中国电信 CHINA TELECOM

NSFOCUS

2015 DDoS威胁报告

DDoS Threat Report

关于中国电信云堤

2008 年以来，中国电信开始着力于网络 DDoS 攻击防护能力建设，已形成了覆盖国内 31 省和亚太、欧洲、北美等主要 POP 点的一体化攻击防御能力。2014 年，中国电信首次在业界系统性提出电信级网络集约化安全能力开放平台框架，并将“云堤”作为对外服务的统一品牌。

几年来，中国电信云堤一方面致力于高效、可靠、精确、可开放的 DDoS 攻击防护能力建设，同时，面向政企客户提供运营商级 DDoS 攻击防护服务。目前已涵盖互联网、金融、能源制造、政府机构等各个行业。

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易。

股票简称：绿盟科技　股票代码：300369

目录

内容提要

纵观 2015 全年 DDoS 威胁态势， DDoS 攻击峰值流量不断上升，甚至出现了 1T 超大流量攻击事件，全年的攻击总流量接近 28 万 Tbytes，大流量乃至超大流量攻击更易于在运营商层面发现及治理。同时攻击形式发生改变，具有多维度两极分化的特性，从而远离大众的视野，更具隐蔽性。

为了探究这些转变，报告呈现及分析多个较为典型的 DDoS 攻击事件，以便从中分析和了解攻击者们所追逐的利益。正是由于这些利益的驱使，攻击者们同样有自己的“老板”，也需要考虑攻击的投资回报率 ROI，攻击者发起攻击的几率大小，一方面取决于其所追逐的利益，另一方面更取决于防守方面临攻击所采取的态度和能力，当收益对比风险的天平倾斜时，攻击者就敢于发动进攻。

面对如此恶劣的 DDoS 攻击态势，为了跟踪及呈现 DDoS 攻击的相关情报，中国电信云堤联合绿盟科技发布《2015 全年 DDoS 威胁报告》。本报告从三个层次进行逐层拆解，先从 DDoS 攻击态势分析流量、协议、攻击源、攻击目标及背后 Botnet 潜在的巨大危害性入手，对应分析 2015 年 DDoS 攻击事件背后所追逐的利益，同时为大家呈现层出不穷的新型攻击手段，探讨 2015 年 DDoS 攻防策略，进而帮助各组织及机构持续改善自己的 DDoS 防护技术及体系。

如果您需要了解更多信息，请联系：

扫描二维码，在线看报告

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

执行摘要

多年来，绿盟科技致力于帮助客户实现业务的安全顺畅运行。每天，绿盟科技的 DDoS 威胁态势感知平台及相关防护产品都会发现数以千计的 DDoS（分布式拒绝服务）攻击危害客户的业务安全。为了跟踪及呈现 DDoS 攻击的相关情报，进而帮助各组织及机构持续改善自己的 DDoS 防护技术及体系，绿盟科技发布《2015 DDoS 威胁报告》。

数据来源

本次报告中涉及的所有数据，来源于绿盟科技的威胁情报系统、全球 DDoS 攻击态势感知平台、SEER 广谱扫描平台、绿盟抗拒绝服务系统，以及两家合作伙伴所提供的数据，他们是中国电信云堤、金山安全。中国电信云堤云堤提供了国内电信运营商的大网数据，便于更为全面的呈现大规模 DDoS 攻击流量及特性；金山安全提供了 Botnet 在全球及中国的分布数据，便于呈现其规模及其潜在的危害性。这两方面的数据结合绿盟科技的各平台的数据及分析，让本报告得以从全网大流量、Botnet 僵木蠕、DDoS 攻防技术等角度立体化呈现 2015 年 DDoS 威胁的发展态势。

分析方法

本报告中流量数据分析基于 NetFlow 协议进行，是业界公认的一种统计方法，便于分析 DDoS 攻击流量构成、协议分布以及攻击行为。其中全局态势分析以中国国内攻击总流量统计数据为基础，进行多维度多层次关联分析；而与事件相关的流量区间及类型分析，则是按照攻击事件来进行统计而非流量大小进行计算的。

基于这些数据，本报告从三个层次进行逐层拆解，先从 DDoS 攻击态势分析流量、协议、攻击源、攻击目标及背后 Botnet 潜在的巨大危害性入手，对应分析 2015 年 10 个 DDoS 攻击事件分析 DDoS 攻击事件所追逐的利益，进而为大家呈现 2015 年 DDoS 攻击手段层出不穷的变化，分析 2015 年 DDoS 攻防策略。

DDoS 攻击态势趋于多变

观点 1　1T 超大流量攻击令人警醒

观点 2　攻击在多维度呈现两极分化

观点 3　受控攻击溯源多来自中俄美

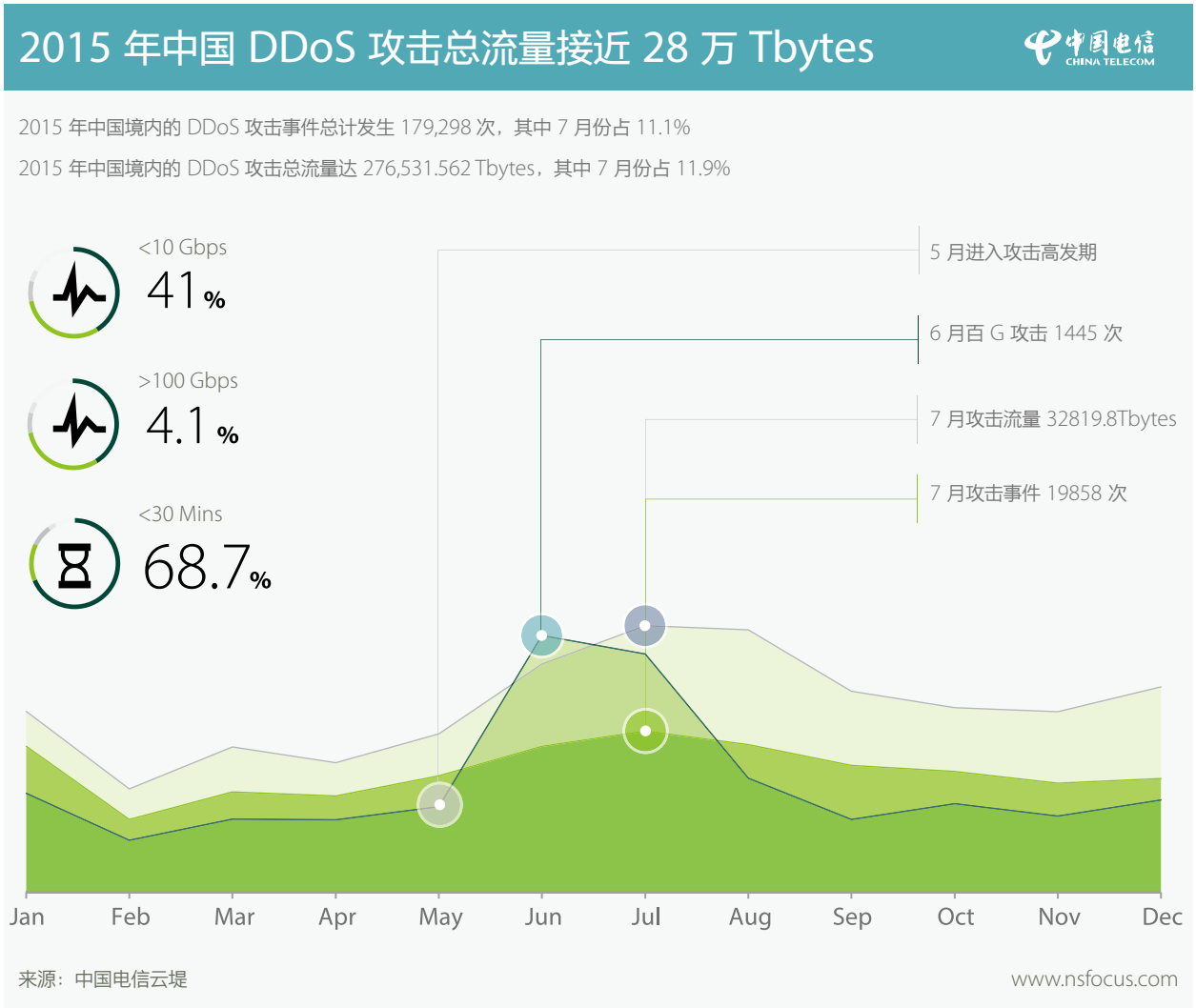
观点 4　BOTNET DDoS 温床危害巨大

观点 1　1T 超大流量攻击令人警醒

2015 年 10 月，某互联网企业进行了一次超大流量 DDoS 攻防演练，攻击峰值达到 1040.5 Gbps，该事件之所以引起了产业界的高度关注，一方面由于超大流量攻击其带来的破坏性毋庸置疑，另一方面进入 2015 年类似的超大流量攻击绝非仅有。但即使是超过 1T 的流量攻击与全国的 DDoS 攻击流量相比，也显得微乎其微了。

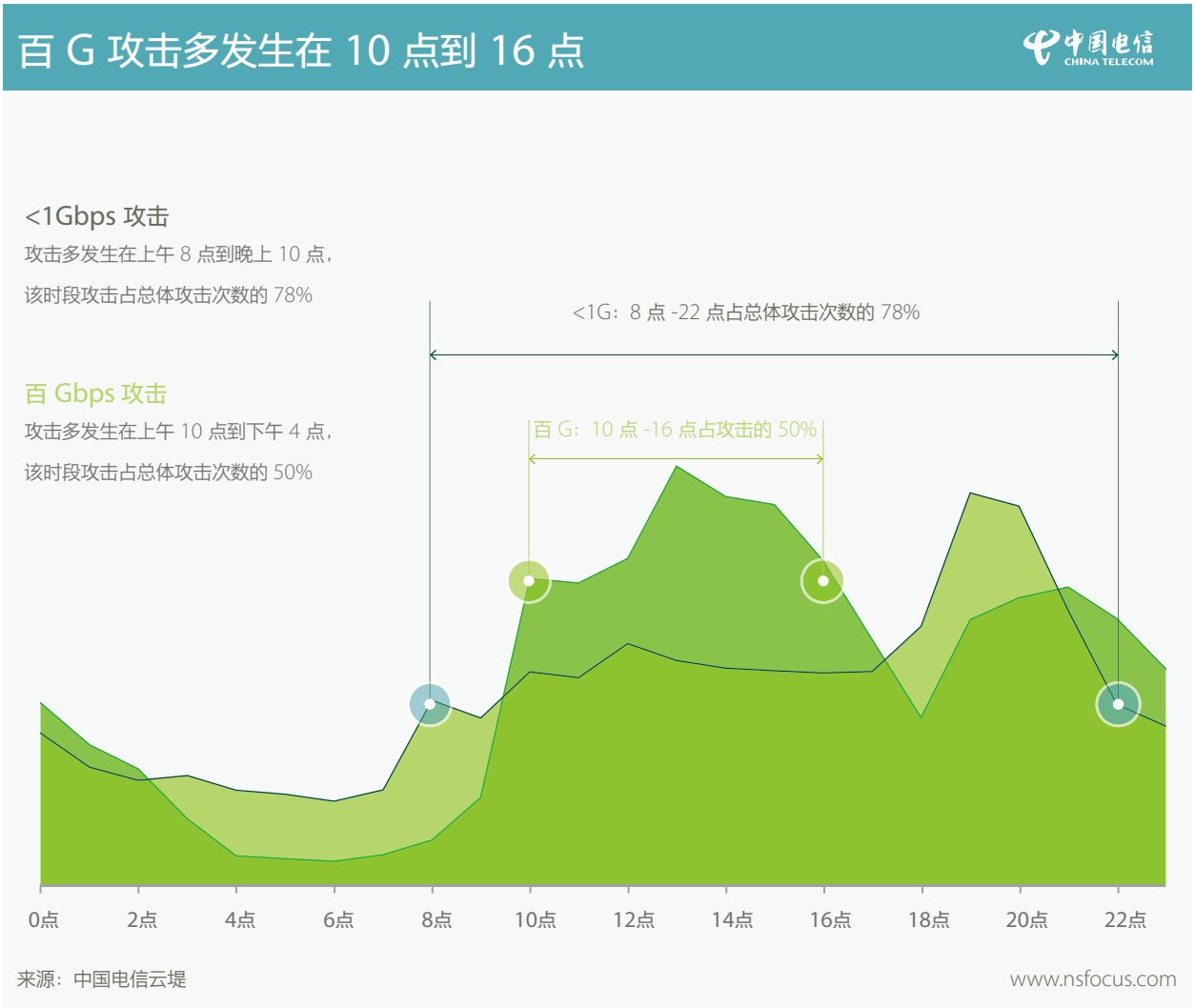
国内攻击总流量接近 28 万 Tbytes

2015 年国内共发生 DDos 攻击 179,298 次，攻击总流量达到 276,531.562 Tbytes，其中 41% 的攻击流量峰值都在 10Gbps 以下， 4.1% 的攻击流量峰值超过 100Gbps；大多数 DDoS 攻击时间都不长，大都在半小时以下。



百 G 攻击多在 10 点到 16 点

从左图中可以很明显看到，5 月以后 DDoS 攻击进入高发期。与此类似，报告从数据分析中还可以找到一些相关的规律，1Gbps 以下和百 Gbps 峰值的攻击时间分布特征不同，前者分布的较为宽阔，即从上午 8 点到晚上 10 点都比较常见，占到总体攻击次数的 78%，后者的攻击时段较为狭窄，多发生在上午 10 点到下午 4 点之间，占到总体攻击次数的 50%。



观点 2　攻击在多维度呈现两极分化

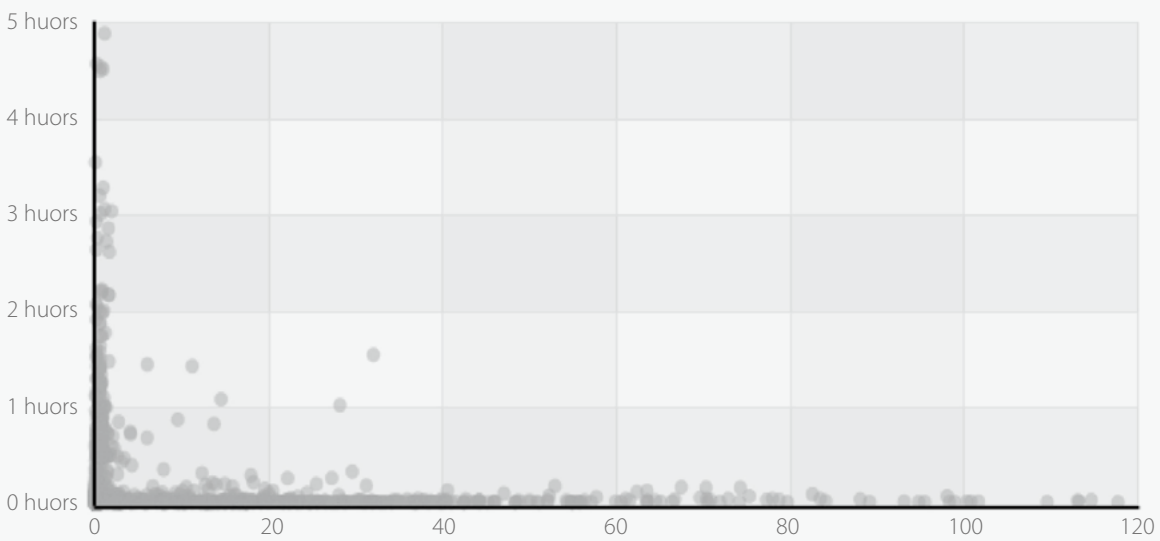
在 2015 年，DDoS 攻击存在大小流量两极分化现象更为明显，而且呈现在多个方面，包括攻击事件中攻击流量与时长的两极分化，攻击目标中针对高性能及业务特性的两极分化。攻击协议中小流量复杂大流量简化的两极分化。

