



云端结合的 Android 智能终端应用审计技术

黄勇军, 刘东鑫, 金华敏, 刘国荣, 汪来富, 沈军

(中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: Android 智能终端的蓬勃发展和快速普及, 促进了互联网的繁荣, 极大地改变了人类社会的运作方式, 也给互联网的黑产经济带来了新的有利条件。从典型高级恶意程序的行为特征出发, 分析了引入网络审计方法的必要性等, 并提出了基于网络行为分析的智能终端应用审计技术实施方案, 包括数据采集方案、审计流程和审计策略管理。

关键词: 智能终端; 应用审计; 云端结合

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018097

Application audit technology based on the combination of cloud and terminal

HUANG Yongjun, LIU Dongxin, JIN Huamin, LIU Guorong, WANG Laifu, SHEN Jun

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: The flourish and popularity of Android terminals have greatly changed the peoples' daily life and also brought new conditions to the internet Dark Industry Chain. The features of advanced malicious programs on intelligent terminals, and the reasons why an audit method of network activities was needed were discussed. At last, a solution was proposed, including the data collecting, the process of auditing and the management of audit policies.

Key words: intelligent terminal, application audit, combination of cloud and terminal

1 引言

随着技术的进步, 智能手机早已成为移动互联网接入的第一大终端。其中, 据第三方数据统计机构 IDC 报道, 2016 年全球智能手机总销量超

过 14.7 亿部, 其中 Android 智能手机所占比例超过 80%, 并在不断上升。Android 智能终端的快速普及推动了移动应用的快速发展, 以移动支付、

收稿日期: 2017-12-11; 修回日期: 2018-01-30

通信作者: 刘东鑫, liudx@gsta.com

基金项目: 国家高技术研究发展计划 (“863” 计划) 基金资助项目 (No.2015AA017205)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No.2015AA017205)

移动社交和共享出行为代表的移动互联网应用已深刻地改变了社会的运转方式,成为推动社会发展的重要力量。进一步地,Android 6.0后的相关版本不断加大了对智能手表、智能驾驶和人机交互等设备的支持,Android 智能终端的类型将变得更加多样,应用类型更丰富。

然而,由于Android系统的开放性,客观上也给恶意程序的发展创造了有利条件。针对Android智能终端的恶意程序(以下简称Android恶意程序)也在“与时俱进”,其数量以远超传统PC端的速度在快速增长,其技术复杂性也从简单的广告推广逐步向高级的APT渗透工具发展。一方面,恶意程序类型、数量多年来保持快速增长,流氓行为类、恶意扣费类和资费消耗类依然占据了大部分的恶意程序类型^[1],如图1所示;另一方面,以DressCode为代表的恶意程序已经显示了作为APT渗透工具的技术能力,恶意程序在逐步走向工具化、模块化。这种发展趋势的背后是网络犯罪链条攻击手法的不断发展,借机不断牟取更大的收益。

