网宿科技
ChinaNetCenter

中国互联网安全报告

2016 上半年

编者的话

随着人类社会信息化与数字化进程的不断推进，互联网在我国政治、经济、文化、社会生活等领域的作用越来越重要。近些年来，伴随着互联网建设与应用的蓬勃发展，网络安全问题层出不穷，给我们的社会经济活动和日常生活带来了极大的危害与损失。

国家互联网应急中心发布的《 2015年中国互联网网络安全报告 》中指出，我国网络安全保障措施不断完善， 网络安全防护水平进一步提升，但网络安全形势依然严峻，木马和僵尸网络、 移动互联网恶意程序、分布式拒绝服务（DDoS) 攻击、信息泄漏、安全漏洞、网页仿冒、网页篡改等网络安全事件仍然难以避免，并表现出新的特点。

网宿科技是国内专业的CDN及IDC综合服务提供商， 向客户提供全球范围内的内容分发与加速、服务器托管与租用、 以及面向运营商的网络优化解决方案等服务。 网宿科技一直重视网络安全，依托“CDN+IDC+云计算”资源，开展云安全服务。 为了实现云安全近源清洗和分散防护的防护目标，网宿科技在云安全方面布局了三步走的战略。首先，打造基于CDN网络的安全平台，建立分布式安全防护系统； 第二，建立智能调度机制，将网络攻击流量分散到不同节点中，实现近源流量清洗； 第三，深耕安全客户需求，丰富产品线，除抗 DDoS、Web应用防护外，打造多样化的云安全服务，通过对用户行为建模，建立信誉库，实现安全服务自动化、 智能化和可视化，以满足安全客户不断升级的防护需求。

本报告是网宿科技发布的第一期互联网安全报告， 报告中的数据来自于网宿科技遍布于全球的600多个CDN加速节点及网宿云安全产品在2016年上半年期间监测到的网络攻击事件和警告。 本期报告重点分析国内互联网中网络层DDoS攻击和WEB应用攻击的各种特征及变化， 并通过案例分析网宿科技对于这两类网络攻击的安全防护。

2016年上半年网宿科技监测到的互联网安全事件一览

DDoS攻击峰值带宽 **495Gbps**

DDoS攻击峰值pps **231Mpps**

46分钟

DDoS攻击
平均持续时长

342小时

DDoS攻击
最长持续时长

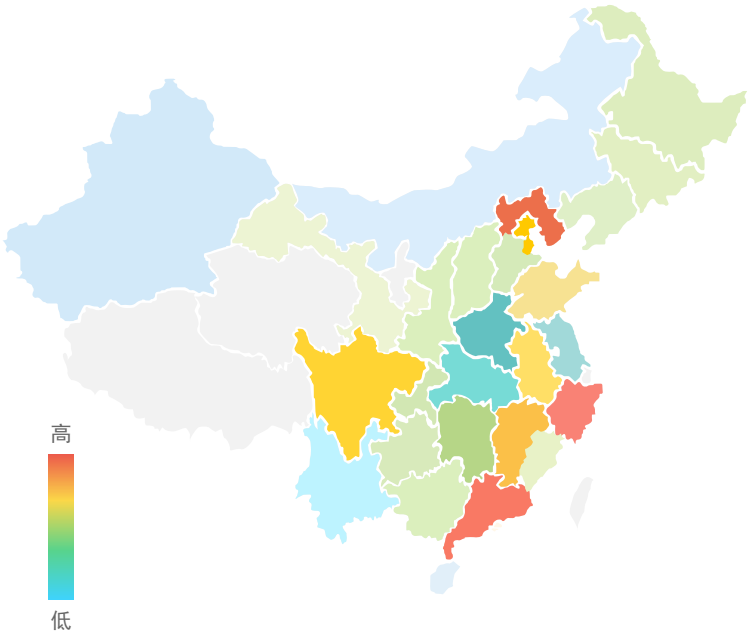
91%

50Gbps以内DDoS攻击
占总攻击比例

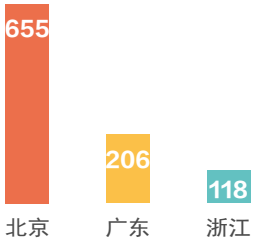
游戏

50Gbps以上DDoS攻击
重点行业

Web应用攻击源IP分布热图



攻击源省份Top3



攻击类型Top3

敏感信息下载　SQL注入　扫描器扫描

目录

网络层DDoS攻击

1.1 DDoS攻击事件概览 3
1.2 DDoS攻击事件的带宽分布 4
1.3 50Gbps以上的DDos攻击事件行业分布 5
1.4 DDos攻击事件持续时长分布 6
1.5 DDos攻击方式 7

Web应用攻击

2.1 Web安全事件概览 11
2.2 Web安全事件类型 13
2.3 Web安全事件持续时长 15
2.4 Web攻击源IP数量地理分布 17
2.5 Web应用攻击HTTP/HTTPS分布 18
2.6 Web应用攻击行业分布 20

网宿科技的网络安全防护

3.1 大规模DDoS攻击防护 21
3.2 Web应用攻击防护 24

CONTENTS

网络层DDoS攻击

1.1 DDoS攻击事件概览

我们对2016年上半年期间检测到的网络层 DDoS 攻击事件进行统计，其中最大规模攻击出现在6月份，带宽峰值为495Gbps。如下图所示，攻击事件数量在2月份有所回落，随后逐步上升，并在6月份达到最高，比同期1月增长108%。上半年带宽峰值呈现较大波动趋势，DDoS事件攻击带宽在3月份及6月份分别达到峰值434Gbps和495Gbps。

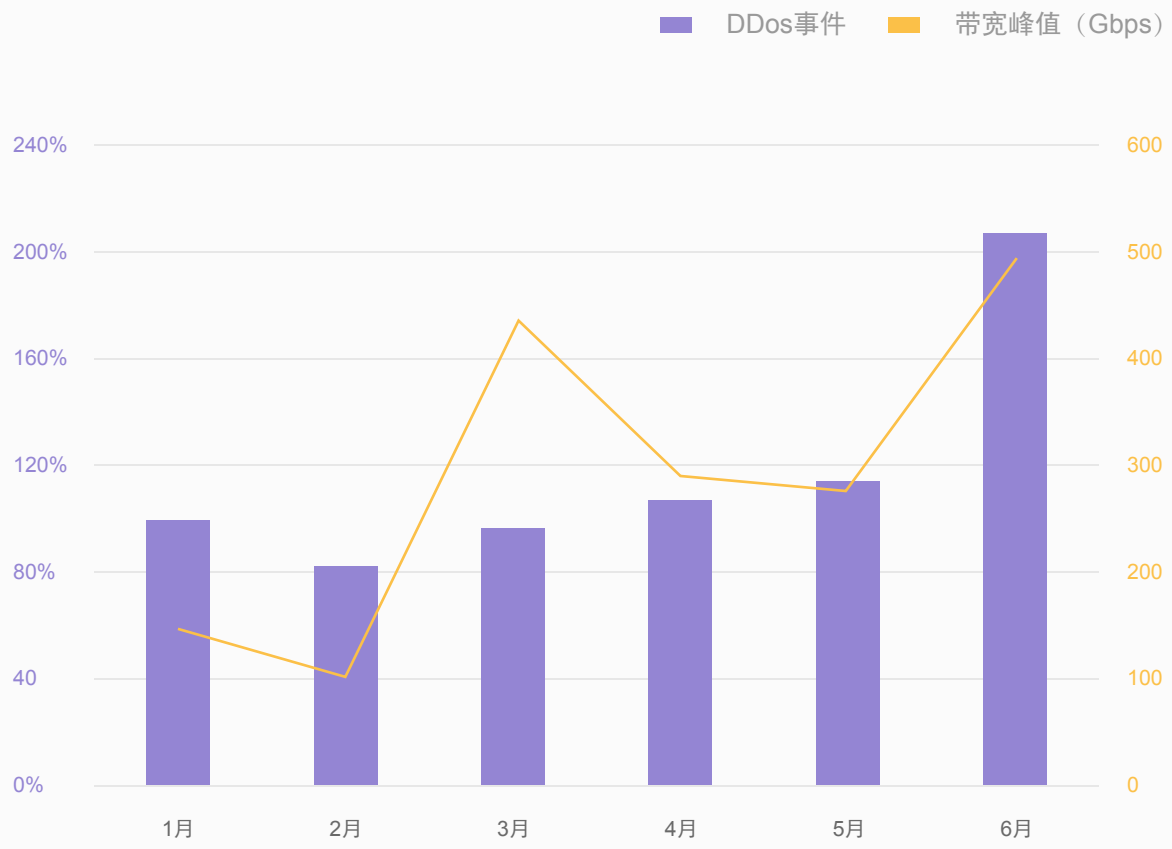


图1：2016上半年DDoS事件及带宽峰值（Gbps）走势图
其中，攻击走势以1月份为基准，其他月份为当月DDoS攻击次数/1月攻击次数

网络层DDoS攻击

1.2 DDoS攻击事件带宽分布

对2016年上半年的网络层DDoS攻击带宽的分布进行分析， 有助于大多数网站了解到自身可能遭受到多大规模的DDoS攻击。DDoS攻击事件带宽分布如下图所示：经统计，多数攻击事件带宽在50Gbps以内， 占整体攻击事件的91%，50Gbps以上的攻击事件带宽主要集中于100-200Gbps之间，占整体攻击事件的4%。