攻击事件　流量与时长两极分化

经过研究分析发现，2015 年峰值在 1Gbps 左右的 DDoS 攻击，攻击时间往往较长，最长甚至持续攻击 5 个小时；而随着攻击峰值的增大，可以持续攻击的时间却不断变小，大多在半小时之内。这种现象从 2013 年以来日益显著，“90% 以上的 DDoS 攻击发生在半小时内，1.5% 的攻击会持续一天以上”

1G 左右的攻击可持续 5 小时
100G 左右的攻击半小时结束

经过分析可以看到，攻击流量越小则攻击时间也越长，反之攻击流量越大则攻击时间较多，当超过 100Gbps 后，大多攻击在半小时内就会结束。



Source: NSFOCUS DDoS Attacks Situation Awareness Platform　www.nsfocus.com

攻击目标　高性能及业务特性的两极分化

而对这种现象的深入分析发现，攻击目标一类是持续的大流量攻击，尤其是针对高性能、高价值、大范围的攻击目标；另一类则呈现小而快、小而慢的形式，进入细分行业，主要是针对小流量及特殊业务目标。

- **大流量方面** 在 DDoS 大流量攻击兴起的同时，为了抵御风险免受其害，许多用户将其业务向云端迁移，云计算技术的诸多优点使得云服务得以广泛应用，也在安全上带来了两个方面的变化，1 客户端轻量化，客户端原本的计算任务大幅度向云端转移，云的流量会越来越大。这将会被大流量 DDoS 攻击所利用；2 环境复杂化，随着业务环境虚拟化，从业务更加灵活多变到运维管理，其中不断产生新的不确定性，都可能为新的 DDoS 攻击形式创造机会，而 SDN 控制器就成为风险之一。

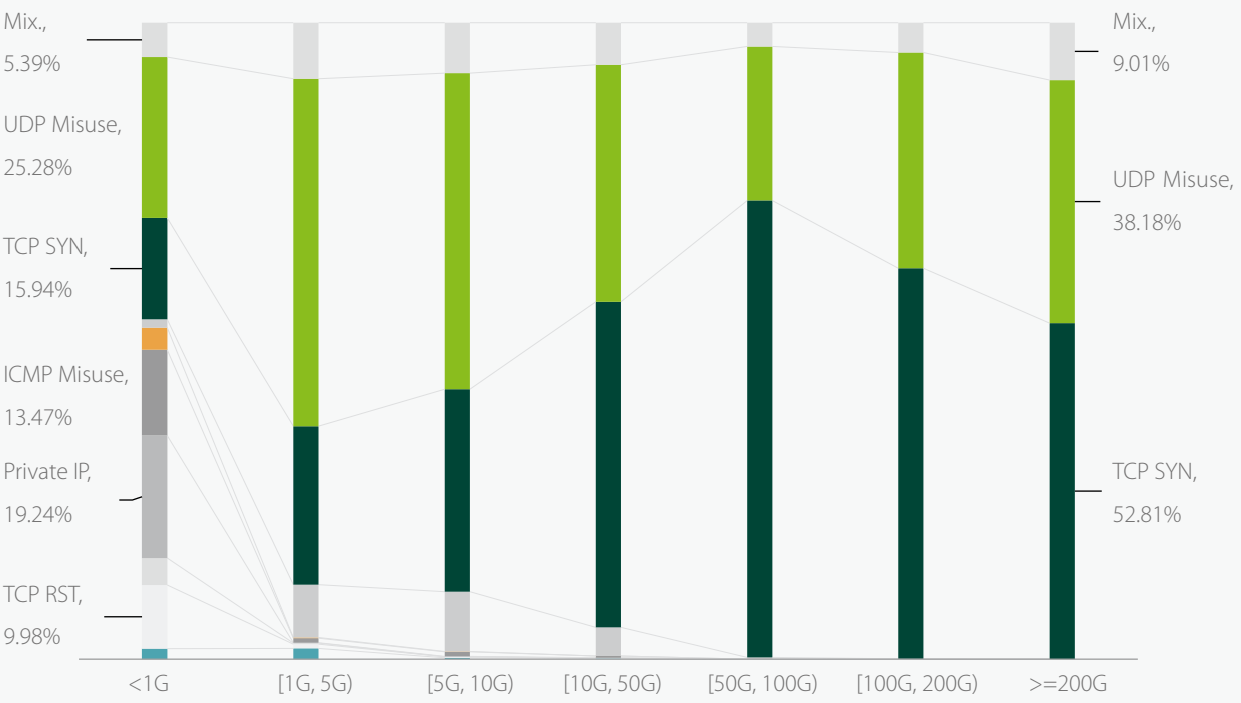
- **小流量方面** 在一些行业，尤其是游戏行业中，小流量攻击有着特殊的目的，与大流量（百 G 以上）及超大流量（500G 或更高）相比，[①] 这些攻击因为其流量小，不会引起业界的关注；2 这些小流量隐藏在大流量其中，难以辨识；3 更有些小流量攻击时长小到防护设备难以捕获，很难完整呈现其攻击过程。这些特点决定了小流量攻击不仅不会被攻击者抛弃，而且将其充分贴近业务特性，形成 DDoS 脉冲攻击（Hit-and-run DDoS）。

攻击协议　小而复杂与大而简化的两极分化

在 2015 年下半年的攻击事件中，统计数据还表现出攻击协议的两极分化的现象。在下图中可以看到，整体上攻击者最常采用的攻击手法仍然是 UDP 攻击及 SYN 攻击，但在小流量攻击中（<10 G）常常伴随着多种协议的组合式攻击，比如 ICMP 包攻击、错误 IP 连接攻击、错误 TCP 标志位连接攻击等攻击类型。随着攻击流量的逐渐上升，这种现象趋向于简化，最终表现最为明显的仍旧是 UDP（38.18%）及 SYN（52.81%）。

大流量以 UDP 及 SYN 为主　小流量攻击更为复杂

两极分化的情况在攻击协议方面也表现出来，在低于 1Gbps 的小流量攻击中，有多种协议的组合进攻；而攻击流量超过 100Gbps 后，以 SYN 为主，UDP 为辅。这种分化现象贴合之前的分析，即大流量攻击高性能业务，而小流量更贴合业务特性。



来源：中国电信云堤

www.nsfocus.com

① Hit-and-run DDoS

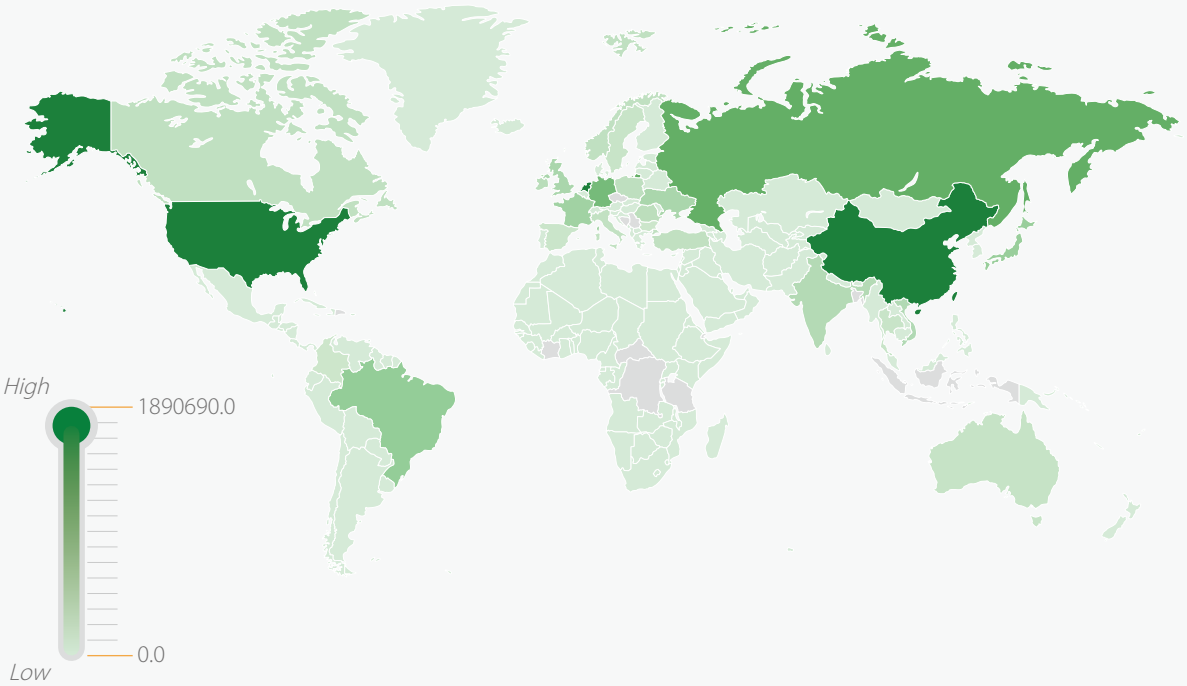
观点 3　受控攻击溯源多来自中俄美

得益于多方的云端 DDoS 攻击溯源系统，此次展示的数据中能够更为全面的看到，这些攻击大多来自美国、中国和俄罗斯，三个国家合计占比 73.32%，其中较多的攻击源都属于受控攻击源。

中、美、俄仍旧是 DDoS 受控攻击源最多的国家

NSFOCUS

根据获取到的数据显示，美国、中国和俄罗斯三个国家中受控制的攻击源数量占 73.32%。



Source: NSFOCUS DDoS Attacks Situation Awareness Platform　　www.nsfocus.com

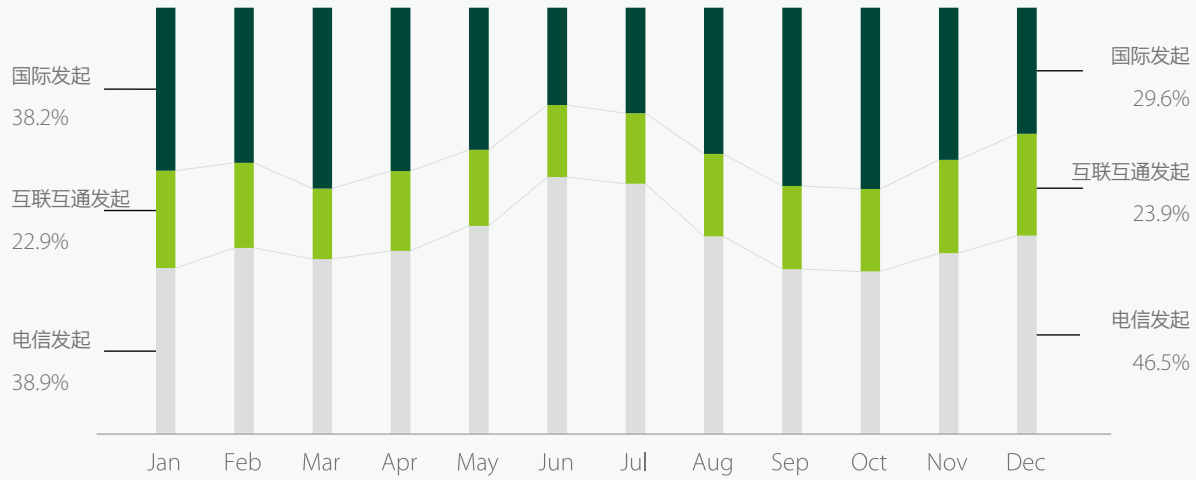
来自国际的攻击对国内造成的影响所占比例达到 35%。中国电信率先开展的全国范围的“虚假源地址管控”专项行动取得了显著效果，由于中国电信固网宽带客户和 IDC 客户占比较高，同时随着中国电信“宽带提速”、“光进铜退”工作的深入开展，单个肉鸡发起的攻击量呈百倍增加，中国电信网络内发起的攻击占全年总攻击流量的 45.5% 。

