几个常见的DDoS botnet及其特点

核心技术部　刘亚　周大

关键字： botnet C&C 通信　DDoS 攻击　样本　通信协议

摘要：利用 botnet 发起 DDoS 攻击依然常见，本文从 bot 种类、C&C 通信协议、DDoS 攻击类型和服务器活跃情况等角度，对我们在过去一年里跟踪过的几十个大陆地区的 DDoS 类型的 botnet 进行了总结。

引言

以 botnet 为平台发起各种形式的攻击，比如 DDoS 攻击、垃圾邮件发送、信息窃取等，这种现象已存在多年，并且依然受黑产界的青睐，如果关注这方面的新闻会发现几乎每天都有相关报道出现。因为语言、文化的差异以及网络管制等原因，不同 botnet 之间往往具有比较大的差异，体现在规模、地理分布、“盈利模式”和技术手段等方面。比如在欧美地区比较活跃的 ZeroAccess、Zbot、Kelihos 等 botnet 在中国大陆地区就比较少见 [1][2]；再比如欧美的 botmaster 常将垃圾邮件发送作为生财手段，但很少见到中国大陆地区的 botnet 采取类似的盈利模式，倒是出现了不少游戏盗号、DDoS 攻击类型的木马。

如果从技术上分析，会发现差别更大：一些“高端”的 botnet 已经开始采用诸如 FastFlux、P2P、公钥认证等这种以往只在正规的大软件系统中才会采用的复杂技术，以提高其健壮性和隐蔽性，而且会在客户端方面采取各种奇技淫巧（比如 bootkit 等）来提高保护等级 [3]，但也有一些 botnet 的客户端简陋到只是集成了有限的几条远控指令，连加壳保护都没有。

观察已有的 botnet 并寻找它们之间的共性是建立分类依据的重要手段，可以帮助我们更好地检测和防御通过 botnet 发起的攻击。本文将以实际数据为基础，对近半年来我们曾检测到的在大陆地区活跃的 13 种、99 个 botnet 做一些总结，分享一下我们的一些发现。

这些 botnet 均为 DDoS 攻击类型。

一、bot 客户端总结

bot 指 botnet 的客户端，在被控主机（俗称僵尸机器、肉鸡）上运行，负责接收和执行 botmaster 的指令，通常被称为病毒、木马（Trojan）或者恶意软件（malware），与其对应的是由 botmaster 运行的控制服务器，负责分发指令，常被简称为 C&C 服务器。对 botnet 的分类通常是依据 bot 客户端，比如基于 bot 家族来源或者所使用的 C&C 协议来划分，我们只依据 C&C 协议对 bot 进行分类，如果两个 bot 的 C&C 协议相同，即使它们的 C&C 服务器 IP 或者端口号不同，或者家族来源不完全一样，也会被认为是同一种 bot。下面介绍我们对所检测到的 botnet 客户端的一些观察和总结。

1.1 bot 种类相对集中

前面提到，我们共检测到过 99 个活跃的 DDoS botnet，实际的 bot 样本近 1000 个，但依据 C&C 协议进行分类后发现只有 13 种 bot，也就是说这 99 个 botnet 的控制者先后为他们的 botnet 分发了近 1000 个 Md5 各不相同的 bot 样本，而这些样本实际上都只是 13 个 bot 的变种而已，有的可能连变种都算不上，只是在每次传播时修改了样本中几个无关紧要的字节使 MD5 值发生变化而已。这说明实际中的 bot 种类远远少于 bot 样本的数量，新类型的 bot 没有那么多。

表 1 bot 家族分布

Bot 名称	出现次数
darkshell.c.2	44
darkshell.c	6
Nitol	14
artemis/storm.b	13
storm	6
neglemir	5
flyboy	2
Netbot	2
nxs	2
storm.a	2
jgjsfgv	1
Jrq	1
oxoddos	1

表 1 是我们对这 13 种 bot 的使用统计，发现被使用最多的是一种名为 darkshell.c.2 的 bot（darkshell.c 是其早期版本），有 50 个这样的 botnet，占所有 botnet 总数的一半以上，这引起了我们的注意。调查后发现原来 darkshell.c 这种 bot 不但具有相对全面的 DDoS 攻击功能，更重要的是其作者开放了源代码，任何人都可以免费获取，这无疑是其出现频率最高的主要原因。与此类似的是后面将要介绍的 RAT 软件 gh0st，也是因为其源代码开放导致使用频率非常高，出现了各种变种。再联想到来自俄国的臭名昭著的 bot 软件 zeus，也是因为源代码被泄露以至于很快就出现了各种变种，有人甚至为其添加了 P2P 和 DGA 功能 [6]。由此似乎可以得出结论，开放源代码的 bot 更受 botmaster 的欢迎。

