国 际 电 信 联 盟

ITU-T X.1213

(09/2017)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 网络安全

对于反击基于智能手机的僵尸网络的安全能力要求

ITU-T X.1213 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务(1)	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议(1)	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	**X.1200–X.1229**
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1213 建议书

对于反击基于智能手机的僵尸网络的安全能力要求

摘要

ITU-T X.1213建议书分析基于智能手机的网络僵尸的背景和潜在的安全威胁，并提供安全能力需求。

随着移动互联网设备的迅速发展以及智能手机的广泛应用，来自世界各地组织的调查显示，僵尸网络，以前主要针对个人电脑（PC）为基础的网络，现在正在迅速复制到智能手机。目前，不同条件和生态系统的国家和地区对智能手机为基础的僵尸网络的传播有不同程度的限制。来自各种安全公司和调查机构的分析报告显示了智能手机为基础的僵尸网络的传播严重程度不同的统计数据。基于智能手机的僵尸网络的潜在威胁在某些地区迅速增加，并可能蔓延到世界各地，并从一个地区性问题变成一个严重的全球性问题。

与个人电脑和服务器相比，智能手机具有更少的处理能力、存储空间和电池寿命。然而，基于智能手机的僵尸网络的对抗影响针对以下原因可能会对用户有更大的反响：1）智能手机常能存储非常重要的个人识别信息（PII）；2)如果智能手机或运营商基础设施攻击发生，由于智能手机的流行和用户对智能手机的依赖，用户体验会严重下降。

历史

版本	建议书	批准	研究组	唯一ID*
1.0	ITU-T X.1213	2017-09-06	17	11.1002/1000/13261

关键词

僵尸网络、指令和控制（C&C）、恶意软件、个人识别信息（PII）、智能手机。

---

* 如欲访问本建议书，请在网页浏览器的地址栏输入URL http://handle.itu.int/，然后输入建议书的唯一ID。例如：http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1213 建议书

对于反击基于智能手机的僵尸网络的安全能力需求

1 范围

本建议书旨在提供安全能力的需求，打击智能手机为基础的僵尸网络。本建议书的目的是研究基于智能手机的僵尸网络呈现的挑战，以及他们的具体威胁和要求，运营商的网络以及智能手机本身。本建议着重于威胁分析和需求列举。其目的是保障运营商的基础设施和智能手机，确保运营商的服务和服务质量，并提高用户体验。详细的技术解决方案，和其他智能终端，如平板设备，超出了这个建议的范围。

2 参考资料

无。

3 术语和定义

3.1 它处定义的术语

本建议书使用了下列它处定义的术语：

3.1.1 机器人程序 bot [b-ITU-T X-Sup.8]: 用于执行为恶意目设计的特定任务的自动化软件程序。它可以与机器人互换。

3.1.2 僵尸主控机 botmaster [b-ITU-T X-Sup.8]: 负责控制和维护僵尸网络的个人。

3.1.3 僵尸网络 botnet [b-ITU-T X-Sup.8]: 远程控制的恶意软件机器人，自主或自动地与由僵尸主控机拥有的服务器指令和控制一起运行于中病毒的计算机中。

3.1.4 个人信息识别 personally identifiable information (PII) [b-ITU-T X.1252]: 任何信息 a) 识别或能用于识别、联系或定位与该信息相关的个人；b) 从这些信息能够获得某个人的识别或联系信息；或 c) 该信息能够直接或间接与一个自然人相关联。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