从国际发起的攻击次数　全年合计占比 35%

中国电信 CHINA TELECOM

下图中将攻击次数横向合计，国际发起的攻击全年合计占比 35%，互联互通发起为 19.4%，电信内发起为 45.5%

电信范围内发起的 DDoS 攻击次数仍占主要比例。

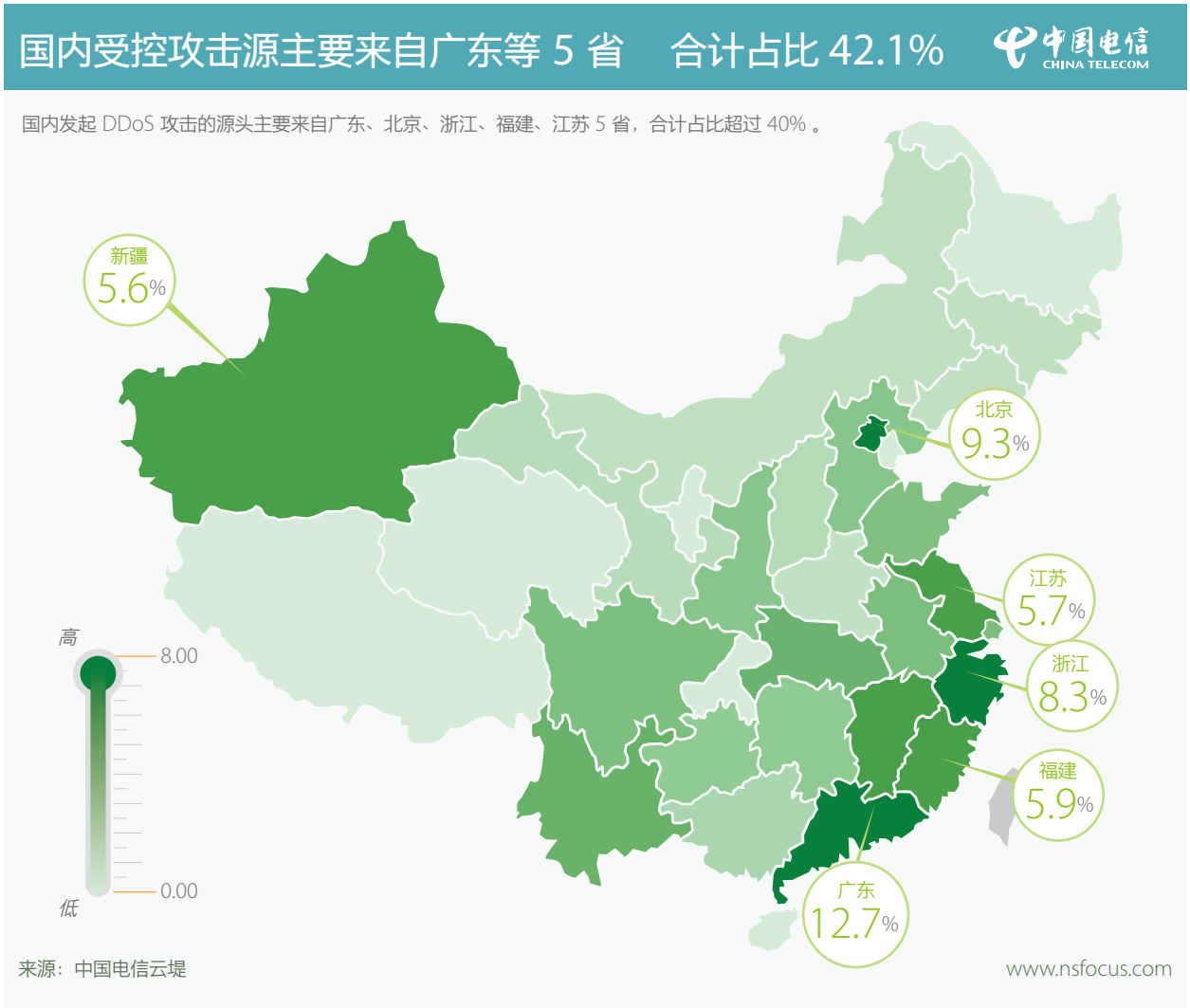


来源：中国电信云堤

www.nsfocus.com

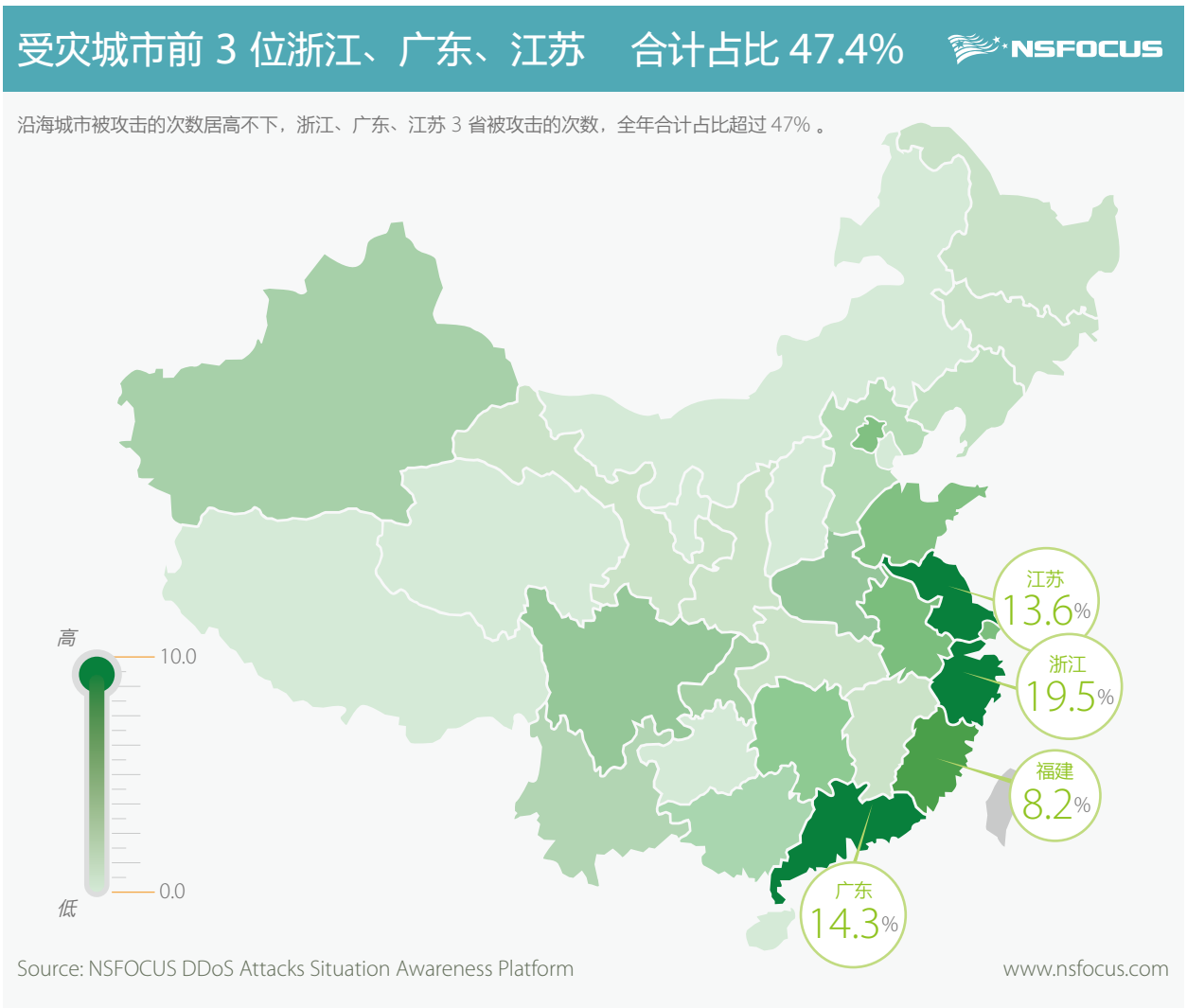
攻击多来自广东等 5 省　42.1%

对 DDoS 攻击源数据进一步聚焦，在中国的东部沿海城市存在较多的受控攻击源，这些城市包括广东、北京、浙江、福建、江苏，这些城市的 DDoS 攻击源合计占比 42.1%。



浙江 广东 江苏被攻击　47.4%

从全球的流量分布来看，中国和美国依然是 DDoS 受灾的重灾区，其中在中国地区东部沿海地区以及中国的台湾地区是受灾较为严重的地区。



9 月开始 UDP 攻击大幅下降到 1%

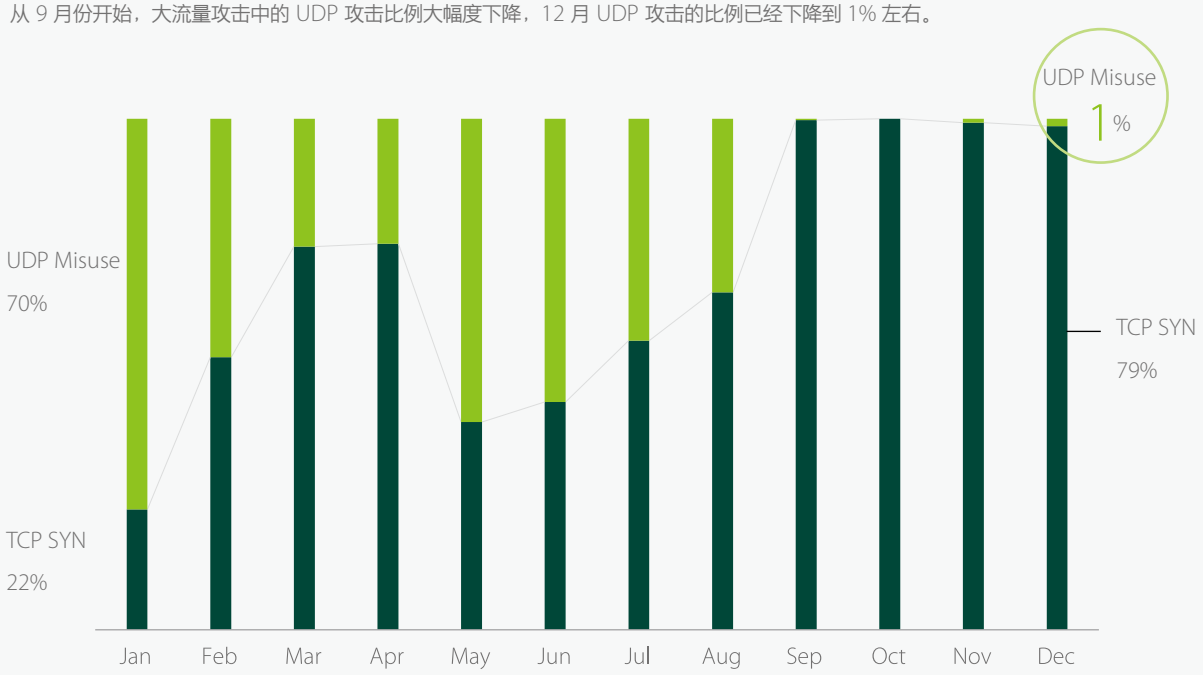
基于 UDP 协议的攻击常见于大流量攻击中，这已经成为共识，各大运营商针对这一突出问题进行了大范围治理。从 2015 年 9 月开始，UDP 攻击占比大幅度下降（降至 1% 左右），而在年初这一比例还高达 70%，这再次显示了运营商在 DDoS 全局治理方面所体现出的积极作用。

大流量 UDP 攻击经过治理　已大幅下降到 1%

中国电信 CHINA TELECOM

在大流量攻击中 UDP 攻击较为常见，这在历次的 DDoS 威胁报告中反复提到，各大运营商显然也注意到这一点，并对 UDP 大流量展开了积极治理。

从 9 月份开始，大流量攻击中的 UDP 攻击比例大幅度下降，12 月 UDP 攻击的比例已经下降到 1% 左右。



来源：中国电信云堤

www.nsfocus.com

观点 4　BOTNET DDoS 温床危害巨大

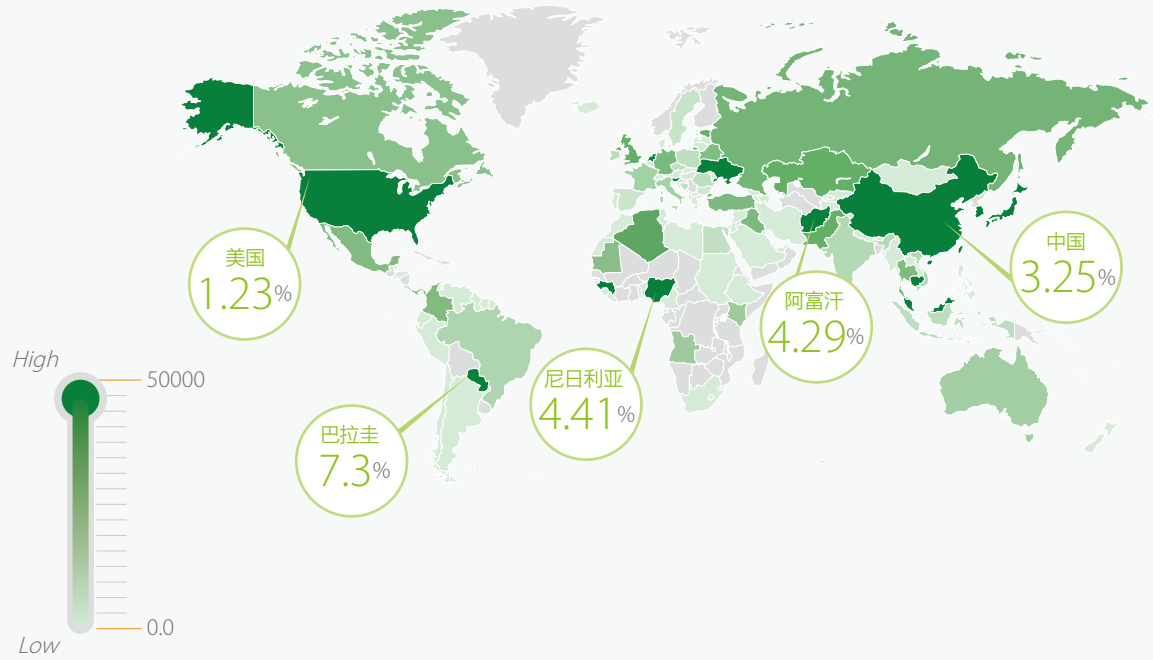
在 DDoS 攻击的背后，总是有多种攻击资源的利用情况，而这其中 Botnet 所产生的影响不得不提。Botnet 或者说 C&C 攻击形式，从本质上来说并不能算是 DDoS 的攻击形式，但随着控制端服务器所控制的主机不断增多，它也就具备了实施 DDoS 攻击的条件，故而 Botnet 的发展态势也成为本次报告的呈现内容之一。

来自金山安全的数据显示，2015 年巴拉圭、尼日利亚、阿富汗、中国等国是 Botnet 中主控机器（botmaster）数量分布较多的地方。

Botmaster 在巴拉圭、尼日利亚、阿富汗、中国等占比较高

攻击者使用多种方式隐藏自己，降低被发现的风险，但他们总是需要在网络上放置 Botmaster，以便能够向 Bot 下发攻击指令，并控制更大范围的 bot，

进而发起大规模的 DDoS 攻击。仅是 Botmaster 的数量就已经相当的庞大，而且遍及全球，排行前 4 位的合计不到 20%。



Source: : Kingsoft Security　　www.nsfocus.com

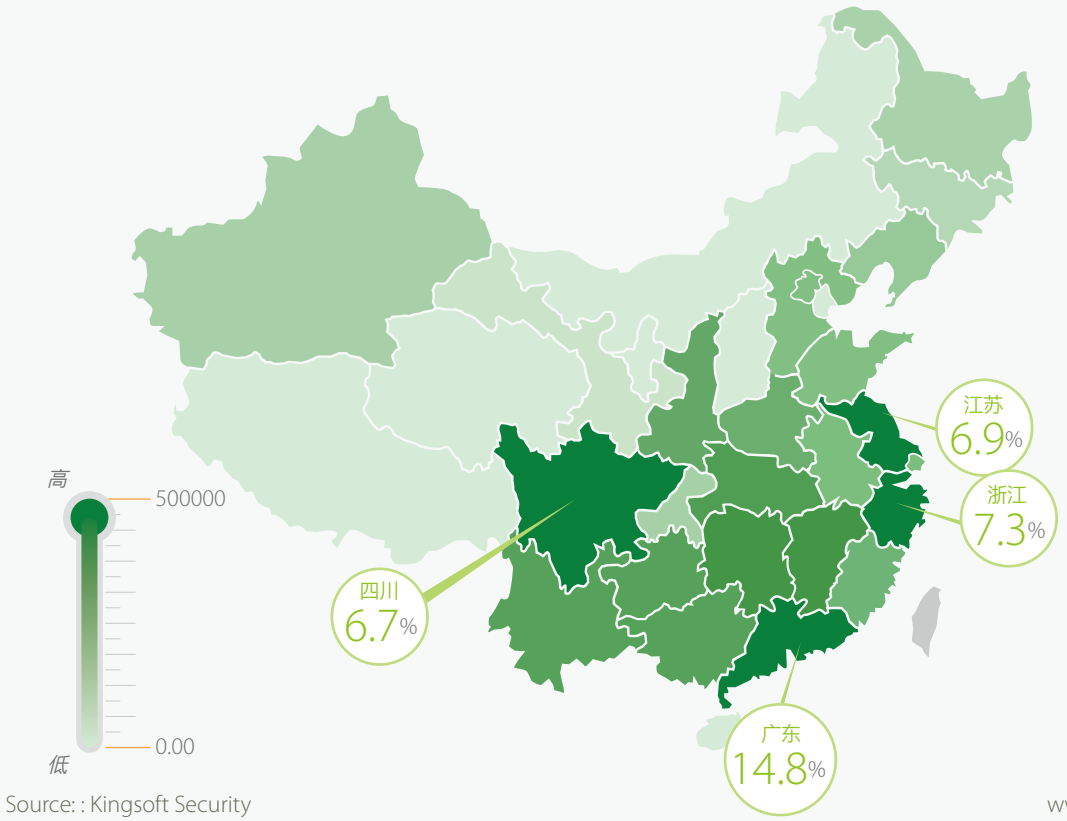
就 Botnet 在国内的发展状况，安全技术专家曾进行过研究[①]，研究过程收集了国内的 99 个 Botnet，经过分析发现它们均为 DDoS 攻击类型，并从中发现了一些规律：

- 相关 13 种 bot 的 C&C 协议都是基于 TCP，而且普遍使用长连接；
- 这些 bot 通常都集成有 3 种以上的 DDoS 功能，但 botmaster 偏爱 TCP 及 HTTP Flood 攻击手段；
- 大多都不会使用标准的应用层协议（比如 HTTP）进行指令传输，端口大多也运行在大于 1024 的非标准端口；
- bot 都留有后门，用途多集中在安装远程控制软件、安装新的 bot 软件（bot 迁移）、跳板攻击、刷流量；
- 大多数 C&C 服务器都会分配域名，而反观国外一些规模较大的 botnet 往往直接使用 IP 连接。

控制者们先后为他们的 botnet 分发了近 1000 个 bot 样本（Md5 各不相同），有些编写者甚至开放了源代码，任何人都可以免费获取，这无疑加剧了 botnet 的发展，国内被感染的 bot 有逐步增多的趋势。来自金山安全的数据显示，2015 年 Bot 在国内主要分布在 5 个省份（合计占比超过 40%），这 5 个省份依次为广东（14.8%）、浙江（7.3%）、江苏（6.9%）、四川（6.7%）、湖南（4.8%）。

