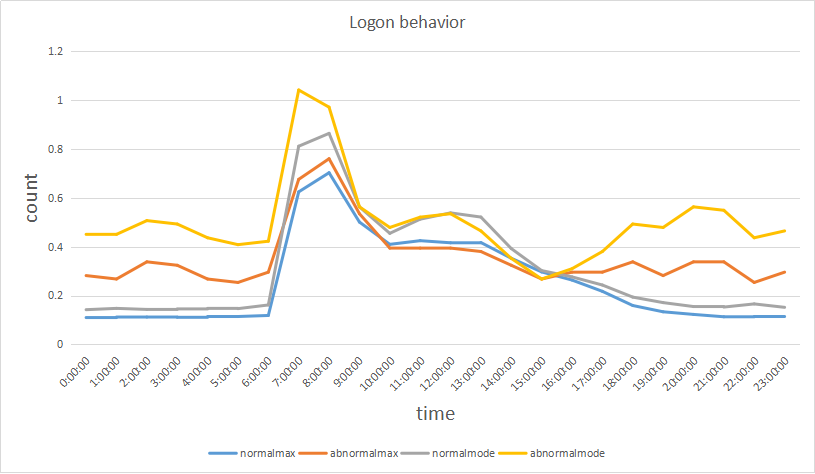
CERT4.2数据集用户行为的数据整理以及图表说明

By 王丹

一．用户登录行为



说明：

图表中

Normalmax：表示正常用户的在每个时间点登录次数的最大值的平均值

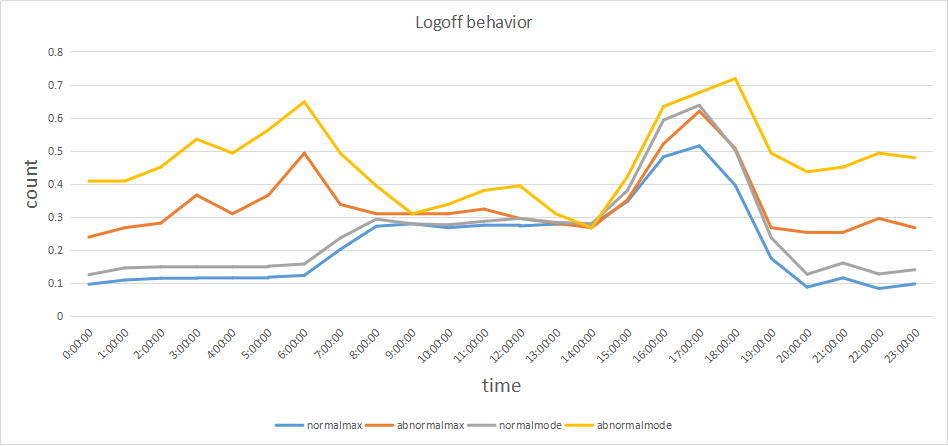
Abnormalmax：表示异常用户子在每个时间点登陆次数的最大值的平均值

Normalmode：表示正常用户在每个时间点登录次数出现最多的次数的平均值

Abnormalmode：表示正常用户在每个时间点登录次数出现最频繁的次数的平均值

由图中可以看出，在每个时间点登录次数最大值上，早上6点到下午5点正常用户和异常用户登录次数基本一致，而在下午6点到第二天早上6点这个时间段，异常用户明显登录的最大次数比正常用户高，这也说明异常用户利用非工作时间进行工作上的事物处理时间更多，成为威胁用户的嫌疑更大；在用户登录次数出现最频繁的值上，异常用户普遍比正常用户的次数更高，尤其是非工作时间段，频繁次数有大幅度的上升，这也表明他们成为威胁用户的概率更高。