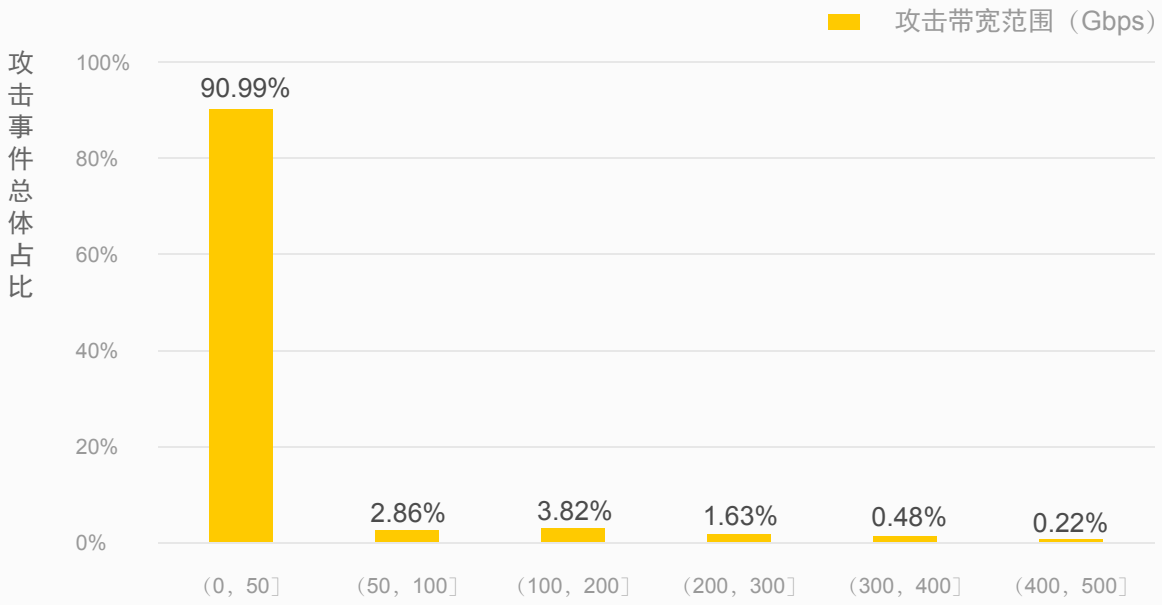


图2：DDoS攻击带宽分布图

对50Gbps以内的攻击事件进一步分析，结果如下图所示，可见其中89%的攻击事件集中于10Gbps以内，占所有攻击事件80.8%。

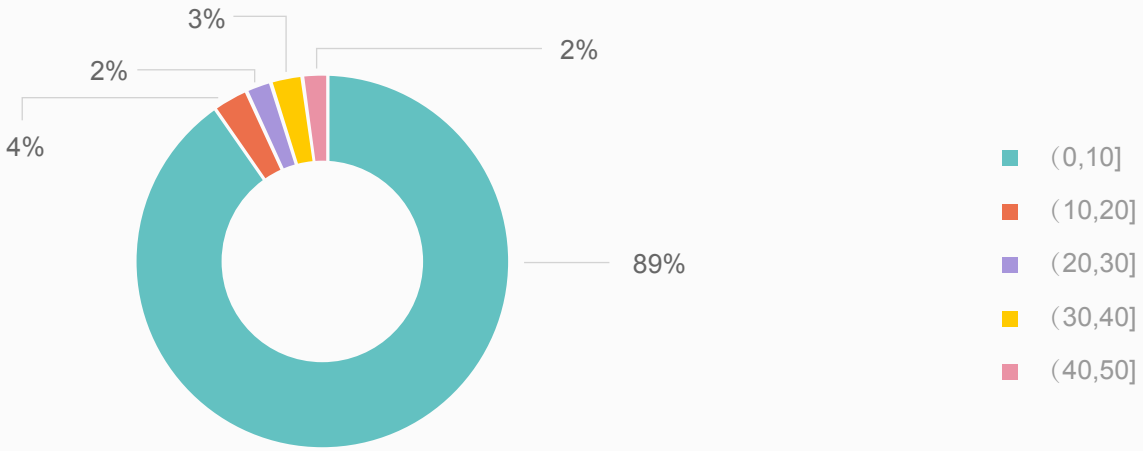


图3：50Gbps以内的DDoS攻击带宽分布比例

网络层DDoS攻击

1.3 50Gbps以上的DDos攻击事件行业分布

50Gbps以上规模的DDoS攻击事件，相对50Gbps以下的攻击更可能对企业业务造成大的影响，同时在应对上也将消耗更多的资源，我们将这部分攻击事件按照游戏、电子信息、金融及其他行业来进行分类，分析结果如下图所示。

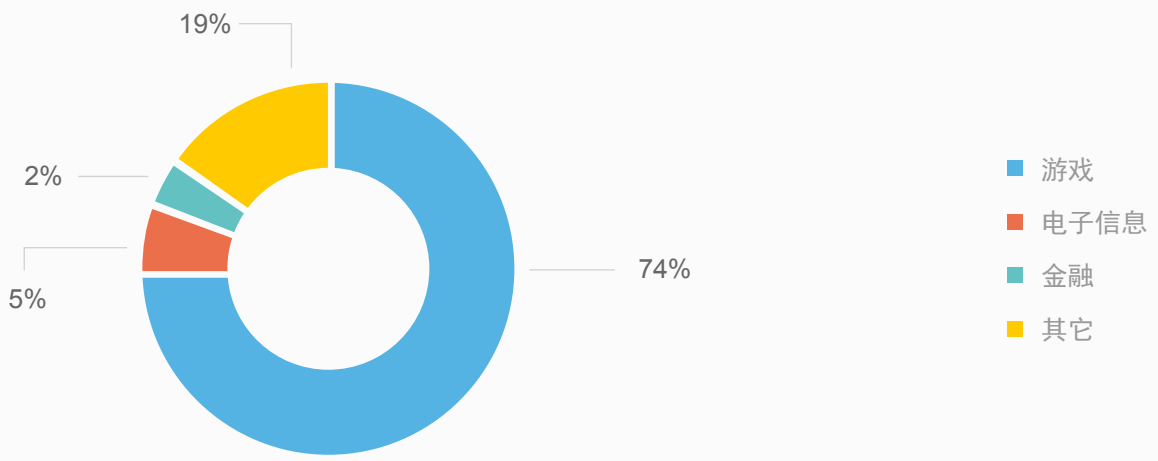


图4：50Gbps以内的DDos攻击事件行业分布情况

可以看到 50Gbps 以上规模的DDoS攻击事件主要针对游戏网站，电子信息与金融行业相对而言占比较小。由于游戏行业具有较强的业内竞争，通过发动DDoS攻击的方式造成竞争对手服务质量下降、 客户流失已经成为了一种常见的恶性竞争手段。 游戏类网站遭受到较大规模DDoS攻击的风险也较其它行业更高。

网络层DDoS攻击

1.4 DDoS攻击事件持续时长分布

对 DDoS 攻击事件的持续时长进行分析，攻击事件整体的平均持续时长为 46 分钟，最长持续时长为342小时。从下图可以看出，DDoS攻击持续时长在各时间段的分布相对均衡，其中22%的攻击事件在1分钟内结束； 61%的攻击事件在30分钟内结束。只有少量攻击会持续2小时以上。

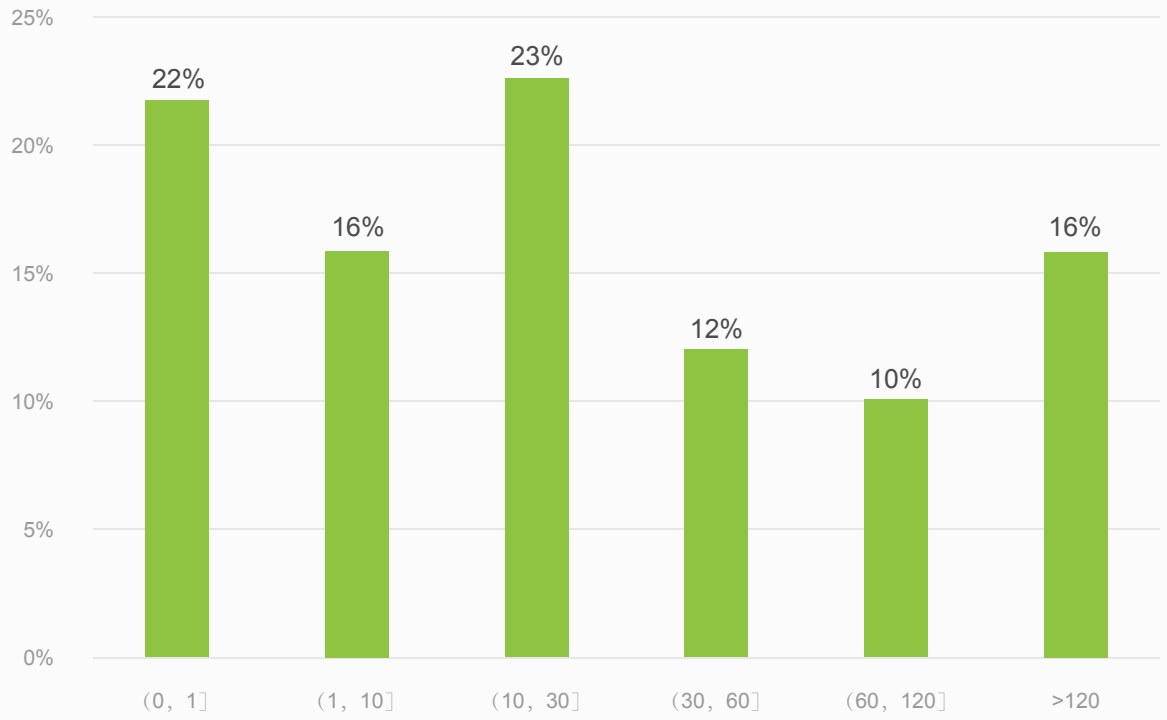


图5：DDoS攻击持续时长分布

网络层DDoS攻击

1.5 DDoS攻击方式

对DDoS攻击流量类型进行分析，其攻击分类见下图。如图所示，每周较大带宽的攻击事件主要为两种攻击模式：一种是以带宽占用为目的SYN Flood攻击，另一种为UDP Flood；ACK Flood与ICMP Flood所占比例较小。多种攻击流量平均分配的情况较为少见。