1.2 C&C 通信基于 TCP

对这 13 种 bot 进行分析发现它们的 C&C 协议都基于 TCP，而且普遍使用长连接，通过 TCP 的 KeepAlive 机制实现存活性检测，未发现基于 UDP 的 C&C 协议。猜测这么做的原因可能是为了简化编程，因

为如果要实现基于 UDP 的 C&C 协议，需要自己处理丢包、乱序等各种繁琐问题，远比使用 TCP 来的复杂。

1.3 TCP 和 HTTP flood 是必备功能

统计发现每种 bot 都有集成了 3 种以上的 DDoS 功能，其中 TCP flood 和 HTTP flood 出现频率最高，有的 bot 甚至在此基础上发展出更多的攻击形式。

1.4 使用私有协议

所有 13 种 bot 的 C&C 协议都是私有协议，未发现使用标准的应用层协议（比如 HTTP）传输指令的情况。各种 bot 的 C&C 协议各不相同，但有一些共同点：

1. 运行时都有个类似注册的过程：bot 连接 C&C 服务器成功后会首先发送一个包含自身配置信息（比如 CPU 频率、操作系统版本等）的报文。

2. botmaster 可以在注册包中设置一些自定义值的实现版本和错误检测。比如 darkshell.c bot 的注册包里就有一个专门用于描述 bot 版本的字符串字段，观察发现不同的 darkshell.c bot 生成的注册包此字段明显不同，甚至即使同一个 botnet 在不同时期分发的 bot 样本，此字段也可能会变化。

3. 运行端口可自由设置。

1.5 样本普遍加壳

从加壳统计看 bot 样本在分发时普遍做了加壳保护，有极个别的未加任何壳，但其 botnet 并不活跃，估计是处于试运行阶段，开发者还未考虑做加壳处理。

有一种 bot 的样本虽然未做加壳处理，但采取了加花机制，通过在样本中添加混淆指令或者混淆原来的执行流程来增加样本的逆向分析难度。

1.6 均留有后门

尽管主要是用于 DDoS 攻击，但分析发现这 13 种 bot 都保留了后门功能，botmaster 能控制僵尸主机下载并执行任意的可执行程序，实现远程安装。此外，不少 bot 都集成了远程关机、重启功能，超过一半的 bot 还集成了 C&C IP/port 更新功能。

后面将会提到，观察发现这些后门中使用最多的是下载 gh0st RAT 工具，让 botmaster 完全控制僵尸主机。

1.7 伴随各种 gh0st 变种

统计下载指令时发现 gh0st 是下载次数最多的一类软件，共检测到 644 个、41 种 gh0st 样本，所以有必要专门分析一下。

gh0st 本来是国内的一款开源 RAT 软件 [4]，用于远程计算机管理，其全面的功能加上源代码开放，使其深受黑产界青睐，常被改做木马使用，以至于出现了各种各样的 gh0st 变种 [5]。

gh0st 通信报文的特点是前面有 13 字节的报文头，里面包含一个特征串和两个长度字段，报文头紧跟的是经过 zlib 压缩的 payload，其压缩前、后的长度分别由报文头中的 2 个长度字段标识。gh0st 变种间的差别在报文上表现为：

