**一．事件列举**

**事件1:**

通过对视图3的观察我们发现，id为1487号员工的用户的ip地址登录错误的的次数明显高于正常范围。（图3.1）

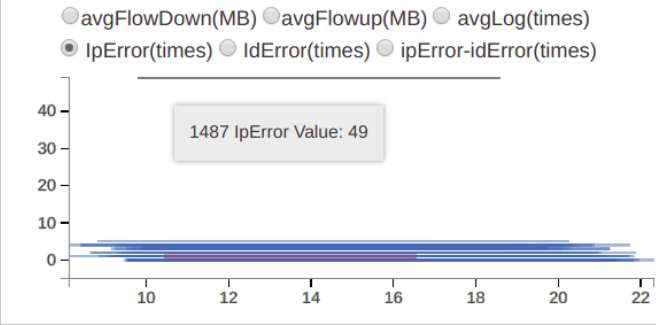


图3.1 各ip地址登录错误次数统计（黑线为1487）

而当统计ip地址登录错误和id被登录错误次数的差值时发现，1487号员工两项统计数据的差值也明显高于正常范围。（图3.2）

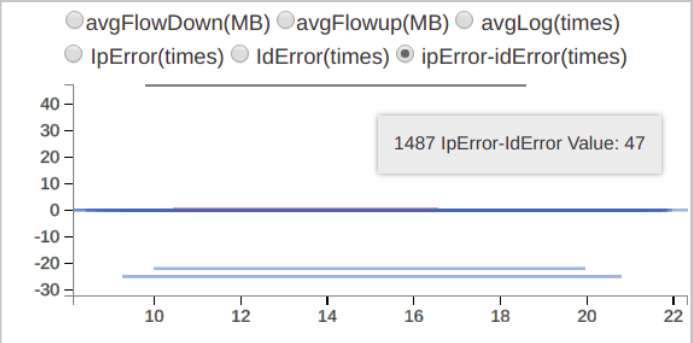


图3.2 各ip地址登录错误次数与各id用户名被登录错误次数差值统计

通过分析，我们认为会产生上述情况的原因是：1487号员工的ip地址的错误登录并非用来登录自己的用户id，而是试图侵入其他员工的用户id。

**事件2**

通过事件1，我们所定了1487号员工为怀疑对像，选中他后，观察视图4我们发现该员工在11月4日在没有产生别的流量协议的情况下产生了ssh协议流量。通过联动，我们在视图五中展示了1487号员工在11月4日的各协议流量情况。（图3.3）

