深入理解GFW：总论

GFW，Great Firewall of China，防火长城，通常把它看作一个国家级的网络审查系统。关于网络审查，人们通常首先会有一番政治性的话要说，不过政治批评这个角度的言论实在是过多，GFW的实体在“GFW”这个这个巨大的外壳之下隐藏了多年，人们只是对着“GFW”这个词空发怒气却并不知道它究竟是什么。实际上GFW除了是一个让网民十分不舒服的系统之外，在技术上它还是一个非常复杂有趣的黑箱，一个通关奖品是网络自由的解谜游戏。接下来一段时间我们便会对GFW进行深入的探索和理解，大家很快就会了解到它的趣味。提示：阅读此“深入理解GFW”系列之前建议读者对TCP/IP协议族、网络安全、反向工程有基本的了解。

GFW的技术结构

知己知彼，百战不殆，我们应该先对GFW有清晰的技术性认识。防火长城条目称GFW的主要技术是域名劫持、IP封锁、关键字过滤阻断、HTTPS证书过滤。实际上这些技术在实现上可以归结为两种技术：IP封锁和入侵检测，其中入侵检测是核心。IP封锁因为比较底层，接近于切光缆拔网线，没有什么技术可言，这种封锁实施以后除了绕道而过也没有更好的解决办法。而入侵检测则是GFW最为强大灵活的功能。

传输层的TCP和UDP解析都是入侵检测业界的标准配置。UDP通常用来做DNS查询劫持，一个附加效果就是国内的域名缓存充满了麤。TCP主要用作阻断，方式很多了，总之只要把攻击者的连接关闭掉/阻止攻击者进行连接就行了。应用层就更加百花齐放了，因为解析一个协议实在不是一件困难的事情。所谓的SSL证书拦截也不过是稍微做了一下SSL/TLS协议的解析而已，并无神秘之处。这就是入侵检测的强大之处。

入侵检测的灵活之处在于它的部署和撤销都很便捷无副作用无延迟，匹配精确无误伤。举一例，要防止一些反动软件通过https访问google docs获取信息，怎么做？在应用层检测证书显然是杀鸡用牛刀浪费性能了；用动态路由封特定IP的特定端口是不行的，因为解析结果在不断地变，动态路由的变化跟不上；用域名污染更不行了，把80端口的web业务也搞掉了，影响太大；所以就在传输层乱发RST做无状态的连接阻断，写个脚本定时更新解析结果，这也就是google的数据中心只有在中国解析出来的那部分被封掉的原因。什么时候领导对谷歌的红包满意了，随时撤掉。

GFW的设备有两种，一种是在北京、上海、广州搭在总交换中心上做旁路监听的入侵检测设备，一种是放在ISP那里的动态路由设备。一般来说入侵检测总是比动态路由来得灵活，所以RST要比封IP更常用。另外，碰到网站无法访问然后traceroute发现线路死在ISP骨干上于是责怪ISP，这是不合理的。中国的ISP的一项主要业务就是接待各个强力部门的插入，纪检、军队、公安之类的部门都会长期插入。

GFW的工作方式

GFW的日常工作方式：当国新办发现了反动文宣，当公安部十一局发现了色情图片，当版署发现了海盗网站，总之当有关部门发现了有害非法信息，就发指令给GFW，然后GFW的政策部门研究一下采取怎样的具体封锁措施为宜，然后将具体操作交给技术部门执行封锁。解封也是一样的渠道，简而言之就是领导一句话胜过千军万马，至于让领导发这一句话靠的就是PR了。举一例，受到NED暗中操控的twitter长期以来充满反动有害信息，但做技术的人都明白twitter的这种架构是没有办法封的。对twitter.com什么办法都用了，效果不大好，结果领导不满意地催促了。这个交不了差是很严重的事情啊，怎么办呢，就对twitter搞破坏吧。凡是跟twitter有关的第三方网站，见一个斩一个，领导你看我都把twitter诛九族了，这已经是自古以来用刑的极致了。再举一例，如何封掉一个网站？先在这个网站上放置一些有害非法信息，再去违法和不良信息举报中心（后台国新办）举报之，等十天就成了。

GFW的研发方式：“国家信息安全管理系统”建设的历史参见《阅后即焚》。当有关部门发现了一个反革命翻墙方法，就告诉GFW，然后GFW的逆向工程人才研究一下这个方法的工作方式，找到它的特定模式和弱点，制定相应的封锁预案。当有关部门指示实施封锁的时候，预案便付诸实施。p2p方面的反动软件比较不好办，于是在第一生产力院成立242项目“P2P协议分析与测量”专门研究之。

