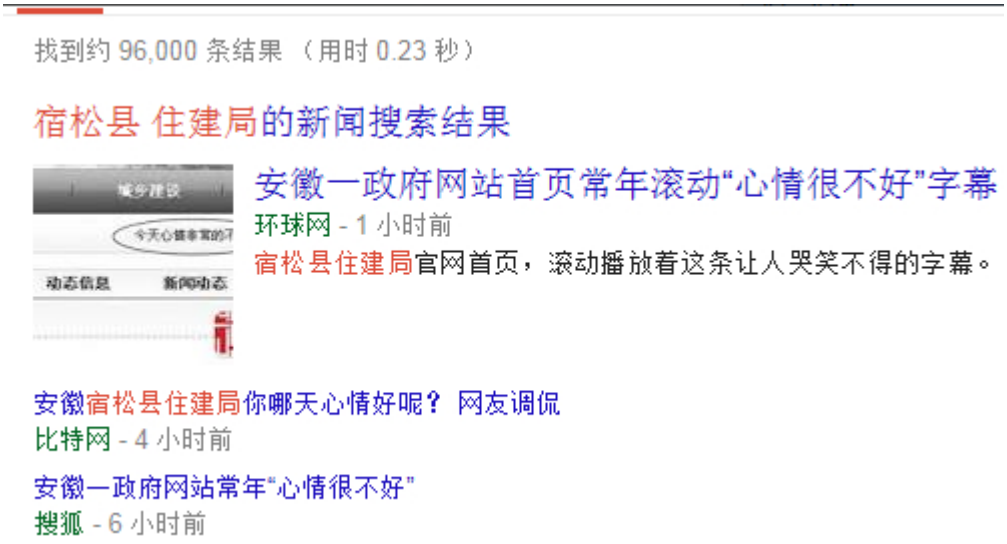
宿松住建局心情很不好 - 深入挖掘公务员搞黑产

作为政府的脸面，官方门户网站通常会格外的引人关注。

最近，以为一条网站广播又火了一个网站门户，宿松县住建局网站。不知道谁最先在微博上吼了一句“安徽一政府网站常年滚动'心情很不好'的字幕”，某政府网站宿松县住建局网站(zjj.susong.gov.cn)立马火了。

