International Telecommunication Union

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 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 legder 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/.

Table of Contents

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.

6.1 Overview of security considerations

Considering the rapidly growing population of smartphone users, smartphone-based botnets must be effectively suppressed and controlled to prevent them from becoming a significant factor that influences societal stability and threatens public security.

For mobile operators, large-scale botnets could severely impair the effective utilization of the operators' network and lower the quality of service (QoS) provided to users, thus leading to user dissatisfaction and loss of subscribers. For users, whose smartphones are hacked and controlled via botnets, their potential loss can be significant as much of their most important personally identifiable information (PII), such as contact lists and online payment information, is often stored on their smartphones.

Therefore, the work of countering smartphone-based botnets is both forward-looking and practical. Operators should increase their security awareness in this field to: suppress the rapid growth of botnets, decrease the loss of subscribers, and reduce user complaints, etc.

6.2 The evolution of botnet threats on smartphones

The emergence of smartphone viruses can be traced back to 2004 when *Cabir*, the first smartphone-based worm, was discovered. In 2009, the malware *iKee.B* began to possess botnet characteristics and could take control of infected iPhones and send back a user's PII to the bot master. In 2011, a representative mobile botnet, *Android.Geinimi*, was found. It could conceal communication methods, had abundant attack modules and was considered highly harmful.

The widespread use of smartphones has been accompanied by extraordinary growth in smartphone-based malware, which mostly use certain smartphone functions as a propagation medium. After being downloaded and installed on a smartphone, malware will frequently and secretly, display advertisements, induce extra smartphone traffic, and deduct fees, etc., causing losses to smartphone users. Moreover, smartphone users may also encounter issues such as: being directed to phishing websites, having their smartphone infected by viruses or Trojans, disclosing or stealing their contact lists and/or address books, or stealing accounts and passwords. Of these crimes, disclosure of PII, personal accounts and passwords happens most frequently.

In recent years, smartphone malware has grown exponentially. Malware is the main cause of botnet virus propagation as an increasingly larger proportion of malware uses remote-controlled backdoor methods or functions, which are a distinctive feature of smartphone-based bots. The primary purpose of botmasters is to reap profits from PII theft and malicious fee deductions. Currently, the most common malware includes: PII theft, malicious fee deduction, rogue behaviour, performance deterioration and malicious propagation.

6.3 Protection for smartphones

Harassing calls, short message service (SMS) spam, and other security events resulting from web browsing, file downloading, mobile payment, etc., are the main security issues facing smartphone users. These threats are mainly mitigated by security software installed on smartphones.

The two main functions of smartphone security software are phone management and security protection. The phone management function includes memory clean-up, standby time extension, automatic-booting program management, SMS management, phone number management, etc. The purpose of the phone management function is to make the smartphone run more smoothly and to improve device usage efficiency. The security protection function mainly includes data traffic monitoring, blocking harassing calls, regular scanning, regular deletion of viruses, etc. The purpose of the security protection function is to protect smartphones from security threats.

The installation of security software could help protect smartphones from certain botnets and malware at the user terminal side, but as the skills of smartphone attackers improve and their attacking approaches diversify, smartphones will continue to face increasing security threats. Along with boosting security protection at the terminal side, operators also need to provide more security protection at the network side. The coordination and cooperation of both sides will greatly enhance the capability of smartphones to withstand attacks from botnets.

7 Characteristics of smartphone-based botnets

The characteristics of smartphones and mobile networks are being exploited by smartphone-based botnets that use the Internet to spread malware on a large scale. By analyzing the characteristics of smartphones and mobile networks, as well as the purpose of botmaster attacks, the characteristics of smartphone-based botnets could be summarized and potential security threats can be recognized.

7.1 Personally identifiable information on bots

Smartphone-based botnets are comprised of a large number of smartphone-based bots. Unlike traditional personal computers (PCs), much PII and privacy information is centrally stored on smartphones, making smartphone-based botnets a greater threat to smartphone users who could suffer a great amount of data loss.

The functions integrated by smartphones include: personal information management, schedule and agenda, diary, task arrangements, multimedia applications, webpage browsing, etc. The abundance of personal information stored in smartphone applications make smartphones a primary target of attackers. Moreover, a smartphone's global positioning system (GPS) enables the acquisition of user location information which is another type of PII. Once this information is acquired by attackers, a user's PII could be disclosed.