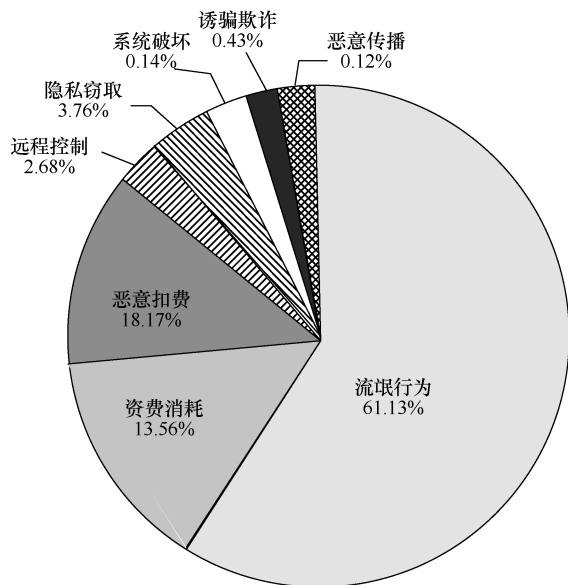


图1 2016年移动互联网恶意程序数量按行为属性统计

本文从几个典型的高级恶意程序出发,分析其典型特征及发展趋势;然后分析引入网络行为

审计方法的必要性,提出网络行为审计技术实施方案,并对部署环境和关键的安全审计策略做了说明和分析;最后针对智能终端,对现有网络行为审计方法的不足做出思考。

2 典型恶意程序及发展趋势分析

2.1 典型恶意程序

(1) FatalSexy 恶意程序分析

FatalSexy 是Android平台上典型的root类恶意程序。这类恶意程序一旦在智能终端设备上运行,如图2所示,将首先调用源代码中已有的提权模块进行root提权,若提权成功,才会进一步完成其他恶意行为模块乃至恶意程序的下载和运行^[2]。由于源代码混淆、加壳等技术的应用,FatalSexy已出现同一家族的大量变种,造成较大影响。

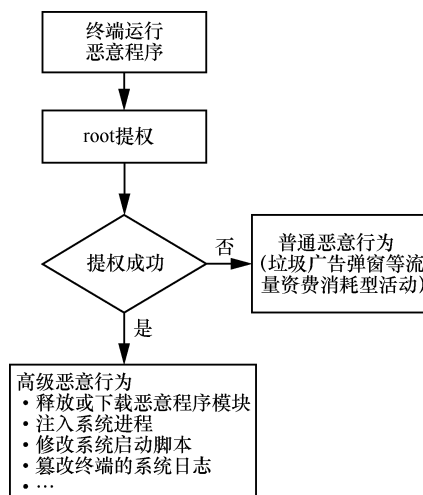


图2 root类恶意程序的常见攻击流程

这类恶意程序主要通过非正规应用商店,利用色情类应用进行传播。用户一旦下载运行该程序,该病毒将进一步下载提权模块,根据Android系统版本的漏洞来获取root权限,并植入恶意elf文件和恶意apk文件到系统目录,可进行各种恶意广告推广、用户敏感信息窃取和资费消耗等恶意行为。这种利用操作系统漏洞提权后所实施的恶意网络行为,具有更大的隐蔽性,可以绕过



Android 的 SEAndroid 等安全机制, 逃脱终端自带安全工具的检测。

(2) Milkydoor 恶意程序分析

Milkydoor 以企业员工的移动智能终端作为跳板, 可以对企业内网进行扫描、敏感数据窃取等高级攻击, 对支持携带自己设备办公 (bring your own device, BYOD) 的企业造成严重威胁。如图 3 所示, Milkydoor 的攻击过程主要包括^[3]: 对于安装了 Milkydoor 的智能终端, 以安全外壳 (secure shell, SSH) 协议客户端主动外连到企业网络外部的 SSH 服务器建立 SSH 连接, 并设置端口转发方式为远程端口转发; 随后, 智能终端作为防火墙安全会话转换协议 (protocol for sessions traversal across firewall securely, SOCKS) 服务器创建一个 Socket, 等待位于本机的 SSH 客户端的连接, 连接成功后就可以读取到 SSH 服务器发送的, 且经过 SSH 客户端解密过的数据。这样黑客就利用 SSH 和 SOCKS 协议建立了一个穿透企业边界防火墙、可逃避常见网络 IDS 检测的虚拟专用网络 (virtual private net-

work, VPN) 隧道, 可以完成进一步的渗透入侵行为。

黑客通过将 Milkydoor 嵌入知名着装指南、绘图应用等进行二度包装, 之后在 Google Play 等应用商店重新发布, 据估计仅通过 Google Play 商店就已感染超过 50 万台设备。Milkydoor 的出现, 标志着针对智能终端的恶意程序已经步入工具化、功能模块化的高级发展阶段, 成为黑客实施渗透入侵方案的重要组成部分。