GFW实体是安管中心（CNCERT/CC），是事业单位。一个事业单位的政治地位可以想是很低的，凡是它的上级都可以向它下指令进行网络封锁，而它本身则没有任何主观能动性，专于业务，勤勤恳恳抓好国家安全基础设施的建设。如果转换角度，从GFW的视角来考虑，那么GFW所做的事情其实并不神秘，其实恰恰符合了它自己的名义。我们来看看精美的“宽带网络环境下恶意代码监测系统”，你们这些反革命访问一下blogger、wordpress那就是URL攻击啊，而且要比一般的钓鱼攻击和病毒更严重，因为危害的是党和国家的安全啊。GFW的研发也与一般的网络安全公司所做别无二致，监视分析网络流量，逆向工程有害软件，阻断恶意攻击，区别只在于：GFW为了国家安全也要处理一下你们这些反革命的攻击；另外GFW还开了金钱无限、人口无限和无敌秘笈。

GFW与网民的生态系统

政府、GFW与网民构成了一个生态系统，政府与GFW共生于食物链的上端，网民处于食物链的下端。有人称之为“猫和老鼠的游戏”。观GFW与网民的互动历史，可以归结为相互提升技术水准的军备竞赛，但尽管如此两者的关系也从来没有打破GFW越来越善于主动追捕网民越来越善于被动逃避的模式。从最开始的普通HTTP代理、SOCKS代理，到以自由门为代表的一批加密代理软件，到种类繁多的网页代理，到VPN、SSH代理，到p2p网络，以及混合方法。然而这些方法都未曾彻底免于GFW的封锁，这是因为GFW很善于进攻，而网民们迄今为止只会不断地四处寻找新的逃避办法。

这种互动模式的问题在于，随着军备竞赛的继续，GFW越来越完善越来越强大，而网民不断地失去手中的牌，翻墙的难度和成本越来越高。GFW是这个领域（网络安全）的专业人士，而网民虽然富有群体智慧，但是其技术能力缺乏有效组织不能与GFW对等。因此如果稍微看得远一些就会了解到，这种模式对于网民来说是不可持续的，总有一天GFW会超过绝大多数网民的技术基准线。所以，唯一的出路便是改变方式，突破这种模式。

应对GFW

网民突破当前被动态势方法的基本原理，在后面的章节中我们会看到，在于利用GFW在善于进攻的同时不善于防守的特点。与其把GFW看作国家网络暴力机关，不如把GFW看作一个网络安全机构，事实上它也是一个网络安全机构（CNCERT/CC）。任何安全系统必然都有漏洞和弱点，它所提供的这个GFW安全解决方案（国家信息安全管理系统）也不例外。网民并非缺乏技术，而是技术没有得到有效组织，没有往这个方向进行有效投射。实际上GFW漏洞和弱点并不少，有一些甚至是理论上无法解决的，这在以后会详细论述。正如《阅后即焚》一文所言，GFW尽管是中国少有的顶尖科研力量与国家强力支持结合的产物，“但也无法摆脱山寨的本性——做一个东西出来很容易，但是要把这个东西做得细致严格就不行了”。

更进一步，除了利用GFW本身的问题以外，网民甚至还可以考虑采取网络正当防卫的方式阻止GFW的非法行为。像GFW这种机构，无行政立法，无舆论监督，无申诉渠道，被少数别有用心的人利用，滥用国家安全之名义，封锁与国家安全毫无关系的网站，对合法的网络通信进行干扰和攻击，“对计算机信息系统正在进行传输的合法数据进行篡改，向计算机信息系统进行攻击令其无法正常运行”，甚至曾多次造成全国性网络故障，已触犯《中华人民共和国刑法》第二百八十六条，情节特别严重，后果特别恶劣，云云。

然而另一方面，GFW与网民之间已经或者即将形成某种稳态，这种稳态是双方斗争状况下的动态平衡，是需要有意识维护的。一个无法控制的网络是无法被政府所容忍的，当网络无法控制时政府是不吝于切断一切网络的（你一定知道我在说什么），稳态的破坏也就意味着环境的毁灭。一个理想的稳态就是网络处于“看起来”可以控制的状态，让GFW处于不断取得小型封锁成功的虚幻胜利感之中，网民个人各自掌握非中心化的翻墙方法。一个中心化的大众翻墙方法（最典型的例子就是设置hosts静态解析）必定无法避免被当局发现并被GFW封锁。下一代的翻墙方法应该是去中心化的（p2p）、小众的、多样化的、混合型的、动态更新的。

参考文献

有两篇重要文献在这里要推荐。

首先是Thomas Ptacek等在98年发表的Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection。这篇是在入侵检测领域具有里程碑意义的论文，是论述入侵检测原理性漏洞的集大成者。其简明介绍早在07年就出现在英文维基，非专业人士可以一睹为快；专业人士建议仔细阅读原文，以后关于探索GFW漏洞的技术都基于此篇论文所描述的原理。