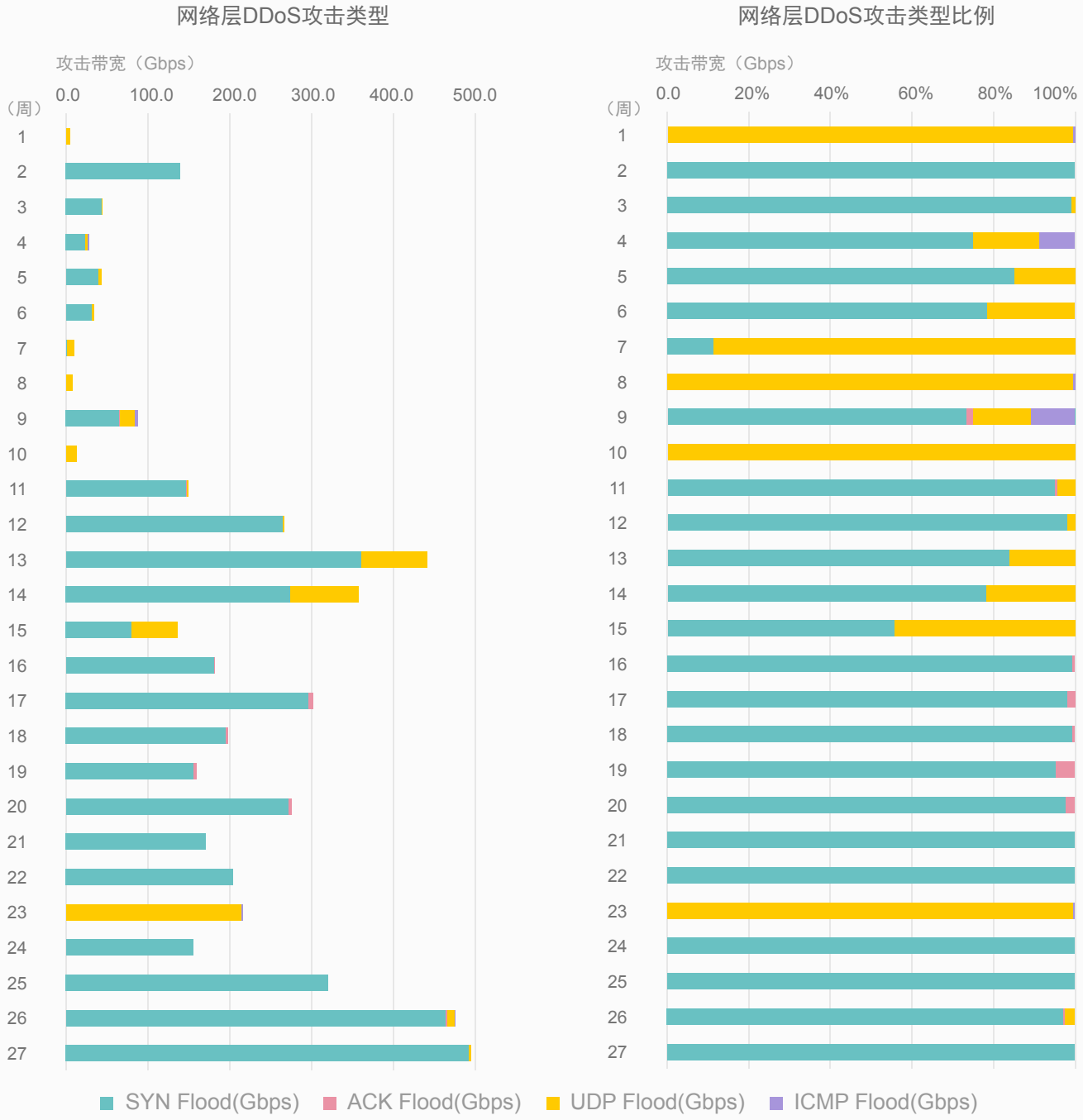


图6：DDos攻击类型带宽分布（Gbps）

网络层DDoS攻击

1.5 DDoS攻击方式

DDoS攻击除开带宽（bps）统计， pps 也是一种衡量攻击强度的指标，表示每秒攻击的报文数量。bps攻击指标考量的是带宽消耗，而pps的攻击指标考量的则是计算资源的消耗。单位时间内需要处理的报文数量越多对网络设备及防护系统的处理性能要求越高。 因此每秒大量的攻击报文可以对网络设备及防护系统造成严重的性能冲击， 影响正常的网络通讯及防护过程。

2016上半年的 DDoS 攻击事件中最大pps值可达到231Mpps，占用带宽 302Gbps，其中SYN Flood攻击占224.73Mpps，ACK Flood占6.39Mpps。

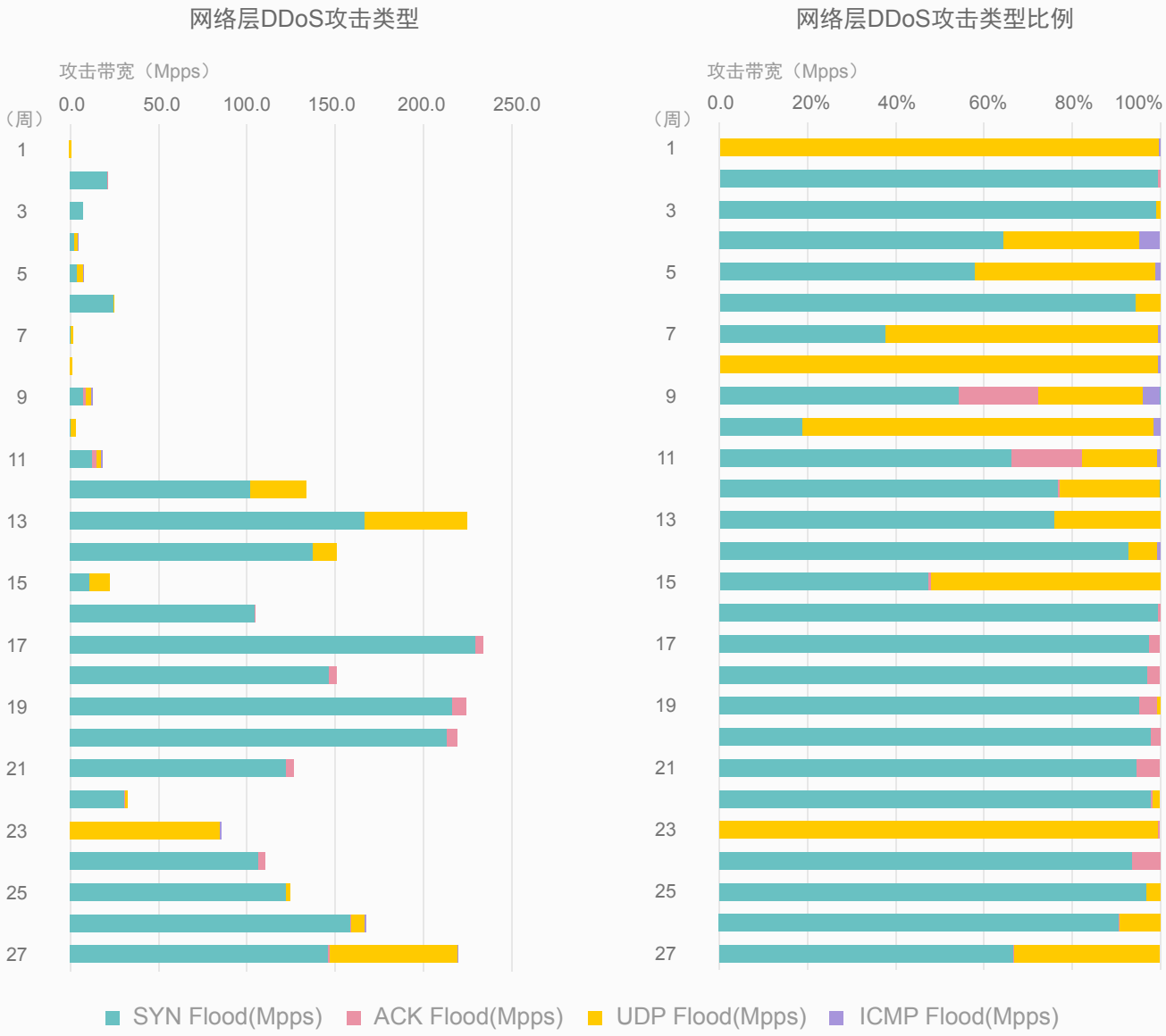


图7：DDos攻击类型带宽分布（Mpps）

网络层DDoS攻击

1.5 DDoS攻击方式

下图是对SYN Flood攻击数据的分析结果，可看到SYN Flood攻击的平均报文长度主要分布在(64-128]、(512-1024]两个区间，分别占比30%与35%。较小报文长度主要集中在100字节左右，较大报文长度主要集中在900字节左右。

