

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1213

(09/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Security capability requirements for countering smartphone-based botnets

Recommendation ITU-T X.1213

ITU-T

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1213

Security capability requirements for countering smartphone-based botnets

Summary

Recommendation ITU-T X.1213 analyses the background and potential security threats of smartphone-based botnets, and provides security capability requirements.

Along with the rapid development of mobile Internet devices and the widespread use of smartphones, surveys from worldwide organizations show that botnets, formerly targeting mostly personal computer (PC)-based networks, are now being replicated very quickly on smartphones. Currently, countries and regions with differing conditions and ecosystems have varying levels of constraints on the propagation of smartphone-based botnets. Analytical reports from various security companies and investigative organizations show noticeably different statistical data on the severity of the propagation of smartphone-based botnets. The potential threat of smartphone-based botnets is increasing very quickly in some regions and could possibly spread worldwide and turn from a regional issue into a serious global issue.

Compared with PCs and servers, smartphones have less processing power, storage space and battery life. However, the adversarial influence of smartphone-based botnets could have greater repercussions on users for the following reasons: 1) smartphones often store very important personally identifiable information (PII) and 2) if attacks on smartphones or on the operator's infrastructure occur, user experience may degrade significantly due to the prevalence of, and user dependence on, smartphones.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1213	2017-09-06	17	11.1002/1000/13261

Keywords

Botnet, command and control (C&C), malware, personally identifiable information (PII), smartphone.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	Background.....	2
	6.1 Overview of security considerations	3
	6.2 The evolution of botnet threats on smartphones.....	3
	6.3 Protection for smartphones.....	3
7	Characteristics of smartphone-based botnets.....	4
	7.1 Personally identifiable information on bots	4
	7.2 Various means of propagation.....	4
	7.3 Openness.....	4
	7.4 Targeted infection.....	4
	7.5 Concealment	5
	7.6 Commercial interests	5
	7.7 Ever-changing network connections	5
8	Security threats	5
	8.1 Personally identifiable information disclosure	5
	8.2 Malicious fee deductions	6
	8.3 Rogue behaviours	6
	8.4 Performance consumption	7
	8.5 Malicious transmission.....	7
	8.6 Loss of credibility.....	7
9	Security capability requirements	7
	9.1 Network security capability requirements.....	7
	9.2 Smartphones security capability requirements.....	9
	Appendix I – Malware connecting to botnet.....	11
	I.1 Foreword.....	11
	I.2 Background.....	11
	I.3 Macroscopic environment in China.....	12
	I.4 iPhone problems	12
	I.5 Examples and some trends of new malware.....	13
	I.6 Conclusion.....	14
	Bibliography.....	15

Recommendation ITU-T X.1213

Security capability requirements for countering smartphone-based botnets

1 Scope

This Recommendation aims to provide security capability requirements for countering smartphone-based botnets. The intent of this Recommendation is to study the challenges presented by smartphone-based botnets, and their specific threats to, and requirements on, operators' networks as well as on the smartphones themselves. This Recommendation focuses on threat analysis and requirement enumeration. The purpose is to safeguard operators' infrastructures and smartphones, ensure operators' services and service qualities, and to enhance user experience. Detailed technical solutions, and other intelligent terminals such as tablet devices are beyond the scope of this Recommendation.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 bot [b-ITU-T X-Sup.8]: An automated software program used to carry out specific tasks designed for malicious purposes. It is interchangeable with a robot.

3.1.2 botmaster [b-ITU-T X-Sup.8]: An individual responsible for controlling and maintaining a botnet.

3.1.3 botnet [b-ITU-T X-Sup.8]: Remotely controlled malicious software robots (bots) that are run autonomously or automatically on compromised computers together with a command-and-control server owned by botmasters.

3.1.4 personally identifiable information (PII) [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G	Second Generation of mobile telecommunication
2FA	Two Factor Authentication
3G	Third Generation of mobile telecommunication
4G	Fourth Generation of mobile telecommunication
API	Application Programming Interface
C&C	Command and Control

CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name System
GPS	Global Positioning System
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
MITM	Man-in-the-Middle
MMS	Multimedia Messaging Service
NFC	Near Field Communication
OTP	One-Time Passcode
P2P	Peer-to-Peer
PC	Personal Computer
PII	Personally Identifiable Information
PNG	Portable Network Graphic
QoS	Quality of Service
QRcode	Quick Response code
SIM	Subscriber Identity Module
SMS	Short Message Service
USB	Universal Serial Bus
WiFi	Wireless Fidelity

5 Conventions

None.

6 Background

Along with the rapid development of mobile Internet devices, mobile terminals are becoming more intelligent with higher performance capabilities. In this Recommendation, the term smartphone refers to the type of mobile phone with the following characteristics:

- an independent operating system;
- an ability to continuously expand the functions and capabilities of the phone via the installation of third-party applications;
- wireless network access capability including the capability to access mobile Internet through a mobile operator's communication network.

In recent years, the population of smartphone users has continued to rapidly grow. While providing convenience to people's lives, security threats to smartphones are also increasing.