另外一篇是《阅后即焚：“GFW”》，是一份关于GFW的详尽的社会调查，澄清了大量关于GFW的误解，本文大量引用此文。这篇文章的重要性从侧面可以发现：前面引用过中文维基的防火长城条目，如果直接访问会发现，这个条目直接访问之后维基百科就被封锁了。这是有原因的，而且原因是可以找到的，寻找原因的方法将在以后几节介绍，这里长话短说原因就是：这个页面中含有一个关键词：“阅后即焚”。与一般的关键词不同，这个关键词很厉害，随便什么地方出现这个关键词都会引起有趣的现象，比如这里，这种现象通常被人们称为深度包检测。像法轮六四这样煽动颠覆的词语都没有成为深度检测关键词，这种顶级过滤的词很少，另一个例子就是GFW头号死敌的名字：“dongtaiwang.com”。一般来说，越是被禁止，就越有趣；越是被否认，就越接近真相。另外注意到，有一篇内容相似的文章《GFW的前世今生》，对比两者发现后者似乎被添加了一些不相关或者夸张性的文字，原文应该是首发在自曲新闻的前者。

在下一次的文章中我们将介绍GFW进行黑箱分析的方法，并得到一些有趣的结果。

Update：“阅后即焚”不再是全文关键词。

深入理解GFW：DNS污染

初识DNS污染

翻墙新手们往往遇到这样的问题：我明明已经设置了socks代理为127.0.0.1:xxxx，为什么还是上不去youtube？这时经验丰富的翻墙高手就会告诉你：firefox需要设置network.proxy.socks\_remote\_dns为true，也就是远程解析域名。这是怎样一回事呢？为什么要远程解析？这就涉及到了GFW的DNS污染技术。

DNS（Domain Name System）污染是GFW的一种让一般用户由于得到虚假目标主机IP而不能与其通信的方法，是一种DNS缓存投毒攻击（DNS cache poisoning）。其工作方式是：对经过GFW的在UDP端口53上的DNS查询进行入侵检测，一经发现与关键词相匹配的请求则立即伪装成目标域名的解析服务器（NS，Name Server）给查询者返回虚假结果。由于通常的DNS查询没有任何认证机制，而且DNS查询通常基于的UDP是无连接不可靠的协议，查询者只能接受最先到达的格式正确结果，并丢弃之后的结果。对于不了解相关知识的网民来说也就是，由于系统默认使用的ISP提供的NS查询国外的权威服务器时被劫持，其缓存受到污染，因而默认情况下查询ISP的服务器就会获得虚假IP；而用户直接查询境外NS（比如OpenDNS）又可能被GFW劫持，从而在没有防范机制的情况下仍然不能获得正确IP。然而对这种攻击有着十分简单有效的应对方法：修改Hosts文件。但是Hosts文件的条目一般不能使用通配符（例如\*.blogspot.com），而GFW的DNS污染对域名匹配进行的是部分匹配不是精确匹配，因此Hosts文件也有一定的局限性，网民试图访问这类域名仍会遇到很大麻烦。

观测DNS污染

“知己知彼，百战不殆”。这一节我们需要用到前面提到的报文监听工具，以及参考其DNS劫持诊断一节。在Wireshark的filter一栏输入udp.port eq 53可以方便地过滤掉其他无关报文。为了进一步减少干扰，我们选择一个并没有提供域名解析服务的国外IP作为目标域名解析服务器，例如129.42.17.103。运行命令nslookup -type=A www.youtube.com 129.42.17.103。如果有回答，只能说明这是GFW的伪造回答，也就是我们要观测和研究的对象。

伪包特征

经过一番紧密的查询，我们可以发现GFW返回的IP取自如下列表：

4.36.66.178

203.161.230.171

211.94.66.147

202.181.7.85

202.106.1.2

209.145.54.50

216.234.179.13

64.33.88.161

关于这八个特殊IP，鼓励读者对这样两个问题进行探究：1、为什么是特定的IP而不是随机IP，固定IP和随机IP各自有什么坏处；2、为什么就是这8个IP不是别的IP，这8个IP为什么倒了GFW的霉？关于搜索这类信息，除了www.google.com之外，www.bing.com有专门的搜索IP对应网站的功能，使用方法是输入ip:IP地址搜索。www.robtex.com则是一个专门收集域名解析信息的网站。欢迎读者留下自己的想法和发现:lol:。

从Wireshark收集到的结果分析（实际上更好的办法是，将结果保存为pcap文件，或者直接使用tcpdump，由tcpdump显示成文本再自行提取数据得到统计），我们将GFW发送的DNS污染包在IP头部的指纹特征分为两类：

一型：

ip\_id == \_\_\_\_（是一个固定的数，具体数值的查找留作习题）。

没有设置“不分片”选项。

没有设置服务类型。

对同一对源IP、目标IP，GFW返回的污染IP在上述8个中按照给出的顺序循环。与源端口无关、与源IP目标IP对相关。

TTL返回值比较固定。TTL为IP头部的“Time to Live”值，每经过一层路由器这个值会减1，TTL为1的IP包路由器将不再转发，多数路由器会返回源IP一条“ICMP time to live exceed in transit”消息。

二型：

每个包重复发送3次。

没有设置“不分片”选项。

设置了“保障高流量”服务类型。

(ip\_id + ? \* 13 + 1) % 65536 == 0，其中?为一个有趣的未知数。ip\_id在同一个源IP、目标IP对的连续查询之间以13为单位递减、观测到的ip\_id的最小值和最大值分别为65525（即-11，溢出了!）和65535。