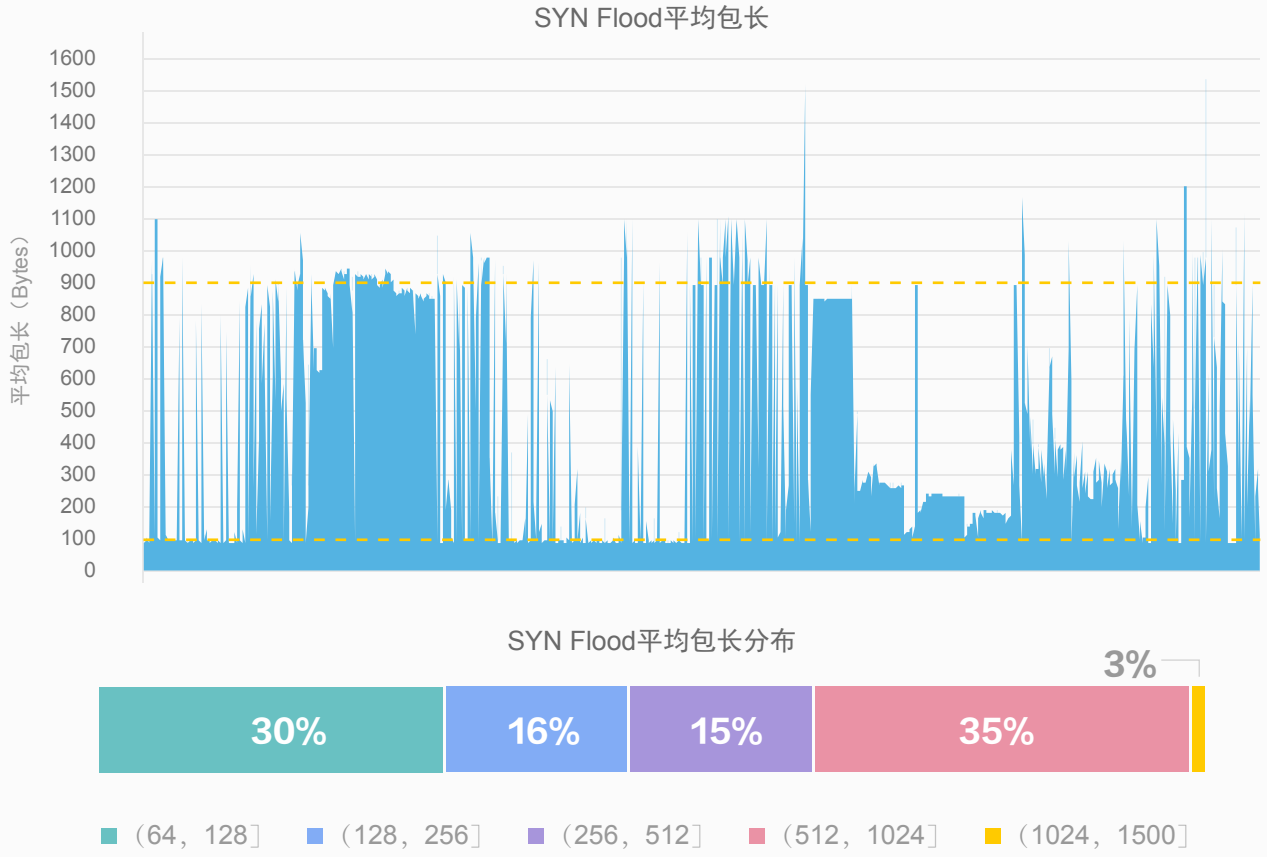


图8：SYN Flood平均报文长度分布情况

一般正常SYN包的报文长度在128字节以内居多，2016上半年的SYN Flood攻击统计中异常大小的SYN包（报文长度大于128字节）占到70%，表明多数的SYN Flood攻击中攻击者无意模仿正常的SYN包传输躲避检测， 完全以攻占带宽为目的构造大SYN包， 与攻击目标站点在带宽资源上进行较量。

网络层DDoS攻击

1.5 DDoS攻击方式

对 SYN Flood 攻击报文的采样进行分析，报文特征如下图所示，SYN数据包被添加的了大量的数据负载，长度达到800字节以上，此类攻击特征较为明显，可作为清洗过滤条件。

Time	Source	Destination	Protocol	Length	Info
0.000000	102.14.25.149	21[redacted]30	TCP	950	55723 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	13.33.152.144	21[redacted]30	TCP	950	54314 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	119.249.42.82	21[redacted]30	TCP	950	38588 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	62.186.161.181	21[redacted]30	TCP	950	63795 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	75.27.133.127	21[redacted]30	TCP	950	49943 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	96.118.190.79	21[redacted]30	TCP	950	37712 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	40.130.56.157	21[redacted]30	TCP	950	57802 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	33.18.108.254	21[redacted]30	TCP	950	17151 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	6.174.206.44	21[redacted]30	TCP	950	28768 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	71.202.138.227	21[redacted]30	TCP	950	10013 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	58.170.11.72	21[redacted]30	TCP	950	35997 → 80 [SYN] Seq=0 Win=65535 Len=896
0.000000	36.12.230.118	21[redacted]30	TCP	950	47736 → 80 [SYN] Seq=0 Win=65535 Len=896

图9：SYN Flood攻击报文采样案例

对UDP Flood的平均报文长度与平均报文长度分布情况进行分析，结果如下图所示。UDP Flood攻击中54%的攻击事件平均报文长度在1024字节以上，符合使用大包占用带宽的UDP Flood攻击方式， 推测此范围的攻击主要由僵尸主机直接构造数据包发起， 其它小于1024字节的攻击主要为反射型攻击，受反射服务的业务内容限制，无法响应过大的数据报文。

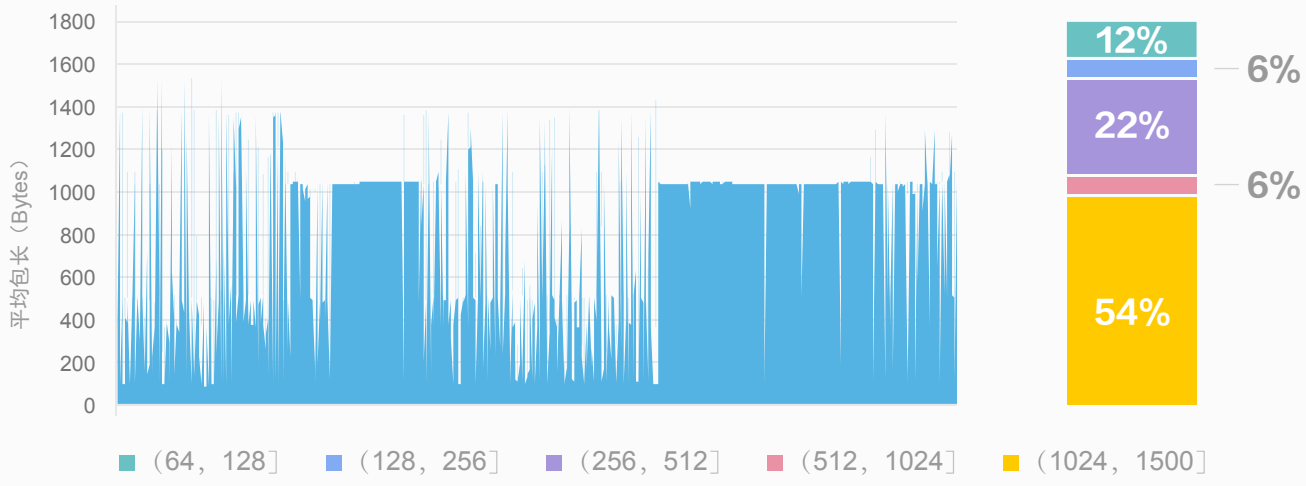


图10：UDP Flood平均报文长度分布情况

Web应用攻击

2.1 Web安全事件概览

我们按照节点对Web攻击告警数据进行采样，以告警时间间隔30分钟以内为一次安全事件，超过30分钟为新的一次安全事件为基准， 共采样Web应用攻击安全事件763次，安全事件次数按时间分布情况如下图所示。

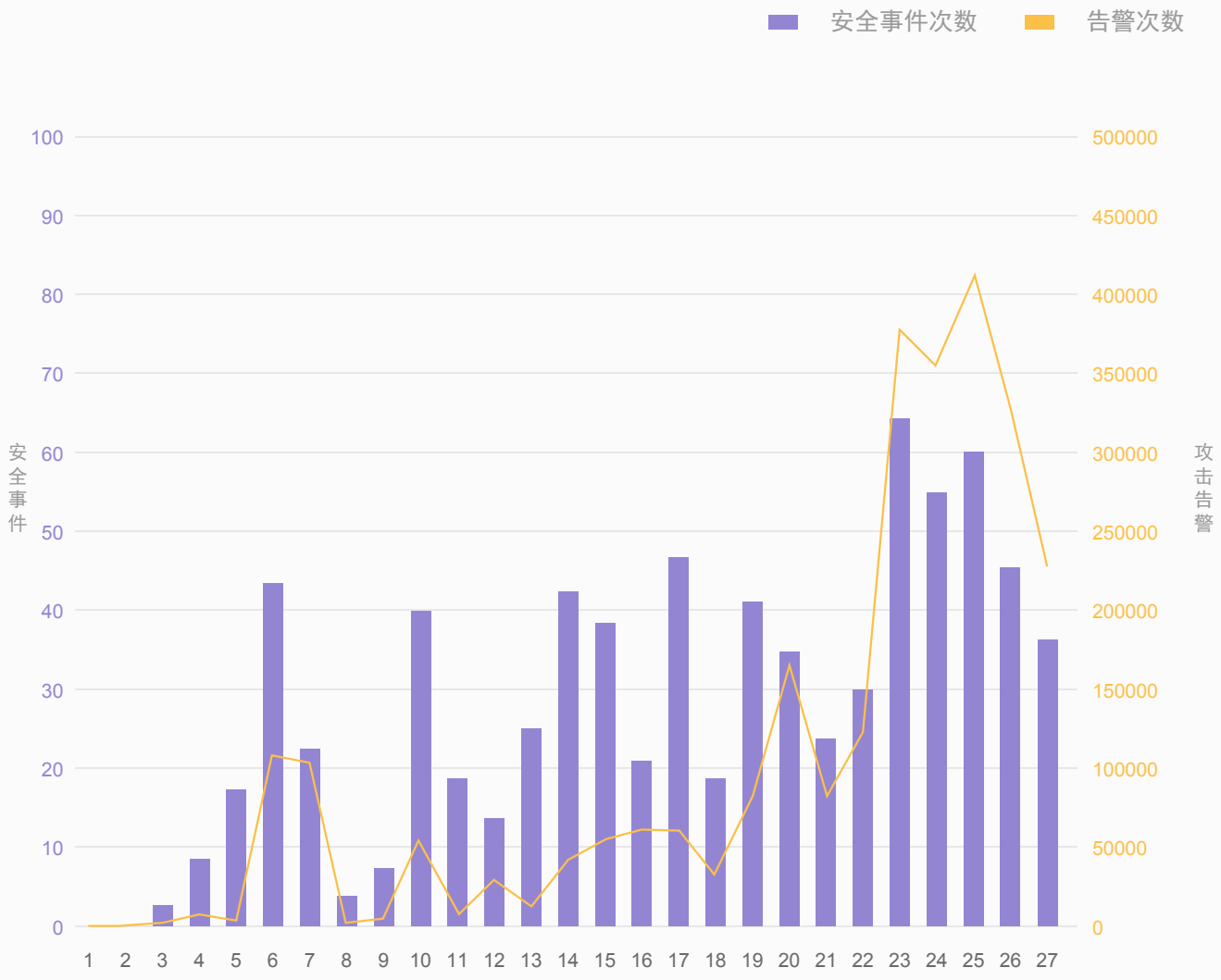


图11：Web应用安全事件及攻击警告周走势图

Web应用攻击

2.1 Web安全事件概览

从年初开始每周的安全事件数量均有一定波动，但整体呈现增长的趋势。 对告警次数进行分析，其时间分布如图11所示，可以看出攻击警告与实际安全事件无明显相关性。其中，攻击警告最高出现在第25周，监测到414072次，对应的安全事件次数为46起。安全事件次数最高出现在第23周，为64起，对应的攻击警告次数为371949。