Bot 国内主要分布在广东等 5 省　合计占比 40.6%

2015 数据显示，Bot 在国内分布主要集中在广东、浙江、江苏、四川、湖南 5 个省份，合计占比超过 40%，改善各种终端设备的安全性，将有利于压缩 Botnet 温床的发展空间，进而降低 DDoS 攻击发生的机会。



Source: : Kingsoft Security

www.nsfocus.com

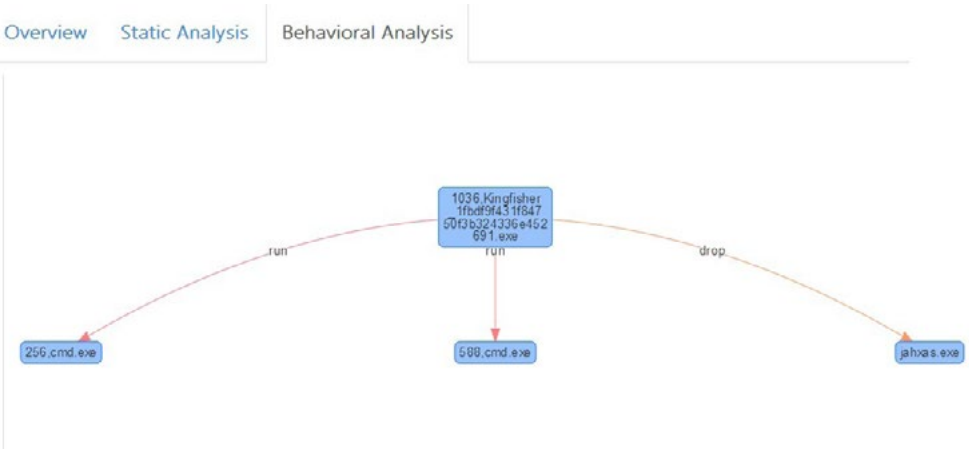
① 绿盟科技技术刊物总第 21 期，《几个常见的 DDoS botnet 及其特点》

DDoS 攻击者反成 bot 肉鸡

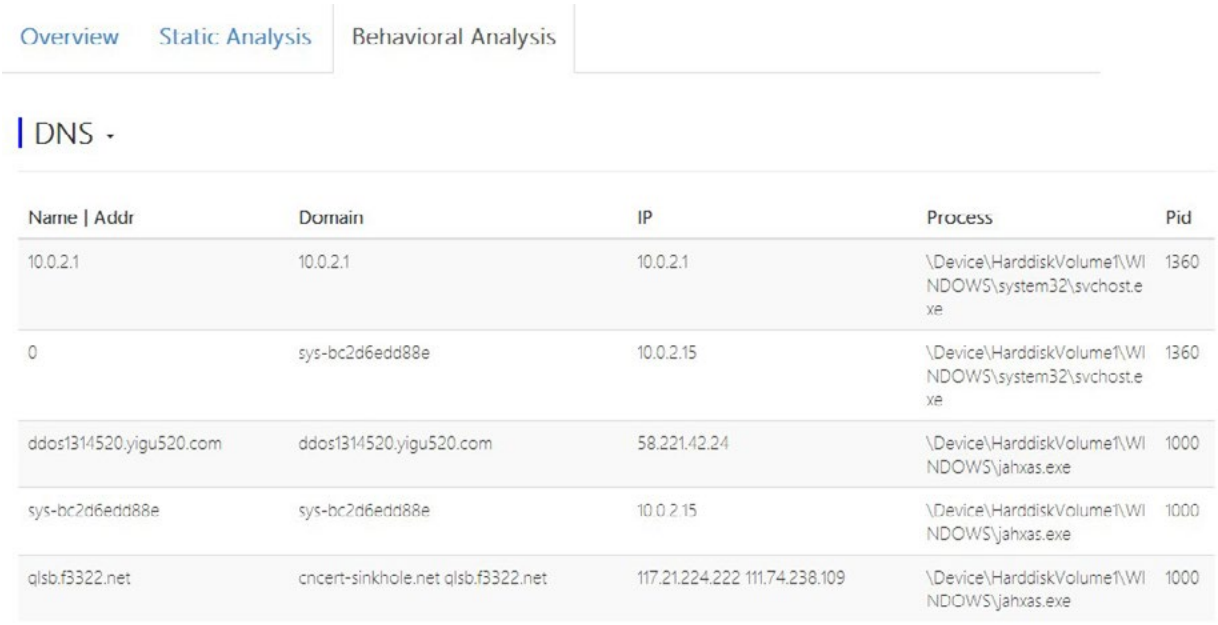
既然 Botnet 的发展空间如此庞大且易于利用，那么 DDoS 攻击者们就没有理由放过任何集中的 bot 资源，一旦哪位攻击者手里掌握了大量的攻击资源，毫无疑问会成为其他攻击者的攻击目标，所谓“螳螂捕蝉黄雀在后”，这种在黑产链条中相互厮杀的类似事件，2015 年的 Hacking Team 就是一例[①]。

而在国内，类似的事情也是屡见不鲜。绿盟科技技术专家曾接到一份恶意程序样本，它是一份国内比较流行的 DDoS 攻击软件，表面上软件中各种 DDoS 攻击功能使用正常，但其实是个 bot 生成工具，兼具 C&C 服务器端 Botmaster。如果购买者想使用这个软件攻击其他人，安装软件的主机也将沦为肉鸡，并有能力进一步感染及控制更多 bot。

经过分析发现，软件使用者一旦安装该软件，软件将释放 im.exe，并在本地开 8080 端口，以便利用 DDoS 攻击者的主机及其所掌握的网络节点。翠鸟恶意软件分析系统呈现了 im.exe 的执行过程。



自动生成的分析报告中，还可以看到这个“黄雀”也与国内的大多数控制者一样，也使用了域名。



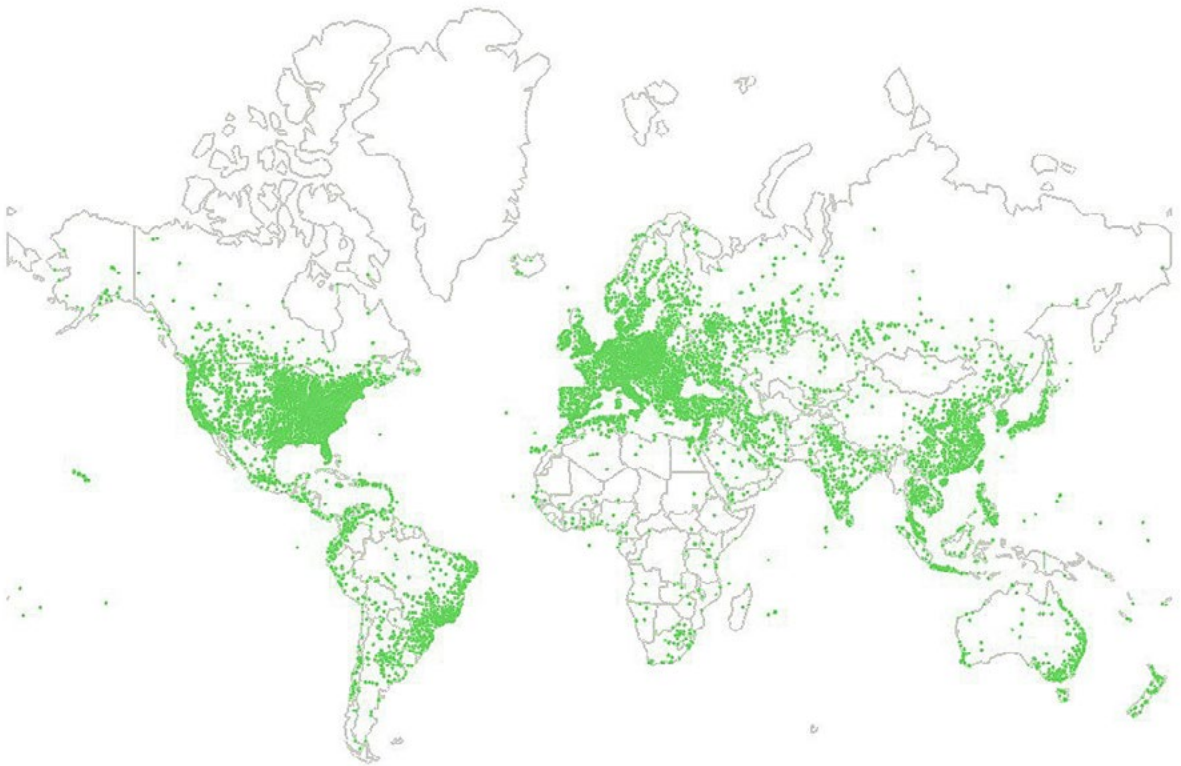
Name | Addr	Domain	IP	Process	Pid
10.0.2.1	10.0.2.1	10.0.2.1	\Device\HarddiskVolume1\WINDOWS\system32\svchost.exe	1360
0	sys-bc2d6edd88e	10.0.2.15	\Device\HarddiskVolume1\WINDOWS\system32\svchost.exe	1360
ddos1314520.yigu520.com	ddos1314520.yigu520.com	58.221.42.24	\Device\HarddiskVolume1\WINDOWS\jahxas.exe	1000
sys-bc2d6edd88e	sys-bc2d6edd88e	10.0.2.15	\Device\HarddiskVolume1\WINDOWS\jahxas.exe	1000
qlsb.f3322.net	cncert-sinkhole.net qlsb.f3322.net	117.21.224.222 111.74.238.109	\Device\HarddiskVolume1\WINDOWS\jahxas.exe	1000

① Hacking Team 数据泄露防护方案

500 万 SSDP 设备成 Botnet 温床

随着互联网技术的不断演进，如今肉鸡的领域已经不再局限于 PC，DDoS 攻击者们将这个范畴扩大到了物联网 IOT 设备的领域，并有继续蔓延的趋势，由于这些 IOT 设备大多采用默认的配置或者存在登录后门及固件漏洞，其攻击及利用成本要小得多，且这些智能设备数量异常庞大。从理论上说，任何能够进行数据交换的网络节点都可能被利用进行 DDoS 攻击，但至少要满足几个条件：1 能够打出流量，要么节点数量庞大，要么单点流量庞大；2 这些节点能够被控制或者被利用，比如僵尸主机、网络设备、网络服务等；3 最终能够触及攻击目标，显然 IOT 设备也满足这些条件。

截至 2015 年 12 月份，全球基于 SSDP 协议的设备多达 5183669 个，这些设备可能包括平板电脑、手机、电视等智能终端，也包括路由器、打印机、摄像头、扫描仪等智能设备。



在国外安全厂商 Incapsula 十月的一份报告中提到其监测到一次 DDoS 攻击，该攻击利用了 900 个 CCTV（closed-circuit television）录像头，就发起了峰值达到每秒 20000 次 http GET 请求，而攻击者之所以能够轻易利用这些摄像头，其原因就是这些摄像头都采用了默认的登录凭证，可远程登录并控制。

小提示：

Botnet 由两部分组成，botmaster 作为控制服务器，负责向 bot 分发指令，常被简称为 C&C 服务器；而 bot 就是被控制的机器，用于直接发起 DDoS 攻击，俗称僵尸机器或者肉鸡，负责接收和执行攻击方 botmaster 的指令，常见的呈现形式包括病毒、木马（Trojan）或者恶意软件（malware），但不存在反之亦然。


中国电信
CHINA TELECOM
NSFOCUS

DDoS 攻击事件追逐利益

DDoS 攻击者们发起了这些攻击，他们都是谁？攻击的原因是什么？最终的目的只是为了破坏吗？被攻击者又是如何应对的？让我们通过 2015 年 10 个 DDoS 攻击事件，来看看其中的玄机。

事件 1　竞争优势：Carphone Warehouse 240 万用户数据被窃

摘录来源：The Telegraph

事件时间：2015 年 8 月 8 日

事件简介：

英国主力智能手机零售商 Carphone Warehouse(手机仓库)遭遇 DDoS 攻击,其网站和互联网服务均被攻击者入侵,受影响的网站包括 OneStopPhoneShop.com，e2save.com 和 Mobiles.co.uk，约有 240 万在线用户的个人信息遭到窃取，其中包含名称、地址、出生日期等信息，甚至包括加密的信用卡数据。稍后的情况显示，这次攻击中可能揉合了一部分 DDoS 攻击作为误导，用于转移 IT 员工的注意力，并趁机窃取数据。

事件 2　实施报复：Lizard Squad 对抗 NCA

摘录来源：ArsTechnica

事件时间：2015 年 9 月 1 日

事件简介：

Lizard Squad 是一个黑客组织，号称“DDoS 之王”。这次发动的 DDoS 攻击持续 2 个小时，攻击的目标是英国国家打击犯罪局（NCA）。这件事情有几个特点：

- **利用攻击推销服务**　目的是为了推销他们的 DDoS 攻击服务 Lizard Stresser，这个服务根据攻击持续时间不同，服务价格从 6 美元到 500 美元不等,但随着 Lizard Squad 名声大噪后,DDoS 攻击服务(云服务）价格也水涨船高，1 小时需要 50 美元。
- **针对政府机构**　虽然这个黑客组织善于隐藏自己，但他们的客户就未必了。8 月 28 日 6 个英国少年因为使用他们的攻击服务，被 NCA 逮捕，结果在 9 月 1 日这天，这个黑客组织对英国国家打击犯罪局（NCA）采取了报复性行动，导致 NCA 官方网站下线 2 小时。
- **从攻击行为走向专业服务**　2014 年 8 月，Lizard Squad 因为发动针对 Xbox Live 以及 PlayStation PSN 的攻击而出名，当时该组织生成是为了阻止对对 ISIL（伊拉克和黎凡特伊斯兰国）的空袭。在 2014 年圣诞节，该组织推出其 Lizard Stresser,。从一份泄漏的 Lizard Stresser 名单中可以看到，至少有 14000 名顾客购买过他们的服务。

事件 3　追求名利：英国 19 岁青年 拿下 FBI“圣杯”

摘录来源：Naked Security

事件时间：2015 年 8 月 27 日

事件简介：

英国 19 岁青年，通过僵尸网络对英国政府与 FBI 某站点进行了 83 分钟的攻击，最终导致该站点停止服务达 5 个小时。此人后续被英国政府逮捕。此事有两大特点：

- **针对政府机构**　该少年主动发起的攻击针对美国联邦调查局 FBI 的政府官方站点。
- **追求名利**　在该领域中，这个群体显然将攻击 FBI 官方网站，视为夺取行业的“圣杯”

事件 4　敲诈勒索：某游戏公司被收保护费 1888 元

摘录来源：中国警察网

事件时间：2015 年 7 月 19 日

事件简介：

因 DDoS 攻击，无锡市惠山区某影视传播有限公司某游戏平台服务器堵塞，引发大量用户投诉。随之一黑客与该公司客服人员联系，以停止攻击为由向该公司实施敲诈，按月收取保护费 1888 元。该公司立即向当地警方报案。接警后，惠山分局高度重视，迅速成立专案小组，开展案件侦查工作，某网络公司安全团队积极配合无锡警方专案组分析和提取了相关材料，犯罪嫌疑人很快落网。事件有几个特点：

- **针对游戏业务的敲诈**　攻击者选择了攻击游戏平台服务器，并以“goodwell”为昵称与该公司客服人员联系，以“不攻击”为由向该公司实施敲诈，以按月收取保护费的形式进行敲诈，显然是看重游戏行业的丰厚收入。
- **BillGates DDoS 木马**　该木马的攻击模式与大多数小流量攻击的特点一样，存在多种攻击模式，包括 TCP-SYN Flood、抓获嫌疑人。此次攻击在公安机关及相关部门、安全公司及用户的通力协作下，最终抓获了敲诈者。据了解，犯罪嫌疑人蒋某 25 岁，是一名网络黑客，曾经因敲诈勒索被依法处理过。