2G 第二代移动通信

2FA 双重验证

3G 第三代移动通信

4G 第四代移动通信

API 应用程序设计接口

C&C 指令和控制

CPU 中央处理器

DDoS 分布式拒绝服务

DNS 域名系统

GPS 全球定位系统

HTTP 超文本传输协议

IDS 入侵检测系统

IoT 物联网

IP 互联网协议

IPS 入侵防御系统

MITM 中间人

MMS 多媒体信息服务

NFC 近场通讯

OTP 一次性密码

P2P 端对端

PC 个人计算机

PII 个人识别信息

PNG 可移植的网络图像文件格式

QoS 服务质量

QRcode 二维码

SIM 用户身份模块

SMS 短消息服务

USB 通用串行总线

WiFi 无线保真

5 惯例

无。

6 背景

随着移动互联网设备的快速发展，移动终端正变得越来越智能化，具有更高的性能。在本建议书中，智能手机术语指的是具有以下特性的手机类型：

– 独立的操作系统；

– 通过安装第三方应用程序，不断扩大电话的功能和能力；

– 无线网络接入能力，包括通过移动运营商的通信网络访问移动互联网的能力。

近年来，智能手机用户的数量持续快速增长。在为人们的生活提供便利的同时，智能手机的安全威胁也在增加。

6.1 安全考虑综述

考虑到智能手机用户的快速增长，智能手机僵尸网络必须得到有效的抑制和控制，防止它们成为影响社会稳定和威胁公共安全的重要因素。

对于移动运营商来说，大规模僵尸网络会严重损害运营商网络的有效利用，降低提供给用户的服务质量，从而导致用户的不满和用户的流失。对于用户来说，他们的智能手机被黑客通过僵尸网络攻击和控制，其潜在的损失可能如同个人可识别信息（PII）那样重要，如联系人列表和在线支付信息，通常存储在他们的智能手机中。

因此，打击基于智能手机的僵尸网络的工作是前瞻性和实用性的。运营商应该提高其在这一领域的安全意识：抑制僵尸网络的快速增长，减少用户的损失，减少用户投诉等。

6.2 僵尸网络对智能手机威胁的进展

智能手机病毒的出现可以追溯到2004年，当时，*Cabir*是首例被发现的智能手机病毒。2009年，恶意软件*iKee.B* 开始具有僵尸网络特征，可以控制被感染的iPhone，并把用户个人信息发送到僵尸主控机。2011年，一个典型的移动僵尸网络，安卓 *Geinimi*，被发现。它可以隐藏通信方法，有丰富的攻击模块，被认为是非常有害的。

智能手机的广泛使用伴随着智能手机为基础的恶意软件的增长，其中大多使用某些智能手机功能作为传播媒介。在被下载并安装在智能手机后，恶意软件会频繁地和秘密地，显示广告，诱导额外的智能手机流量，并扣除费用等，给智能手机用户造成损失。此外，智能手机用户也可能遇到的问题，如：被引导到钓鱼网站，他们的智能手机感染病毒或木马程序，泄露或窃取他们的联系人列表和/或地址簿，或窃取账户和密码。这些罪行中，个人信息，个人账户和密码泄漏发生最频繁。

近年来，智能手机恶意软件成倍增长。恶意软件是僵尸网络病毒传播的主要原因，因为越来越多的恶意软件使用远程控制后门程序的方法或功能，这是基于智能手机僵尸网络的一个显著特点。研究者的主要目的是从PII盗用、恶意扣费中获取利润。目前，最常见的恶意软件包括：PII盗窃、恶意扣费、欺诈行为、性能恶化和恶意传播。

6.3 对智能手机的防护

骚扰电话，短消息服务（SMS）垃圾邮件，以及其他由网页浏览造成的安全事件，文件下载，移动支付等，是智能手机用户面临的主要安全问题。这些威胁主要是通过安装在智能手机上的安全软件减轻的。

智能手机安全软件的两个主要功能是电话管理和安全保护。电话管理功能包括内存清理、待机时间延长、自动开机程序管理、短信管理、电话号码管理等。电话管理功能的目的是使智能手机运行更加顺畅，提高设备使用效率。安全防护功能主要包括数据流量监控、阻断骚扰电话、定时扫描、定期删除病毒等。安全防护功能的目的是保护智能手机免受安全威胁。

安全软件的安装可能有助于在用户终边保护智能手机不受某些僵尸网络和恶意软件入侵，但随着智能手机攻击者的技能提高和他们的攻击方式多样化，智能手机将继续面临越来越多的安全威胁。随着终边安全防护的提高，运营商还需要在网络端提供更多的安全防护。双方的协调与合作将大大提高智能手机抵御僵尸网络攻击的能力。

7 基于智能手机的僵尸网络特性

智能手机和移动网络的特性正在被智能手机为基础的僵尸网络利用，利用互联网传播大规模的恶意软件。通过对智能手机和移动网络特点，以及对僵尸主控机攻击目的分析，可以概括出基于智能手机的僵尸网络的特性并可识别潜在的安全威胁。

7.1 机器人程序上的个人识别信息

基于智能手机的僵尸网络是由大量的基于智能手机的机器人程序组成的。不同于传统的个人电脑（PC）、多数PII和隐私信息集中存储在智能手机上，使基于僵尸网络的智能手机对可能遭受数据丢失的用户产生更大的威胁。

智能手机集成的功能包括：个人信息管理，日程安排和议事日程，日记，任务安排，多媒体应用，网页浏览等。存储于智能手机应用程序中丰富的个人信息使智能手机成为攻击者主要目标。此外，智能手机的全球定位系统（GPS）可能获得用户的位置信息，位置信息是另一种类型的PII。一旦这些信息被攻击者获取，用户的PII就可能泄漏。