在第19周以前，每周普遍呈现较多安全事件但告警数量较少的情况，经分析这期间的多数安全事件都只产生了少量的告警，攻击行为以小范围的漏洞探测行为居多。自20周开始呈现安全事件数量与告警数量均同步增长的情况，平均每个事件产生的告警数量达到5664个，最大达到7228个，显示此段时间出现了一定成规模的攻击扫描事件，外部威胁呈现上升趋势。单次安全事件平均告警数量如下图所示。

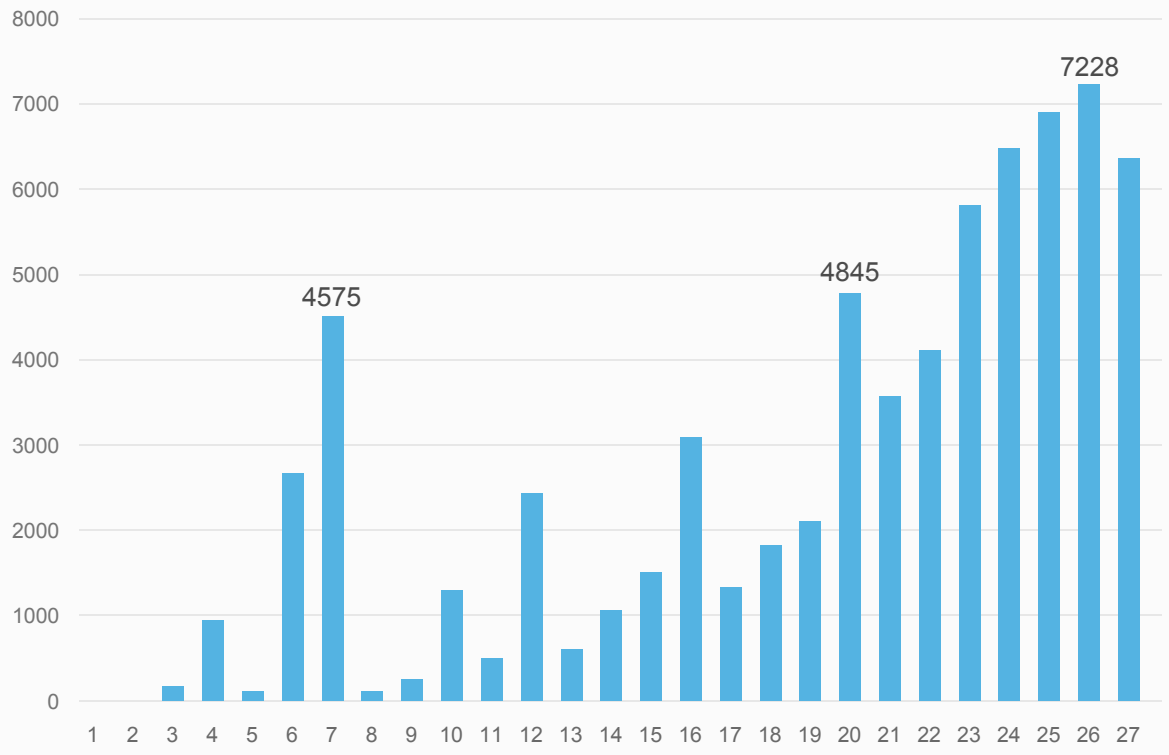


图12：单次安全事件平均告警数分布

Web应用攻击

2.2 Web安全事件类型

对安全事件进行分类，占据前三位分别为敏感信息下载、 SQL注入与扫描器扫描，总共占据所有攻击类型的91%。Web安全事件告警类型分布如下图所示：

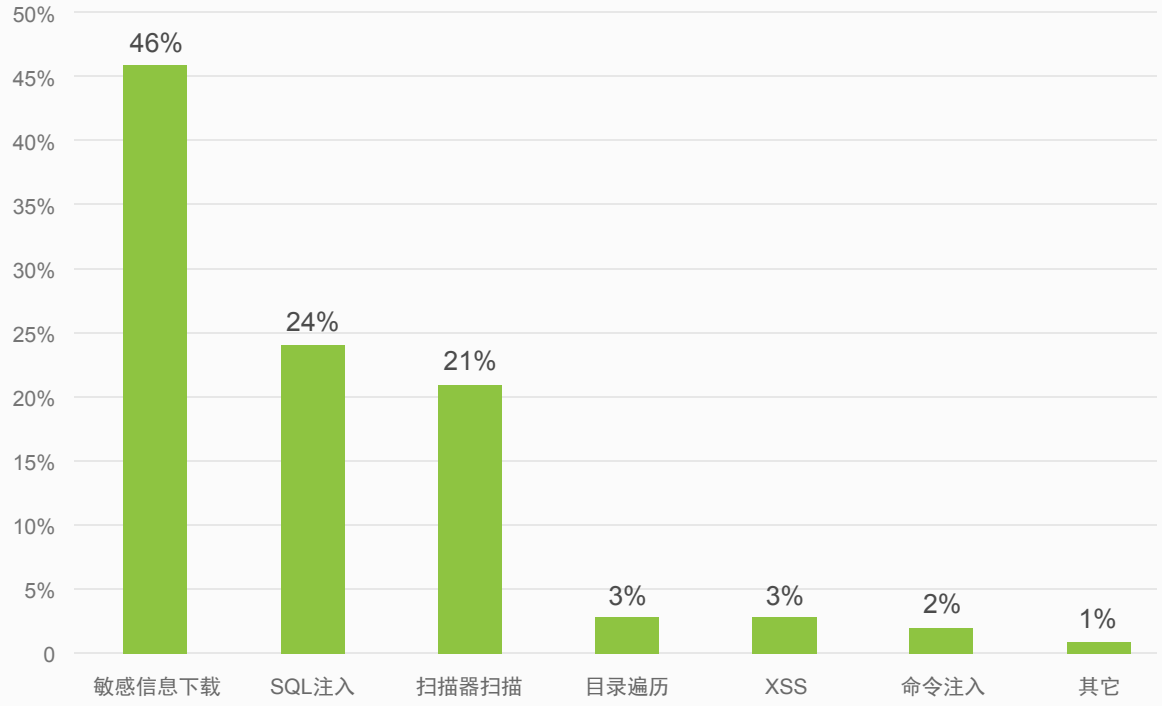


图13：Web应用安全事件攻击告警类型分布

其中敏感信息下载主要表现为针对一些可能泄露站点重要信息的数据、 文件来推测其是否存在并企图下载的行为，攻击者探测的此类数据、文件一般包含以下信息：

- 系统帐号口令文件
- 服务/应用配置文件
- 数据库文件
- 站点/数据库备份文件
- 存在已知漏洞的软件/应用
- 常用后台路径
- 常见后门文件路径等

如果上述文件可以下载，那么攻击者可以获得更多的站点关键信息，可通过离线的暴力破解、文件内容分析、代码审计等方式，进一步获得相关服务器、应用相关的数据类型如下文：

Web应用攻击

2.2 Web安全事件类型

- 主机帐号密码
- 配置错误导致的漏洞
- 内部服务器拓扑结构或信息
- 业务数据（交易记录、帐号信息、用户个人信息等）
- 数据库、其它主机内部IP、帐号、密码等信息
- 后门程序路径等信息

此类敏感信息下载攻击的特点是攻击方在一段时间内往往使用相同的探测数据进行测试，主要探测的内容并不会因站点所使用的架构、中间件、编程语言不同而呈现出差异，如针对一个由Java编写的站点仍会探测是否存在asp、php的后门程序；而不同的攻击方所使用的探测数据会呈现一定的差异。

Web应用攻击告警类型按周分布的情况如下图所示，多数的攻击以敏感信息下载与扫描器扫描为主，辅以 SQL 注入攻击，在20周后非法下载与扫描器扫描的占比及告警数量有明显增加。