7.2 Various means of propagation

First, smartphone-based botnets could maliciously spread through infected applications which users typically find and download from app stores or mobile phone forums that do not require secure authentication.

Second, smartphone-based botnets could spread through Bluetooth, wireless fidelity (WiFi), universal serial bus (USB) and other peripheral interfaces of smartphones.

Third, smartphone-based botnets could spread through hypertext transfer protocol (HTTP), SMS, multimedia messaging service (MMS), quick response code (QRcode), etc.

Various propagation media make smartphone-based botnets relatively easy to spread, which correspondingly places higher demands on security protections.

7.3 Openness

Open mobile operating systems provide smartphones with a great number of application program choices, but at the same time these programs also expose smartphones to more potential threats and hackers. The openness allows hackers to embed viruses or Trojans into extended applications, facilitating easier propagation of smartphone-based botnets.

Smartphones have multiple types of peripheral interfaces including: Bluetooth, near field communication (NFC) and USB. Any of these peripheral interface connections could be utilized by attackers. Moreover, smartphones generally support second, third, or fourth generation (2G, 3G or 4G) of mobile network access as well as WiFi access, through which users can access the Internet. These functions have unique application and commercial value, but also provide many attacking channels to attackers.

7.4 Targeted infection

Smartphone-based botnets usually aim at certain types of targets, infecting them through direct copying or by tricking users into downloading malware or Trojans. Attackers can also target smartphones that run the same operating systems for infection. This method greatly increases the efficiency of the attack while at the same time decreasing the cost of the attack.

7.5 Concealment

Smartphone-based botnets are becoming more complex. Some botnets are capable of concealing their attacking behaviours by deleting all traces of installation after successfully infecting a smartphone. Some botnets can erase their network connection and outbox traces after they send the user's PII via Internet access. Others can even order customized services from specific service providers and automatically block verification messages from mobile operators.

Some smartphone Trojans and malware, which steal PII or cause malicious fee deductions, do not launch their attacks immediately after they have been successfully installed. Instead, they will launch attacks according to the time periods set by the malware or by utilizing the idle times of the infected smartphones.

Today, a larger and larger proportion of malware have remote-controlled backdoors as a basic function, which is one of the distinctive features of smartphone-based bots.

Many botnets propagate through malicious programs embedded in popular mobile applications. When a user downloads and installs applications from app stores or mobile phone forums without secure authentication mechanisms, the malicious programs concealed in the applications will be triggered.

7.6 Commercial interests

Unlike most traditional malware, whose purpose is to sabotage, the purpose of smartphone-based botnets is often profit-driven. For example, smartphone-based botnets profit from stealing a user's PII or from initiating malicious fee deductions; thus forming a dark industry of Internet fraud. Commercial profits are motivating attackers to invest more resources into developing smartphone-based botnets and promoting the development of an Internet fraud industry. This means that smartphone-based botnets will create more security threats to users, and it will be increasingly difficult to protect against such threats.

7.7 Ever-changing network connections

The high-mobility characteristics of smartphones lead to ever-changing network connections, which results in increased variability of smartphone-based botnets. Smartphones may roam not only between networks using the same networking technologies, but also between networks using different networking technologies, e.g., from a 3G network to a WiFi hotspot. Hence, compromised smartphone bots may need to change their communication channel with the command and control (C&C) server more frequently than PC-based bots. This leads to additional complexity in detecting smartphone-based botnets through identifying their communication channels.

8 Security threats

8.1 Personally identifiable information disclosure

– Subscriber identity module (SIM) card information:

  Once a smartphone becomes infected with a bot, botmasters could steal the user's phone card information including phone registration information, hardware configuration parameters, etc. Botmasters can generate greater financial gains by selling or disclosing this PII. Of greater concern is that botmasters may launch more dangerous attacks on smartphones with the same configurations by analysing the vulnerabilities of these phones.

– Phone storage:

  The botmasters of smartphone-based botnets can use the cloud to implement remote control of all their bots. In this way, botmasters can steal from the bot: a user's PII including their phone number, contact list, call logs, e-mails, location information, photos and videos, etc. Botmasters can instruct bots to upload this information to remote servers.