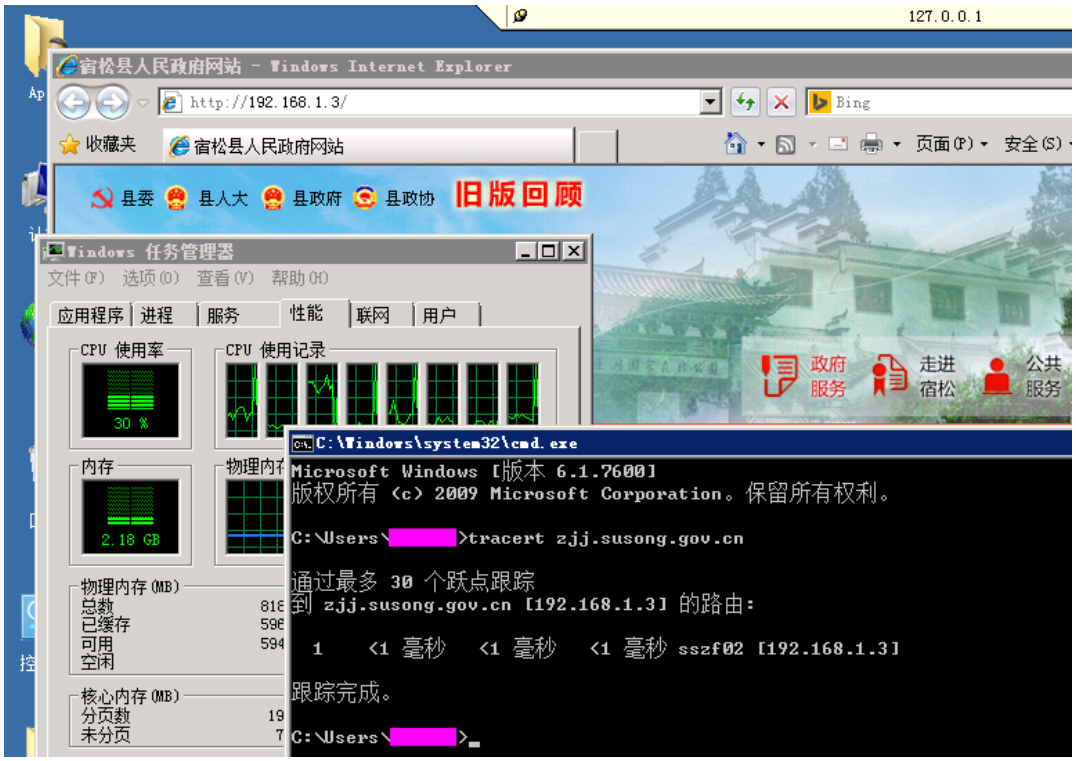


这条新闻刚火，小编就发现网站已经打不开了。究其原因并不是管理员处理动作快，而是。。。大量的访问如同 DDoS 一般。。。挂了。习科论坛某会员(xiaotianx)深入分析发现，网站“心情很不好”是有深层原因的。。

220.180.202.28，该 ip 下有多个 susong.gov.cn 的网站(包括宿松县门户主站)，应该归属同一部门管理。至于住建局归谁管。。。其实这不重要。一起看下去。

站点多了，难免有很(Bu)多(Shang)漏(Xin)洞，就像产品线长了会出很多问题一样。某一个非常非常低级的问题，导致了某一台同局域网下的机器可以轻松获得管理员权限(经过检查，已然是马场，会员 xiaotianx 出于好心已经做了临时修补)。