对同一对源IP、目标IP，GFW返回的污染IP在上述8个中按照给出的顺序循环。与源端口无关、与源IP目标IP对相关。

对同一对源IP、目标IP，TTL返回值时序以1为单位递增。TTL在GFW发送时的取值有64种。注：源IP接收到的包的TTL被路由修改过，所以用户观测到的TTL不一定只有64种取值，这是由于网络拓扑变化的原因导致的。一型中的“比较固定”的“比较”二字也是考虑到网络拓扑偶尔的变化而添加的，也许可以认为GFW发送时的初始值是恒定的。

（以上结果仅保证真实性，不保证时效性，GFW的特征随时有可能改变，尤其是时序特征与传输层特征相关性方面。最近半年GFW的特征在很多方面的变化越来越频繁，在将来介绍TCP阻断时我们会提到。）

还可以进行的实验有：由于当前二型的TTL变化范围是IP个数的整数倍，通过控制DNS查询的TTL使得恰好有GFW的返回（避免动态路由造成的接收者观察到的TTL不规律变化），观察IP和TTL除以8的余数是否有对应关系，在更改源IP、目标IP对之后这个关系是否仍然成立。这关系到的GFW负载平衡算法及响应计数器（hit counter）的独立性和一致性。事实上对GFW进行穷举给出所有关于GFW的结果也缺乏意义，这里只是提出这样的研究方法，如果读者感兴趣可以继续探究。

每次查询通常会得到一个一型包和三个完全相同的二型包。更换查询命令中type=A为type=MX或者type=AAAA或者其它类型，可以看到nslookup提示收到了损坏的回复包。这是因为GFW的DNS污染模块做得十分粗制滥造。GFW伪造的DNS应答的ANSWER部分通常只有一个RR组成（即一条记录），这个记录的RDATA部分为那8个污染IP之一。对于二型，RR记录的TYPE值是从用户查询之中直接复制的。于是用户就收到了如此奇特的损坏包。DNS响应包的UDP荷载内容特征：

一型

DNS应答包的ANSWER部分的RR记录中的域名部分由0xc00c指代被查询域名。

RR记录中的TTL设置为5分钟。

无论用户查询的TYPE是什么，应答包的TYPE总是设置为A（IPv4地址的意思）、CLASS总是设置为IN。

二型

DNS应答包的ANSWER部分的RR记录中的域名部分是被查询域名的全文。

RR记录中的TTL设置为1天。

RR记录中的TYPE和CLASS值是从源IP发送的查询复制的。

其中的术语解释：RR = Resource Record：dns数据包中的一条记录；RDATA = Resource Data：一条记录的数据部分；TYPE：查询的类型，有A、AAAA、MX、NS等；CLASS：一般为IN[ternet]。

触发条件

实际上DNS还有TCP协议部分，实验发现，GFW还没有对TCP协议上的DNS查询进行劫持和污染。匹配规则方面，GFW进行的是子串匹配而不是精确匹配，并且GFW实际上是先将域名转换为字符串进行匹配的。这一点值得特殊说明的原因是，DNS中域名是这样表示的：一个整数n1代表以“.”作分割最前面的部分的长度，之后n1个字母，之后又是一个数字，若干字母，直到某次的数字为0结束。例如www.youtube.com则是"\x03www\x07youtube\x03com\x00"。因此，事实上就可以观察到，对www.youtube.coma的查询也被劫持了。

现状分析

4.36.66.178，关键词。whois：Level 3 Communications, Inc. 位于Broomﬁeld, CO, U.S.

203.161.230.171，关键词。whois：POWERBASE-HK位于Hong Kong, HK.

211.94.66.147，whois：China United Network Communications Corporation Limited位于Beijing, P.R. China.

202.181.7.85，关键词。whois：First Link Internet Services Pty Ltd.位于North Rocks, AU.

202.106.1.2,whois：China Unicom Beijing province network位于Beijing, CN.

209.145.54.50，反向解析为dns1.gapp.gov.cn，新闻出版总署的域名解析服务器？目前dns1.gapp.gov.cn现在是219.141.187.13在bjtelecom。whois：World Internet Services位于San Marcos, CA, US.

216.234.179.13，关键词。反向解析为IP-216-234-179-13.tera-byte.com。whois：Tera-byte Dot Com Inc.位于Edmonton, AB, CA.

64.33.88.161，反向解析为tonycastro.org.ez-site.net, tonycastro.com, tonycastro.net, thepetclubfl.net。whois：OLM,LLC位于Lisle, IL, U.S.