– Bank accounts and passwords:

  When a user makes a payment via a smartphone, attackers may be able to acquire full control of the user's smartphone by utilizing its vulnerabilities, and can then steal the user's bank accounts and passwords. Furthermore, attackers can intercept the SMS verification code and initiate malicious money transfers, and at the same time erase any trace of the attack. In this way attackers can steal money easily, without being perceived by the smartphone user.

– Application accounts and passwords:

  By the same means, attackers can steal a user's accounts and passwords for applications. They may utilize this information to commit further fraud and generate profits accordingly.

8.2 Malicious fee deductions

– Automatic download or deletion of software:

  Once a smartphone is controlled by a bot, it will receive instructions issued by a C&C server, and the botmaster can instruct the phone to do almost anything. As instructed by the botmaster, the smartphone may automatically download unnecessary applications, or it may uninstall specified applications. These behaviours may lead to increased data traffic consumption charges and result in financial loss to the user.

– SMS spam:

  Some malware can instruct smartphones to send SMS spam using the smartphone's contact list. First, an attacker tricks the user into downloading and installing malware, then once infected the smartphone will automatically contact the C&C servers for instructions. After receiving SMS spam instructions, the smartphone will send SMS spam messages according to the phone's contact list, resulting in a performance drop and malicious fee deductions billed for Internet access and SMS messaging. Frequent SMS spam may jam mobile channels, leading to a performance drop in, and unavailability of the smartphone. Moreover, if a compromised smartphone belongs to a certain company or public institution, the company's reputation may be undermined as the contact list stored in the smartphone may contain important business partners or government contacts. Upon frequent reception of SMS spam, from the infected smartphone, the smartphone number may be added to the recipients' blacklists leading to unpredictable financial loss and damage to business cooperation.

8.3 Rogue behaviours

– Distributed denial of service (DDoS) attacks:

  Along with the widespread use of smartphones and the rapid growth of mobile Internet applications, botmasters may launch DDoS attacks if the number of controlled bots is very large. Botmasters may control a large number of infected smartphones and can launch simultaneous attacks at a specific website, leading to failures of web servers. Specially, if the compromised smartphones belong to certain companies or public institutions, their reputation might be considerably undermined as the contact lists stored in these smartphones probably contains important business partners or government contacts. Upon detection of a DDoS attack, the target will respond by blocking the attackers' phone numbers which may also lead to unpredictable financial loss and damage to business relationships.

– Malicious advertisement deception:

  An infected smartphone may be turned into a spam advertisement receiver. Users may receive various advertisements and each click will generate revenue to the botnet. In this way, botmasters amass huge profits from fraudulent advertisement fees. However, the advertisement is not actually clicked on by the smartphone user, but rather by the malicious bot installed on the smartphone.

– Unauthorized access to the enterprise network:

  Smartphone-based botnets can allow attackers to gain access to secure enterprise networks via infected network devices. An infected device can analyse the vulnerability of hosts in the enterprise network and report back to the botmaster. Attackers may further exploit this vulnerability to attack hosts in the enterprise network and steal confidential information.

8.4 Performance consumption

Botmasters may induce performance drops in smartphones via the following ways:

– Virus components may be disguised as portable network graphic (PNG) images, whereas in reality they are automated scripts. After infection, the virus will be loaded automatically when the smartphone starts up, and will persistently run in the background, leading to a grave performance drop in the operating system;
– Frequently connecting to Trojan servers for instructions, will lead to persistent damage to the smartphone;
– Automatically downloading spam applications in the background, will result in battery consumption and a grave performance drop in a short period of time;
– Botmasters persistently send SMS spam to infected smartphones causing the smartphone to no longer operate and the battery to be completely drained.

8.5 Malicious transmission

Certain malware can download applications to an infected smartphone, in the background, without a user's permission, and can later pop-up fraudulent messages, tricking the user into touching the screen and thus causing installation of the malware. Once the application is installed, it will access a specific website in the background to boost its download ranking, thus deceiving more users into downloading the malicious applications. In this way, the scale of the botnet is expanded, and the attackers gain more profits.

8.6 Loss of credibility

Botnet-infected smartphones could be used to send spam e-mails or participate in DDoS attacks; these behaviours not only increase network costs and battery consumption, but also lead to loss of user credibility. For example, when a botnet-infected smartphone sends bulk spam messages or e-mails to contacts stored in the smartphone, the sender (smartphone owner) will lose credibility. In particular, if the compromised smartphone belongs to a certain company or public institution, the loss may be much greater, as the contacts stored in these smartphones probably contain important business or government partners.