1. 报文头结构不同：特征串可能在前（gh0st1），也可能位于报文头末尾（gh0st2）。

2. 报文原始报文长度（len2）不同。

下面列出我们曾检测过的 gh0st 变种，更多的变种信息可以参考 [5]。值得注意的是，我们还发现了多个集成了 DDoS 攻击功能的 gh0st 变种，相关的指令检测工作正在进行中。

```
gh0st1 -signature Black -len2 280
gh0st1 -signature ChEnA -len2 688
gh0st1 -signature Eyes1 -len2 1012
gh0st1 -signature Eyes2 -len2 932
gh0st1 -signature FKJP3 -len2 228
gh0st1 -signature Gh0st -len2 280
gh0st1 -signature Gh0st -len2 300
gh0st1 -signature Gh0st -len2 316
gh0st1 -signature Gh0st -len2 328
gh0st1 -signature Gh0st -len2 332
gh0st1 -signature Gh0st -len2 336
gh0st1 -signature Gh0st -len2 372
gh0st1 -signature Gh0st -len2 376
```

```
gh0st1 -signature Gh0st -len2 388
gh0st1 -signature Gh0st -len2 412
gh0st1 -signature Gh0st -len2 552
gh0st1 -signature Gh0st -len2 656
gh0st1 -signature Gh0st -len2 664
gh0st1 -signature HeiSe -len2 368
gh0st1 -signature HGChU -len2 720
gh0st1 -signature https -len2 284
gh0st1 -signature KrisR -len2 588
gh0st1 -signature Shado -len2 368
gh0st1 -signature Tyjhu -len2 416
gh0st1 -signature Winds -len2 364
gh0st1 -signature Winds -len2 664
gh0st1 -signature XIAOO -len2 228
gh0st1 -signature Xjjhj -len2 332
gh0st1 -signature Xjjhj -len2 412
gh0st1 -signature Xjjhj -len2 632
gh0st1 -signature Xjjhj -len2 636
gh0st1 -signature Xjjhj -len2 712
gh0st1 -signature YinLe -len2 496
gh0st2 -len2 248
```

```
gh0st2 -len2 312
gh0st2 -len2 324
gh0st2 -len2 332
gh0st2 -len2 352
gh0st2 -len2 412
gh0st2 -len2 520
gh0st2 -len2 680
……
```

二．C&C 服务器特点

在统计 botnet 时我们用 3 元组（bot 类型、C&C 服务器、C&C 运行端口）惟一标识一个 botnet，所以 botnet 种类和 botnet 个数是一对多的关系。C&C 服务器统计主要从域名使用、地理分布、IP 地址解析等角度入手，下面的描述反映了我们对检测到的 89 个 C&C 服务器的分析情况。

2.1 大多数 C&C 服务器分配了域名

在检测到的 89 个 C&C 服务器中，只有 15 个没有域名，其他均分配了域名，这说明给 C&C 服务器分配域名在国内是主流。

反观欧美一些规模比较大的 botnet，往往会不分配 C&C 域名，而是直接使用纯 IP 连接。为何有这种差别，现在还不太清楚，需要继续观察。

从所使用的域名后缀看，3322.org 后缀的域名出现最多，达 20 个。值得一提的是 2012 年 9 月份微软为了打击 Nitol botnet “劫持”不少 3322.org 域名，那段时间我们一直观察的几个域名也在被劫持之列，域名都解析到了美国的 IP，所以那段时间内新出现的 gh0st bot 多使用 IP 连接 C&C 服务器，而且自那次事件以后，陆续出现了采用新后缀的 C&C 域名，我们观察到的非 3322.org 域名大部分自那以后出现。

2.2 运行端口非标准

统计发现 bot 种类和其运行端口不存在绑定关系，而且大部分 botnet 运行在大于 1024 的非标准端口上，不到 1/3 的 botnet 运行在标准端口上，但均与标准端口本来的使用意图无关。比如我们发现多个运行在 81 端口的 botnet，该端口本来分配给了 Kerberos 用于身份认证，但实际的 C&C 通信与 Kerberos 完全无关。

2.3 C&C 域名和 IP 的对应

分析域名解析情况时发现实际解析的 IP 数要大于 C&C 域名数，实际检测到的 C&C 域名加 C&C IP 共有 89 个，但先后检测到的 C&C 服务器 IP 有 212 个，这说明 C&C 域名和 IP 存在一对多的关系。

绝大部分域名都会固定地解析到有限的几个 IP 上，只有极个别域名映射 IP 较多，比如有 1 个 C&C 域名在近 3 个月的时间内曾先后解析到 32 个不同的 IP。目前还不清楚这些 IP 确实为该 botmaster 所拥有还是使用了被黑的服务器，但我们确实发现过国外的 botnet 拿被黑的服务器充当 C&C 服务器的情况，先后检测到其 C&C IP 有 100 多个，而且地理上是全世界分布。