可见上面的IP大多数并不是中国的。如果有网站架设到了这个IP上，全中国的Twitter、Facebook请求都会被定向到这里——好在GFW还有HTTP URL关键词的TCP阻断——HTTPS的请求才构成对目标IP的实际压力，相当于中国网民对这个IP发起DDoS攻击，不知道受害网站、ISP是否有索赔的打算？

我们尝试用bing.com的ip反向搜索功能搜索上面那些DNS污染专用IP，发现了一些有趣的域名。显然，这些域名都是DNS污染的受害域名。

例如倒霉的edoors.cn.china.cn，宁波中国门业网，其实是因为edoors.cn被dns污染。一起受害的还有chasedoors.cn.china.cn，美国蔡斯门业（深圳）有限公司。

还有\*.sf520.com，似乎是一个国内的游戏私服网站。www.sf520.com也是一个私服网站。可见国内行政体系官商勾结之严重，一个“国家信息安全基础设施”竟然还会用来保护一些网游公司的利益。

此外还有一些个人blog。www.99tw.net也是一个游戏网站。

还有www.why.com.cn，名字起得好。

还有www.999sw.com 广东上九生物降解塑料有限公司生物降解树脂|增粘母料|高效保水济|防洪 邮编:523128……这又是怎么一回事呢？不像是被什么反动网站连坐的。还有人问怎么回事怎么会有那么多IP结果。

www.facebook.comwww.xiaonei.com，怎么回事呢？其实是因为有人不小心把两个地址连起来了，搜索引擎以为这是一个链接，其实这个域名不存在，但是解析的时候遭到了污染，就以为存在这个域名了。

倒霉的www.xinsheng.net.cn——武汉市新胜电脑有限公司，因为www.xinsheng.net被连坐。

DNS劫持的防范和利用

之前我们已经谈到，GFW是一套入侵检测系统，仅对流量进行监控，暂没有能力切断网络传输，其“阻断”也只是利用网络协议容易被会话劫持（Session hijacking）的弱点来进行的。使用无连接UDP的DNS查询只是被GFW抢答了，真正的答案就跟在后面。于是应对GFW这种攻击很自然的想法就是：

根据时序特性判断真伪，忽略过早的回复。

通常情况对于分别处于GFW两端的IP，其RTT（Round-trip time，往返延迟）要大于源IP到GFW的RTT，可以设法统计出这两个RTT的合适的均值作为判断真伪的标准。另外由于GFW对基于TCP的DNS请求没有作处理，于是可以指定使用TCP而不是UDP解析域名。也可以通过没有部署GFW的线路到没有被DNS污染的NS进行查询，例如文章一开始提到的“远程解析”。但黑体字标出的两个条件缺一不可，例如网上广为流传的OpenDNS可以反DNS劫持的说法是以讹传讹，因为到OpenDNS服务器的线路上是经由GFW的。

本质的解决办法是给DNS协议增加验证机制，例如DNSSEC（Domain Name System Security Extensions），客户端进行递归查询（Recursive Query）而不查询已经被污染了的递归解析服务器（Recursive/caching name server）。然而缺点是目前并非所有的权威域名解析服务器（Authoritative name server）都支持了DNSSEC。Unbound提供了一个这样的带DNSSEC验证机制的递归解析程序。

另外GFW的DNS劫持还可能被黑客利用、带来对国际国内互联网的严重破坏。一方面，GFW可能在一些紧急时刻按照“国家安全”的需要对所有DNS查询都进行污染，且可能指定污染后的IP为某个特定IP，使得全球网络流量的一部分直接转移到目标网络，使得目标网络立刻瘫痪。当然我们伟大的祖国郑重承诺“不率先使用核武器”…另一方面，GFW将伪造的DNS返回包要发送给源IP地址的源端口，如果攻击者伪造源IP，会怎样呢？将会导致著名的增幅攻击：十倍于攻击者发送DNS查询的流量将会返回给伪源IP，如果伪源IP的端口上没有开启任何服务，很多安全配置不严的系统就需要返回一条ICMP Port Unreachable消息，并且将收到的信息附加到这条ICMP信息之后；如果伪源IP的端口上开启了服务，大量的非法UDP数据涌入将使得伪源IP该端口提供的服务瘫痪。如果攻击者以1Gbps的速度进行查询，一个小型IDC（DNSpod被攻击事件）甚至一个地域的ISP也会因此瘫痪（暴风影音事件）。攻击者还可能设置TTL使得这些流量恰好通过GFW产生劫持响应，并在到达实际目标之前被路由丢弃，实现流量“空对空不落地”。攻击者还可能将攻击流量的目标IP设置伪造成与伪源IP有正常通信或者其他关联的IP，更难以识别。这样实际上就将一个国家级防火墙变成了一个国家级反射放大式拒绝服务攻击跳板。

最为严重的是，这种攻击入门难度极低，任何一个会使用C语言编程的人只要稍微阅读libnet或者libpcap的文档，就可能在几天之内写出这样的程序。而GFW作为一套入侵防御系统，注定缺乏专门防范这种攻击的能力，因为如果GFW选择性忽略一些DNS查询不进行劫持，网民就有机可乘利用流量掩护来保证真正的DNS通信不被GFW污染。尤其是UDP这样一种无连接的协议，GFW更加难以分析应对。“反者道之动，弱者道之用。”

参考文献

闫伯儒, 方滨兴, 李斌, 王垚. "DNS欺骗攻击的检测和防范". 计算机工程, 32(21):130-132,135. 2006-11.