事件 5　未知利益：世界互联网大会期间 浙江某网站抵御攻击

摘录来源：绿盟科技官方微信

事件时间：2015 年 12 月 18 日

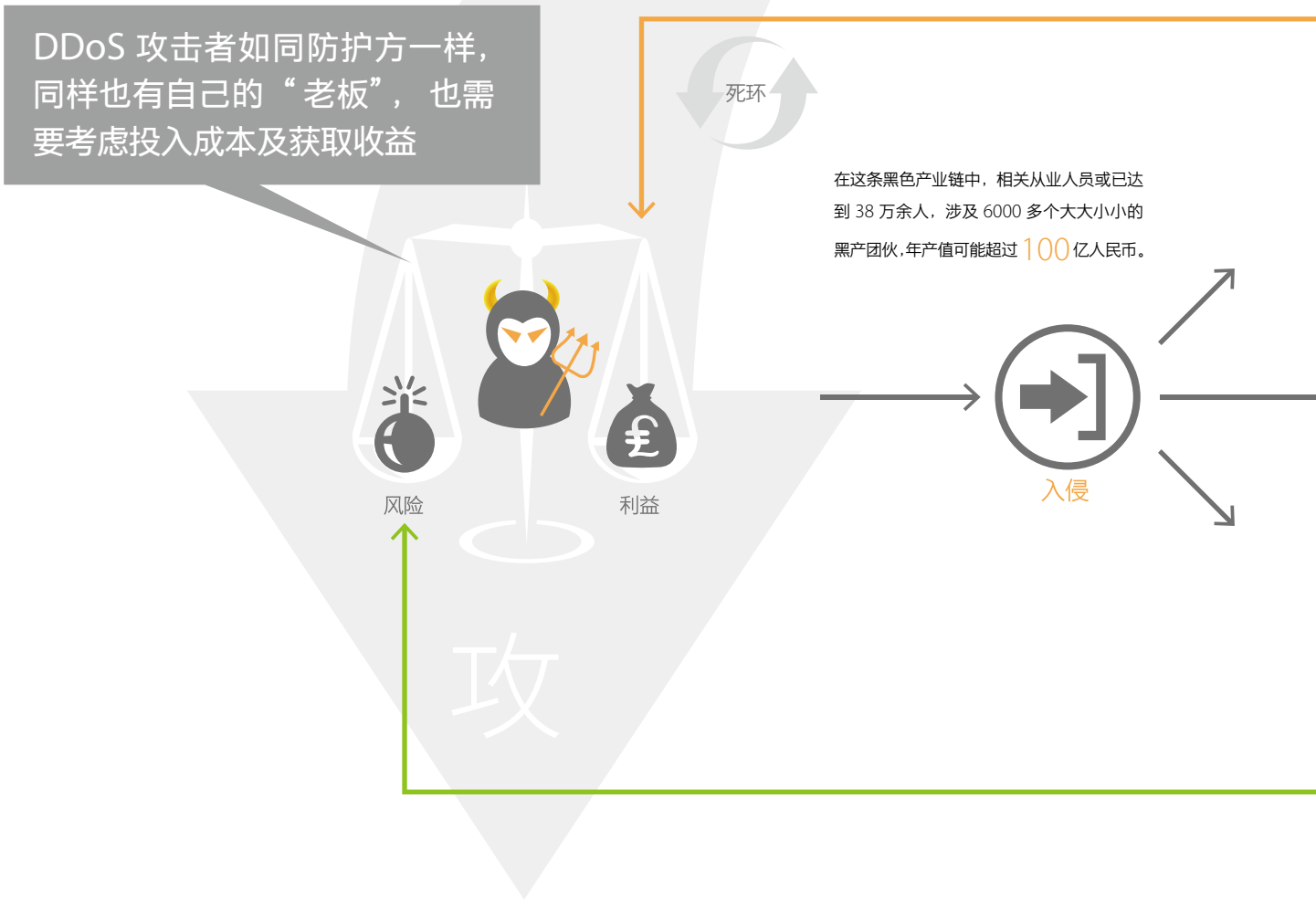
事件简介：

在中国浙江省乌镇召开的第二届世界互联网大会进行到最后一天，凌晨 2 点多，浙江省内某门户网站遭受大流量 DDOS 攻击，攻击持续时间一个多小时，最高峰值 12Gbps。后经过运营商、安全厂商等多方协作，该门户网站成功抵御了攻击。该事件有几个特点：

- **攻击发生在世界互联网大会期间**　仅针对互联网大会的发布渠道及运维提供者的攻击就有 3 次，峰值 10Gbps
- **混合式攻击 UDP 为主**　攻击者采用混合攻击的手法，以 UDP 流量攻击为主，同时包含 SYN Flood、ACK Flood、ICMP Flood 以及应用层的 Connection Flood。DDoS 防护设备清洗总流量超过 10Tbits，其中 UDP 占比达到 90%
- **表象可见深层未知**　虽然这些攻击目标很明确，攻击者想要制造的影响也很明确，但由于没有任何组织声称对此次事件负责，背后的深层利益无法确定，故归类为未知利益。

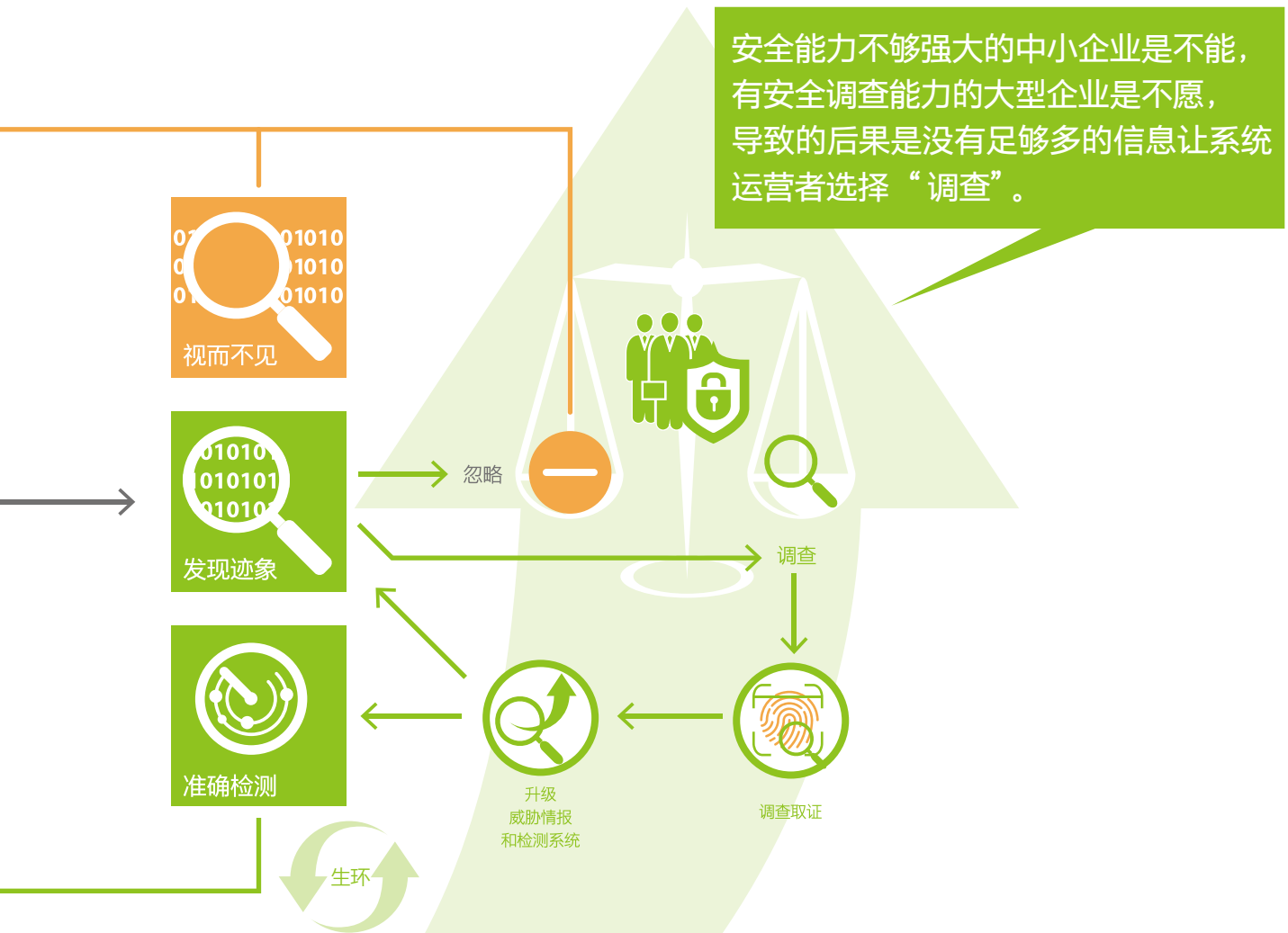
DDoS 事件的警醒及展望

对比第一章节的数据分析，我们就可以知道，现实网络环境中的 DDoS 事件远不止上面列出的那 10 个事件，有大量的攻击事件由于各种原因没有被发现，或者没有被报道出来，这是为什么？我们通过一张图可以做一个初步的了解。



在这张图中，大家可以看到，如今 DDoS 攻击者如同防护方一样，同样也有自己的“老板”，也需要考虑投入成本及获取收益，当收益对比风险的天平倾斜时，攻击者就敢于发动进攻，而这个天平不只是取决于攻击者，更取决于防守者的态度及能力。如果面对黑客的攻击视而不见，那么就等于在攻击者利益的一端增加砝码，从某方面来说，这无异于是鼓励攻击者进攻。由于防守者态度及能力的问题，导致 DDoS 攻击事件能够被曝光的事件比较少，有公开的组织声称负责的就更少，更多的 DDoS 攻击事件都在水面之下或者存在发生的可能。

让我们来看一组数据，一份来自腾讯研究院的研究报告中显示，“在这条黑色产业链中，相关从业人员或已达到 38 万余人，涉及 6000 多个大大小小的黑产团伙，年产值可能超过 100 亿人民币。”这个庞大的链条，如果没有众多的 DDoS 攻击作为支撑，显然是难以生存的。



面对这样恶劣的形式，我们回过头来对已经发生的 DDoS 攻击事件进行分析和反思，从中找到一定的规律，一方面是让防守者进一步提高自己的防范意识，另一方面也是通过这个过程，让这些攻击者们的攻击行为更多的曝光，同时也呼吁更多的同行们加入进来，共享这些信息，从而为防守者们争取时间，改变攻防过程中“敌暗我明”的不利局面。


中国电信
CHINA TELECOM
NSFOCUS

在 2015 年众多的 DDoS 攻击事件中，可以看到 DDoS 攻击不再是单打独斗，而是时常与其他类型的攻击相结合，越来越有 APT 攻击的特征，这些攻击事件背后往往涉及更多利益及更深入的目标。

同时，DDoS 攻击者们为了提升攻击效果，也开始考虑投入产出比 ROI，他们常常使用更低的成本、获得更多的资源、获得更好的效果、更好的隐藏自己，随之产生的或者有可能发生的新应用及协议利用形式，新目标设备、新攻击方法、新攻击工具，这些都值得我们深入思考，也需要调整相应的防护技术及方案。

DDoS 攻击手段考虑 ROI

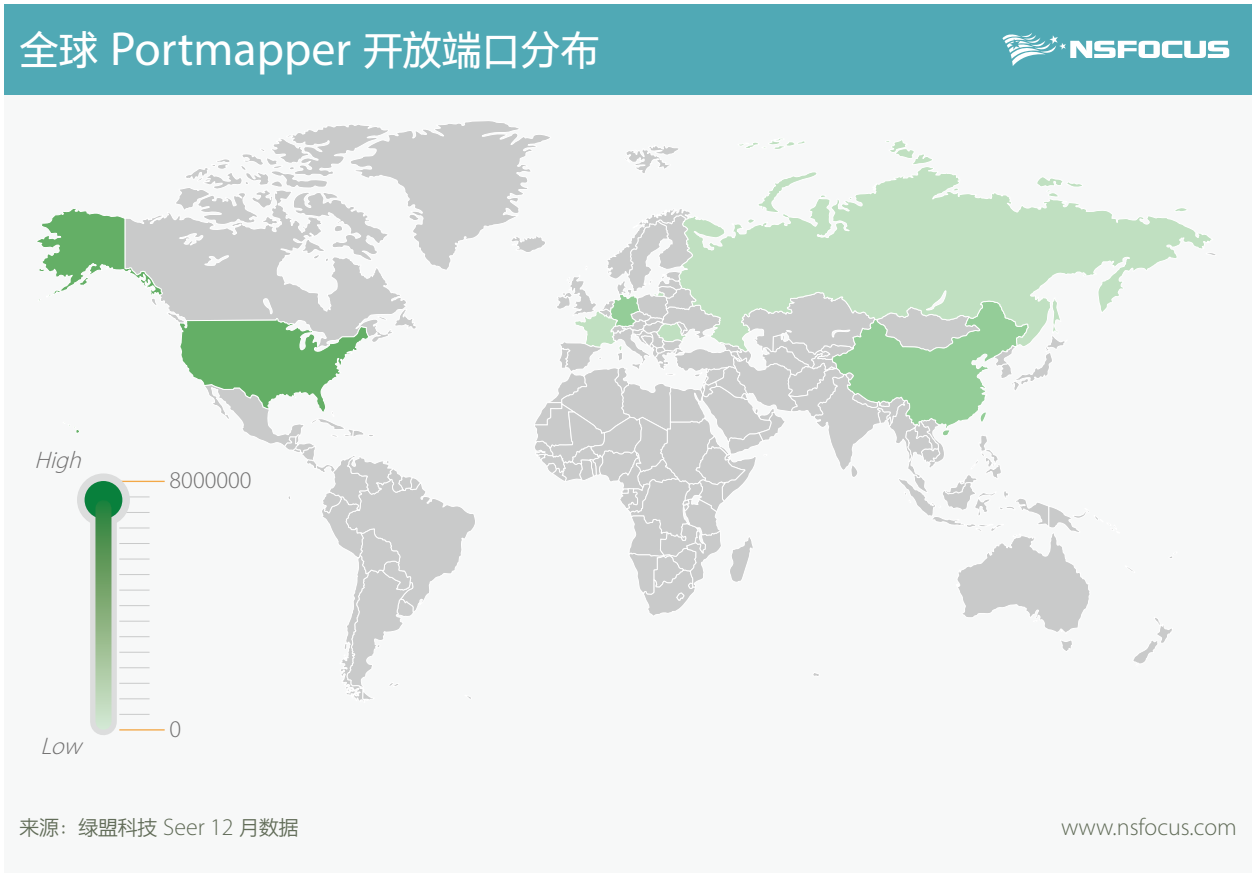
观点 5　新的协议利用形式　网络服务

在流量式的 DDoS 攻击中，攻击者常见的方法是通过寻找可利用的协议，然后利用协议的包放大功能进行攻击。例如，黑客常常利用 UDP 协议进行反射攻击，运行这些 UDP 协议的主机被称作放大器。在 2015 年，又有一些新的协议利用形式被暴露出来，DDoS 攻击者们将可能利用正常业务的服务及开放网络资源发动 DDoS 攻击。

Sentinel license 攻击

RMS 是一套提供授权管理的解决方案，在这个解决方案中包括本地授权和网络授权两种方式，其中在网络授权中使用到一个服务端软件 Sentinel RMS License Manager。在网络的授权交互中涉及到一套协议，在这个协议中使用的端口号为 5093 端口，使用的是 UDP 协议，从 nexusguard 公司对该私有协议的解析上看到，只需要向运行了该服务的端口发送非常简单的一个 UDP 数据包就可能可以得到一个非常大的返回包，返回包内容部分从 2944 字节到 0 字节不等，而发送的 UDP 数据包承载的数据仅 6 个字节。