统计还发现存在单个 IP 对应多个域名的情况，这说明同一个 botmaster 可能运行了多个 botnet。

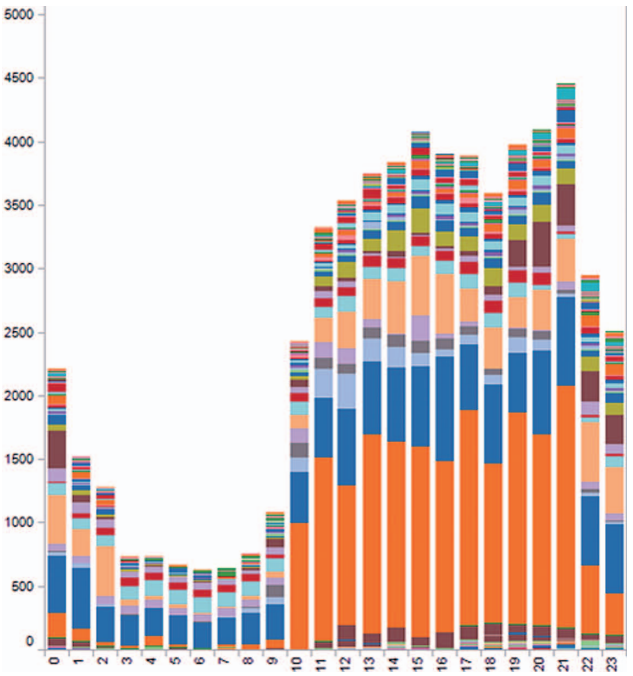

图 1 攻击指令 24 小时分布图

三．运行和活跃情况

活跃情况主要依据攻击指令数和攻击频率来衡量，我们半年来陆续检测到 27 万多条 DDoS 攻击指令，被攻击目标有 17000 多个。如果将这些攻击指令按照 24 小时分布统计，可以看出攻击主要发生在上午 10 点到晚上 12 点之间，其中下午是最活跃的时段，如图 1。

对被攻击目标分布统计表明，被攻击目标主要位于大陆地区，私服和电子商务网站出现比例最高，也有个别政府、教育网站，有意思的是攻击目标中多次出现了 DDoS “服务商” 网站。

从具体攻击参数看，尽管每种 bot 都集成了多种类型的 DDoS 攻击功能，但 botmaster 明显只偏爱某几种类型的攻击，其中 TCP 和 HTTP flood 是使用最多的攻击手段。

从后门指令的使用看，大部分 botnet 都检测到了后门指令，而远程安装指令使用最多，共检测到 11000 多条，其他诸如关机、重启和更新 C&C 配置这些功能则极少使用，不超过 100 条。

从统计看，远程安装的内容集中在如下几种情况：

1. 安装 RAT 类软件，最常见的是 gh0st 软件，这个前面已经介绍。猜测这么做的原因是为了完全控制僵尸主机。

2. 安装新的 bot 软件，组建新的 botnet。

3. 将僵尸主机作为跳板，继续攻击其他机器。

4. 安装一些刷流量的软件，这种情况比较少见。

从后门的使用频率看 botmaster 非常希望完全控制僵尸主机，以榨取更多的利益。另外，某些 bot 尽管可以通过指令将已有 bot 迁移到新的 botnet 中（不同的 C&C 服务器 IP 和端口），但 botmaster 更喜欢通过远程安装新 bot 的方式来实现迁移。

四、总结

本文跟大家分享了我们观察到的大陆地区一些 DDoS botnet 的现象和特点，实际中应该还有不少这类 botnet 未被观察到，所以我们不能说这些特点对其他的都适用，但管中窥豹，我们相信在 botnet 的种类、运维方式、DDoS 攻击的手段等方面，本文所总结的特点应该具有一定的代表性，希望对大家有所帮助。

参考文献

[1] Over 9 million PCs infected - ZeroAccess botnet uncovered, http://nakedsecurity.sophos.com/2012/09/19/zeroaccess-botnet-uncovered/。

[2] Zeus Tracker, https://zeustracker.abuse.ch/。

[3] Win32/Gapz: New Bootkit Technique，http://blog.eset.com/?p=16288。

[4] Gh0st，红狼安全小组，http://www.wolfexp.net/。

[5] The many faces of Gh0st Rat，http://www.norman.com/about_norman/press_center/news_archive/2012/the_many_faces_of_gh0st_rat/en/。

[6] Zeus (Trojan horse)，http://enc.tfode.com/Gameover_%28trojan_horse%29。