Graham Lowe, Patrick Winters, Michael L. Marcus. The Great DNS Wall of China. 注：这篇文章虽然试图通过统计特性了解GFW，但由于实验条件控制不佳、实验结果观察不细致，加上缺乏对GFW的整体观，故没有提供什么有意义的结论。然而美国同学的这种科学态度与实验精神值得我们学习和思考。事实上，这篇文章仍然提供了珍贵的历史资料，读者不妨按照本文逻辑来分析这篇参考文献。阅读过这篇文献的敏感的读者还将在我们后续的文章中看到熟悉的数字。

KLZ毕业. 入侵防御系统的评测和问题. 注：本文对DNS污染包的分类就是从这篇文章的分类继承而来。

LABELS: GFW-METRICS, UNDERSTANDING GFW

深入理解GFW：路由扩散技术

GFW的重要工作方式之一是在网络层的针对IP的封锁。事实上，GFW采用的是一种比传统的访问控制列表（Access Control List，ACL）高效得多的控制访问方式——路由扩散技术。分析这种新的技术之前先看看传统的技术，并介绍几个概念。

访问控制列表（ACL）

ACL可以工作在网络的二层（链路层）或是三层（网络层），以工作在三层的ACL为例，基本原理如下：想在某个路由器上用ACL控制（比如说是切断）对某个IP地址的访问，那么只要把这个IP地址通过配置加入到ACL中，并且针对这个IP地址规定一个控制动作，比如说最简单的丢弃。当有报文经过这个路由器的时候，在转发报文之前首先对ACL进行匹配，若这个报文的目的IP地址存在于ACL中，那么根据之前ACL中针对该IP地址定义的控制动作进行操作，比如丢弃掉这个报文。这样通过ACL就可以切断对于这个IP的访问。ACL同样也可以针对报文的源地址进行控制。如果ACL工作在二层的话，那么ACL控制的对象就从三层的IP地址变成二层的MAC地址。从ACL的工作原理可以看出来，ACL是在正常报文转发的流程中插入了一个匹配ACL的操作，这肯定会影响到报文转发的效率，如果需要控制的IP地址比较多，则ACL列表会更长，匹配ACL的时间也更长，那么报文的转发效率会更低，这对于一些骨干路由器来讲是不可忍受的。

路由协议与路由重分发

而GFW的网络管控方法是利用了OSPF等路由协议的路由重分发（redistribution）功能，可以说是“歪用”了这个本来是正常的功能。

动态路由协议

说路由重分发之前先简单介绍下动态路由协议。正常情况下路由器上各种路由协议如OSPF、IS-IS、BGP等，各自计算并维护自己的路由表，所有的协议生成的路由条目最终汇总到一个路由管理模块。对于某一个目的IP地址，各种路由协议都可以计算出一条路由。但是具体报文转发的时候使用哪个协议计算出来的路由，则由路由管理模块根据一定的算法和原则进行选择，最终选择出来一条路由，作为实际使用的路由条目。

静态路由

相对于由动态路由协议计算出来的动态路由条目，还有一种路由不是由路由协议计算出来的，而是由管理员手工配置下去的，这就是所谓的静态路由。这种路由条目优先级最高，存在静态路由的情况下路由管理模块会优先选择静态路由，而不是路由协议计算出来的动态路由。

路由重分发

刚才说到正常情况下各个路由协议是只维护自己的路由。但是在某些情况下比如有两个AS（自治系统），AS内使用的都是OSPF协议，而AS之间的OSPF不能互通，那么两个AS之间的路由也就无法互通。为了让两个AS之间互通，那么要在两个AS之间运行一个域间路由协议BGP，通过配置，使得两个AS内由OSPF计算出来的路由，能通过BGP在两者之间重分发。BGP会把两个AS内部的路由互相通告给对方AS，两个AS就实现了路由互通。这种情况就是通过BGP协议重分发OSPF协议的路由条目。

另外一种情况，管理员在某个路由器上配置了一条静态路由，但是这条静态路由只能在这台路由器上起作用。如果也想让它在其他的路由器上起作用，最笨的办法是在每个路由器上都手动配置一条静态路由，这很麻烦。更好的方式是让OSPF或是IS-IS等动态路由协议来重分发这条静态路由，这样通过动态路由协议就把这条静态路由重分发到了其他路由器上，省去了逐个路由器手工配置的麻烦。

GFW路由扩散技术的工作原理

前面说了是“歪用”，正常的情况下静态路由是由管理员根据网络拓扑或是基于其他目的而给出的一条路由，这条路由最起码要是正确的，可以引导路由器把报文转发到正确的目的地。而GFW的路由扩散技术中使用的静态路由其实是一条错误的路由，而且是有意配置错误的。其目的就是为了把本来是发往某个IP地址的报文统统引导到一个“黑洞服务器”上，而不是把它们转发到正确目的地。这个黑洞服务器上可以什么也不做，这样报文就被无声无息地丢掉了。更多地，可以在服务器上对这些报文进行分析和统计，获取更多的信息，甚至可以做一个虚假的回应。