9 Security capability requirements

9.1 Network security capability requirements

9.1.1 Network traffic monitoring

Operators should offer the ability to monitor a smartphone's Internet traffic. They could establish a traffic monitoring mechanism or a table containing all users, and intelligently analyse a smartphone's Internet traffic. When abnormal traffic is detected, operators could immediately forward an alarm or relevant information to a user, and if necessary intercept the suspicious traffic.

9.1.2 Mobile malicious code detection

The security protection devices in an operator's network should detect and analyse malicious code in its applications. If malicious code is detected in an application, the operator could forward an alarm or relevant information, in a timely manner, to users who are downloading or using the application.

9.1.3 Encrypted transmission of sensitive information

An operator's network should support the encrypted transmission of information sent by smartphones. After smartphone users turn on this function, the operator's network devices should guarantee the integrity and confidentiality of the transmitted information, including contact lists, locations, accounts and passwords, etc.

9.1.4 Use of a honeypot network

An operator's network should set up a honeypot computer system to act as a decoy to lure botnets and malicious programs into accessing the smartphone. After detecting the botnets and gathering their controlling information, the operators could apply observation and tracing to learn how to better protect smartphones.

9.1.5 Protection from DDoS attack

– The security protection devices and domain name system (DNS) servers in an operator's network should be able to provide security policy configuration which could prevent hosts of botnets from connecting to their controllers.
– Firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs) and other security protection devices in an operator's network should be able to provide security policy configurations which block traffic attacks.
– The network and security protection devices in an operator's network should be able to provide DDoS traffic-blocking policy configurations which should block the target server's DDoS traffic in other domains.

9.1.6 Detection of botnets

The security protection devices in an operator's network should be able to detect the mutation of botnets and collect and share the global credit of Internet protocol (IP) addresses, thus an IP address credit database of botnet controllers and hosts could be established to provide malicious traffic filtering, analysis of bot actions, IP address credit mechanisms and other protection methods.

9.1.7 Detection and disposition of SMS spam

An operator's network should have the mechanisms for detecting and disposing of SMS spam. When a mobile terminal that receives a great amount of spam messages is observed, timely blocking of the spam should be provided to prevent a collapse caused by the reception of mass spam messages. During detection, operators should be able to inform users so that they can apply relevant measures to handle this condition.

9.1.8 Blacklist and whitelist mechanism

Security protection devices in an operator's network should have the ability to add malware, malicious codes, and malicious websites to its blacklists. If botnet controllers request their controlled hosts to connect to a malicious website or to download malware, which is part of a blacklist, the security protection devices should be able to block these connections in a timely manner.

Accordingly, the security protection devices in an operator's network should also offer a whitelist mechanism. On some special conditions, users are allowed to connect to trusted websites and to download trusted applications which are part of a whitelist.

9.1.9 Cooperation ability

To improve the integrity and credibility of security software, operators should be able to cooperate with smartphone security product providers. Through this cooperation mechanism, security protection against botnets could be accomplished on both the network and mobile-terminal sides.

Moreover, operators should also cooperate with governmental and administrative departments. If a smartphone becomes a bot, operators should inform the smartphone's owner through administrative departments. Furthermore, to stop smartphone-based botnets and their malicious behaviours, operators should cooperate with governmental and administrative departments to develop appropriate courses of action and legislation.

9.1.10 Assurance of identity

If a user's (especially a group of users) smartphone is compromised and begins to send group spam messages, etc., this may cause the user to lose the trust of the spam recipients. If the infected smartphones belongs to certain companies or public institutions, the loss may be much greater as their contact lists probably contain important business partners or government institutions.

In order to avoid this loss of trust, operators should have the capability to assure the identity of a smartphone user (especially for group users) when abnormal operations, such as group messaging, are detected. For example, an operator should be able to detect a user's group messaging operations, and based on predefined policies, choose to inform them via messaging, or temporarily suspending the group messaging operation and asking for the user's confirmation before the user proceeds with the operation.

9.2 Smartphones security capability requirements

9.2.1 Encrypted storage of personally identifiable information

Smartphones should support encrypted storage of contact lists, SMS messages, photos, call records and other PII. The PII should be stored in the smartphones using encryption methods.