2.2 Android 恶意程序的发展趋势

从技术来看, 这些恶意程序的泛滥主要利用了终端操作系统、系统重要配置的安全漏洞, 最终实现了恶意订购、广告弹窗等恶意网络行为。在 Android 系统中, 由于不同厂商的开发和支持能力差异, 部分厂商对操作系统漏洞的响应不及时。总体来看, Android 恶意程序呈现出以下发展趋势。

- 攻击目标从资费消耗开始向加密勒索、构建僵尸网络方向发展。2015 年, Android 应用市场中出现了 Lockerpin.A 的勒索

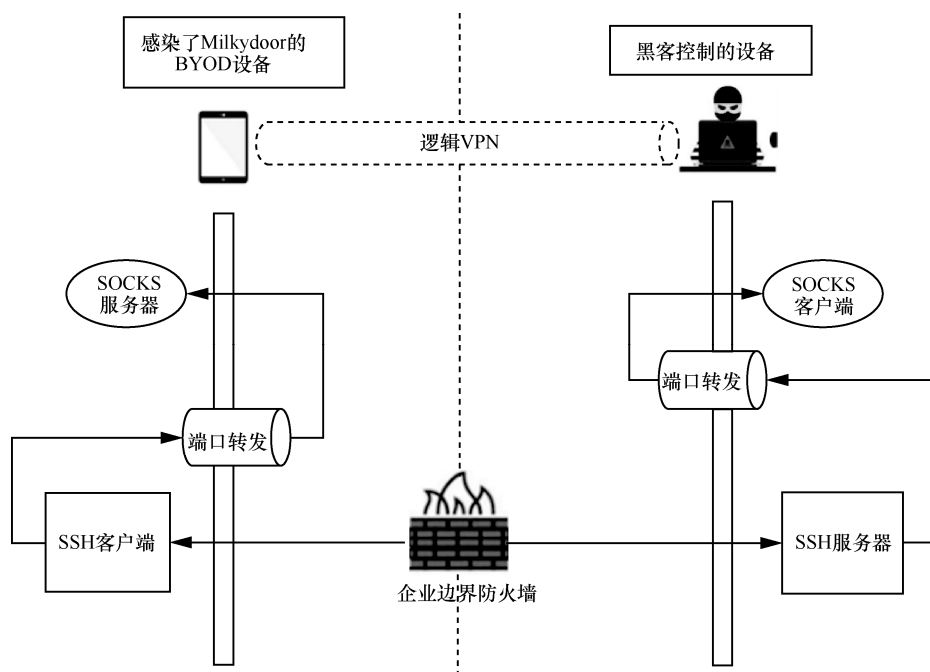


图 3 Milkydoor 的攻击过程

软件,通过伪装成系统更新来申请获得用户的管理权限,随后就会使用随机数字更换用户的锁屏 PIN 码,并向受害者勒索 500 美元/450 欧元的解锁费用。攻击目标的转变主要包括两个方面的原因:一方面,随着手机在日常工作生活中的重要性不断提升,攻击者通过加密勒索的方式有更高的概率获得高额赎金;另一方面,在 Android 智能终端种类和数量爆发式增长、终端一直保持在线和网络接入带宽不断提升的背景下,构建僵尸网络成为一种维持非法得利的自然选择。

- 攻击方法从利用操作系统代码漏洞,向系统配置漏洞、建立隐蔽通道等全面扩展,发起攻击的门槛进一步降低。以 FatalSexy 为代表的恶意程序利用操作系统实现 root 提权后,实现对智能手机的完全控制,并进一步下载其他恶意模块实施恶意行为;而以 Milkydoor 为代表的恶意程序已经具备集成资产扫描、漏洞扫描及利用和端口跳转等行为能力,功能上逐步向 PC 端的恶意程序靠拢。这一系列利用安全漏洞所实施的恶意行为具有更大的隐蔽性,往往可以逃脱各种安全工具的检测,而恶意行为工具的模块化进一步降低了攻击者的使用门槛。

