International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 9
(09/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1205 – Supplement on guidelines for reducing malware in ICT networks

ITU-T X-series Recommendations – Supplement 9

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	
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	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	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
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

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

Supplement 9 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on guidelines for reducing malware in ICT networks

Summary

This supplement to Recommendation ITU-T X.1205 provides guidelines that can be utilized by end users to reduce malware in information and communication technology (ICT) networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 9	2011-09-02	17

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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/.

Table of Contents

Introduction

Malware is the general term for various types of software instances intended to, or exhibiting characteristics that can, harm or threaten computers or computer systems. Malware includes viruses, worms, spyware, trojans, bots, etc. As it has become more complex, the distinctions among these types have tended to disappear. Indeed, malware types today may be polymorphic – that is, they adapt and evolve as they propagate.

Incidents of malware infection and related damage are increasing exponentially due in part to the proliferation of ICT end-user devices and application software that are autonomously connected to open network infrastructures worldwide. This damage can include excessive network traffic, reduced available bandwidth, loss of sensitive data, lost end-user device resources, and loss of end-user confidence. Malware has also become a major means of undertaking cybercrime, and is produced as part of criminal enterprise. As a result, malware constitutes a major threat to ICT networks and services.

Malware mitigation is increasingly difficult to accomplish, even by expert end users. New techniques – particularly automated ones implemented through continuous security monitoring platforms – are beginning to leverage new capabilities for sharing malware analysis and heuristics information. Malware Attribute Enumeration and Characterization, as described in [b-MAEC], is one of the most prominent of these capabilities and included as part of [b-ITU-T X.1500]. End-user awareness and behaviour can also mitigate malware propagation and important measures are included in this supplement.

Supplement 9 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on guidelines for reducing malware in ICT networks

1 Scope

This supplement provides guidelines for end users to reduce malware in ICT networks, including propagation in end-user devices, applications, and external and portable devices. These guidelines can be implemented manually or through automated techniques for cybersecurity information exchange described in [b-ITU-T X.1500].

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 bot [b-ITU-T X.1244]: Bot is a contraction of "robot", which is a program that operates as an agent for a user or another program to simulate a human activity.

3.1.2 certificate [b-ITU-T X.1252]: A set of security-relevant data issued by a security authority or a trusted third party, which, together with security information, is used to provide the integrity and data origin authentication services for the data.

3.1.3 firewall [b-ITU-T X.1205]: A system or combination of systems that enforces a boundary between two or more networks. A gateway that limits access between networks in accordance with local security policy.

3.1.4 P2P communications [b-ITU-T X.1161]: Communications on P2P network, whereby each peer communicates with another peer directly for sharing information, resources, etc.

3.2 Terms defined in this supplement

This supplement defines the following terms:

3.2.1 end-user device (EUD): A network-attached terminal generally under the control of a network subscriber, whether hardware or software based, mobile and/or stationary, and including personal computer (PC)s, multimedia terminals, and mobile phones.

3.2.2 end-user firewall: A software application running on a single machine, and protecting network traffic into and out of that machine to permit or deny communications based on an end-user-defined security policy.

3.2.3 instant messaging: A real-time communication service between two or more users, generally via the network, which enables the sending of messages and files to other users.

3.2.4 malware: Software instances intended to, or exhibiting characteristics that harm or threaten computers or computer systems.

3.2.5 service set identifier (SSID): A name that identifies a particular wireless access point.

3.2.6 smartphone: A mobile phone that offers more advanced computing ability and connectivity than a contemporary feature phone.

NOTE – Smartphones and feature phones are handheld computers integrated with a mobile telephone.

4 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

EUD	End-User Device
HDD	Hard Disk Drive
ICT	Information and Communication Technology
ID	IDentification or IDentifier
LAN	Local Area Network
OS	Operating System
P2P	Peer-to-Peer
PC	Personal Computer
PDA	Personal Digital Assistant
SSID	Service Set IDentifier
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
WLAN	Wireless LAN

5 Conventions

None.

6 Guidelines for reducing malware in ICT networks

6.1 Mitigation in end-user platforms

6.1.1 Software management

End users today are enabled to install many types of software on their devices. However, the software, including updates, can be used to propagate hidden malware. Users should manually, or by automatic means:

– use software provided (and, ideally, signed using strong certificates) by reputable vendors

– keep all software on the end-user device up-to-date

– enable software security updates to run automatically with user review

– understand and use security options

– watch continuously for threats manifested by installed software.