9.2.2 Encrypted access of personally identifiable information

Smartphones should provide an encrypted access mechanism for contact lists, SMS messages, photos, call records and other PII. Smartphone users should be able to establish passwords, fingerprints or other patterns to access certain types of personal information (such as some specific photos or SMS).

9.2.3 Use of security software

Smartphone users should install security protection software on their smartphones. This could help users to detect and dispose of potential threats or vulnerabilities, and provide necessary protection measures if under attack. If the smartphone does not have protection software, the smartphone should have the ability to prompt a user to install it. If the software has been installed, the smartphone should be able to remind the user to inspect the system regularly and update the security software to the latest version.

9.2.4 Bank account binding warning

If a user chooses to save account numbers or passwords while using mobile payment functions, the smartphone should be able to warn the user that it is not recommended to save account numbers or passwords in the smartphone.

9.2.5 Internet traffic monitoring on smartphones

Security protection software on smartphones should be able to intelligently analyse a user's Internet traffic usage. When it detects abnormal traffic over a short period of time, it should be able to block suspicious traffic, as soon as possible, and prompt the user to turn off network connections or stop browsing any suspicious websites.

9.2.6 Mobile malicious code disposal

After detecting malicious code in applications or malware, the smartphone should be able to inform the user. The user should decide if they need to delete the software and report the information to the relevant authorities.

9.2.7 Secure usage of WiFi

To protect a user's PII, such as account numbers and passwords, and to prevent man-in-the-middle (MITM) attacks when using WiFi, smartphones should provide measures to guarantee secure usage of WiFi. For example, when a user turns on a WiFi connection, the smartphone should be able to automatically turn on the encrypted transmission function, and to automatically turn it off when the WiFi connection is off.

9.2.8 Third-party verification mechanisms

When a smartphone user is using a mobile payment or another application that requires account login, the smartphone should support third-party verification for the payment action, such as voice recognition or use of an image verification code.

9.2.9 Performance consumption monitoring

A smartphone should be able to monitor its central processing unit (CPU) performance and power consumption. When CPU performance consumption or battery power is abnormal, it should generate a warning notification to inform the user.

Appendix I

Malware connecting to botnet

(This appendix does not form an integral part of this Recommendation.)

I.1 Foreword

This appendix is based on desktop research using existing research, rather than primary research. Data and analytic reports were gathered from Chinese and worldwide consultation organizations, as well as antivirus software companies. The conclusion of these companies and organizations is believed to be based on a vast amount of collected data and big-data analysis.

Countries have diverse cultures, cultural habits, laws, regulations, and regulatory enforcement laws, resulting in different ecosystems and ecological environments for the propagation of smartphone viruses and malware. For reasons of their own, antivirus companies, for example, may tend to overestimate the number of detected attacks based on loose definitions and favourable analysis perspectives. Hence, the reports from different companies and organizations may show different statistical figures. However, the basic conclusion and trends generally remain the same.

In addition: 1) many, if not most, detected malware have features and capabilities that could easily be utilised by botnets; 2) surveys of malware trends and experiences on smartphones suggest the threat of smartphone-based botnets in the near future; 3) today, due to globalisation, some regional issues of mobile malware and botnets may be transplanted to other regions and become larger issues in the future, making it necessary to be prepared.

I.2 Background

The rapid growth of smartphones is, perhaps, one of the greatest successes of our time. In China, for example, the total number of mobile phone users has reached over 1.3 billion, among which more than 0.68 billion are both smartphone users and netizens.

Today's smartphones are designed with as few flaws as possible, leading to fewer virus infections. In fact, smartphone design has resulted in smartphone products of which only a small portion shall be compromised. However, even if the chance of infection is small, an infected phone may cause unbearable and irreversible loss to a user whose most important PII, such as bank account numbers, passwords, home address and intimate family photos, may be stored on their smartphone.

The increasing popularity of smartphones has caused virus and malware development, focusing on PCs, to transfer to smartphones - which are now the prime target of attacks from hackers. In addition, most cybercrimes targeting smartphones are not motivated by personal interest and curiosity, but rather are motivated by financial gains via ransom and financial fraud. Behind cybercriminal activities there is a dark industry of Internet fraud which has little chance of changing in the near future. Furthermore, Internet of things (IoT) is connecting smart terminals together for the purpose of efficient transmission and sharing of data and information. Recent Gartner research [b-Gartner] predicts that there will be more than 4.9 billion IoT-connected devices in consumer smart-home environments in 2015, and 25 billion in 2020. However, this will become an even greater threat to users' PII as one flaw/loophole/leak in the dataflow chain, or fragmentation information gathering of IoT links may lead to the leaking of users' PII and will create new challenges to mobile security.