2.3 引入网络审计方法的必要性

目前,业界对于恶意程序的分析主要是静态分析法和动态分析法。前者是指对未知的应用程序进行反编译,然后依据已知的恶意程序特征码进行匹配。大量 root 类恶意程序的家族变种表明,恶意程序已经使用复杂的加密、加壳和多态等技术,以逃避源代码层面的静态分析,后者通常是在一个安全沙箱中执行未知的应用程序,通过监视其运行过程的各种行为数据,例如 API 调用、内存状

态和网络通信等,然后依据已知恶意/正常程序的行为特征对其进行识别。相对于前者,后者是一个巨大的进步,通过行为分析检测,可以识别未知恶意程序,辅以人工分析,大幅提升恶意程序检测率。

静态分析和动态分析法,既可在终端也可在云端进行,但单纯的终端或云端存在一定的缺陷和不足。

- 恶意程序、应用行为分析需占用大量的资源,受终端资源限制,终端侧持续的应用行为分析将对用户体验带来不良影响。
- 云端检测具有更充裕的资源优势,对用户影响较小,但采用沙箱模拟的运行环境,容易被恶意程序所识别,从而中止运行躲避检测,难以进行有效分析。如以 Dendroid 为代表的恶意程序已经具备对运行环境的检测能力。只有在满足一定条件时,才会进一步下载其他模块,从而可以躲避安全沙箱的检测。
- 应用行为分析与恶意程序在同一个环境运行,也易被恶意程序识别、伪装甚至篡改运行痕迹,影响分析结果的准确性。

尽管恶意程序的代码机制千变万化,但是其网络行为却始终“有迹可循”,借助网络的大数据资源与威胁情报,可以极大提升对未知威胁的检测能力^[4]。本文采用的云端结合的应用行为审计技术,可结合终端、云端检测的优势,进一步提升应用审计和恶意程序检测能力。尤其在智能穿戴、智能驾驶等物联网应用场景中,由于设备计算能力的巨大差异,传统的静态分析法和动态分析法的应用受到限制,而通过采用云端结合的体系架构对同一未知程序做行为检测和海量用户反馈,有助于快速更新异常行为检测模型,大幅度提高对未知程序的判断精度,发现未知恶意程序。



3 基于网络行为分析的 Android 智能终端应用审计技术

3.1 数据采集方案

本文采用“网络中间人+终端数据采集”构建数据采集方案，如图 4 所示。其中，“网络中间人”的实现方式是：在一台笔记本电脑通过安装 Wi-Fi 接入软件、Wireshark 网络分组抓取软件和 Fiddler 分组抓取软件，完成对网络层流量和 HTTP/HTTPS 流量的劫持。“终端数据采集”的实现方式是：在一个轻量级安全增强 Android 终端，周期性获取 `/proc/net/tcp` 文件和 `ps` 命令输出的信息。这种做法的主要原因包括以下几方面。

- 无论 Android 终端是否被恶意程序获取 root 权限，在网络侧以“网络中间人”方式获取的网络连接数据都是可信任的。
- 仅通过在网络侧以“网络中间人”方式获取的网络连接数据，还无法关联到具体的应用程序进程，需要结合 Android 终端的 `/proc/net/tcp` 文件、`ps` 命令输出的信息，从而实现网络连接数据到应用进程及其名称的关联。
- 在现有的 Android 安全机制下，一旦恶意

程序成功获取 root 权限，`/proc/net/tcp` 文件、`ps` 命令输出的信息就面临被篡改的威胁，因此需要有相关的完整性保护机制。

简单来说，本文的轻量级安全增强 Android 系统功能主要包括以下 3 方面：

首先，书写了包括调用 `ps` 和 `cat/proc/net/tcp` 命令以及设置属性命令的 shell 脚本，使这个脚本能以临时的 root 权限被调用；

其次，修改 `init.rc` 文件，将这个 shell 脚本设置为开机自启动；

最后，增加了数据完整性校验模块，如果这个 shell 脚本被篡改，将提示告警。

3.2 网络数据审计流程

恶意程序需要传播及与背后的控制者通信，就必须通过网络发送和接收网络数据分组。对于攻击者而言，只要旧的技术和资源还能起作用，就会继续使用。在一些缺乏高级技巧的恶意程序中，这种情形体现得更加明显，网络层数据的安全分析仍然具有一定潜力。本文采用如图 5 所示的网络数据审计流程，主要包括以下 4 个关键步骤。