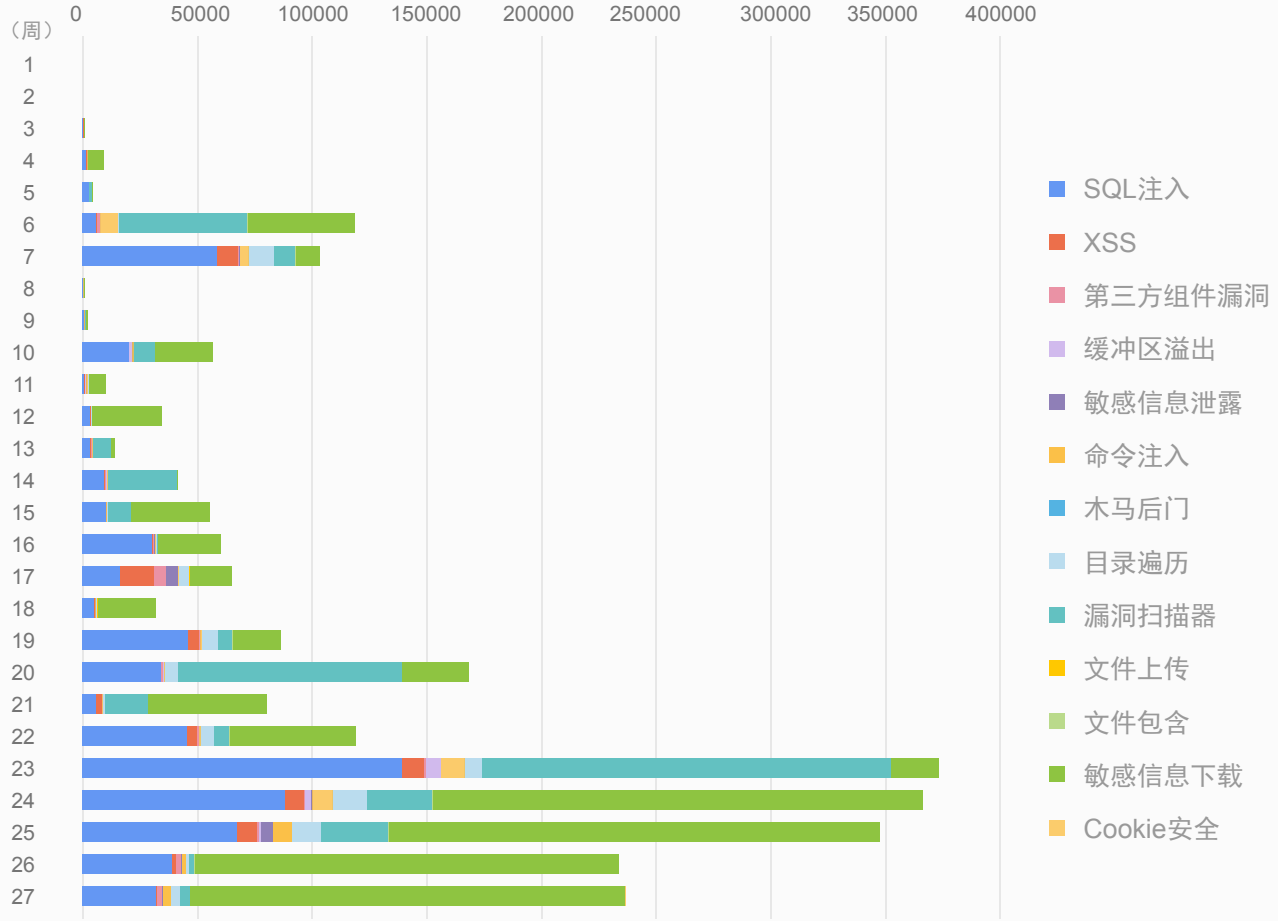


图14：Web应用攻击告警类型按周分布图

Web应用攻击

2.3 Web安全事件持续时长

本章节对于持续时长的分布范围采用区间的方式，单位为分钟，如(1,10]表示大于1分钟、小于等于10分钟的时长。 对所有安全事件的持续时长进行分析，结果如下图所示。可以看到持续时长在（1,10]之间的事件数量占总体的37%，其次为（10,30]之间，占比23%。占比84%的安全事件持续时长均在2小时以内，另外有16%的安全事件持续时长超过2小时。

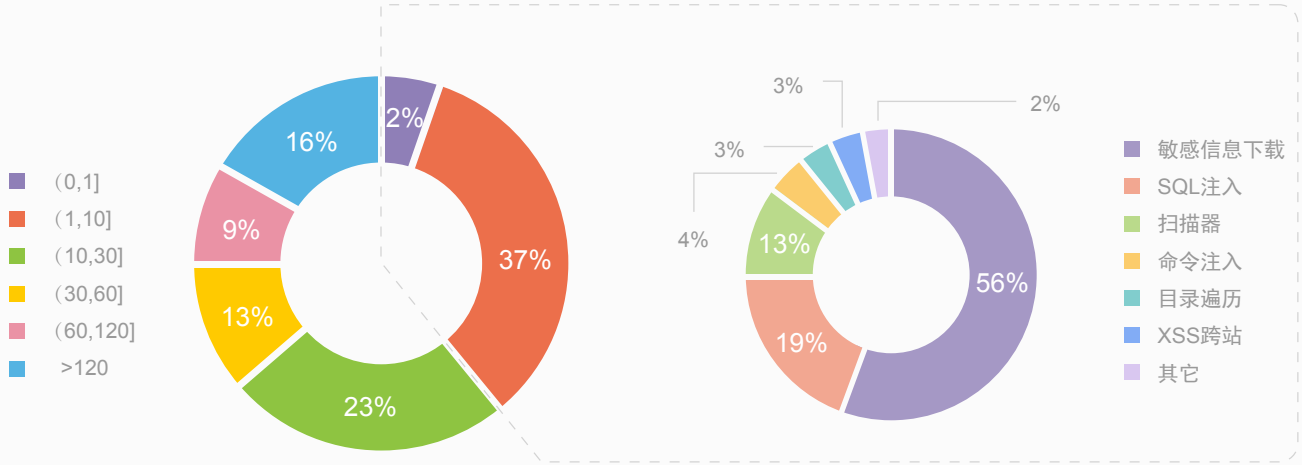


图15：攻击持续时长分布及10分钟内的安全事件告警分布

针对10分钟以内的攻击事件告警类型进行统计，发现告警事件主要由敏感信息下载、SQL注入与扫描器的扫描攻击等触发，占比分别为56%、19%与13%。

下图为安全事件持续时长的分布情况，可以看到间歇性地存在超长持续时长的攻击事件，持续时长在1至5天不等。

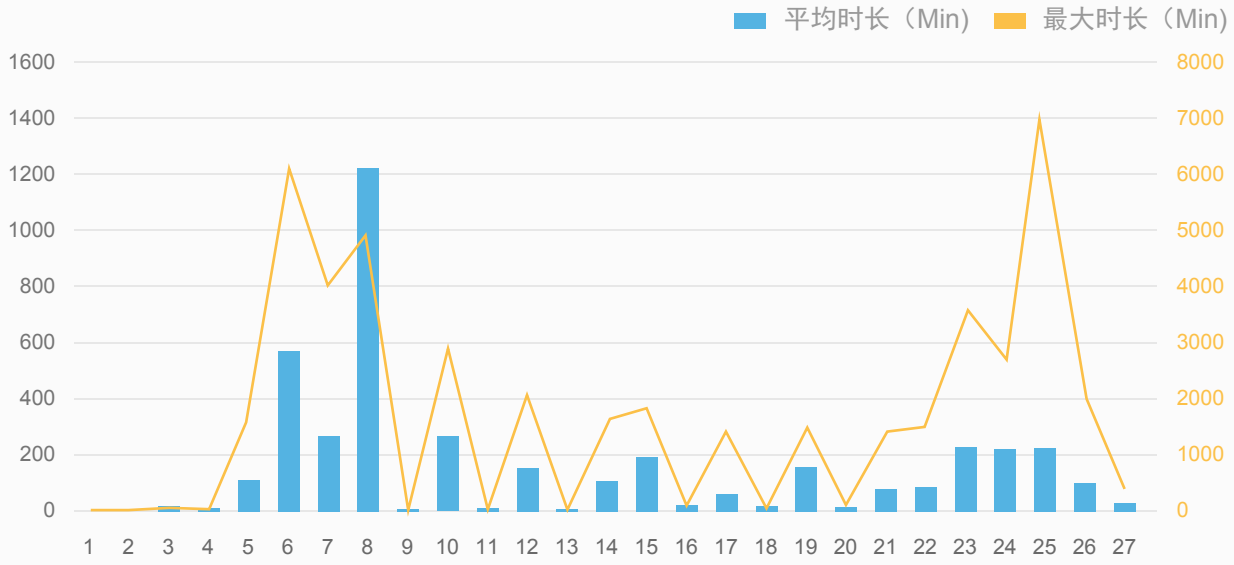


图16：Web应用安全事件持续时长

Web应用攻击

2.3 Web安全事件持续时长

对不同行业的安全事件持续时长进行统计分析，结果如下图所示。 在各个行业中持续时长1至10分钟的安全事件占绝大多数，说明对于多数行业短时间的漏洞探测与攻击尝试都是普遍存在的；而其中持续时间较长的安全事件主要集中在政府类网站。