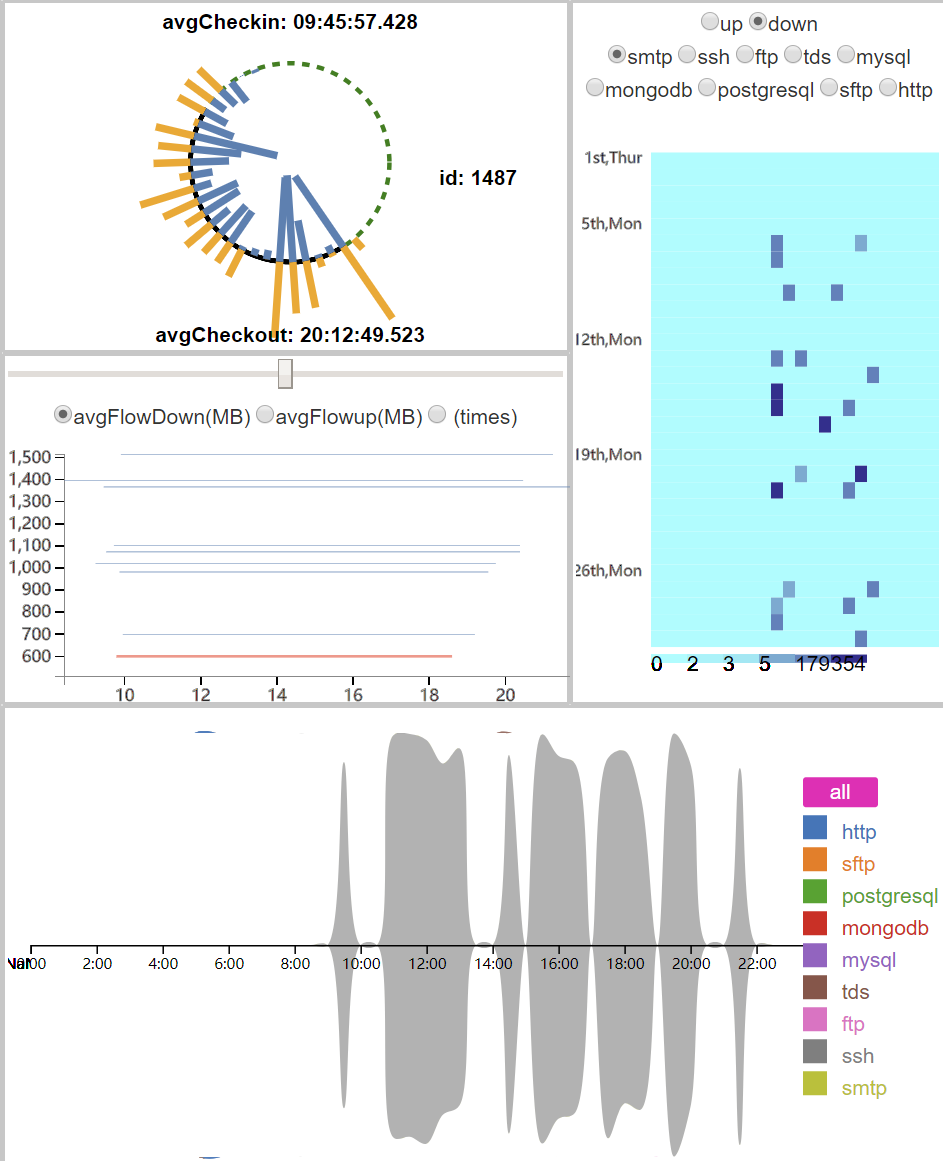


图3.3 1487号员工11月4日流量汇总图

从图3.3 中我们可以看出，1487号员工在11 月4日当天没有到公司签到，也没有登录自己的用户id。并且除了ssh流量外没有产生别的协议流量，这基本排除了他远程工作的可能性。因此1487号员工极有可能在11月4日通过自己的ip地址使用ssh建立连接试图侵入其他员工的用户id。

**事件3**

为了寻找被1487号员工在11月4日侵入的用户id，我们从视图3的统计中，ip地址登录错误和id被登录错误的差值为负数并且明显小于其他员工的员工id，它们是 1211，1080，1228。（图3.4）