二．用户登出行为



说明：

图表中

Normalmax：表示正常用户的在每个时间点登出次数的最大值的平均值

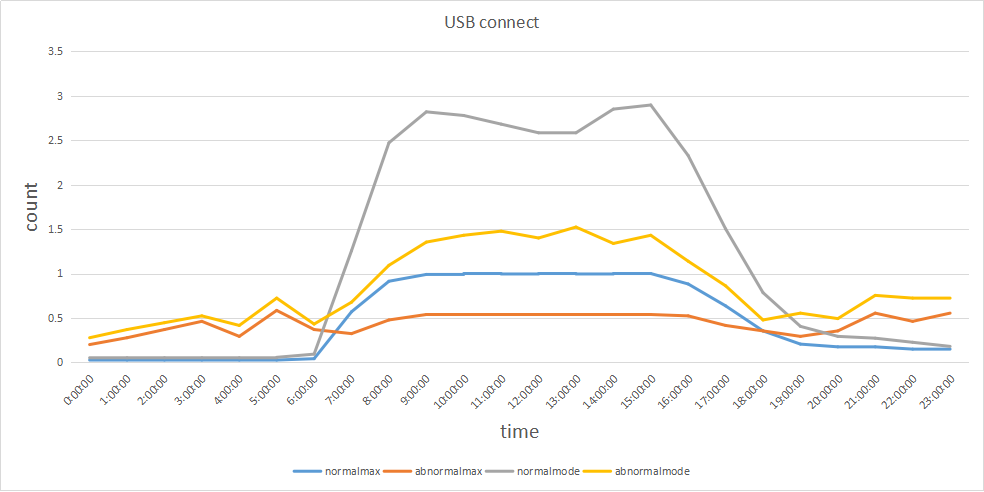
Abnormalmax：表示异常用户子在每个时间点登出次数的最大值的平均值

Normalmode：表示正常用户在每个时间点登出次数出现最多的次数的平均值

Abnormalmode：表示正常用户在每个时间点登出次数出现最频繁的次数的平均值

这和前一张图的用户登录操作是相照应的，异常用户普遍在登出次数最大值以及登出次数出现最频繁值上面在非工作时间段比正常用户高出许多，这增大了他们异常行为的概率。

三．用户连接USB移动设备行为



说明：

图表中

Normalmax：表示正常用户的在每个时间点连接上USB移动设备次数的最大值的平均值

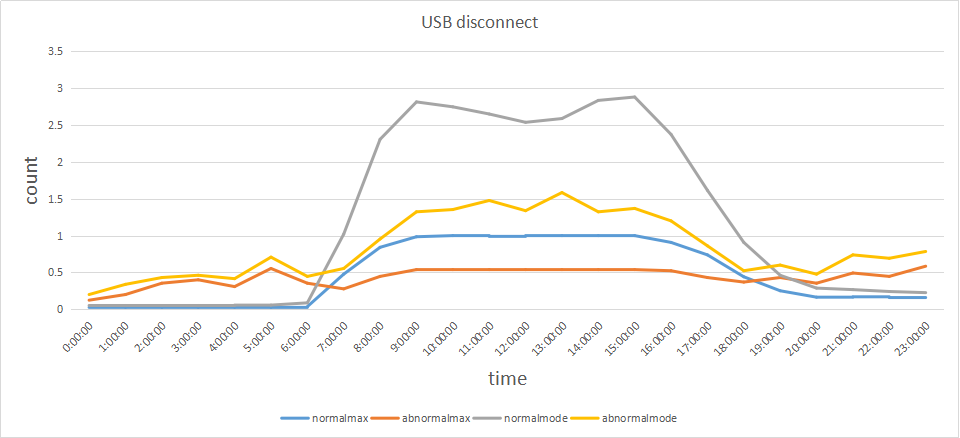
Abnormalmax：表示异常用户子在每个时间点连接上USB移动设备次数的最大值的平均值

Normalmode：表示正常用户在每个时间点连接上USB移动设备次数出现最多的次数的平均值

Abnormalmode：表示正常用户在每个时间点连接上USB移动设备次数出现最频繁的次数的平均值

由上图可以看出，在工作时间也就是早上6点到下午6点这个时间段，正常用户的连接USB移动设备的最大次数以及出现最频繁的次数都普遍比异常用户高，这可理解为他们在工作时间的正常工作行为，而在非工作时间，异常用户的连接USB移动设备的最大次数以及出现最频繁的次数都比较高，而正常用户在凌晨0点和6点之间几乎没有操作，这段时间使异常用户有了更大概率的异常行为操作，例如，拷贝公司内部文件等。

四．用户断开USB移动设备行为



说明：

图表中

Normalmax：表示正常用户的在每个时间点断开USB移动设备次数的最大值的平均值

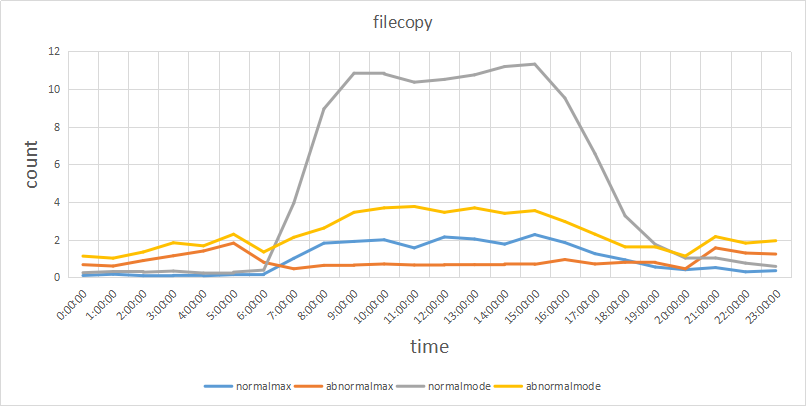
Abnormalmax：表示异常用户子在每个时间点断开USB移动设备次数的最大值的平均值

Normalmode：表示正常用户在每个时间点断开USB移动设备次数出现最多的次数的平均值

Abnormalmode：表示正常用户在每个时间点断开USB移动设备次数出现最频繁的次数的平均值

这和前一张图的用户连接USB移动设备操作是相照应的，异常用户普遍在断开次数最大值以及断开次数出现最频繁值上面在非工作时间段比正常用户高出许多，这增大了他们异常行为的概率。

五．用户拷贝文件行为



说明：

图表中

Normalmax：表示正常用户的在每个时间点拷贝文件次数的最大值的平均值

Abnormalmax：表示异常用户子在每个时间点拷贝文件次数的最大值的平均值

Normalmode：表示正常用户在每个时间点拷贝文件次数出现最多的次数的平均值

Abnormalmode：表示正常用户在每个时间点拷贝文件次数出现最频繁的次数的平均值

由图可知，正常用户在工作时间进行文件拷贝的最大次数比较多，而工作时间中在出现次数最频繁的值中，是普遍偏高的，这可理解为是相关部门专门从事文件操作的事物，而他们在非工作时间上，在下午6点到晚上12点可理解部分加班操作，而晚上12点到6点基本上没有操作的，而异常用户在平时的工作时间对文件的操作次数普遍比正常用户低，这说明他们平时需要接触文件工作的事物不多，而在非工作时间，尤其是晚上12点到凌晨6点这个时间段，他们却很活跃，对文件的操作次数比正常用户要高，这说明他们很有可能在进行一些不为人知的事情，例如拷贝公司重要文件，重要数据等操作。这符合他们异常用户的身份。