7.2 各种传播方式

首先，基于智能手机的僵尸网络可以通过感染的应用程序恶意传播，用户通常会发现并且从不需要安全认证的应用商店或手机论坛下载这些程序。

其次，基于智能手机的僵尸网络可以通过蓝牙，无线网络（WIFI），USB接口及其他智能手机外设接口传播。

第三，基于智能手机的僵尸网络可以通过HTTP、SMS、MMS、QRcode等等传播。

各种传播媒介使得基于智能手机的僵尸网络相对容易传播，相应地对安全防护提出了更高的要求。

7.3 公开性

开放的移动操作系统为智能手机提供了大量的应用程序选择，但同时这些程序也使智能手机暴露在更多的潜在威胁和黑客前。开放性允许黑客将病毒或木马嵌入到扩展应用程序中，方便基于智能手机的僵尸网络的传播。

智能手机有多种类型的外设接口，包括：蓝牙，近地域通信（NFC）和USB。攻击者可以利用这些外设接口连接。此外，智能手机通常支持第二、第三或第四代（2G、3G或（4G）的移动网络以及WiFi接入，通过它们，用户可以访问互联网。这些功能具有独特的应用价值和商业价值，同时也为攻击者提供了多种攻击渠道。

7.4 针对性的感染

基于智能手机的僵尸网络通常针对某些类型的目标，通过直接复制或诱使用户下载恶意软件或木马来感染。攻击者还可以针对运行相同操作系统的智能手机进行感染。这种方法大大提高了攻击的效率，同时降低了攻击成本。

7.5 隐匿处

基于智能手机的僵尸网络变得越来越复杂。一些僵尸网络在成功感染智能手机后，通过删除所有安装痕迹来隐藏其攻击行为。有些僵尸网络通过互联网接入发送用户PII后，可以抹去他们的网络连接和发件箱的痕迹。其他人甚至可以从特定的服务供应商那下达定制服务指示，并自动阻止移动运营商的验证消息。

一些窃取PII或造成恶意扣费的智能手机木马和恶意软件在成功被安装后不会立即发起攻击。相反，他们将会通过恶意软件或利用受感染的智能手机的空闲时间，根据时段设置，发动攻击。

今天，越来越多的恶意软件拥有远程控制后门程序作为一个基本的功能，这是基于智能手机的机器人程序的特点之一。

许多僵尸网络通过嵌入在流行的手机应用程序中的恶意程序传播。当用户在没有安全认证机制的应用商店或手机论坛下载并安装软件时，隐藏在应用软件中的恶意程序将被触发。

7.6 商业利益

不像大多数传统的恶意软件，其目的是破坏，基于智能手机的僵尸网络的目的往往是利益驱动。例如，基于智能手机的僵尸网络依靠窃取用户的PII或发起恶意扣费盈利；从而形成一个网络诈骗黑色产业。商业利益刺激攻击者投入更多的资源开发基于智能手机的僵尸网络并促进互联网欺诈行业的发展。这意味着，基于智能手机的僵尸网络将对用户造成更多的安全威胁，而保护这些威胁将变得越来越困难。

7.7 日新月异的网络连接

智能手机的高移动性特性导致网络连接不断变化，从而导致基于智能手机的僵尸网络的可变性增加。智能手机不仅可以在使用相同网络技术的网络之间漫游，而且还可以在使用不同的网络技术（例如，从3G网络到WiFi热点）的网络之间漫游。因此，受到损害的智能手机僵尸程序可能需要比基于PC的僵尸程序更频繁地用指令和控制（C&C）服务器来改变他们的通信通道。这导致了通过识别其通信通道来检测基于智能手机僵尸网络的额外复杂性。

8 安全威胁

8.1 个人识别信息泄露

– 用户识别模块（SIM）卡信息:

  一旦手机感染僵尸，僵尸主控机可以窃取用户的手机卡信息，包括电话登记信息，硬件配置参数等，可以通过出售或者泄露PII产生更大的经济利益。更令人关注的是，僵尸主控机可能会通过分析这些手机的漏洞进而用相同的配置对智能手机产生更危险的攻击。

– 手机存储：

  基于智能手机的僵尸网络主控机能利用云对所有其僵尸程序进行远程控制。这样，僵尸主控机可以从僵尸程序中盗取：用户的PII，包括他们的电话号码、联系人列表、通话记录、邮件、位置信息、照片和视频等，僵尸主控机可以指导僵尸程序这些信息将上传到远程服务器。

