某厅级服务器挖矿简单调查报告

通过对之前宿松市住建局公务员利用公职便利参与黑色产业链的了解，习科近期对流量挖矿现象进行了调查，发现多地政府服务器存在流量挖矿。习科对此展开了深入调查，发现大多政府公职人员存在利用公职便利参与黑产不多，小黑盘踞服务器挖矿的居多。

此调查让习科建设的国内黑色产业花名册的数据来源又多了一条可靠的途径(之前一直从乌云等平台收集黑色产业人员数据)。习科选取其中一个案例对其简单分析，借此警示各地服务器管理员和黑色产业从业者，且挖且珍惜。

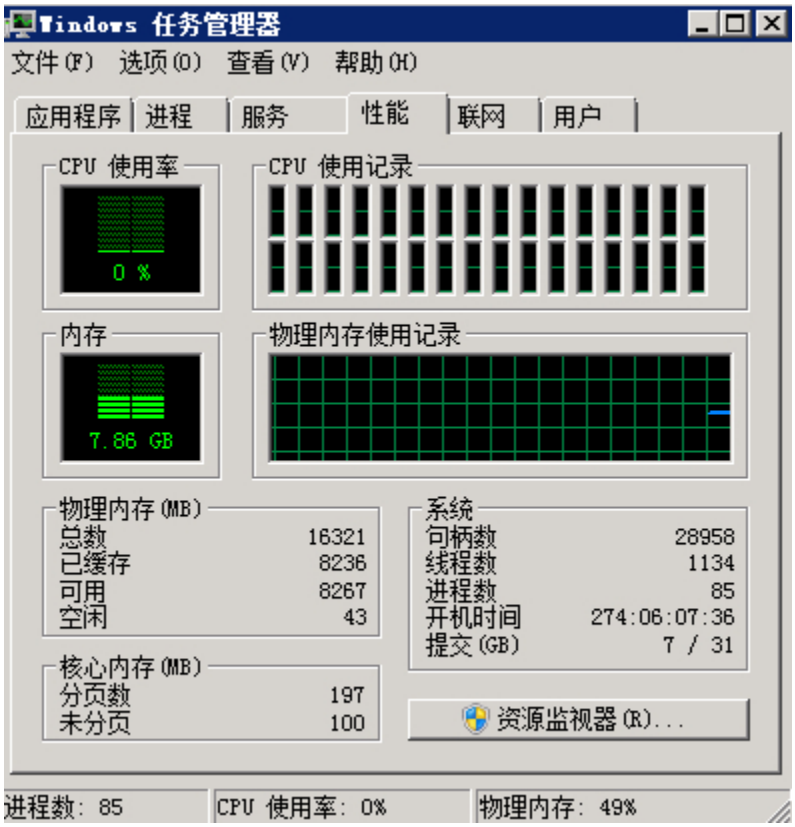
服务器是某省厅级的服务器，一般来讲政府服务器上跑流量矿石有两种可能。

第一，内部公职人员利用职务便利使用服务器资源，一般这种情况发生在较基层的政府部门，雇佣的公职人员不多，薪酬较少，偶尔也发生在第三方外包公司里面。

第二种可能就是服务器被小黑搞上以后有人在偷偷跑流量矿石，国内但凡存在漏洞的政府单位服务器，基本上都被小黑占据了，服务器上面不是挂了黑链就是挖矿。

根据前面调查的数据，一般厅级服务器内部人员挖矿的可能性不高，所以调查从这里开始了。

这台机器在内网环境，但是可以转发到外网，是一台 2008 R2 的服务器，配置还不错，16G 内存，志强 E7 4820 的 CPU 共 32 个线程。

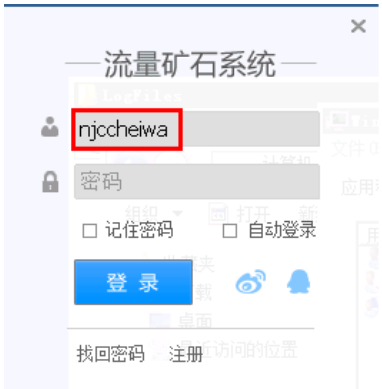


这种配置高，带宽高，稳定性高的内网环境高配服务器可谓是深受挖矿人士喜爱。