Portmapper 攻击



从分布图中可以看到开放 portmapper 端口资源的主机，主要分布在美国、中国、俄罗斯、韩国以及欧洲部分国家。这种攻击的放大倍数在 7-28 倍之间。在 DNS、NTP、SSDP 等可以进行反射攻击的 DDoS 的协议上，portmapper 也开始被攻击者使用。

portmapper 是 RPC 服务中的一部分， 运行 RPC 的程序，其 program number 和 program port 与 TCP/UDP 端口有一个映射关系，portmapper 服务正是用于提供这样的查询。所以如果客户端程序想要和某一个特定的 RPC 程序进行

对话，首先需要和 portmapper 进行通话，查询具体的服务端程序所使用的端口号。一般情况下，portmapper 服务默认使用的端口是 111 端口，当然这个端口是可以被改变的。

BITTORRENT 攻击

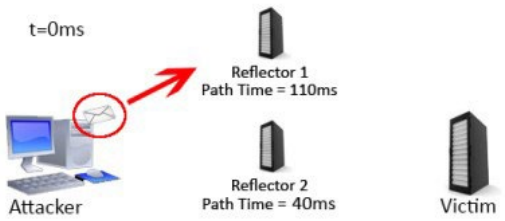
2015 年 8 月 27 日 BitTorrent 发表声明回应 usenix 研究者提出来的一项新的攻击技术，利用 µTP 协议实现上的漏洞进行 DDoS 放大攻击。该协议是 UDP 下的一个协议，由于在 libutp 中，对这个协议进行实现的时候，服务端没有针对状态 ST_STATE 做验证，从而导致这些安装了服务端的机器成为 DDoS 攻击放大器，这种攻击的平均放大倍率在 50 倍左右。

观点 6　新的目标设备　移动终端

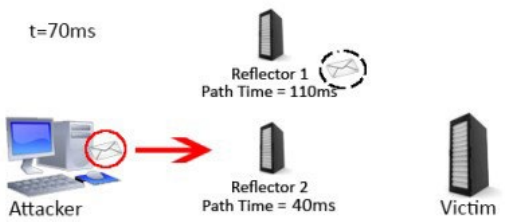
在 Carnegie Mellon University 的一份研究报告中指出 LTE 网络的实现中存在安全隐患，由于安卓系统对应 LET 网络并没有一套合理的权限控制，导致手机通过 INTERNET 权限就可以直接发送 SIP/IP 数据包，访问 LTE 网络打电话，这样一来很可能造成 LTE 网络中的 DDoS 攻击，并且大量消耗用户本身的电话费。

观点 7　新的攻击方法　延时攻击

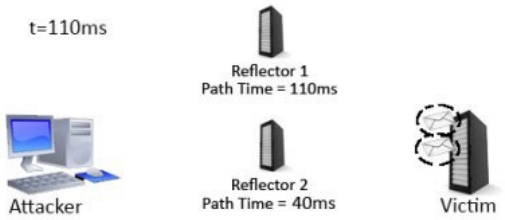
这个技术提出于一篇名为《Temporal Lensing and its Application in Pulsing Denial-of-Service Attacks》的论文，论文中展示了一种通过时间延迟进行流量放大攻击的方法，使得同一时间到达受害者的攻击流量达到一个更明显有效的高峰值，中文一般称为临时透镜攻击，它的攻击原理如下图所示。



(a) At $t = 0\ ms$, the attacker sends one packet towards reflector 1

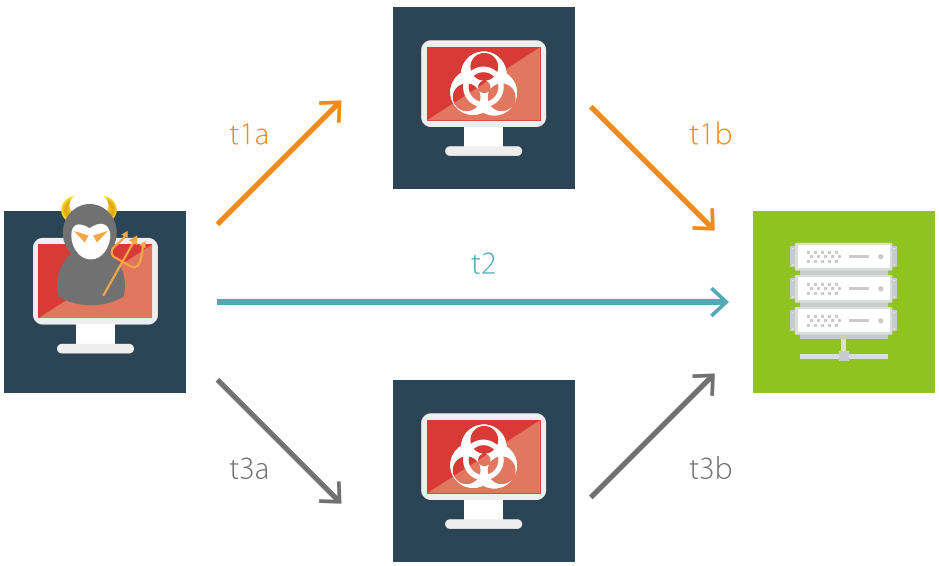


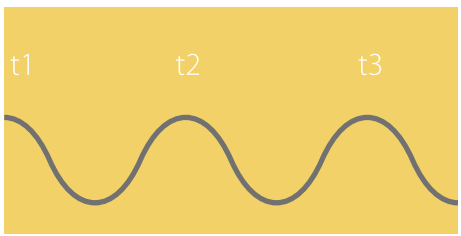
(b) At $t = 70\ ms$, the first packet is about 60% along its path to the victim and the attacker sends another packet to reflector 2



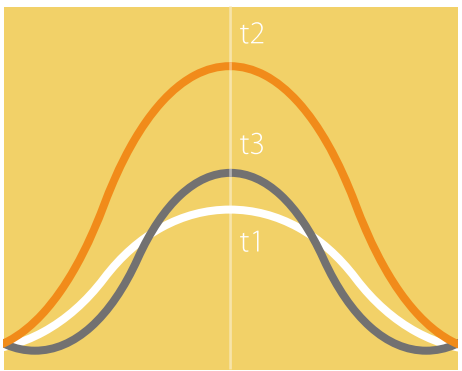
(c) At $t = 110\ ms$, both packets arrive at the victim

这个词汇及中文翻译较为难以理解，所有本报告中将上面的原理图做了一个转化，这样大家对比看起来可能就比较容易明白，这个攻击形式是个典型的延时攻击形式，“以时间换数量”。如果攻击者能够控制多个时间段的多个数据包，让他们同时到达攻击目标，那么这些数据包将会叠加形成波峰，这样导致的危害更大。





顺序到达的常规攻击



同时到达的叠加攻击

观点 8　新的攻击工具　DDoS 木马

一些攻击软件黑客仍然在不断升级版本，不断适应新的攻击环境，整合新的攻击技术，这导致很多新的攻击行为或者攻击工具都还没有浮出水面，一直到东窗事发。下面 3 款攻击软件，防守者们应该尽快升级防护产品及方案，以便抵御这些工具带来的攻击。

- **Chikdos**　黑客首先通过 SQL 注入获取 mysql 服务器的权限，利用 mysql 的 UDF 功能，下载 Chikdos 木马，将主机转化为僵尸。
- **Xor.DDoS**　这是一个针对 Linux 主机的控制软件，主要功能是利用 Linux 主机发动 DDoS 僵尸攻击，这个僵尸网络是由 Akamai 公司发现并命名的，该僵尸网络具备 150Gbps 的攻击能力。
- **Jinfinity**　这是一个典型的应用层攻击工具，它针对 Java 应用程序的反序列化过程实施攻击，让目标耗尽所有的内存，最终造成拒绝服务。这个工具可以完全绕过现有的对于反序列化的保护。

针对这些攻击工具的防御方法包括两个方面，一方面可以从基础设施的改进来缓解攻击影响，比如带宽扩容，增强服务器的处理性能、采用合理的网络部署结构等；另外一方面可以在网络边界出入口采用专用的防护技术，这些防护技术主要有 4 大类：

- **动态挑战算法**　模拟传输层和应用层协议栈行为，代替服务器回应数据报文，对正常的客户端发送挑战报文，只有完成挑战认证的客户端的流量才能放行。动态挑战算法比较常用的有 SYNCookie, DNS Ncookie 和 SIP cookie。
- **多层次限速**　基于各种粒度和层次，分别从源 IP、目标 IP、传输层和应用层 session，对 IP 流量进行限制。这是对流量型攻击常用的防护方法，比如 UDP Flood，ICMP Flood。
- **智能的访问控制**　从三层到七层灵活的访问控制策略。从 IP 地址到七层应用层协议，比如 HTTP 协议，可对报文的 URL，user-agent，cookie 设置丢弃、信任和限速策略，而对 DNS 协议，则可对报文中 QUERY 名字、类型、RR 记录设置类似策略。
- **行为分析和信誉机制**　基于数据分析技术对 IP 行为和流量特征建模分析，建立通用信誉库包括 IP、URL 和文件信息，输出异常流量特征指纹，自动完成流量清洗。这对僵尸网络以及报文发送异常的攻击工具防护都非常有效，比如 Slowloris Header。


中国电信
CHINA TELECOM
NSFOCUS

DDoS 防护走向生态化

正如 RFC 4732 对 DDoS 所描述的那样，传统互联网架构是非控制性的网络架构。因此，从技术角度来说，DDoS 不可能完全杜绝，只能最大程度的“缓解”。作为防护方，应该思考怎样从传统的动态防御、限速、行为分析方式，转变为网络安全的态势感知与云计算及大数据分析相结合的模式，形成防护的闭环。同时，在 DDoS 攻击已经发生的情况下，需要采取各种方式减少 DDoS 攻击造成的影响，从而保障其服务的可用性。

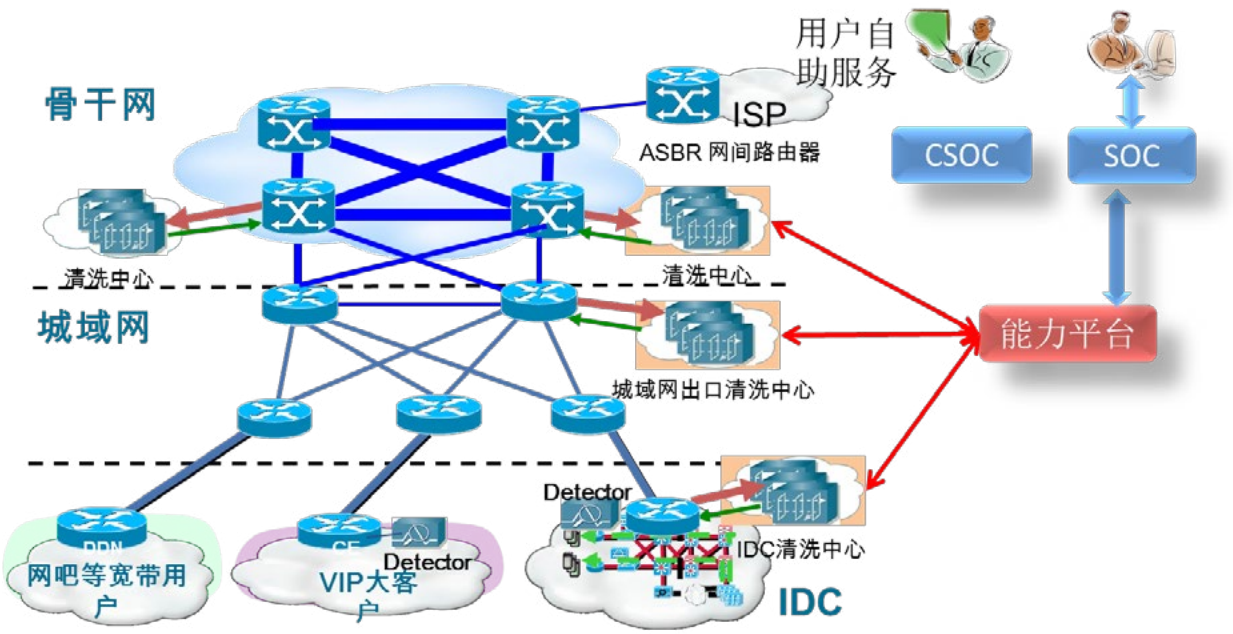
而另一方面，DDoS 涉及到业务的方方面面，从主管机构、行业机构、社会组织、安全厂商到用户，单独哪一方面也很难完全实现 DDoS 的防护，而且攻击者形成的地下产业链已经很成熟，这就需要建立一个多方协同的机制，感知可能发生的，阻止正在发生的 DDoS 攻击，抑制其攻击规模，消除其安全隐患，我们称之为“治理”。

下面从 DDoS 治理及 DDoS 缓解两个方面，来说明 DDoS 防护技术及方案的发展情况和方向。

治理　运营商治理大流量

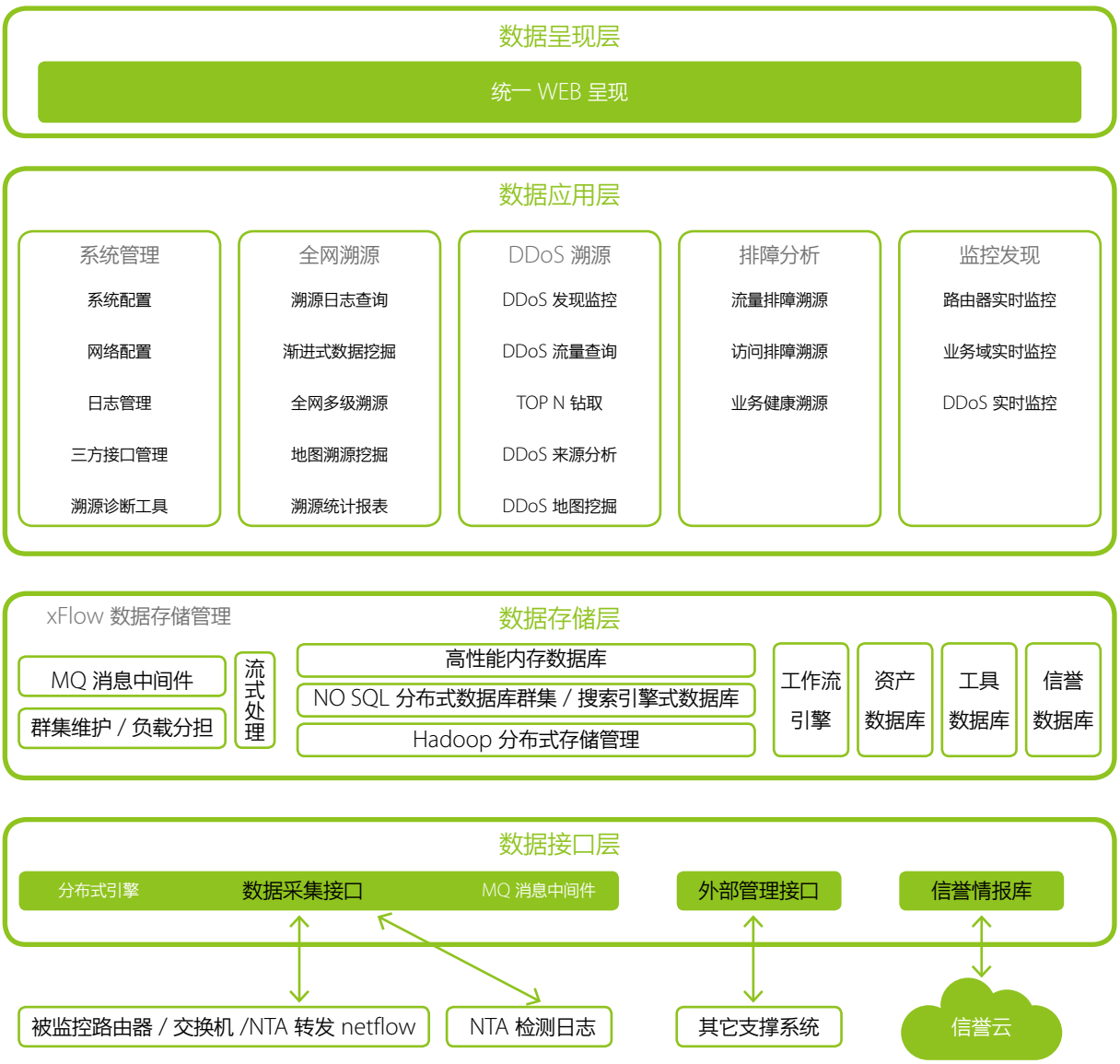
一级运营商管理运营丰富的骨干网带宽资源，对于大流量及超大流量 DDoS 攻击具有先天性的压制优势，云堤就是中国电信推出的运营商级 DDoS 攻击防护产品，并提供相关解决方案。凭借该方案，可以通过 4 种方式实现大流量压制，包括国内网间攻击阻断、国际网间攻击阻断、国内网间 + 国际网间攻击阻断、全网攻击阻断。