– 银行账户和密码：

当用户通过智能手机支付，攻击者可以通过利用其漏洞获得用户的智能手机的完全控制，然后可以窃取用户的银行账户和密码。此外，攻击者可以拦截短信验证码，并启动恶意的金钱转移，并在同一时间抹去任何痕迹的攻击。这样，攻击者可以轻松地窃取金钱，而不被智能手机用户感知到。

– 应用程序账户和密码：

以同样的手段攻击者可以窃取用户应用软件的账户和密码。他们可以利用这些信息进行进一步欺诈，并产生相应的利润。

8.2 恶意扣费

– 自动下载和删除软件:

一旦智能手机由僵尸程序控制，它将接收到C＆C服务器发出的指令，并且僵尸主控机可以让手机做几乎任何事情。通过僵尸主控机的指示，智能手机可能会自动下载不必要的应用程序，也可以卸载指定的应用程序。这些行为可能会导致增加的数据流量消费费用，导致用户的经济损失。

– 垃圾短信：

一些恶意软件可以利用联系人名单指示智能手机发送短信。首先，攻击者欺骗用户下载和安装恶意软件，然后一旦感染智能手机，将自动联系C&C服务器来指示。在收到垃圾短信指示后，智能手机将根据手机的联系人列表发送垃圾短信，导致性能下降和因为互联网接入和短信发出造成的恶意扣费。频繁的短信垃圾可能堵塞移动渠道，导致性能下降，智能手机不可用。此外，如果一个被损坏的智能手机属于某个公司或公共机构，该公司的声誉可能会受到破坏，因为存储在智能手机中的联系人列表可能包含重要的业务合作伙伴或政府联系人。频繁地从受感染的智能手机中接收垃圾短信，其手机号可能被收信人加入黑名单，导致不可预知的财务损失和业务合作的伤害。

8.3 欺诈行为

– 分布式拒绝服务 (DDoS) 攻击：

随着智能手机的广泛使用和移动互联网应用的快速增长，如果控制的僵尸程序数量非常大，僵尸网络主控机可以发动DDoS攻击。僵尸网络主控机可以控制大量受感染的智能手机，并且可以在一个特定的网站同时发起攻击，导致网站服务器故障。特别是，如果被损坏的智能手机属于某些公司或公共机构，他们的声誉可能会大大削弱，因为存储在这些智能手机的联系人列表可能包含重要的业务合作伙伴或政府联系人。一经DDoS攻击检测，目标将通过阻止攻击者的电话号码作出回应，这也可能导致不可预知的财务损失和破坏业务关系。

– 恶意广告欺诈：

受感染的智能手机可能变成垃圾广告接收器。用户可能会收到各种广告，每次点击将对僵尸网络产生收入。这样，僵尸网络主控机通过欺诈广告费积累巨额利润。然而，智能手机用户实际上并没有点击广告，而是由安装在智能手机上的恶意僵尸程序所为。

– 未授权访问企业网络：

基于智能手机的僵尸网络可以让攻击者通过受感染的网络设备获得安全的企业网络访问。受感染的设备可以分析在企业网络中主机的漏洞并向僵尸网络主控机报告。攻击者可能进一步利用这个漏洞攻击企业网络中的主机并窃取机密信息。

8.4 性能消费

僵尸网络主控机可能会通过以下方式引起智能手机的性能下降：

– 病毒组件可以伪装成便携式网络图形（PNG）图像，而在现实中，他们是自动化脚本。感染后，智能手机启动时，病毒会自动加载，并将持续运行在后台，导致操作系统性能严重下降。

– 经常连接到木马服务器进行操作，会导致智能手机持续受损；

– 在后台自动下载垃圾应用程序，短时间内，会导致电池消耗和性能严重下降；

– 僵尸网络主控机向感染的智能手机持续发送垃圾短信导致手机不再运作，电池完全耗尽。

8.5 恶意传输

某些恶意软件可以下载应用程序到一个被感染的智能手机，在后台，没有用户的许可，可以弹出诈骗短信，诱骗用户触摸屏幕，从而导致恶意软件安装。一旦应用程序被安装，它将在后台访问特定的网站，以提高其下载排名，从而欺骗更多的用户下载恶意应用程序。这样一来，僵尸网络的规模扩大，攻击者获得更多的利润。