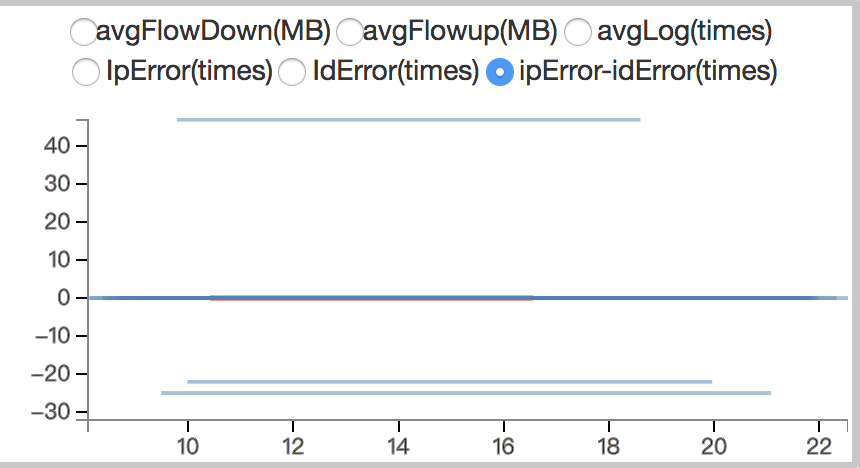


图3.4 各ip地址登录错误次数与各id用户名被登录错误次数差值统计

通过观察三位员工在11月4日当天的流量汇总图，我们发现1211号员工的流量在11月4日存在明显异常。（图3.5）

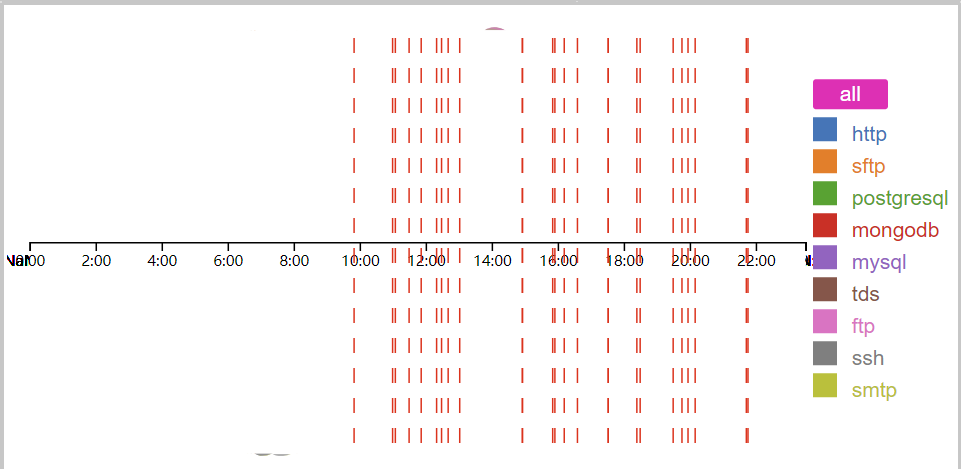


图3.5 1211号员工11月4日流量汇总图

从图3.5中我们可以看出，在11月4日的10:00 到22:00，1211 号员工的用户id被连续多次试图登录并失败，但1211号员工在当天未来到公司也没有产生与工作相关的协议流量。

因此我们猜测在11月4日，1487号员工通过ssh建立链接，从10:00 到22:00 之间一直试图侵入1211号员工账号。

**事件4**

而对于和1211号员工一样账号明显在11月中某些时间被人不断试图入侵的员工 1080。我们采用视图4和视图6联动的方法动态观察他11月每一天的流量汇总情况。发现在11月3日，该员工的账号被多次入侵失败。（图3.6）