步骤 1 IP 地址/URL 黑白名单过滤。

依据已有的 IP 地址和域名威胁情报库，可以

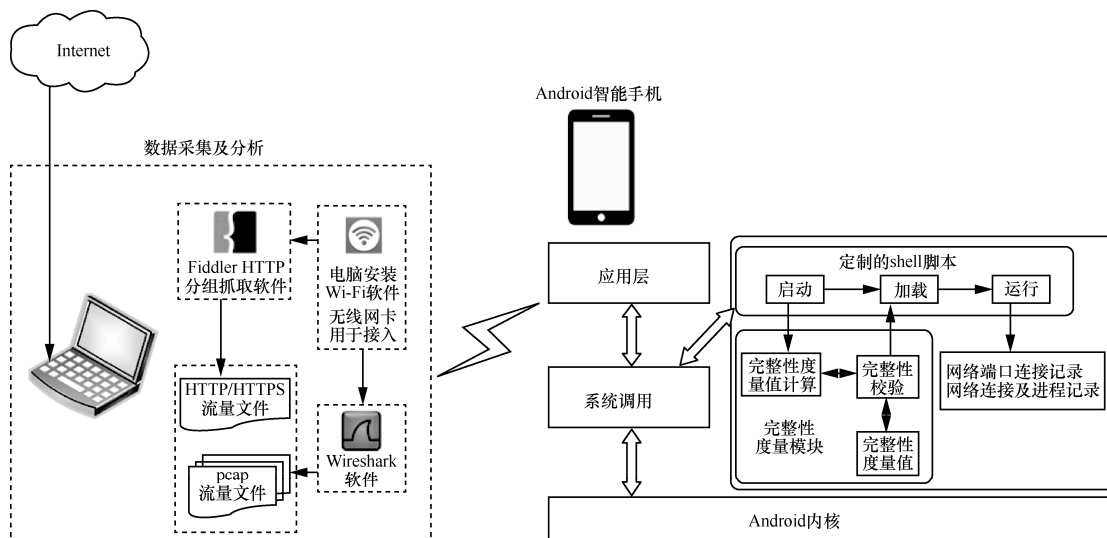


图 4 网络数据采集方案

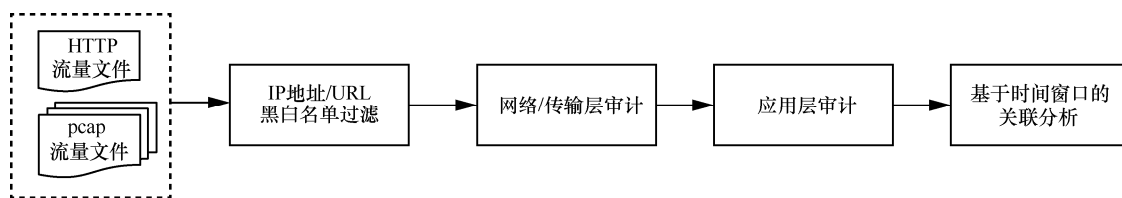


图5 网络数据审计流程

发现已知恶意程序的网络行为，直接输出分析报告结果。对于不同的智能终端设备类型，根据已知的管理IP地址或可靠的域名，设立白名单，可以减轻后续的分析负担，现实中往往需要通过长时间的观察才能总结得到，白名单的设置应该慎重。从Mirai僵尸网络发起DDoS攻击的案例来看，构建虚假源地址报文是恶意程序的重要手段。因此，对于存在虚假源地址的报文，可以直接过滤出来，输出为安全事件。