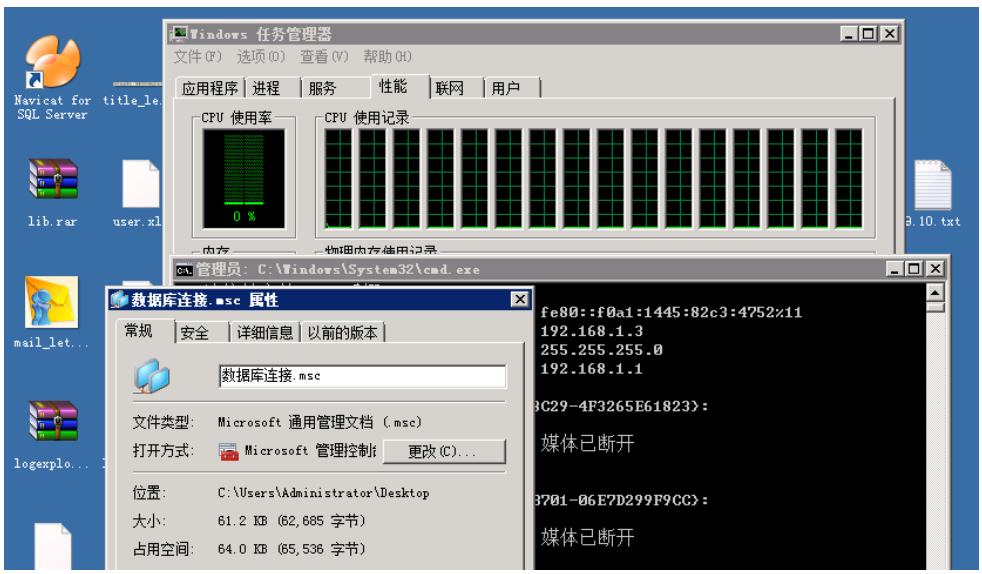
然后看一下宿松县住建局在内网哪台服务器。



目标在 192.168.1.3，估计所有站都在上面了。

PS:其实小编很在意这台服务器的配置，答案 xiaotianx 稍后为大家揭晓。

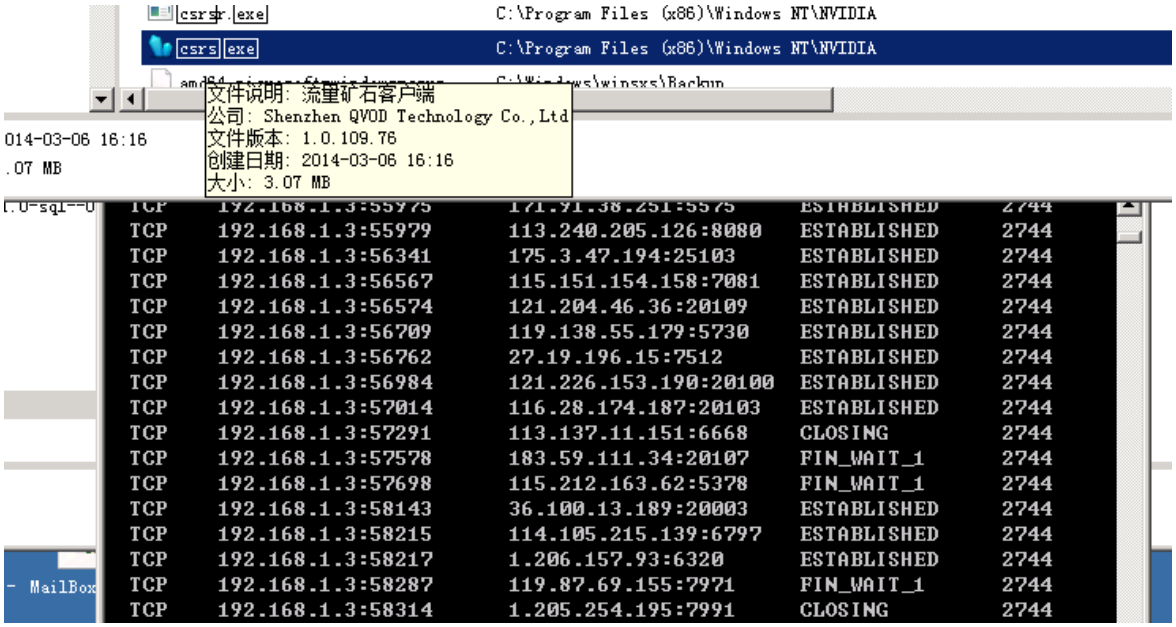
显然这种水平的防护对于内网渗透来说形同虚设。稍后便登陆了目标站点所在的服务器 192.168.1.3。顺便提一句，管理员非常人性化的把数据库服务器的管理钥匙直接做成连接，双击就自动登陆 3389，核心数据库服务器唉。



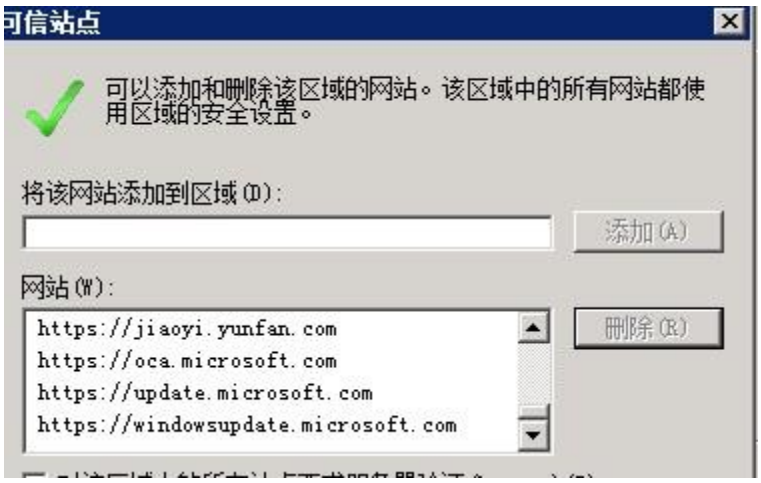
没完呢。到底管理员因为什么心情很不好呢？这么高的配置，这么多的服务器。

宿松县，人口 80 万左右，生产总值 140 亿，历史名城，拿着纳税人的钱。。。

呵呵，自己看吧。



小编也很想知道，这是什么？ QVOD 的流量矿石，这个软件是干什么的，圈里的人一眼就明白，不明白的小编也不多发表评论。小编其实一直想说，这是黑客装的吧？xiaotianx 告诉小编，这是管理员自己装的。



每一台服务器配置都很高，每一台服务器都只有 administrator 用户和被禁的 guest 用户，每一台服务器都没有远控木马，每一台服务器的信任列表。。每一台服务器的卡巴斯基都很猛。。。

想必“心情很不好”绝对不是偶然或者意外，这种管理员。。。麻烦县政府下次招人的时候认真点好吗？

挖社会主义墙角，搞社会主义黑产，拿纳税人的钱发点意外小财，真的很有想法，发改委不请你去真的可惜了人才。

在 Google 以私服等为关键字搜 gov.cn 或者 edu.cn 的数量很多很多，真的都是黑客所为？

其中有很大部分比例都是公务员自己干的，呵呵，青年政治学院高配高带宽放 17G 肛交电影+种子，电子科技大学高配高带宽服务器架 VPN 装(Zi)free(You)gate(Men)。请问你们拿着纳税人的钱都干了什么？