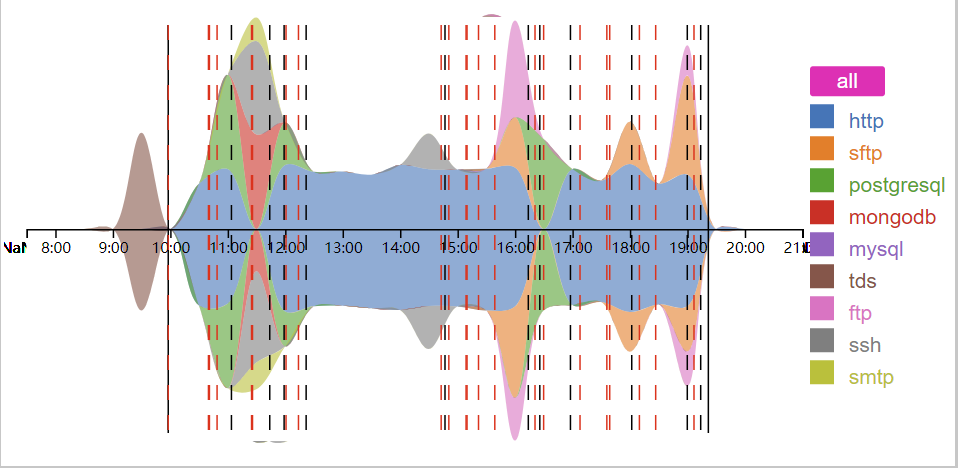


图3.6 1080号员工11月3日流量汇总图

**事件5**

同样的对于1228号员工，我们在动态观察后发现，他在11月6日，也出现了账号被多次入侵失败的异常情况。（图3.7）

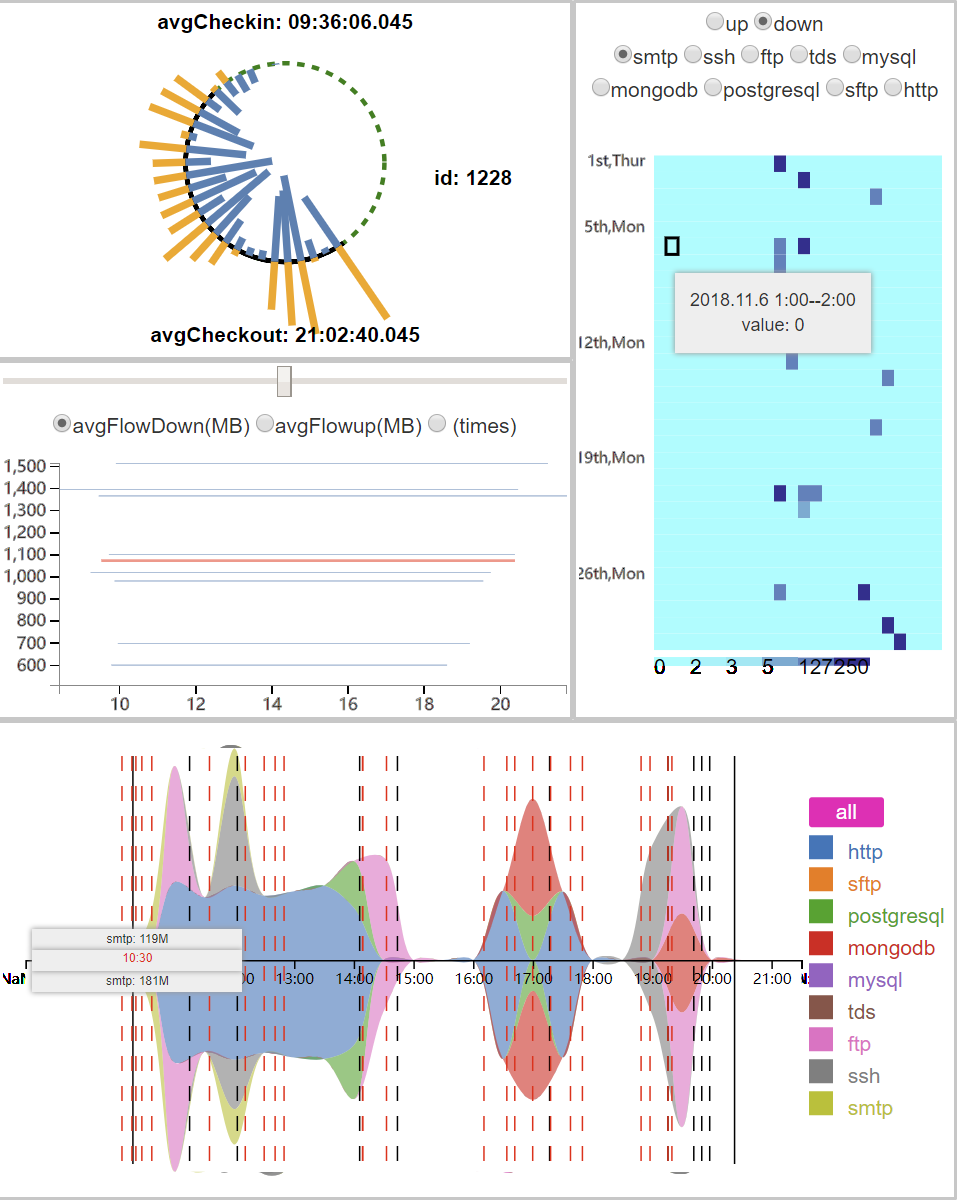


图3.7 1228号员工11月6流量汇总图

**事件6**

联动观察后发现，ip为1281的研发部门员工在他的同组成员中，所产生的下行流量明显要多并且落差很大（图中红线为1281号员工，蓝线表示同组其他员工）（图3.8）

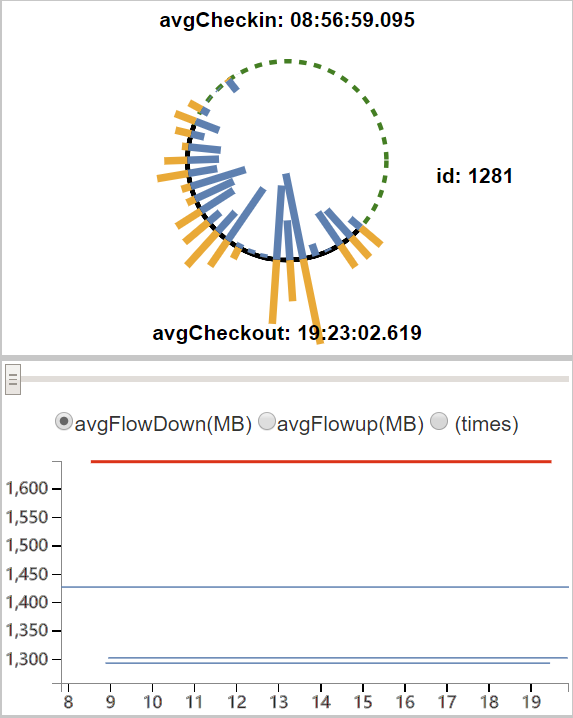


图3.8 1281号宇员工平均下行流量图

**二．事件关联分析**

**人物分析:**

1、事件1，2中试图侵入其他员工账号的1487号员工，事件3，4，5中被侵入账号的1211，1080，1228号员工，和事件6中下行总流量异常的1281号员工都属于研发部门。

2、1080，而被侵入账号的1211，1228号员工都是隶属id为1059的研发部门领导下的二级领导。

3、1487号员工是以1228号员工为二级领导的研发部门小组的成员。

**数据库定向查询添加的信息**

为了得到更多的信息，我们把有问题的员工id在后台mysql数据库中进行了定向查询。得到了以下信息。

1、试图侵入1211、1080，1228号员工账号的ip地址为 10.64.105.4, 即1487号员工的id。

2、1487号员工曾经成功访问过他的领导1228号员工的账号三次，时间分别为：11月6日 19:42:57；11月16日 20:22:04；11月24日12:43:41.

在观察1228号员工 16日和24日的流量情况后（11月6日的流量汇总图在图3.7中已经显示）我们发现在被1487号员工入侵的时间里，1228号员工id产生的流量基本为mysql、mongodb这样的数据库协议和ftp即传递文件协议。（图3.9，图3.10）