步骤2 网络/传输层审计。

恶意程序的传播往往具有网络扫描行为，需要对同一局域网内其他IP地址及其常见端口的扫描，体现为某个时间窗口内，ping分组、针对某个IP地址的TCP SYN分组急剧上升。这也是发现如TCP SYN flood、UDP flood等DoS/DDoS攻击最重要的方法。进一步地，将原始的TCP/UDP数据分组整合成类似Netflow格式的数据，可以实现对某个时间窗口内同一流量（以“源IP地址、目的IP地址、源端口、目的端口、传输层协议类型”五元组进行区分）的归并统计，得到同一流量及其反向流量的流量大小，有利于在如智能摄像头等智能设备中发现敏感数据外泄攻击。

步骤3 应用层审计。

Android和iOS智能手机的应用程序极其丰富，沉淀了大量高价值的用户信息，已经成为用户日常生活的重要组成部分。对于攻击者而言，获取用户隐私信息、进行骚扰广告推广等行为往往比构建僵尸网络发送DoS/DDoS攻击流量能获取更大的经济利益。这一系列的恶意行为通过不同的应用层协议实现，包括

DNS、HTTP/HTTPS、SMTP和FTP等。在以Milkydoor为代表的Android高级恶意程序中^[2]，已经具备类似传统PC端恶意程序的内网渗透功能，其背后是网络及漏洞扫描、端口反弹、漏洞利用和数据传输等模块代码的标准化趋势，通过网络应用层协议所表现出的行为特征日趋稳定。

步骤4 基于时间窗口的关联分析。

安全漏洞无法预测，每个新恶意程序的网络行为也不完全相同。在网络/传输层审计、应用层审计发现的异常，往往只是恶意程序一系列网络行为的其中一个步骤。通过时间窗口的前后查找，把属于同一“源IP地址，目的IP地址”及其对应的反向IP地址数据分组过滤出来，形成网络行为的上下文数据，从而进一步发现恶意程序的功能和行为全貌，这在分析如Milkydoor为代表的高级恶意程序尤其重要。

3.3 安全审计策略管理

从攻击者角度来看，网络安全是一个发散问题，挖掘目标对象不同层次的漏洞信息决定了入侵攻击方法的有效性；而从安全审计者角度来看，发现安全事件是收敛的问题，无论攻击者采用何种攻击手段，其最后的攻击目标一定是在网络及端口扫描、数据窃取、密码暴力破解和发送DoS/DDoS攻击流量等几个有限的安全事件集合。

传统的网络入侵检测设备主要依赖对已知恶意程序的签名特征库实现对威胁的检测，对于网络异常行为的检测能力往往较弱。尽管各类型智能终端可以支持的应用类型和各类恶意



程序所利用的网络协议有所差异，但是这些恶意程序在不同类型终端上的行为却高度收敛。例如，从近年来所曝光的安全事件来看，智能手机的恶意程序主要集中在敏感信息窃取，而智能家居设备的恶意程序往往集中在发送 DoS/DDoS 攻击流量。

本文以密码暴力破解、敏感信息窃取、发送 DoS/DDoS 攻击流量、网络及端口扫描作为 4 个类型的安全审计策略，对网络层、传输层和应用层的主要协议进行分析，具体见表 1。

(1) 网络层和传输层协议

安全审计策略聚焦在发送 DoS/DDoS 攻击流量、网络及端口扫描。在检测智能终端是否发送 DoS/DDoS 攻击流量时，应特别关注虚假源地址的检测，如今虚假源地址几乎成为大型 DDoS 攻击的标准配置，用以延长攻击时间，降低僵尸网络被发现的概率；在发现网络及端口扫描行为时，应特别关注对 ICMP、TCP SYN 报文的统计，前者是局域网内存活 IP 地址发现的手段，后者是检测一个 IP 地址是否开放 TCP 端口的必备条件。