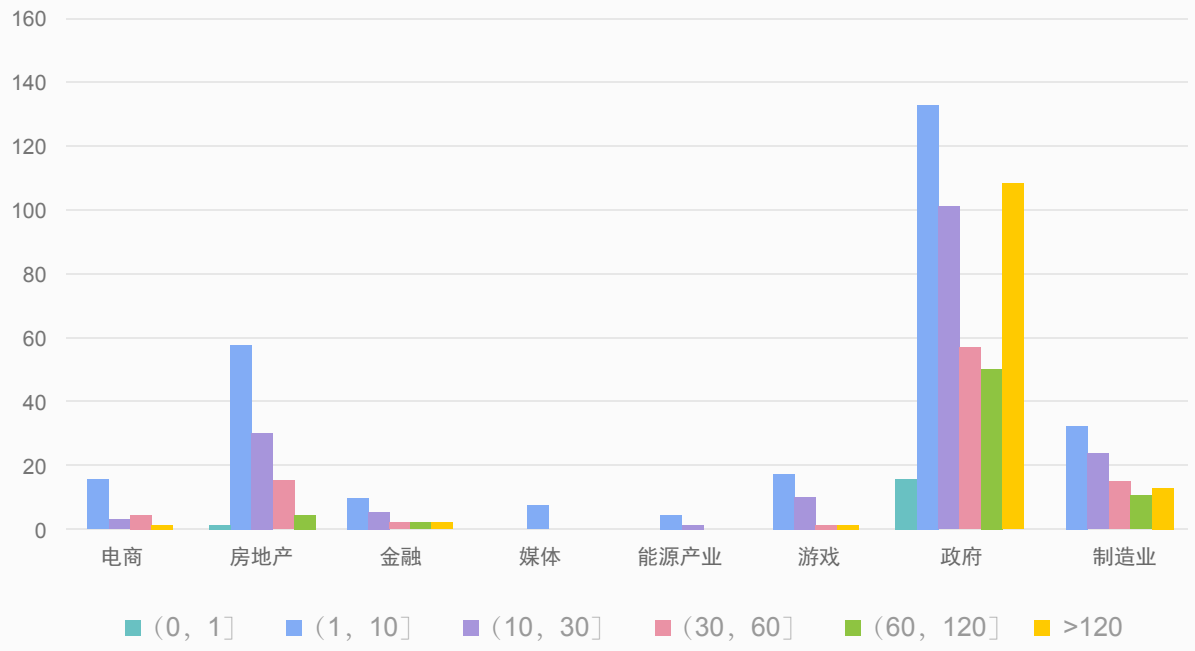


图17：Web应用安全事件持续时长按行业分布

Web应用攻击

2.4 Web攻击源IP数量地理分布

对Web攻击源IP进行划分， 发现主要攻击源IP来自于国内， 少量来自于美国、法国等国家。对国内的攻击源IP按省份进行划分， 前十位分别为北京、广东、浙江、江西、天津、四川、江苏、山东、河南、湖北。其中北京占据了国内43%的攻击IP数。

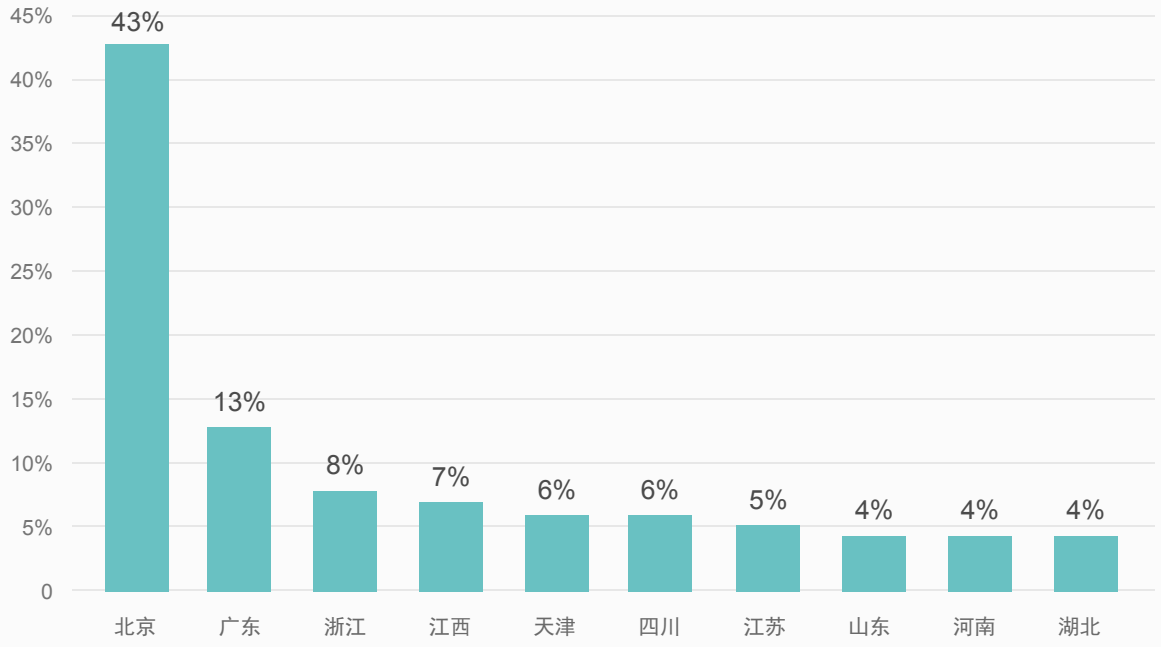


图18：Web攻击源IP的地理分布比例

Web应用攻击

2.5 Web应用攻击HTTP/HTTPS分布

HTTP与HTTPS站点的取样比例如下图所示，有79%的站点为HTTP站点，针对HTTP站点的攻击占绝大多数，此比例在一定程度上也反映了当前网站中HTTP与HTTPS站点的比例。网站上的多数内容展示、信息发布类的内容仍然使用HTTP协议进行传输，仅重要/敏感业务，如登录认证、管理、交易类的业务使用HTTPS传输。HTTP与HTTPS站点安全事件中，85%的攻击事件均是针对HTTP站点发起，绝大多数的告警均来自于HTTP站点，占比97%。

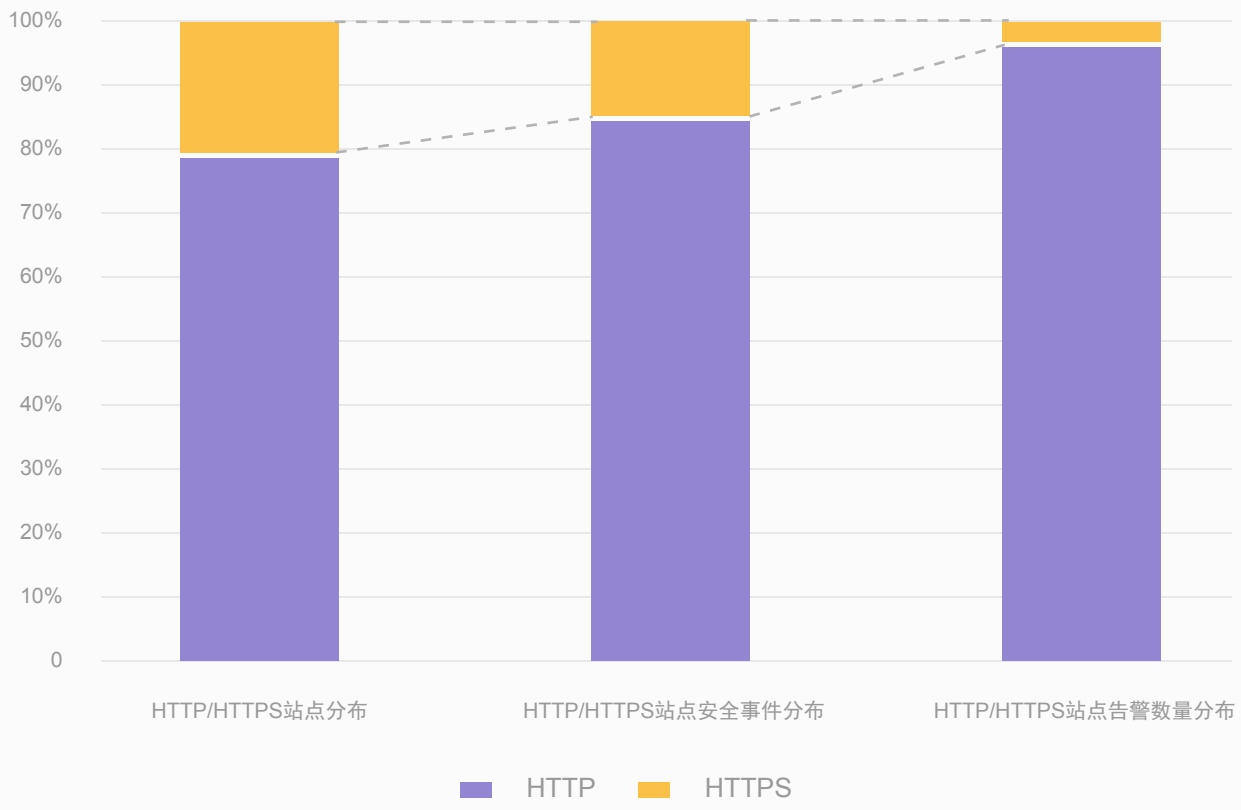


图19：HTTP/HTTPS站点分布、各自检测到的安全事件分布、告警数量分布情况

尽管HTTPS站点往往承载了更高价值的业务内容，但无论是攻击事件的分布还是告警数量的分布都趋向于以HTTP站点为主， 从攻击数据上来看HTTPS站点并没有因此被攻击者格外关注。