Hence, smartphone users tend to pay more attention to mobile security especially when protecting their PII. Worldwide analytical company, *mSecurity* [b-mSecurity], reports that mobile security investment reached USD 11 billion in 2014, and will increase at a compound growth rate of 20% in the next six years [b-GNSM].

I.3 Macroscopic environment in China

There are concrete data supporting the exponentially increasing trend in mobile malware.

In China, for example, the popularity of smartphones has grown rapidly in recent years. Based on the surveys from *Qihoo 360*, one of the largest network and information security software companies in China, the number of mobile phone users increased from 1 billion in 2012 to 1.3 billion in 2015, during the same period of time the number of smartphone users (netizens) increased from 270 million in 2012 to 680 million in 2015.

Numerous security problems emerged during this period of time. In 2012, 175,000 new mobile malware samples were found, and smartphones were infected 71 million times. In 2015, 18.7 million new mobile malware samples were found, and smartphones were infected 370 million times. With PII leakage under free WiFi, and extra traffic generation by malware scripts, users were forced to purchase insurance for unexpected mobile payment loss, harassing phone calls, PII leakage from second-hand smartphones, PII leakage due to social networking software, and all sorts of spam. For a smartphone to operate in a healthy and safe environment, it is essential to have virus and malware protection, traffic monitoring, PII protection, network speed monitoring and WiFi security monitoring. The trend is that mobile security software companies need to cooperate closely with smartphone manufacturers for better protection and security of smartphones.

I.4 iPhone problems

Apple iPhone maintains a stronger degree of control over software that users may install, compared to other platforms such as Android. Apple claims better security [b-AppleSecurity] because it has the motivation and takes action to design such a software ecosystem. Apple has progressively moved towards a model where hardware and operating systems are closely integrated, and users, in general, acquire software from the official App Store.

However, it has been reported that a rising number of malware is being designed to infect devices running iOS [b-AppleThreat]. New investigations show that the general perception of iPhone security is being undermined along with the rapid growth of iPhone users and iPhone applications.

XcodeGhost (detected by Symantec as OSX.Codgost on Mac OS X computers and IOS.Codgost on iOS devices), is a modified version of Xcode development environment and is considered malware. It configures apps to collect information on devices and upload the information to C&C servers. In addition to this, the Trojan apps are capable of receiving commands from C&C servers in order to carry out phishing attacks. A large number of apps created using XcodeGhost managed to bypass Apple's own security checks and were hosted on the official app store, demonstrating that the screening process did not a guarantee a malware-free App Store. In November of 2015, a new variant of XcodeGhost was discovered in unofficial versions of Xcode 7, which enabled developers to create applications for iOS 9.

Surveys show that nearly half of iPhone users no longer think that their iPhone is absolutely safe. Investigations show that nearly 33% of smartphones have been compromised, whereas the figure for iPhones is 23.9%.

Currently, unlike Android phones, Apple phones have better control over the execution of apps/codes through a developer-permission-key mechanism. Once these malicious apps/codes are found on Apple devices, Apple can stop them from working on all its devices by simply rejecting the developer's signing key.

Even though it is a non-open source software platform, iOS still has its own pain points, namely harassing phone calls and phishing. For this reason, in June, 2016 at Apple Worldwide Developers Conference (WWDC) which took place in San Francisco, Apple publicly disclosed its Ident-A-Call application programming interface (API). This will significantly relieve iPhone users from receiving harassing phone calls and phishing, and this also demonstrates that mobile security is becoming a very serious issue. It is not a pure technical issue anymore, it is also becoming a social issue.

I.5 Examples and some trends of new malware

I.5.1 Example 1

Social networking software and mobile payment software are becoming new targets of viruses and malware; this is mainly due to their close relationship, and to each becoming more and more important in people's lives.

A malware named "*a.privacy.BankSteal.a*" disguises itself as a well-known social networking software application with the same well-known logo, making it hard for users to distinguish between the malware and the legitimate software. After a smartphone has been compromised, the malware tricks the user into inputting PII such as bankcard numbers, passwords, user names, identity card numbers and phone numbers, and then begins running in the background; it intercepts a user's SMS messages. The malware then sends this information to hackers via e-mail. This malware significantly compromises a user's PII and the safety of the user's property.

