telecommunication services" is pleased to inform you that we have started a new work item (X.msec-7) on the management of infected terminals in mobile networks. We also agreed to proceed with checking other organization's activities related to this work item. The scope of this new work item is defined as follows:

> This Recommendation provides guidelines to manage infected terminals by utilizing technologies in the mobile networks. Within the scope of this Recommendation, the following topics are addressed:
>
> - Classification and effects of malicious software in mobile networks
> - Framework and process to manage the infected terminals on the network-side
> - Management measures and corresponding technologies during various phases, including discovery, governing and informing

Draft Recommendation ITU-T X.msec-7 is to mitigate the vicious effects caused by the terminals after they are infected in mobile networks. X.msec-7 plans to guide mobile operators in managing the infected terminals by utilizing technologies in the mobile network through processes of discovery, governing and informing.

- Discovery: including sample collection and recognition; to discover the infected mobile terminals and new malicious software.

- Governing: including restriction and prevention; to limit the capability of the (suspiciously) infected terminals, to disable part or full functions of the infected terminals on the network-side, and to isolate the malicious sources (i.e. phishing websites).
- Informing: including customer service and information share; to inform and assist customers to fix or overcome the problem and to share the statistics and the trends with co-operation organizations and authorities.

The intention of this liaison is to learn about the existing activities regarding management of infected terminals and seek advice for this work item.

ITU-T Study Group 17 Question 6 would appreciate your feedback in this regard, and is looking forward to further collaboration on this new work item.