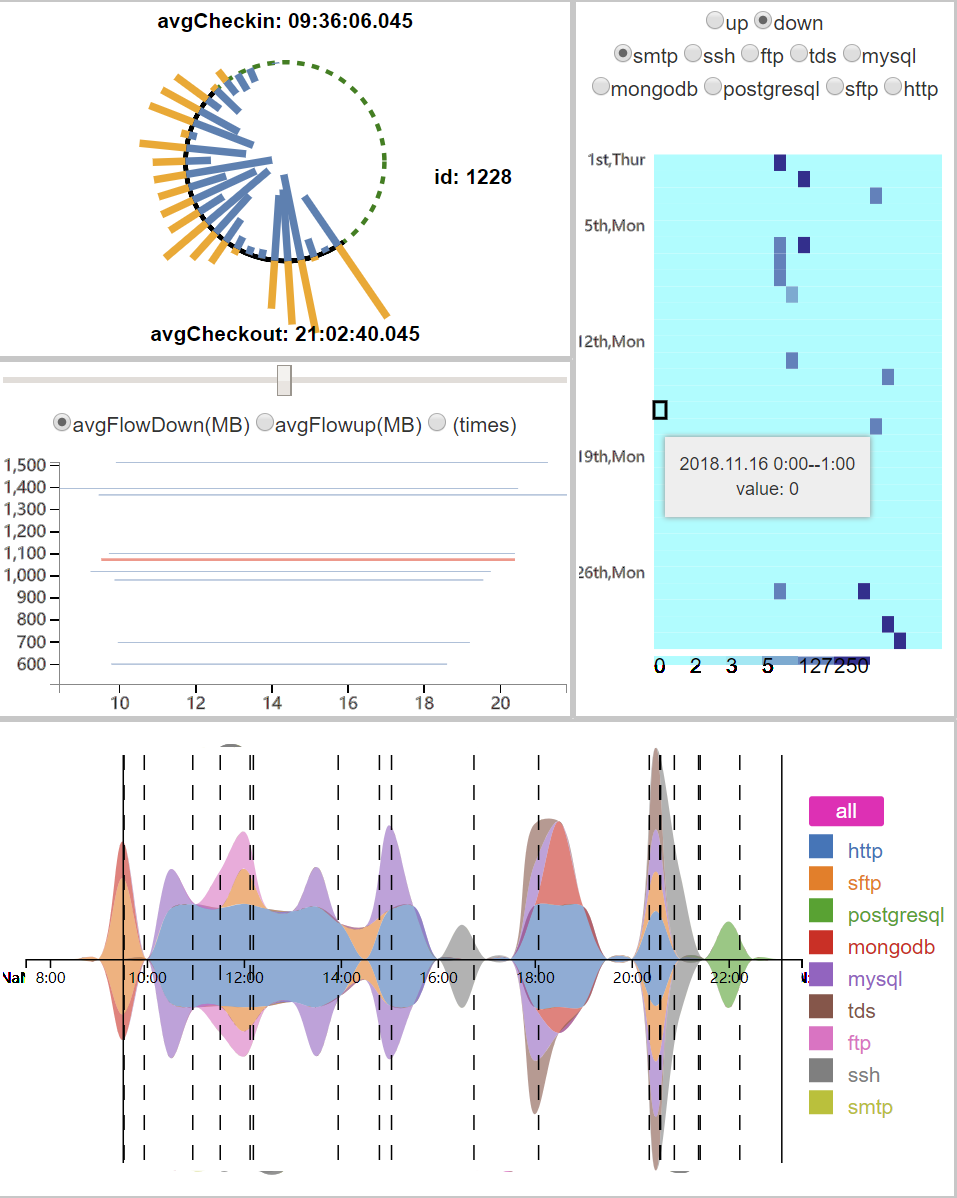


图3.9 1228号员工11月16日流量汇总图

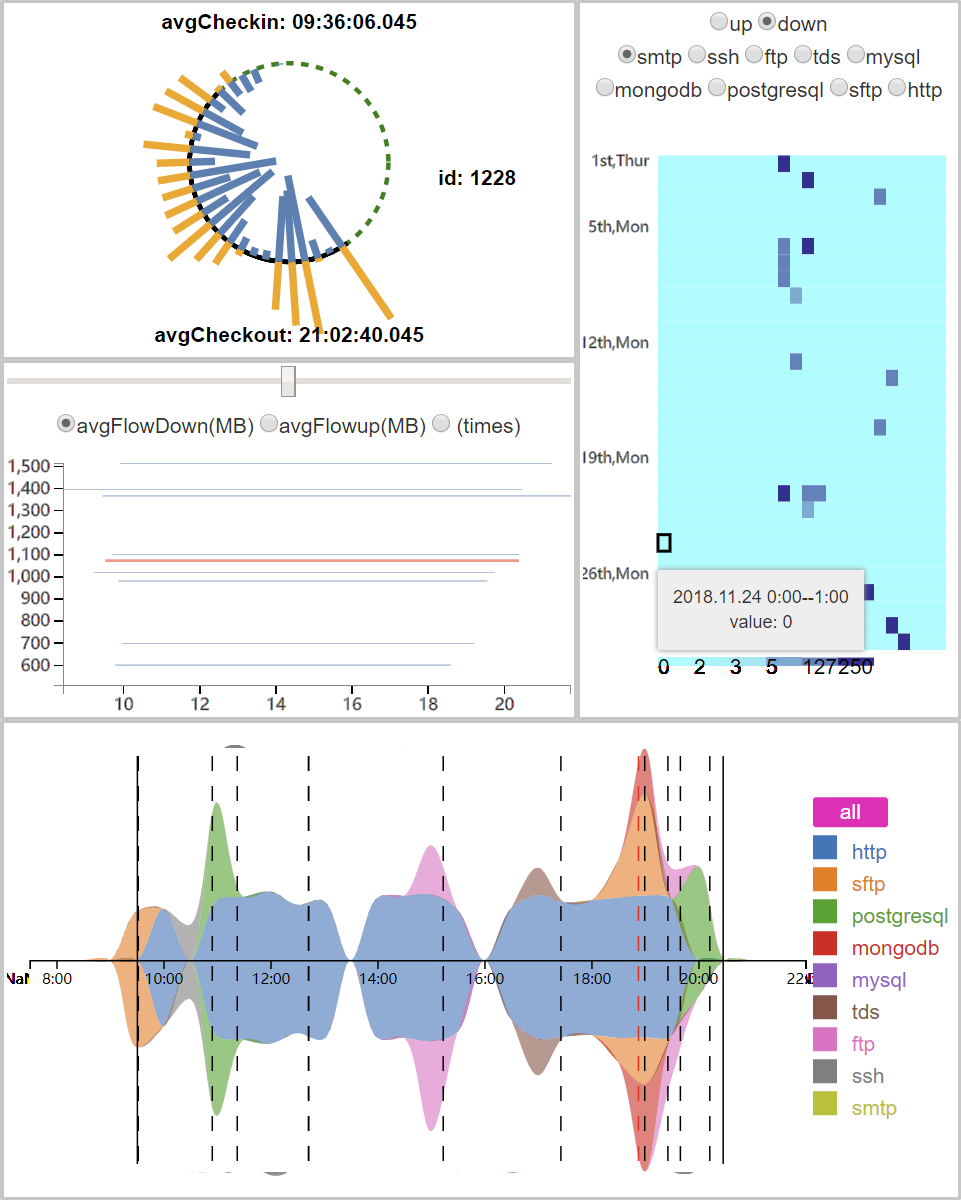


图3.10 1228号员工11月24日流量汇总图

3、 而事件5中流量异常的1281号员工在我们从数据库中定向查询后发现，他和1487号员工同时在11月27日提出了辞职申请。同一天提出辞职申请。而同一天还有1376号员工也提出了辞职，该员工则与同样被是图侵入用户的1211号员工在同一小组。

4、1487号员工的网页浏览协议数据中我们还发闲了其曾经浏览过招聘广告

**分析和猜想**

被1487试图入侵账号的三个员工都是隶属id为1059的研发部门领导的二级领导。他们的账号中很有可能有关于新产品的信息内容

因此我们揣测，很有可能是1487号，1281号，1376号员工共同试图窃取公司新产品的信息向外界传递并且在事后后辞职。