另外凭借骨干网的多层级架构，云堤还可实现近源清洗，即快速发现攻击源并靠近攻击源所在骨干节点实施流量清洗，进而实现纵深防护。



大数据下的 DDoS 态势感知

从中国电信云堤的近源清洗方案中可以看到，其关键要素在于实现事前的态势感知或者事中的攻击溯源，从而利用大数据的优势实现更有效的 DDoS 治理能力。其中攻击溯源包括 APT 攻击溯源，DDOS 攻击溯源，僵木蠕溯源等。这方面中国电信云堤已经与安全厂商展开有效协作并形成了一整套方案。



在这套方案中，以大数据技术作为支撑，实现快速有效的 Flow 数据采集，结合实时的计算与入库，通过关联化的呈现实现了 Flow 流量的分析能力，针对 DDoS 可通过多个维度进行钻取统计，例如攻击类型、具体的攻击事件、攻击 IP、被攻击 IP、攻击流量大小排序等。这种大网下的态势感知能力，有效的改善了网络环境，有效缓解 DDoS 攻击，提供更有效的保护。另外，一级运营商可以结合自己丰富的高性能基础设施提供 DDoS 清洗服务，例如通过云清洗的方式实现服务交付，并可实现用户自助抗 D 服务以及流量可视化管理，可以为用户提供更好的网络环境管理手段。

治理　互联网公司阻断 DDoS 攻击工具传播

在事前阶段，通过监控及治理 DDoS 攻击工具及相关恶意软件，也可以有效的遏制 DDoS 攻击事件，而互联网公司涉及了互联网用户交互行为的方方面面，显然互联网公司在这个方面的治理更有优势，但实际操作过程中面临了相当多的难题，比如：

- 侦测 DDoS 发起攻击，往往是大流量比较容易察觉，但如果 DDoS 攻击采取小流量及慢速攻击，甚至采取加密及伪装成正常应用，就很难察觉他们；
- 针对 DDoS 攻击工具样本的分析需要一定的时间，这个时间相对于 DDoS 攻击时间来说，往往是滞后的，这就导致响应速度较难提升。

但基于互联网大数据的积累，至少有几个方面是可以考虑进行的：

- **DDoS 攻击工具的清理**　大量用于 DDoS 攻击的工具及木马乃至更广范围的恶意软件样本，经常的在各类社交网络及相关网络服务中传播，可以根据对这些样本的分析及监控，在相应服务的网络通讯及存储环节，层层拦截；
- **追踪 DDoS 发展态势**　可以看到互联网公司已经与网络安全公司展开合作，不断追踪可能发起 DDoS 的行为，相关恶意软件样本及 DDoS 攻击事件分析，从而能够为企业或组织制定防护策略提供依据；
- **打击僵尸网络**　就一些可以明确知道及追溯的僵尸网络，可以进行多方面形成联合机制，对其实施打击动作，这方面国外软件厂商微软曾经有过成功案例。

缓解　网络安全公司强化 DDoS 攻防技术

从前述章节可以看到，DDoS 攻防战如同其他网络攻防一样，并不是机器之间的对抗，而是人与人之间的对抗，攻击者在不断创造新的攻击技术，防守者也需要不断提升 DDoS 防护技术，这个方面网络安全公司责无旁贷。未来 DDoS 防护技术发展将会至少包括 3 个方面：

- **特征 + 行为**　传统针对特征的扫描和防护，越来越难以应对未知攻击形式，而后者将会更多的利用虚拟环境及动态跟踪的方法，一方面以避免攻击者对于攻击环境的侦测，另一方面跟踪其攻击行为提高识别率；
- **过滤手段高级化**　包括基于威胁环境和正常业务环境的过滤技术，比如云端威胁 IP 信誉库，云端威胁指纹库，基于业务正常环境的“白”的过滤技术，如地理位置，业务端口，时间段等。
- **智能化防御技术**　为了降低安全运营的复杂性，应该增加建模、自学习、自动化技术，比如自学习用户业务环境，生成正常业务基线参数；感知设备攻击效果而自动化轮换防御算法等。

虚拟化执行技术

在特征 + 行为方面，绿盟科技在针对恶意软件越来越多的具备对抗查杀的功能，推出了更高级的检测机制，虚拟化执行。

检测原理

- 将恶意样本或恶意样本部分片段，置于虚拟环境中进行执行，然后记录样本的运行行为，通过运行行为来判断样本是否为恶意；
- 传统的签名类设备，是基于特征串进行匹配（即抽取样本中的某些二进制字符序列来识别该样本）。这种基于特征串的匹配方式只能匹配已知的恶意样本，且很容易被各种加壳给轻易绕过，对于新出现的恶意样本则完全没有办法，需要不断地更新签名库来适应新的恶意样本出现；
- 虚拟执行技术是基于行为判断的，攻击行为的类型则变化要缓慢的多。不管新样本如何变化或加壳，运行之后最终都是要执行恶意行为（如执行 shellcode、回连 CnC 等），这些行为一般情况下是没办法隐藏的。

虚拟执行分类

- 根据虚拟环境的不同，又可以分为轻量级虚拟执行和系统级虚拟执行。
  轻量级虚拟执行主要是实现指令片段的模拟执行，根据指令序列的逻辑行为来判断恶意样本。
- 系统级虚拟执行则完整模拟整个操作系统和应用程序环境，最大限度模拟真实环境，然后判断样本的运行行为。
  - 系统级虚拟执行，目前有传统基于 API 监控的虚拟执行和基于动态翻译的虚拟执行，前者只能做到 API 级别的行为，一般传统的沙盒使用此技术。
  - 而基于动态翻译的虚拟执行可以监控到指令级别，可以识别更多的恶意行为和虚拟执行逃逸行为，目前 TAC 采用了此技术。

虚拟执行逃避技术

- 当然，目前也出现了针对虚拟执行技术的逃避技术，这些逃避技术可以逃离部分虚拟执行引擎的检测。
- 目前已有针对这些逃避技术的检测技术，用来专门检测逃避虚拟执行的恶意样本。

多层次防护过滤机制

在过滤手段高级化方面，已经可以出现多层次 DDoS 攻击防护机制和算法，比如多层次防护过滤机制（“反欺骗”、“协议栈行为模式分析”、“特定应用防护”、“用户行为模式分析”、“动态指纹识别”、“带宽控制”等）及智能行为防御算法进行纵深防御，准确地区分出恶意的 DDoS 流量和正常访问的网络数据报文并实施过滤，支持以下流行的攻击类型：

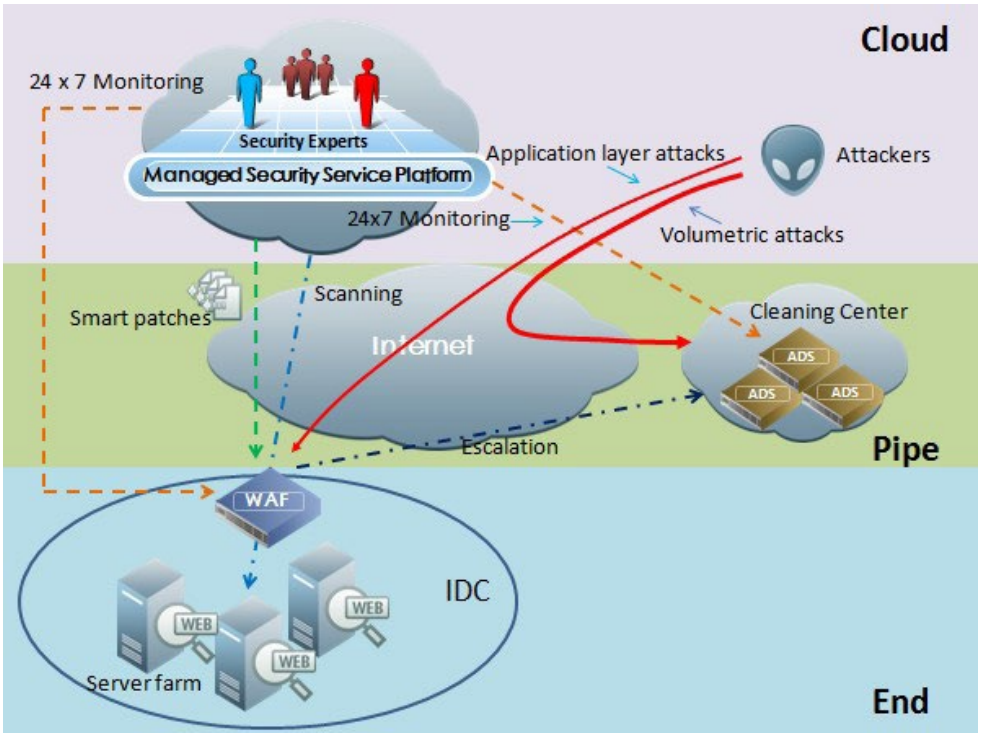
- 系统可以防护各种传输层的拒绝服务攻击，如 SYN Flood，SYN-ACK Flood，ACK Flood，FIN/RST Flood ，UDP Flood，ICMP Flood，IP Fragment Flood、Stream flood 等。
- 系统可以防护 HTTP get /post flood 攻击，慢速攻击，TCP 连接耗尽攻击，TCP 空连接攻击等应用层攻击。
  - 系统可针对 DNS 服务攻击，游戏服务攻击、音视频服务攻击等危害更大的应用层拒绝服务攻击进行有效防护。
  - 系统能够对利用各种代理服务器如 CDN，WAP 网关等发起的 DDoS 攻击进行防护。
  - 系统能够有效的防护利用各种 annoymous 攻击工具和僵尸工具发起的 DDoS 攻击。

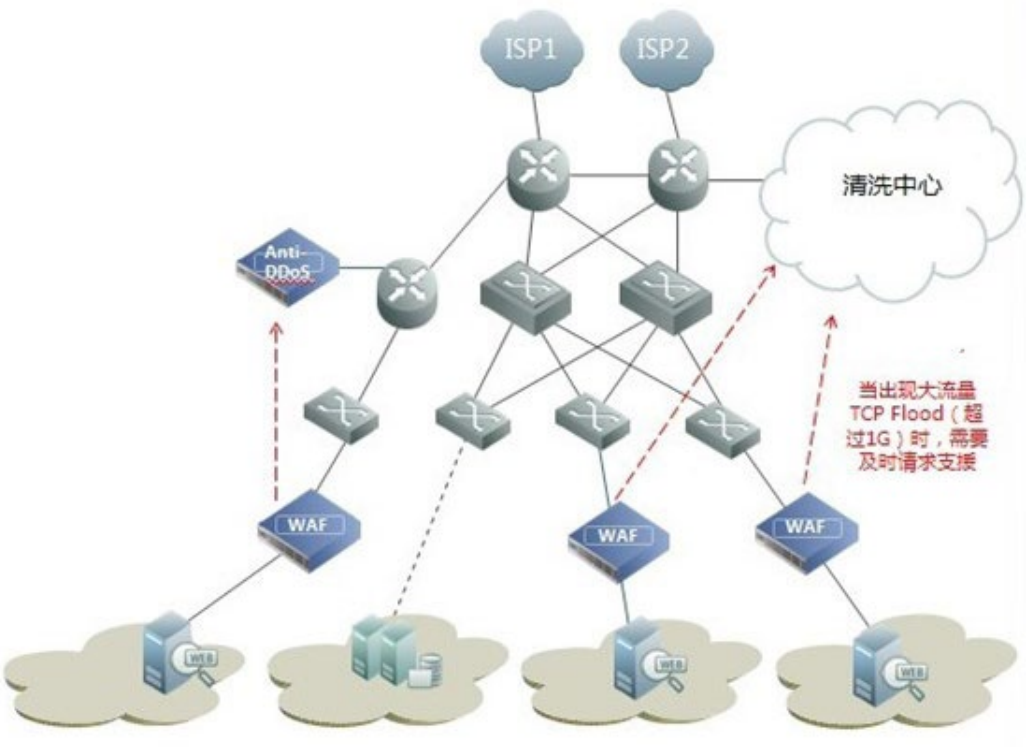
WAF 与 ADS 联动模式

在智能化防护技术方面，尤其在处理传输层与应用层混合攻击模式问题时，系统间纵深、协同的防护机制能够在网络较高层面清洗大流量攻击（如云计算中心出口），在较低层面（如应用服务器前或虚拟机前）解决小流量应用型攻击，两者之间应能进行智能联动从而实现协同防御，实现和其他网络层面的设备实现分层协同的防护，达到业务信息高效共享、防护性能灵活分配，从而实现快速、全面、精准和自动化的安全防护体系。

Web 应用层攻击非常复杂，因为 Web 攻击应用层受攻击的对象是 Web 应用本身，而 Web 应用程序根据业务特点是非常多样化的，很难用一套方案解决所有的问题。Web 应用层攻击的流量一般不大，如 SQL Injection，但其攻击载荷存在于数据层面，需要深入解析 HTTP，并支持多种编码方式的解码，再配合上不断更新的威胁知识库和智能算法，才能精准检测。

当应用层攻击与传输层攻击组合进攻的时候，单一层面的防护手段容易失效，那么就需要让这两种安全设备进行联动，如 Web 应用防火墙，其应用层防护能力与 ADS 的大流量防护能力相结合，能够有效缓解 DDoS 混合攻击模式。在这套方案中，将 WAF 部署在企业近端做下级流量缓解，当流量到达到阈值的时候，将流量向上牵引至 ADS 进行大流量清洗，同时将清洗后的流量进行回注。


Cloud
24 x 7 Monitoring
Security Experts
Managed Security Service Platform
Application layer attacks
Attackers
24x7 Monitoring
Volumetric attacks
Scanning
Smart patches
Internet
Cleaning Center
ADS
ADS
ADS
Escalation
Pipe
WAF
IDC
WEB
WEB
WEB
Server farm
End


ISP1
ISP2
清洗中心
Anti-DDoS
当出现大流量TCP Flood（超过1G）时，需要及时请求支援
WAF
WAF
WAF

未来 DDoS 防护不再是单个硬件产品形态能解决的问题，从技术上需要一个防御体系，就像攻击态势中提到的那样，有大流量的方面，有小流量的方面。小流量应用性攻击在本地防御更为有效，大流量方面更适合在外部进行，而介乎于两者之间的部分，将部分 IDC 或云中心会建立自己的本地清洗中心。同时，伴随智能化、前瞻性理念在 DDoS 防护领域的应用，将会出现更多的 DDoS 防护增值服务的出现，这些多维度、多形式的防护形式，将需要信誉等联动机制的出现，才能在整体防护效能上趋于合理。