8.6 信誉损失

僵尸网络感染的智能手机可以用来发送垃圾邮件或参与DDoS攻击，这些行为不仅增加了网络成本和电池消耗，但也导致用户的信誉损失。例如，当僵尸网络感染的智能手机发送大量垃圾短信或电子邮件到存储在手机中的联系人，发件人（智能手机拥有者）将失去信誉。特别是，如果被损坏的智能手机属于某个公司或公共机构，损失可能会更大，因为存储在这些智能手机的联系人可能包含重要的业务或政府合作伙伴。

9 安全能力需求

9.1 网络安全能力需求

9.1.1 网络流量监测

运营商应该提供监控智能手机互联网流量的能力。他们可以建立一个流量监控机制或包含所有用户的表，并智能分析智能手机的互联网流量。当检测到异常流量时，运营商可以立即向用户发出报警或相关信息，并在必要时拦截可疑流量。

9.1.2 移动恶意代码检测

运营商网络中的安全保护设备应在其应用程序中检测和分析恶意代码。如果在应用程序中检测到恶意代码，则操作员可以及时向下载或使用该应用程序的用户发送告警或相关信息。

9.1.3 敏感信息加密运输

运营商的网络应该支持智能手机发送的信息的加密传输。智能手机用户打开此功能后，运营商的网络设备应保证传输信息的完整性和保密性，包括联系人列表、位置、账户和密码等。

9.1.4 诱捕系统的使用

运营商的网络应该建立一个诱捕计算机系统作为诱饵引诱僵尸网络和恶意程序进入智能手机。在检测僵尸网络并收集其控制信息后，运营商可以通过观察和追踪来了解如何更好地保护智能手机。

9.1.5 DDoS攻击防护

– 运营商网络中的安全保护设备和域名系统（DNS）服务器应该能够提供安全策略配置，这可以防止僵尸网络的主机连接到他们的控制器。

– 防火墙、入侵检测系统（IDS），入侵防御系统（IPSS）和运营商的网络中的其他安全保护装置应能提供阻止流量攻击安全策略配置。

– 运营商的网络中的网络和安全保护设备应该能够提供可以在其他领域阻止目标服务器的DDoS流量阻止策略配置。

9.1.6 僵尸网络检测

运营商网络中的安全保护装置应能检测到僵尸网络的突变并收集和分享互联网协议（IP）地址的全球信用，因此可以建立僵尸网络控制器和主机的IP地址信用数据库以提供恶意流量过滤、僵尸网络行为分析、IP地址的信用机制等保护方法。

9.1.7 垃圾短信的检测和处理

运营商网络本应该有检测和处理垃圾短信的机制。当发现接收到大量垃圾邮件信息的移动终端时，应及时拦截垃圾邮件，以防止接收到大量垃圾短信引起的崩溃。在检测过程中，运营商应该能够通知用户，以便他们可以应用相关的措施来处理这种情况。

9.1.8 黑名单和白名单机制

运营商的网络安全保护装置应该具备将恶意软件，恶意代码和恶意网站添加到黑名单的能力。如果僵尸网络控制器要求其受控主机连接到恶意网站或下载恶意软件，这是黑名单的一部分，安全防护设备应该能够及时阻止这些连接。

因此，在运营商的网络安全保护装置还应提供白名单机制。在某些特殊情况下，允许用户连接到受信任的网站下载可信任的应用程序，这是白名单的一部分。

9.1.9 合作能力

为了提高安全软件的完整性和可信性，运营商应该能够与智能手机安全产品提供商合作。通过这种合作机制，对抗僵尸网络的安全保护，可以在网络和移动终端双方完成。

此外，经营者还应与政府和行政部门合作。如果智能手机成为僵尸程序，运营商应该通过行政部门通知智能手机的所有者。此外，为了阻止基于智能手机的僵尸网络及其恶意行为，运营商应该与政府和行政部门合作，制定适当的行动和立法的条例。

9.1.10 身份保证

如果用户（特别是一组用户）智能手机受到威胁，并开始成组发送垃圾信息等，这可能会导致用户失去垃圾信息收件人的信任。如果被感染的智能手机属于某些公司或公共机构，损失可能会更大，因为他们的联系人名单可能包含重要的商业合作伙伴或政府机构。

为了避免这种信任损失，运营商应该有能力，当检测到异常的操作，如组消息时以确保智能手机用户（尤其是组用户）的身份。例如，操作员应该能够检测用户的组消息操作，并且基于预定义的策略，选择通过消息传递通知他们，或者暂时中止组消息操作并在用户进行操作之前请求用户的确认。