6.1.2 Anti-malware product installation and management

Anti-malware products for specific end-user devices or platforms are important for detecting and responding to malware. Users should manually, or by automatic means:

– use compatible anti-malware products (and, ideally, signed using strong certificates) by reputable vendors

– use anti-malware software regularly to run a full scan on end-user devices

– keep the anti-malware software and signatures current

- install or enable an end-user firewall, and configure it to filter traffic coming into and leaving end-user devices.

6.1.3 Operating-system management

An operating system (OS) is software, consisting of programs and data, that runs end-user devices, manages the EUD hardware resources, and provides common services for the execution of various application software. Careless OS account management may allow an attacker to use a device in a way that leads to leakage of sensitive information and propagation of malware. Consequently, appropriate OS management is very important for reducing malware propagation. Users should manually, or by automatic means:

- create strong passwords – especially for administrator or root accounts
- frequently change account password.

6.1.4 WLAN configuration

Wireless LANs are vulnerable to attacks and misuse if their access points/routers are not properly configured. Users should manually or by automatic means:

- use a strong password for the WLAN access point administrator password
- restrict WLAN access by using strong encryption and passwords
- use a firewall in the WLAN router.

6.2 Mitigation in applications

6.2.1 E-mail, including instant messaging

E-mail is a common means for transferring files together with messages. However, malware can be propagated through such files. Propagation may also occur via a linked file or link address. Malware may propagate more widely by sending itself to another e-mail address stored in the infected end-user device using e-mail addresses generated from user contact lists. Users should manually, or by automatic means:

- select strong e-mail security settings
- be wary of unsolicited attachments, even from people known to them
- be wary of clicking on unknown URLs
- save and check any attachments using anti-malware software before opening them
- turn off options for automatically downloading attachments.

6.2.2 File sharing

File sharing involves using technology that allows networked users to share files on end-user devices. Peer-to-peer (P2P) applications, such as those used to share music files, are some of the most common forms of file-sharing technology. However, P2P applications can be used as a means for propagating malware. Users should manually, or by automatic means:

- disable file-sharing when not using it
- save and check downloaded files for malware before opening them.

6.2.3 Web

A web browser is an application that finds and displays web pages. To increase functionality or add design embellishments, web sites often rely on scripts that execute programs within the web browser. This active content can be used to create splash pages or options like drop-down menus. These scripts are often used as a way for attackers to download or execute malware on an end-user device. Secure usage and management of the web browser is important for preventing devices from being infected with malware. Users should manually, or by automatic means:

- check a web site's certificate, favouring extended validation certificates that offer far greater assurance levels that the site is genuine
- use web TLS capabilities by typing in "https:" followed by the URL, or verifying that the https exists as the URL prefix, when additional security is desired as, for instance, in the case of financial transactions, conveying of sensitive information, or downloading software
- keep the browser application software and security patches up-to-date
- not use predictive text input for ID and password
- remove temporary files periodically
- delete the browser cookies periodically
- not use automatic login
- be wary of clicking on unknown URLs and avoid access to web sites that are not familiar or trusted
- not click and download unidentified files and programs
- scan downloaded files for malware, as for any software.

6.3 Mitigation in external and portable devices

6.3.1 USB-based memory devices

USB memory devices are popular as a convenient means for physically transferring files. However, these devices can be used to propagate malware. Users should manually, or by automatic means:

- enable device USB security features
- not use unknown USB memory devices, and employ anti-malware products to check any new device
- ensure that USB memory device auto running functions are disabled.

6.3.2 Cell phones, smartphones, and networked personal digital assistant (PDA) devices

Most contemporary cell phones and PDAs have wireless packet data capabilities. Smartphones are end-user devices with the characteristics of both a mobile phone and a portable computer, with access to one or more packet data services via either the mobile phone service provider or a WLAN. Like a portable computer, these devices, operating systems, and applications may be subject to the same malware-based threats as any networked computer device, and all the above guidelines apply.

6.3.3 Bluetooth terminals

Bluetooth is a widely available end-user device wireless technology. Malware can be introduced locally through Bluetooth access ports. In general, Bluetooth ports should be operated in hidden mode and disabled when not in use.

Bibliography

[b-ITU-T X.1161] Recommendation ITU-T X.1161 (2008), *Framework for secure peer-to-peer communications.*

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications.*

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange.*

[b-MAEC] Malware Attribute Enumeration and Characterization, <http://maec.mitre.org>.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012