评价

有了这种新的方法，以前配置在ACL里的每条IP地址就可以转换成一条故意配置错误的静态路由信息。这条静态路由信息会把相应的IP报文引导到黑洞服务器上，通过动态路由协议的路由重分发功能，这些错误的路由信息可以发布到整个网络。这样对于路由器来讲现在只是在根据这条路由条目做一个常规报文转发动作，无需再进行ACL匹配，与以前的老方法相比，大大提高了报文的转发效率。而路由器的这个常规转发动作，却是把报文转发到了黑洞路由器上，这样既提高了效率，又达到了控制报文之目的，手段更为高明。

这种技术在正常的网络运营当中是不会采用的，错误的路由信息会扰乱网络。正常的网络运营和管控体系的需求差别很大，管控体系需要屏蔽的IP地址会越来越多。正常的网络运营中的ACL条目一般是固定的，变动不大、数量少，不会对转发造成太大的影响。而这种技术直接频繁修改骨干路由表，一旦出现问题，将会造成骨干网络故障。

所以说GFW是歪用了路由扩散技术，正常情况下没有那个运营商会把一条错误的路由信息到处扩散，这完全是歪脑筋。或者相对于正常的网络运营来说，GFW对路由扩散技术的应用是一种小聪明的做法。正常的路由协议功能被滥用至此，而且非常之实用与高效，兲朝在这方面真是人才济济。

测量

GFW动态路由系统概括起来就是：人工配置(c)样本路由器(sr)的静态路由(r)，向各ISP的出入口路由器(or)扩散此路由(r)，将特定网络流量转到黑洞服务器(fs)进行记录。因此可以进行测量的项目有：

(r)被封锁的IP列表：可以通过协作报告机制收集用户报告，也可通过扫描著名站点获得；（传言：GFW动态路由系统的容量是几十万条规则）

(or)受到GFW影响的ISP出入口路由器：通过在广域多ISP内的节点协作traceroute可以测得；

(or)-(c)从关键词生效到动态路由生效的延迟：通过建立蜜罐并提交给GFW然后观察其响应；

(fs)黑洞服务器的健壮性：用伪源噪音流量对黑洞服务器进行填充，观测其响应。

参考文献

刘刚, 云晓春, 方滨兴, 胡铭曾. "一种基于路由扩散的大规模网络控管方法". 通信学报, 24(10): 159-164. 2003.

李蕾, 乔佩利, 陈训逊. "一种IP访问控制技术的实现". 信息技术, (6). 2001.

NOV 2, 2009

GFW钓鱼计划

社会工程从来都是在安全领域最有趣味的话题。钓鱼（phishing）是社会工程的一种。最近韩寒童鞋揭露了出现在上海的某种钓鱼小把戏，我们也不妨来讨论一下某种GFW钓鱼小把戏。面对GFW这个黑箱，我们希望对它的内部的行政机制有所了解，这当然是技术性的逆向工程无法解决的问题，所以这里主要讨论社会工程的方法。

原理

对GFW进行黑箱式分析，就会发现一种非常确定的刺激-反应的行为模式。一般来说是这样的过程：1）一个网站处于含有敏感内容的状态；2）在某个时刻GFW感知到这个网站（“先期侦察”）并受到刺激；3）然后通过GFW内部的某种过程；4）最后形成对这个网站的封锁反应。一般只有最后的封锁反应是公开可观测的GFW特征，然而由于GFW的封锁采取伪造的方式进行，我们很难从这种封锁动作中获得信息。而如果我们特制一个网站并作为网站控制者让GFW对它进行感知，并利用GFW自认为置身暗处而不采取防护的漏洞，那么在刺激这个环节就很有可能观测到GFW的真实信息。简而言之GFW你不是特别会封吗？这次我造一个网站让你封，来啊。然后将GFW在这个环节泄漏的信息全部记录下来。这就是钓鱼，有人也把这个叫做蜜罐，在蜜罐里放一些GFW特别喜欢的东西，苍蝇循着香味飞进来就黏住了。根据先验知识我们还可以知道，在对目标进行侦察之后，GFW内部还会有关于反应方式的评估。这个过程虽然是无法观测的，不过当蜜罐收集到的数据量比较充分之后进行分析，就会找到这个过程的某些模式，分离出时间周期、地域、主题偏好等要素，对GFW内部的机制有一个轮廓性的刻画。