缓解　用户加固特定业务

在业务方面，只有用户自己才最了解自己的业务特性，结合业务的流量特性并针对业务的薄弱环节进行加固，将在 DDoS 防护上起到事半功倍的效果。但限于组织内部等因素，可能用户自己实施缓解措施及制定加固方案存在一定的困难及风险，其原因在于：

- 需要考虑业务系统的可用性；
- 需要考虑整体实施方案制定；
- 需要尽可能降低加固动作对业务环境的二次伤害。这就需要企业自身、漏洞相关厂商、安全厂商、运营商一起协作才能形成快速、安全、有效的行动方案，避免业务系统在获得安全加固之前遭受攻击。

常见业务场景及防护思路

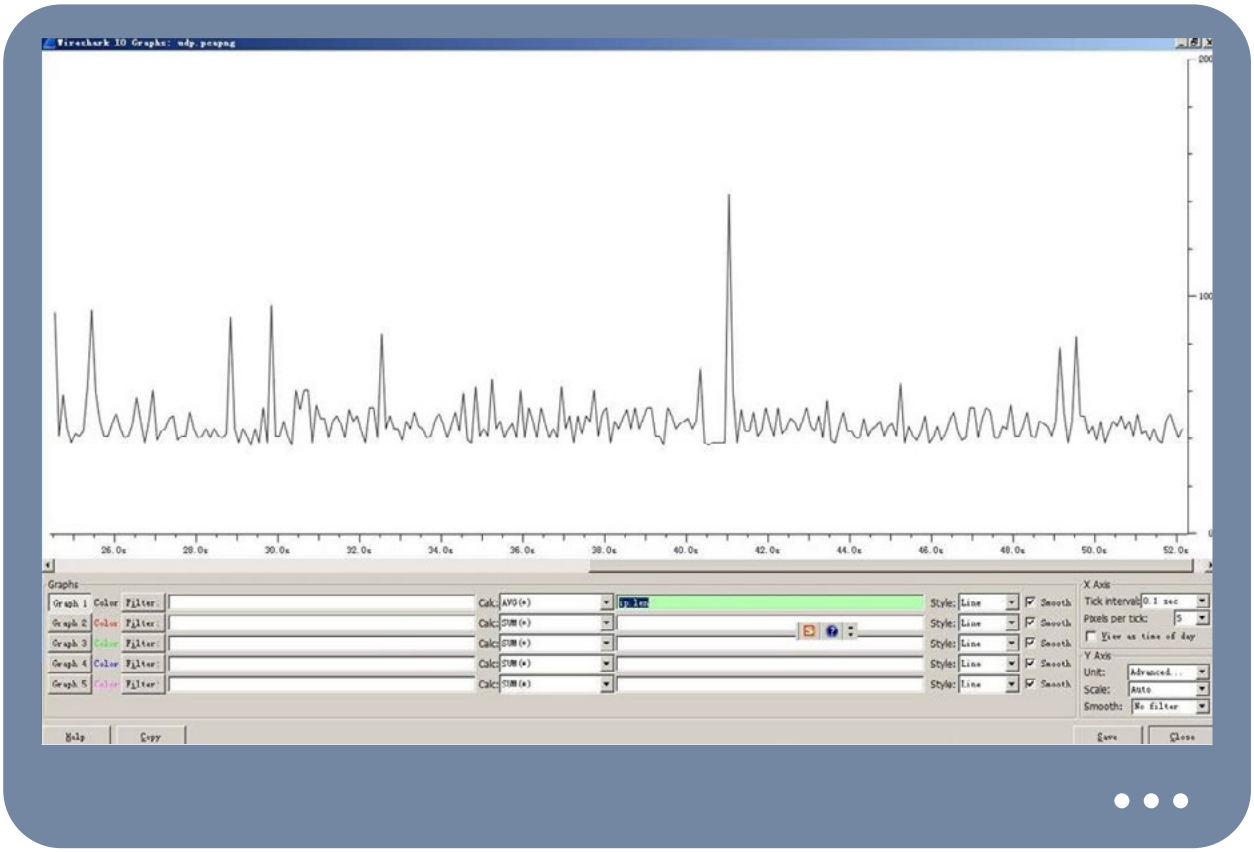
业务场景	业务特点	常见攻击	防护思路
HTTP 业务防护	• 基于 HTTP 协议的业务。主要是 B/S 架构的 web 系统，比如企业门户网站、政府网站、证券公司网站、银行网银网站等。 • 目前也有许多 C/S 架构的系统也基于 HTTP 协议，比如手机或者 PC 终端的网上银行、证券交易系统等。	CC SYN Flood ACK Flood Connection Flood	• 使用探测包验证源 IP 的真假性。 • 使用 HTTP302 跳转、JS、图片等人机识别技术验证客户端行文 • 限制源 IP 的连接数。 • 基于大数据的异常行为识别、信誉过滤。 • 也会遇到攻击者使用 UDP 大流量攻击 HTTP 业务的情况，防护者可直接封禁此类非业务流量。 • 在网络边界直接封禁常见的反射攻击（该策略对其他业务场景也适用）。
网吧 业务防护	• 网吧的流量主要是下行流量，且网吧基本不对外提供服务。 • 流量成分以 ACK、UDP 为主，报文的源端口大部分为知名业务端口。	UDP Flood ACK Flood	• 因网吧基本不对外提供业务，因而非常适合使用业务封禁策略，比如可封禁 SYN 80。 • UDP 源限速。 • 游戏是大部分网吧的主营业务，为保证在 DDoS 防御过程中游戏不掉线，可采用自学习策略提升用户体验。
DNS 业务防护	• DNS 业务通常使用 UDP 报文来承载，但其协议上也支持 TCP。 • 对于运营商的递归 DNS 服务器来说，查询源主要是用户终端。 • 对于企业的权威 DNS 服务器而言，查询源主要是运营商的递归服务器。	DNS Query Flood DNS Response Flood	• UDP 转 TCP 防护思路，用来验证源 IP 的真假，但实际效果不佳 • 域名学习思路，基于域名信誉的防御。 • GEOIP 防御思路，如运营商的递归 DNS 只对本地用户提供访问 • 白名单思路，如企业的权威 DNS 只对运营商的 DNS 开放，但需要防范白名单被突破的情况（可结合使用 TTL 等技术）
游戏 业务防护	• 游戏业务对网络质量敏感。 • 很多游戏使用私有协议，造成了 DDoS 防御的困难	各种 Flood	• 依然可使用反向探测等技术验证源 IP 的真假，过滤掉较为初级的攻击。 • 使用自学习策略提升游戏用户体验。 • 直接封禁非游戏业务端口的报文。 • 使用水印防护算法。游戏客户端在发送数据报文时，可在报文中插入一个“水印”，防护设备基于此“水印”进行识别和过滤。

基于业务特征的智能指纹识别

通常来说，针对 UDP 攻击，流量清洗设备普遍采用的方法是在达到服务器的流量超过阈值时触发防护设备的防护机制，然后通过预先设定好的防护算法和策略进行清洗，其中最常见的方法是根据源 IP 以及源端口进行判别、限流。但是，这种方法存在明显的劣势，例如：

- 现在非常常见的一些工具，例如 HPING3、DoSend 等，发出的流量都是一些源 IP 随机的攻击包，这也就意味着通过这些攻击工具打出的流量对于 ADS 设备来讲，每一个攻击包都是一个新的 session，所以原有的限流机制对于这种流量无法进行有效的拦截；
- 有很多比较常见的攻击工具，可以轻松突破基于限流的方法进行防御的防护措施；
- 常见的 UDP 攻击工具，如 hping3/DoSend/LOIC 等发送的是固定了大小的数据包，但是像另外一些工具如：Txddos 等，发送的都是一些数据包大小很随机的数据包；这使得传统的检测数据包大小的方法可能达不到预期的效果。

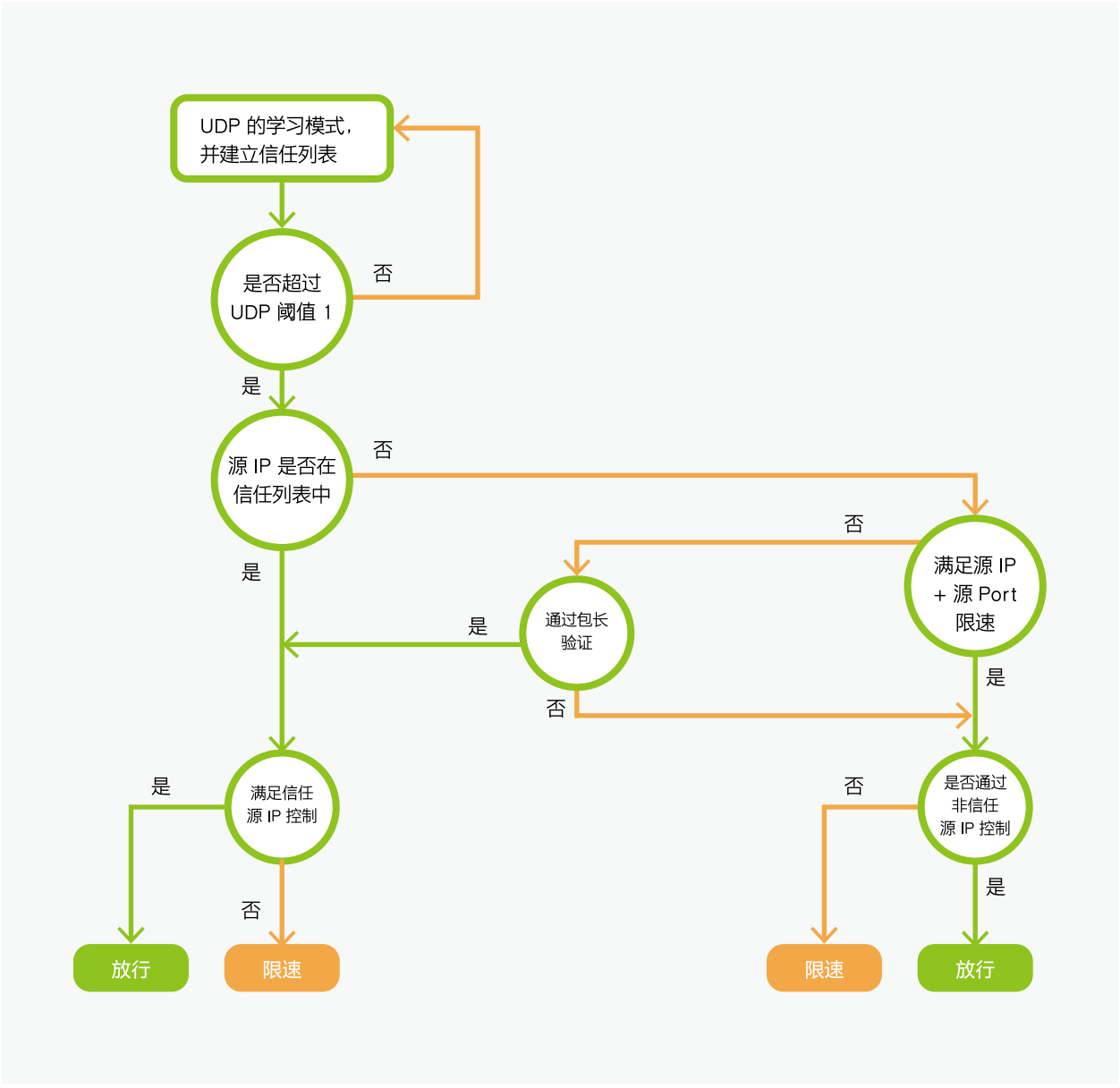
但在业务环境分析中，被防护的业务中 UDP 数据包具备一定的统计分布规律，下图第一张是实际抓取的该业务数据包特征：



分析之后，可以提出这样一个实施构想：

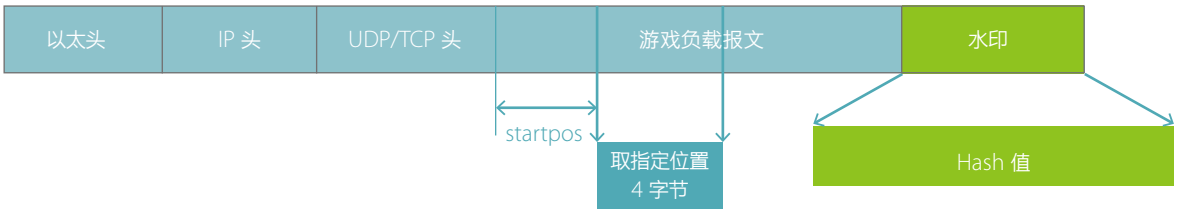
- 通过对设备升级将该游戏业务的 UDP 数据包大小特点的特征库导入到 ADS 中；
- 当到达该游戏业务服务器的 UDP 数据包超过了设备的阈值时，ADS 将会启用 UDP 的防护算法；
- 进入了 UDP 防护模式的 ADS 会抓取每个源 IP 的发送的 100 个数据包作为样本，ADS 分析该样本中数据包特征，同时将使用特征与该游戏业务数据库中的特征进行对比，如果发现数据包的特征与数据库中的特征一致，就可认为该 IP 为正常用户，并将该 IP 加入到 ADS 的信任表中；如果发现某一个源 IP 发送的数据包不符合该游戏业务数据库的包特征，则会丢弃该数据包，这样想固定包大小的攻击，以及包大小很随机的端口，都可以通过此种包大小特征的比对方式被过滤掉。

具体流程图可以用下图表示：



水印算法

这个算法一般在游戏业务中使用较多，游戏服务器或客户端在负载报文的末尾插入水印防护相关的字段，攻击发生时，防护设备校验水印值的合法性来决定是否丢弃报文。一般用来生成水印的元素可能包括，服务器时间、客户端 IP、负载报文中指定的字节，以及一个只有游戏厂商和防护设备知道的 hash 密钥。这里有很多种实现的方式，例如：



生态　DDoS 防护生态环境

从上面几个方面我们可以看到，无论是 DDoS 的治理还是缓解，都不是单一组织或者单一产品及服务形态可以完成的，不仅是技术层面，更重要是经济层面，在有的环节，有效性和投入并不对等，这就需要主管机构、运营商、标准组织、安全厂商及最终用户共同协作，打造 DDoS 防护生态环境（DDoS Prevention Eco-System），才能最终有效抑制这种攻击，我们期待未来这方面会看到更多更好的体系诞生。

结束语

在上面的分析中我们可以看到，2015 年 DDoS 的攻击呈现两极分化形式，一类持续大流量攻击，尤其是针对高性能、高价值、大范围的攻击目标；另一类则呈现小而快、小而慢的形式，进入细分行业，主要是针对小流量及特殊业务目标；同时，我们也发现这两类攻击并非格格不入，而是伴随着环境、业务、时间、流量、设备的变化而组合演变，这些演变将与云计算及大数据一起，催生 DDoS 防护向下一代 DDoS 防护及 APT 时代迈进。

作　者

陈颐欢	绿盟科技
刘紫千	中国电信云堤
常力元	中国电信云堤
张　敏	中国电信云堤
李国军	绿盟科技
何　坤	绿盟科技
周　振	绿盟科技
王　洋	绿盟科技

DDoS 威胁报告

SECURITY

DDoS（分布式拒绝服务）作为网络安全威胁中的典型攻击手段，从诞生的那天起就从未停止，而网络安全威胁也正在变得日益复杂，各类攻击目标、手段就来源始终在不断的发生着变化，随之企业及各类组织需要不断关注这些发展趋势，以便能够理解与预测未来可能遭遇到的恶意攻击，进而让应对复杂变化所带来的挑战。

本次报告即为 2015 全年的 DDoS 威胁报告，帮助大家：

- 持续了解及掌握 DDoS 威胁发展态势
- 在遭遇到攻击后，可以快速理解及检测可能的伤害程度
- 不断强化网络安全意识，完善解决方案

中国电信 CHINA TELECOM

NSFOCUS

2015 DDoS Threat Report