(2) DNS 协议

安全审计策略聚焦在发送 DoS/DDoS 攻击流量和敏感信息窃取。经过了网络层的虚假源地址

检测，需要特别关注对 NXDomain 类型的 response 报文检测。当智能终端查询一个不存在的域名时，最后一个递归服务器会把 NXDomain 结果返回给智能终端，公共的缓存 DNS 服务器对于 NXDomain 的报文内容并不会保存到缓存中。当一个智能终端不断发起对这个域名的查询时，这个过程会不断重复，从而形成对公共缓存 DNS 服务器的 DoS/DDoS 攻击。在企业内网环境中，还应特别注意对 NXDomain 报文大小和 payload 的检测，因为基于 NXDomain 报文可以构建 DNS tunnel，并用于敏感信息窃取。

(3) SMTP

安全策略聚焦在发送 DoS/DDoS 攻击流量和敏感信息窃取。智能终端利用 SMTP 大量外发垃圾邮件的行为，可被认为是 DoS/DDoS 攻击行为。在检测智能终端是否利用 SMTP 发送 DoS/DDoS 攻击流量时，主要关注在一个较长的时间窗口内，比如 6 h 或 24 h 内，终端外发邮件的数量，如果超过一个阈值，则可认为是有发送 DoS/DDoS 攻击流量行为。在检测是否利用 SMTP 敏感信息窃取的攻击行为时，可以使用正则表达式在 payload 中发现是否有手机号等敏感信息。大部分窃取隐私类的恶意程序主要关注智能手机的联系人列表、通话记录和短信记录。在 2016 年

表 1 安全审计策略管理

协议栈层次	网络协议具体类别	安全审计策略			
		密码暴力破解	敏感信息窃取	发送 DoS/DDoS 攻击流量	网络及端口扫描
应用层	HTTP/HTTPS		√	√	
	FTP		√		
	SMTP		√	√	
	SSH	√	√		
	DNS		√	√	
传输层	TCP			√	√
	UDP			√	√
网络层	IP 地址			√	√

以短信 URL 流行一时的相册类恶意程序^[5], 以用户无感知的方式进行安装, 并以 SMTP 发送到指定的邮箱。

(4) FTP

安全策略聚焦在敏感信息窃取。智能终端利用 DNS 协议窃取用户敏感信息的行为, 同样可以用 FTP 实现, 二者都是明文协议, 检测方法类似。

(5) SSH

安全策略聚焦在密码暴力破解、敏感信息窃取。在 Milkydoor 恶意程序家族中, SSH 协议成为黑客构建到企业内网 VPN 的基础协议。由于 SSH 协议是加密的, 无法从明文内容发现恶意网络行为。在支持 BYOD 的企业内网情境中, 应特别关注 SSH 连接的失败次数, 既有可能是黑客在外网尝试内网渗透的活动, 也有可能是智能终端本地的 SOCKS 端口转发配置暂时出现问题。在检测智能终端是否利用 SSH 协议进行敏感信息窃取时, 只能从 SSH 协议的上/下行流量对比做分析。在敏感信息窃取发生时, 上行的 SSH 流量远远大于下行的 SSH 流量。

(6) HTTP/HTTPS 协议

安全策略聚焦在敏感信息窃取、发送 DoS/DDoS 攻击流量。随着 B/S 型互联网应用架构的流行, HTTP/HTTPS 协议的重要性不断提升, 企业边界防火墙对于 HTTP/HTTPS 协议往往采取开放的策略, 给恶意程序的通信创造了可乘之机。在检测智能终端是否利用 HTTP/HTTPS 协议进行敏感信息窃取的攻击行为时, 可通过 Fiddler 获取的 payload 明文信息, 利用正则表达式发现是否有手机号等敏感信息; 在检测利用智能终端是否利用 HTTP/HTTPS 协议发送 DoS/DDoS 攻击流量时, 主要关注一个时间窗口内, 如 1 h 内, HTTP get/post 报文的数量, 如果超过一个阈值, 则可以认为是有发送 DoS/DDoS 攻击流量行为。