I.5.2 Example 2

Across all regions in 2015, an increase in the use of smartphones for online banking services was observed. Many institutions now offer an Android application that uses two factor authentication (2FA). This further expedited the mobile malware trend [b-FinancialThreat].

The most common method of attack is to intercept text messages that are part of the 2FA process and forward them to the malware's C&C server to be used by the attacker. As usual with Android malware, the application requests permission to receive, write, and send text messages, as well as several other permissions during its installation phase.

In a typical 2FA system, the second factor, normally a generated one-time passcode (OTP), is sent to a user's registered mobile number through SMS. To improve the security of OTP delivery, some financial organizations have begun delivering OTPs through voice calls instead of SMS. In the last quarter of 2015 a new variant of *Android.Bankosy* was found. It is an information stealing Android threat which is capable of deceiving 2FA systems that use voice calls. The C&C server of the threat can instruct the infected smartphone to forward all calls by using a special service code.

Another class of attack that has increased is the use of fake standalone bank applications. These can be very convincing to users, such as when mobile malware poses as a legitimate 2FA token app. The most dangerous aspect of this type of malicious app is that it asks the user for their account name and password during the installation phase, gaining all information needed for the scam to work. This can lead to defrauded bank accounts without using an infected desktop computer. In other cases, attackers replace legitimate and already-installed mobile banking software with their own malicious software. Another Android threat called *Android.Fakelogin* uses flexible social-engineering techniques to steal banking credentials from a wide range of users. Rather than disguising itself as a specific app, *Android.Fakelogin* identifies the banking app that's running on the user’s device and overlays a customized, fraudulent login page over the user interface. It does this by accessing cloud-based logic hosted on a remote C&C server to determine the exact phishing page to display. If the user tries to log in through the fraudulent page, their login credentials will be sent directly to the attacker's C&C server. Although the malware targets legitimate apps available on Google Play, the apps that download *Fakelogin* are not available on Google Play.

I.5.3 Example 3

One of many new trends is that new malware is becoming more rogue and brazen in blackmailing smartphone users. For example, since 2014 more mobile malware began to target individual users via peer-to-peer (P2P) attacks.

A malware named "*a.rogue.SimpleLocker.a*" forces a user's smartphone to run the malware at top priority and locks the smartphone's screen frequently. The smartphone user is required to pay a fee for unlocking the screen; otherwise, no other applications can run on the smartphone. In the background, the malware is connected via the Internet and can remotely unlock the screen after a fee is paid. The malware no longer conceals itself, turning rogue and boldly jumping to the top priority to blackmail users for ransom. The greater the number of smartphones that are compromised, the greater the revenue the hackers can make.

I.6 Conclusion

Along with the rapid development of mobile Internet, smartphones are gaining in both intelligence and performance capabilities. The rapid growth in the usage of smartphones is perhaps one of the greatest achievements of our time, and surveys show that PC-based botnets are being replicated on smartphones very quickly. The replicating speed of viruses and malware is just as stunning as the growing use of smartphones. Hence, the work of countering smartphone-based botnets is both practical and forward looking.

Bibliography

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

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

[b-ITU-T X.1546] Recommendation ITU-T X.1546 (2014), *Malware attribute enumeration and characterization*.

[b-ITU-T X-Sup.8] ITU-T X-series Recommendations – Supplement 8 (2010), *ITU-T X.1205 – Supplement on best practices against botnet threats*.

[b-AppleSecurity] Webpage: *Apple Claims Better Security with iOS 9, Gets Hacked before Its Release*, September 13, 2015.
<https://lifars.com/2015/09/hacker-cracks-ios-9-with-a-jailbreak-before-its-public-release/>

[b-AppleThreat] O'Brien, Dick (2016), *The Apple threat landscape*, Symantec Security Response, Version 1.02, February 11, 2016.

[b-FinancialThreat] Candid, West (2015), *Financial* threats, Symantec Security Response Version 1.0, March 22, 2016.

[b-Gartner] Gartner Press Release, November 11.
<http://www.gartner.com/newsroom/id/2905717>

[b-GNSM] *Global Network Security Market 2015-019*.

[b-mSecurity] Mobile Security (mSecurity) Market Forecast 2014-2024.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017