9.2 智能手机安全能力的需求

9.2.1 个人可识别信息加密存储

智能手机应该支持联系人列表、短信、照片、通话记录和其他PII的加密存储。PII应该使用加密方法存储在智能手机中。

9.2.2 个人识别信息的加密访问

智能手机应该为联系人列表、短信、照片、通话记录和其他个人识别信息提供一个加密的接入机制。智能手机用户应该能够建立密码，指纹或其他模式来访问某些类型的个人信息（如一些特定的照片或短信）。

9.2.3 安全软件使用

智能手机用户应该在他们的手机上安装安全防护软件。这可以帮助用户检测和处置潜在的威胁或漏洞，并在遭受攻击时提供必要的保护措施。如果智能手机没有保护软件，应该有能力提醒用户安装它。如果软件已经安装，智能手机应该能够提示用户定期检查系统和更新安全软件的最新版本。

9.2.4 银行账户绑定警告

如果用户选择使用移动支付功能时保存账号或密码，智能手机应该能够警告用户，不建议在智能手机中保存账号或密码。

9.2.5 智能手机移动互联网流量监测

智能手机上的安全防护软件应该能够智能地分析用户的互联网流量使用情况。当它检测到异常流量在很短的时间内，它应该能够阻止可疑的流量，并尽快提示用户关闭网络连接或停止浏览任何可疑网站。

9.2.6 移动恶意代码处理

在应用程序或恶意软件上检测出恶意代码后，智能手机应能通知用户。用户应决定是否需要删除该软件并向相关部门报告信息。

9.2.7 无线网络的安全使用

为了保护用户的PII，如账号和密码，使用WiFi时以防止中间人（MITM）攻击，智能手机应提供措施保证WiFi使用安全。例如，当用户打开WiFi连接时，智能手机应该能够自动打开加密的传输功能，当关闭WiFi时，自动关闭。

9.2.8 第三方验证机制

当智能手机用户使用移动支付或其他需要账户登录的应用程序时，智能手机应支持第三方验证支付行为，如语音识别或使用图像验证码。

9.2.9 性能消耗监控

智能手机应该能够监控其中央处理器（CPU）的性能和功耗。当CPU性能消耗或电池电量异常时，应生成警告通知用户。

附录 I

连接僵尸网络的恶意软件

(本附录不构成本建议的组成部分。)

I.1 前言

本附录是基于使用现有研究的桌面研究，而不是主要研究。数据和分析报告，收集来自中国和世界各地的咨询机构，以及防病毒软件公司。这些公司和组织的结论被认为是基于大量的收集到的数据和大数据分析。

国家有不同的文化、文化习惯、法律、法规和监管执法，为智能手机病毒和恶意软件的传播造成了不同的生态系统和生态环境。出于自身原因，例如，反病毒公司可能倾向于高估基于不精确定义和有利的分析视角的攻击检测数量。因此，来自不同公司和组织的报告可能会显示不同的统计数字。然而，基本结论和趋势通常保持不变。

另外：1) 许多，如果不是大多数，恶意软件检测具有可以很容易被僵尸网络利用的特性和功能；2) 对智能手机上的恶意软件的趋势和经验调查表明，在不久的将来，基于智能手机僵尸网络的威胁；3) 如今，由于全球化，移动恶意软件和僵尸网络的一些区域问题可能被移植到其他地区，在未来成为更大的问题，因此有必要准备。

I.2 背景

智能手机的快速增长，也许，是我们这个时代最伟大的成功之一。在中国，例如，移动电话用户总数已达13亿，其中超过6亿8000万都是智能手机用户和网民。

今天的智能手机的设计有尽可能少的缺陷，导致较少的病毒感染。事实上，智能手机的设计已经导致智能手机产品，其中只有一小部分会受到损害。然而，即使感染的机会很小，被感染的手机可能会导致用户的最重要个人信息的无法忍受和不可逆的损失，如可以存储在他们的智能手机中的银行账号、密码、家庭住址和亲密的家人的照片。

智能手机的日益普及，导致病毒和恶意软件集中于个人电脑向智能手机转移的发展-这是黑客攻击的主要目标。此外，大多数针对智能手机的网络犯罪不是出于个人兴趣和好奇心，而是通过赎金和金融诈骗实现财务收益。在网络犯罪活动中，有一个网络诈骗的黑色产业，在不久的将来具有改变的机会不大。此外，物联网将智能终端连接在一起，实现数据和信息的高效传输和共享。最近的高德纳研究[b-gartner]预测2015年消费者的智能家居环境中将有49亿以上的物联网连接的设备、到2020年，实现250亿。然而，这在数据链中，作为一个缺陷/漏洞/泄漏，将对用户的PII有更进一步的威胁，或物联网信息采集环节的碎片可能会导致用户的PII泄漏并对移动安全产生新挑战。