4 结束语

IT 产业的摩尔定律极大地提高了各类智能终端的计算能力, 客观上也给互联网黑色产业经济提供了更广阔的发展空间。随着智能手机、可穿戴设备、智能家居等 Android 类智能终端的不断发展和普及利用, 利用其安全漏洞获取设备控制权限, 进一步形成大规模的僵尸网络, 或用于发送 DoS/DDoS 流量, 或用于敏感信息窃取等其他互联网黑色产业交易。长期来看, 在 Android 类终端的恶意程序检测中, 结合传统的动态分析方法, 网络行为分析方法可以提供重要的特征补充, 为机器学习算法的应用创造更有利的条件, 其重要性在不断提升。

参考文献:

- [1] 中国互联网协会、国家互联网应急中心. 图说《中国移动互联网发展状况及其安全报告(2017)》[J]. 信息化建设, 2017(6): 50-51.
China Internet Association and National Internet Emergency Center. "The development of the China Mobile Internet and its security report (2017)"[J]. Information Construction, 2017(6): 50-51.
- [2] 腾讯反诈骗实验室. 2017 年 Q1 安卓 ROOT 类恶意病毒发展趋势研究报告[R/OL]. (2017-05-23)[2017-12-29]. <http://www.itnobug.com/detail/23/583.html>.
Tencent Anti Fraud Laboratory. Research report on the development trend of Q1 Android root malware in 2017. (2017-08-18)[2017-11-29]. <http://www.itnobug.com/detail/23/583.html>.
- [3] 360 互联网安全中心. 内网穿透—Android 木马进入高级攻击阶段(二)[R/OL]. (2016-12-01)[2017-11-29]. <http://www.freebuf.com/articles/terminal/121634.html>.
360 Internet Security Center. Intranet penetration-Android trojan horse into advanced attack phase (two)[R/OL]. (2016-12-01)[2017-11-29]. <http://www.freebuf.com/articles/terminal/121634.html>.
- [4] 汪来富, 金华敏, 刘东鑫, 等. 面向网络大数据的安全分析技术应用[J]. 电信科学, 2017, 33(3): 112-118.
WANG L F, JIN H M, LIU D X, et al. Application of security analysis technology for network big data[J]. Telecommunications Science, 2017, 33(3): 112-118.
- [5] 360 互联网安全中心. 2016 年中国手机安全状况报告[R/OL].



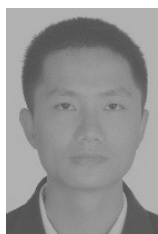
(2017-02-08) [2017-11-29]. <http://www.chinanews.com/it/2017/02-08/8143948.shtml>.

360 Internet Security Center. Report on the safety of mobile phone in China in 2016. (2017-02-08)[2017-11-29]. <http://www.chinanews.com/it/2017/02-08/8143948.shtml>.

[作者简介]



黄勇军（1970-），男，中国电信股份有限公司广州研究院副院长、高级工程师，国务院特殊津贴专家，长期从事通信网络发展规划、新技术应用研究等工作，主要研究方向为 IP 网技术、云计算和网络安全。



刘东鑫（1985-），男，中国电信股份有限公司广州研究院工程师，曾获得 CCIE、CISSP 和 CISA 等认证。主要研究方向为网络与信息安全、大数据安全。



金华敏（1972-），男，中国电信股份有限公司广州研究院高级工程师，主要研究方向为 IP 网、云计算、大数据安全、网络安全。



刘国荣（1978-），男，中国电信股份有限公司广州研究院高级工程师，主要研究方向为移动互联网安全、云计算安全。

汪来富（1976-），男，中国电信股份有限公司广州研究院高级工程师，主要研究方向为 IP 网、云计算、大数据安全、网络安全。

沈军（1976-），女，中国电信股份有限公司广州研究院高级工程师，主要研究方向为云计算安全、移动互联网安全及 SDN/NFV 安全等。