

## 上网行为管理 协议分析系列

### —— QQ 协议概述

**相关主题:** 上网行为管理,PatrolFlow,信息安全网关,带宽管理,流量控制,P2P 控制,BT 下载,邮件监控,IM 控制,游戏监管,聊天监控,内容审计,多链路负载均衡,Web 推送,防火墙,防毒墙

#### 正文内容:

QQ 的版本:

QQ的版本升级比较频繁,而且与多数的软件不同的是,它客户端的升级往往伴随着协议相应的改变。

目前,对研究QQ协议版本比较重要的是:

QQ2000c。它对应的客户端协议版本是 08xx,目前对这个版本的研究比较多。

QQ2003 (0808) 这是腾讯最新公布的QQ版本,目前发现它对应的客户端协议版本是 0A1D。目前对这个版本的研究才刚刚开始,此版本对协议做了比较大的改动。

#### 协议类型:

我们尝试把QQ的协议进行分类:

文字聊天协议族 (TCPF, Text Chatting Protocol Family): 它主要支持与其它QQ客户端进行文字聊天。TCPF是建立在UDP协议之上。UDP数据包中的第一个字符 02 为这个协议族的标识。TCPF的服务器使用 8000 号端口,腾讯的QQ客户端软件一般从 4000 号端口开始尝试使用,但实际上,对客户端使用的端口号并没有限制。目前的研究集中在TCPF上。

其它未知可能存在的协议族:

我们观察到QQ除了与TCPF服务器通信以外,还有与其它的服务器使用UDP进行通信。目前我们观察到的服务器为 218.17.217.111 : 8000。客户端使用与TCPF不同的端口。目前观察到的从客户端发出的包以 06 开头,而服务器返回的包则以 01 开头。目前其具体作用未知。我们注意到一个有趣的现象是,如果选择离线后重新上线,那么在发出登录包之前,这个通讯已

经开始。我们暂时把它命名为数据传输协议族（DTPF，Data Transfer Protocol Family）。最新的研究发现，它传递的是QQ Show的图片数据。

语音、视频聊天：目前还没有开始分析，尚未知道是使用UDP还是TCP协议。

聊天室：没有分析，应该是TCP协议。

随着对这些协议分析的开始，我们会给它们更精细的划分和恰当的命名。

#### TCPF:

TCPF是建立在UDP协议上的协议族，主要支持文字聊天功能。TCPF是以请求—响应模式工作的。也就是说，客户端发出一个请求，服务器端会给出一个相应的响应；服务器向客户端发送信息，客户端也会给服务器相应的响应。请求和响应通过相同的序列号来进行配对（请求代码也应该相同）。而且每种请求的发起方都是相同的。目前，已知的请求包括：

0x0001 注销登录

0x0002 心跳信息

0x0004 更新用户信息

0x0005 搜索用户

0x0006 获取用户信息

0x0009 不需认证方式添加好友

0x000a 删除好友

0x000b 需要认证的方式添加好友

0x000d 设置隐身、示忙等状态

0x0012 确认收到系统消息

0x0016 发送消息

0x0017 收到消息（服务器发起）

0x001a 未知作用。

0x001c 在对方好友列表上删除自己

0x001d 未知作用。

0x0022 登录

0x0026 获取好友清单

0x0027 获取在线好友

0x0030 群操作指令

0x0080 收到系统消息（服务器发起）

0x0081 收到好友状态改变消息（服务器发起）

更多信息请登录 <http://www.byzoro.com>