因此，智能手机用户更倾向于关注移动安全，尤其是当保护他们的PII时。全球分析公司*mSecurity*[b-mSecurity]报道，移动安全投资在2014年达到110亿美元，并将在未来六年中，以20%的复合增长率增长[b-GNSM]。

I.3 中国的宏观环境

有具体的数据支持移动恶意软件成倍增加的趋势。

在中国，例如，智能手机的普及，近年来增长迅速。根据奇虎360，一个中国最大的网络和信息安全软件公司的调查，手机用户的数量从2012年10亿增加到2015年的13亿，智能手机用户（网友）数量在同一时期从2012年的2亿7000万增加到2015年6亿8000万。

在这段时间里出现了许多安全问题。2012年，发现了175000个新的移动恶意软件样本，智能手机被感染了7100万次。2015年，发现了1870万个新的移动恶意软件样本，智能手机被感染了3亿7000万次。随着受到免费WiFi造成的PII泄漏，并通过恶意软件脚本生成额外的流量，用户被迫为意外移动支付损失，骚扰电话，二手手机的PII泄漏，由于社交软件造成的PII泄漏，以及各种各样的垃圾邮件购买保险。对于智能手机能够在健康、安全的环境中运行，重要的是有病毒和恶意软件防护、流量监控、PII保护，网络速度监控和无线安全监控。趋势是，移动安全软件公司需要与智能手机制造商密切合作，为了智能手机更好的保护和安全。

I.4 苹果手机的问题

与其他平台，例如安卓相比，苹果手机对用户可以安装的软件的控制程度更高。苹果声称更安全[b-applesecurity]因为它有设计这样一个软件生态系统的动机和行动。苹果逐步走向硬件和操作系统紧密结合的模式，用户一般从官方应用商店获取软件。

然而，据报道，越来越多的恶意软件被设计来感染运行iOS [b-applethreat]设备。新的调查显示，随着iPhone用户和iPhone应用程序的快速增长，人们对iPhone安全性的总体认知正在被削弱。

XcodeGhost（赛门铁克检测到MAC OS X系统上的OSX.Codgost木马和IOS设备上的IOS.Codgost木马），是Xcode开发环境的一个修正版本，并且被看作为恶意软件。它安装程序来收集设备上的信息并将信息上传到指令和控制服务器。此外，此木马程序的功能是，从指令和控制服务器接收指令来进行网络钓鱼攻击。大量使用XcodeGhost创建的应用程序设法绕道苹果自身安全检查并被托管在官方应用商店中，表明筛选过程中不能保证应用程序商店中没有恶意软件。2015年11月，在Xcode7非官方版本中发现了XcodeGhost的变体，这使开发者能够为IOS9创建应用程序。

调查显示，近半数iPhone用户不再认为自己的iPhone绝对安全。调查显示，近33%的智能手机受到损害，而iPhone的数量占23.9%。

目前，与Android手机不同，苹果手机可以通过开发者许可密钥机制更好地控制应用程序/代码的执行。一旦这些恶意应用程序/代码在苹果设备上被发现，苹果通过简单地拒绝开发者的签名密钥来阻止他们在所有的设备上工作。

即使是非开源软件平台，iOS仍然有自己的痛点，即骚扰电话和钓鱼。为此，2016年6月，在旧金山举办的苹果全球开发者大会（WWDC）上，苹果公开披露其Ident-A-Call应用程序接口（API）。这将大大缓解iPhone用户接收骚扰电话和网络钓鱼的烦恼，这也表明，移动安全正在成为一个非常严重的问题。它不再是一个纯粹的技术问题，它也成为一个社会问题。

I.5 新恶意软件的例子和一些趋势

I.5.1 案例1

社交网络软件和移动支付软件正在成为病毒和恶意软件的新目标，这主要是由于它们之间的密切关系，并由于在人们的生活中，这两者变得越来越重要。

名为“*a.privacy.BankSteal.a*”的恶意软件伪装成具有相同标识的知名社交网络软件应用程序，使用户难以区分恶意软件和合法软件。 智能手机遭到入侵后，恶意软件将会哄骗用户输入PII，如银行卡号、密码、用户名、身份证号码和电话号码，然后开始在后台运行；它拦截用户的短信。 恶意软件然后通过电子邮件将这些信息发送给黑客。 这种恶意软件会严重影响用户的PII和财产的安全性。