方法

在8月份我们就进行了这样一次钓鱼。钓鱼有这么几个要件：诱饵，钩子，鱼，渔。在这里鱼是GFW，渔是我们，诱饵是一个充满了敏感词的网站，钩子是这个网站内置的日志记录器。诱饵的建设是体力活，比较麻烦，行为跟spammer差不多了。首先寻找国外的免费空间和免费域名，然后用一个php+.htaccess/mod\_rewrite做一个网页反向代理，代理到某个特别敏感的网站，然后php内置日志记录器将访问时间和访问者的IP地址和HTTP头全部记录下来。网站看起来是一模一样的，差别只在域名，这就建好了。然后到伟大光荣正确的国新办网站net.china.cn举报之，尽情选最高最反动的那档，然后坐等鱼儿上钩、苍蝇入罐。

数据和讨论

等的过程这里读者就不用体验了（高兴的读者可以自行体验）直接给出结果，就是这个表格。这次钓鱼的一个很大失误就是忘记设置robots.txt，让搜索引擎的爬虫造成了大量噪音，给日志分析带来很大困难，这里展示的数据已经把搜索引擎直接产生的噪音去掉了，但是搜索引擎引来的访问者却很难办。

我们来对数据进行一些分析。首先拿到IP要做一下whois，看看究竟who is it。这就有结果了，看whois那栏，一个是公安部的网监，一个是BAOSHAN-POLICE，呵呵，上海的。它们的其他各项header相似性很高，其中奇怪的是Accept-Language是en-us的，其他header也给得很少。难道我们机智的警警察察已经人人都考过英语四级了，用英语版Windows？显然不是，根据先验知识加以推测，这应该就是金盾网的内网出口。根据这一特征，又找到CHINANET-FJ和CHINANET-GD 的两个警警察察。注意到，在31日就有报告说整个co.cc被封，9月1日的那位还能访问，这说明两件事情：1）警警察察枪决罪犯以后要验尸；2）警警察察上网没有墙。

那个UNICOM-TJ的是怎么回事？我们来分析一下这个诱饵是怎么被咬掉的。我们建立的诱饵之一域名是shangwang.co.cc，然而最终被封掉的却是co.cc。我们来观察一下17日凌晨这位来自天津的朋友他的referrer是：http://www.google.cn/search?q=gfw+co.cc+dns&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:zh-CN:official&client=firefox。就是说这位朋友通过在谷歌中文搜索“gfw co.cc dns”这个关键词找到了这个网站，为什么要这样搜索呢？为什么过了几天整个co.cc就被封了呢？这无疑是抓你一个，杀你全家的做法。结合当时的情况，net.ru在这之前被封掉，idv.tw在这之后被封掉，做法都是直接把cctld列为关键词，我们不难这样推测GFW的习惯：看见一个不熟悉的域名，先谷歌一下看你是不是属于大户人家，一搜发现哦原来net.ru和co.cc你们都是些免费的弃儿，就杀你全家，斩草又除根春风吹不生，反正没人知道。不过天津的那位又是谁呢？难不成是坐落在天津的公安部麾下“国家计算机病毒应急处理中心”？天津这位朋友后来居然还会从瑞士走代理来访问，而且我们设置的两个诱饵他都碰了，这确实非常先进了。

未来研究

这只是一次孤立的钓鱼，数据还是不具有普遍性，如果这样的实验成规模地重复，那么GFW的工作周期和口味都能有更清晰的了解。如果利用javascript甚至更侵入性的手段，还可收集到更多信息。另外一个直接的提示就是，网站管理者应该调查APNIC的whois数据库查出属于网监的IP段并“软性屏蔽”之，这样对于避免安全问题可以起到一定效果。一个需要考虑的问题是，如果以后GFW在先期侦察和验尸的时候都注意隐藏信息，调查访问者身份就会增加一些困难，但是如果搜索引擎隔离得足够好还是问题不大的。

结论

我们通过利用GFW在侦察目标时自认为置身暗处而不采取防护的漏洞，进行了一次钓鱼实验并获取了适量数据进行分析，证实了net.china.cn举报平台与GFW在工作流程上的密切关系，并发现了可能来自金盾网的举报验证，以及证实了金盾网使用“防外线”不受GFW影响的传言。我们还分析发现了一种GFW对于小站点的极端封锁策略，以及一种封锁实施后验证封锁的行为方式。不幸的是，这次钓鱼带来一个意想不到的后果就是co.cc全军覆没，对那些采用co.cc做域名的站长们在这里只好抱歉了。我们原来还试图生成一个de bruijn序列来高效证明著名的法轮猜想——“任意其他GFW关键词的长度都大于"falun"”，没想到短短时间就又出现一个长度为5的新秀与老牌关键词falun并驾齐驱，真是出乎意料。

总结这次实验，钓鱼的哲学有两条：一条是钓鱼比的是想象力，感兴趣的童鞋可以观赏Mitnick的The Art of Deception会有更多收获；另外一条是，钓鱼需要耐心，这次钓鱼实验持续近半个月一无所获，“那是极端反动的大妓院啊怎么不快快封掉？！”我们几乎以为失败，鱼最终才上钩，如果没有比鱼更多的耐心是钓不到的。同理推之不难想象，上海的哪个闲得蛋疼人士也可以开着一辆破车去钓鱼，只要把一个对方的“钩子”钓到自己车上，之后想做什么那都好办了。