管理员的不上心，一般会助长小黑们的嚣张气焰，像这台服务器流量矿石和 TeamViewer 的图标都直接放在桌面上，小编就不吐槽了。

服务器的稳定性高，流量矿石跑的很欢。打开任务管理器后发现流量矿石挂在一个叫做 sql 的用户的进程上。

直接在任务管理器里将进程杀死，然后再重新打开一遍。本来想要看看小黑挖了多少矿石，不过看到有用户名，那就先去调查一下矿主吧。

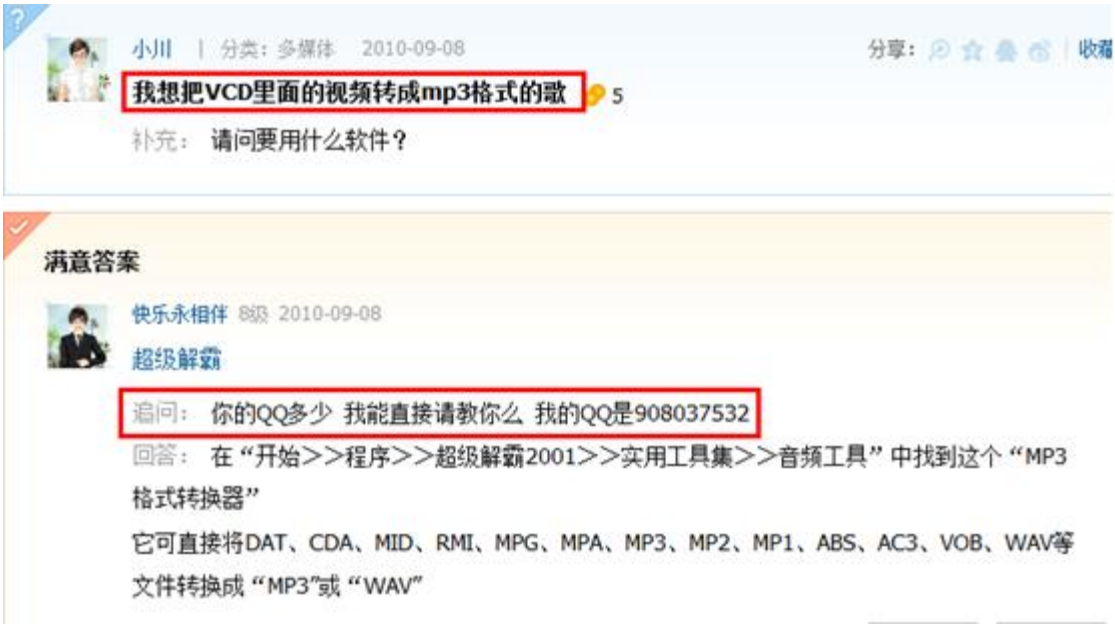


现在已经知道小黑的快播用户名是 njccheiwa，随便百度了一下，小兄弟你在网上的资料还真不少。比如微博(t.qq.com/njccheiwa)。

通过花名册数据库和户籍系统的比对，微薄上写的资料除了认证和生日(没记错应该是 19891212)以外，其他基本上属实。

这让小编想起了冒用绿盟认证的 GoodDog，小编不得不说，现在的年轻人意淫症真的是愈发严重了。

按照微薄上的资料顺藤摸瓜找到了 QQ 号码 908037532 与挖矿的矿主是同一个人。



进一步搜索，从 2010 年小兄弟还年轻的时候，到三年后自己都做卡盟了。这个网站被黑过，而且域名已经失效，域名的 whois 信息已经收集不到了。不过嘛。。。

从服务器日志中的 ip，到论坛的匿名 ip，基本已经可以查到水表精准位置了。

小兄弟果然还是涉世不深，**南江县长赤镇环城路神马的**，小编就不说了，小兄弟可能常年给别人送快递，有没有想过哪天自己被别人送快递呢？

常在河边走哪有不湿鞋，黑产不归路，不要以为靠某某平台洗白了就没事了，花名册都给你记着呢。谁帮小编 AT 一下四川网警，大家一起来找茬？