I.5.2 案例2

在2015年的所有地区，观察到使用智能手机进行网上银行服务的情况有所增加。许多机构现在提供使用双重身份验证（2FA）的Android应用程序。 这进一步加快了移动恶意软件的趋势[b-FinancialThreat]。

最常见的攻击方法是拦截作为2FA进程一部分的文本消息，并将其转发到恶意软件的C＆C服务器以供攻击者使用。与Android恶意软件一样，应用程序在安装阶段请求接收，写入和发送短信以及其他许多权限。

在典型的2FA系统中，第二个因素（通常是生成的一次性密码（OTP））通过SMS发送到用户的注册手机号码。为了提高OTP交付的安全性，一些金融机构已经开始通过语音电话而不是SMS进行OTP。在2015年的最后一个季度，发现了一个*Android.Bankosy*的新变体。 这是一个窃取Android威胁的信息，它能够欺骗使用语音通话的2FA系统。受威胁的C＆C服务器可以指示受感染的智能手机通过使用特殊服务代码转发所有呼叫。

增加了另一类攻击，即独立假银行应用程序的使用。这些使用户非常信服，例如当移动恶意软件伪装成合法的2FA令牌应用程序时。这种恶意应用程序最危险的方面是，它在安装阶段向用户询问其账户名称和密码，并获得所有可用于诈骗工作的信息。这可能导致不使用受感染的台式电脑，银行账户受到欺诈。另一种情况，攻击者会使用自己的恶意软件取代合法和已经安装的手机银行软件。另外一种叫做*Android.Fakelogin*的Android威胁，使用灵活的社会工程技术来窃取大量用户的银行凭证。*Android.Fakelogin*不是伪装成特定的应用程序，而是识别在用户设备上运行的银行应用程序，并通过用户界面覆盖自定义的欺诈性登录页面。它通过访问远程C＆C服务器上托管的基于云的逻辑来确定要显示的确切的网络钓鱼页面。如果用户尝试通过欺诈页面登录，他们的登录凭证将被直接发送到攻击者的C＆C服务器。虽然恶意软件针对Google Play上的合法应用，但下载*Fakelogin*的应用程式在Google Play上无法使用。

I.5.3 案例3

许多新趋势之一是，新的恶意软件在黑客智能手机用户中变得越来越凶猛和无所顾忌。例如，自2014年以来，更多的移动恶意软件开始通过点对点（P2P）攻击来针对个人用户。

名为“*a.rogue.SimpleLocker.a*”的恶意软件强制用户的智能手机首先运行恶意软件，并经常锁定智能手机的屏幕。智能手机用户需要支付解锁屏幕的费用；否则，其他应用程序都不可以在智能手机上运行。在后台，恶意软件通过互联网连接，并且可以在支付费用后远程解锁屏幕。恶意软件不再隐藏自身，而是将流氓大胆跳跃到抢夺用户赎金的行为作为首要任务。智能手机受感染的数量越多，黑客的收入就越大。

I.6 总结

随着移动互联网的飞速发展，智能手机的智慧和表现能力也越来越高。智能手机使用量的快速增长可能是我们这个时代最伟大的成就之一，调查显示，基于PC的僵尸网络正在迅速地复制到智能手机上。病毒和恶意软件的复制速度与智能手机日益增长的使用同样令人惊叹。因此，打击智能手机僵尸网络的工作既有实用性又有前瞻性。

参考资料

[b-ITU-T X.1205] ITU-T X.1205建议书 (2008)，网络安全概述。

[b-ITU-T X.1252] ITU-T X.1252建议书 (2010)，基线身份管理术语和定义。

[b-ITU-T X.1546] ITU-T X.1546建议书 (2014)，恶意软件属性列举和特征描述。

[b-ITU-T X-Sup.8] ITU-T X-系列建议书 – 补充 8 (2010)，ITU-T X.1205建议书 – 对僵尸网络威胁的最佳实践补充。

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

[b-AppleThreat] 赛门铁克公司安全响应，1.02版，2016年2月11日

[b-FinancialThreat] 赛门铁克公司安全响应，1.0版，2016年3月22日，Candid Wueest: 金融威胁，2015年版

[b-Gartner] Gartner新闻稿，11月11日 <http://www.gartner.com/newsroom/id/2905717>

[b-GNSM] 全球网络安全市场2015-019期

[b-mSecurity] 2014-2024年移动安全（mSecurity）市场预测

ITU-T 建议书系列

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