Web应用攻击

2.5 Web应用攻击HTTP/HTTPS分布

HTTPS站点告警类型分布相较于整体告警情况的变化情况如下图所示：

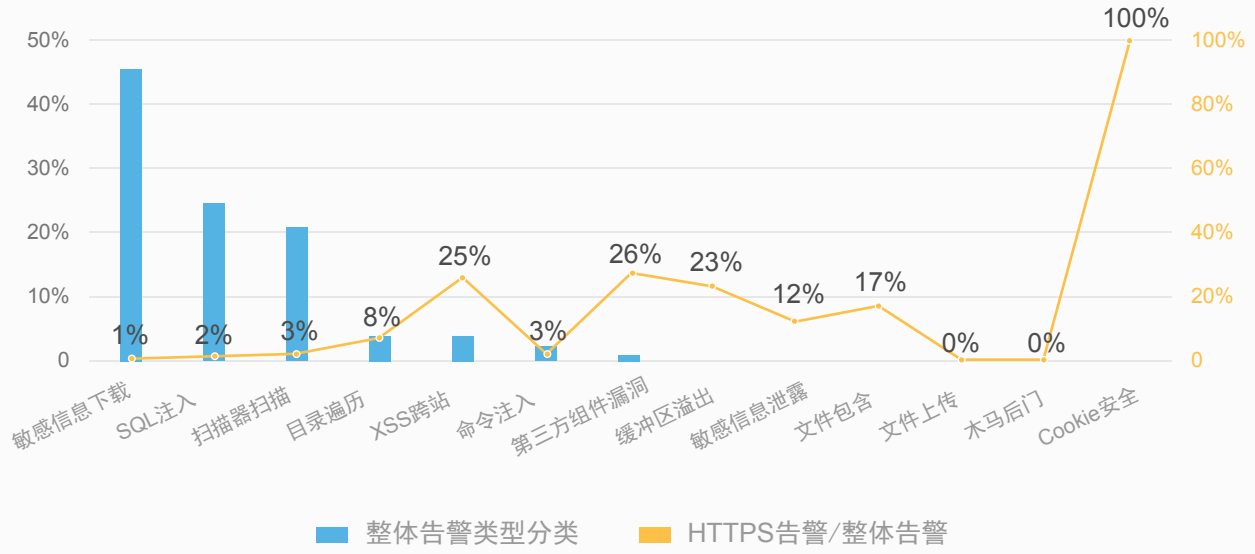


图20：HTTPS站点告警分布倾向

在整体告警数量中排名前三的告警类型依次为： 敏感信息下载、SQL注入与扫描器扫描告警，合计占总比的91%，三种类型的告警中分别仅有1%、2%及3%来自于HTTPS站点，远小于HTTPS站点的比例，这是由于这种攻击手段上特殊的倾向性导致HTTPS站点的告警数量在整体告警中占比较小，推测这种攻击手段上的倾向性可能由以下原因导致：

1）攻击者刻意避开对HTTPS站点的攻击

HTTPS站点作为重要业务的承载平台往往也有着更为严密的监控防护措施，因此，对此类系统发起的攻击成功率相对较低且有着更高的法律风险，以抓取傀儡机为目的的扫描攻击行为可能会刻意避免对此类系统的检测与攻击。

2）自动化工具无法有效地对需要登录认证的站点进行检测

HTTPS站点由于其业务的重要性，多数页面都需要在登录认证及图片验证码验证后才可以访问，对于无法通过登录认证及图片验证码验证的自动化工具无法完整地探测HTTPS站点的漏洞，由此产生的告警数量也会大幅减少。

Web应用攻击

2.6 Web应用攻击行业分布

对抽样样本进行分类，可以看出政府、制造业与房地产类的站点受到攻击的频率较高、规模较大，是黑客重点关注的对象。

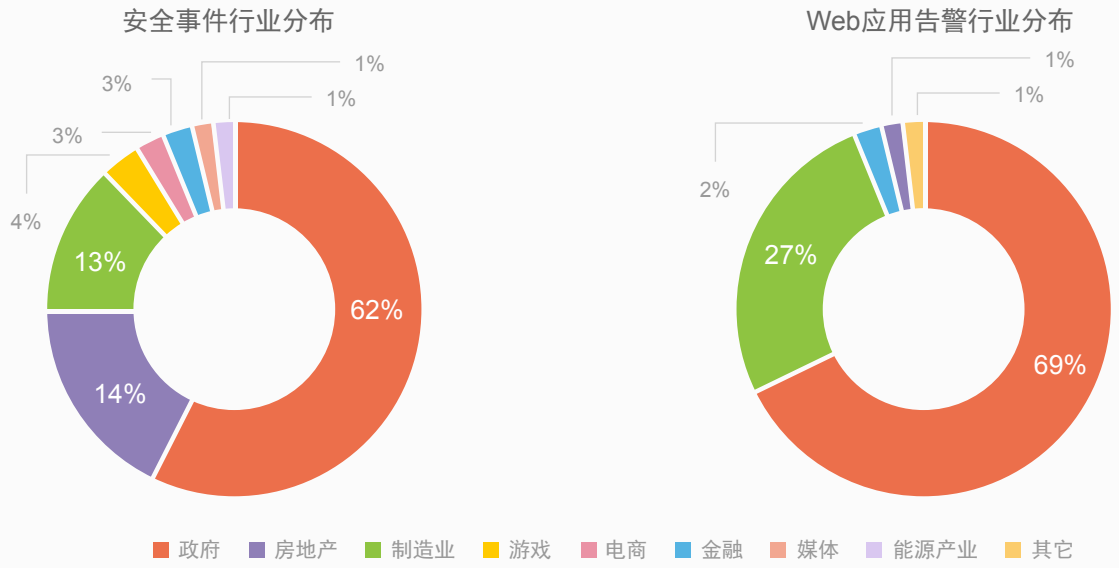


图21：安全事件及告警次数按照行业进行分布

其中针对政府网站的攻击时长呈现两个极端的趋势，短时间攻击与长时间攻击均占据较大比例；其中10分钟以内的攻击事件攻击类型如下图所示：

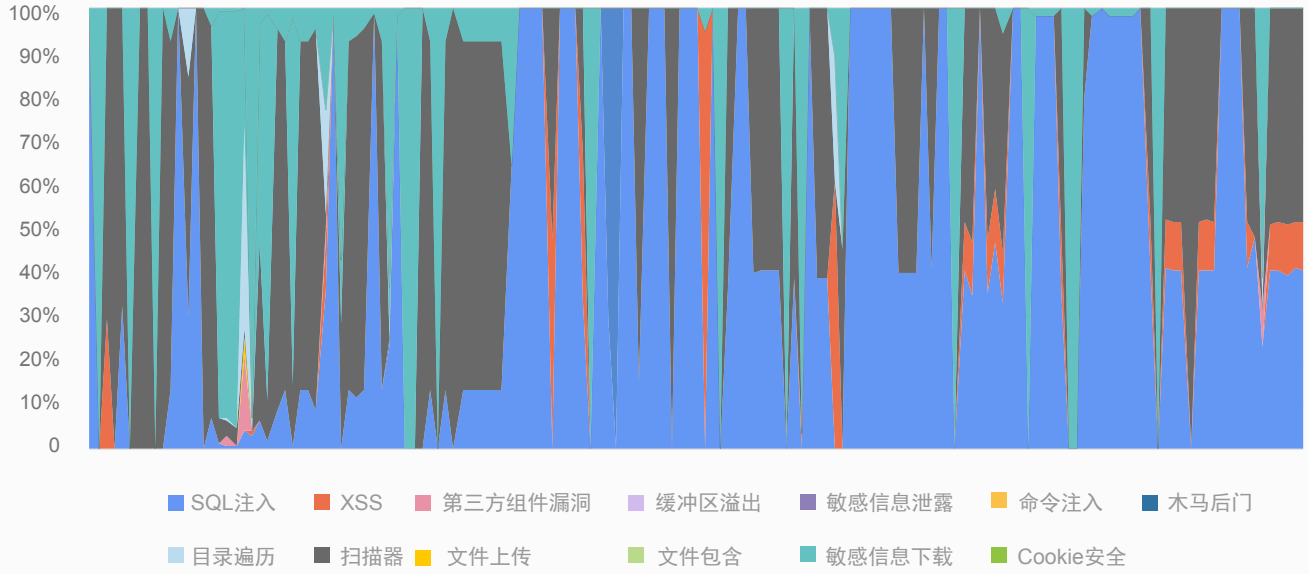


图22：10分钟以内的政府网站安全事件攻击类型组成分布图

Web应用攻击

2.6 Web应用攻击行业分布

攻击类型主要为SQL注入与命令注入为主， 短时间（<=10min）的此类攻击体现出较为直接的攻击性与较强的危害性。

较长时间（>120分钟）的持续攻击事件的攻击类型组成如下图所示，主要以扫描器扫描、SQL注入与敏感信息下载为主，表现为对网站发起频繁大量的漏洞扫描一类的行为，表现出耐心、持续的网站漏洞探测倾向。

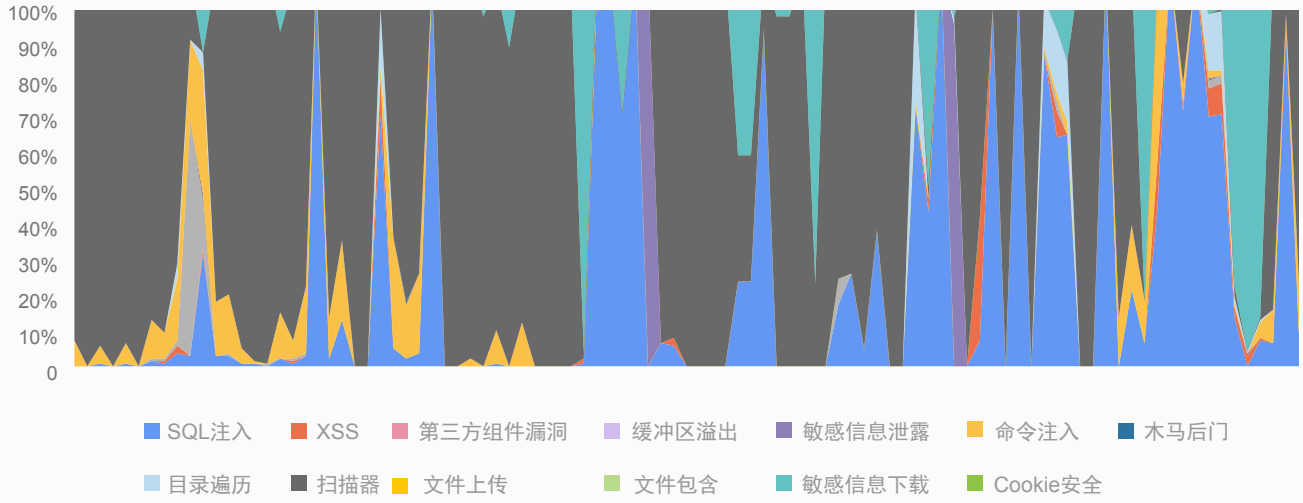


图23：120分钟以上的政府网站持续安全事件攻击类型组成图

政府类网站中有较多的小型地市、下属单位网站，整体上的安全性相对较低，容易成为攻击者的入侵目标，以便用于傀儡机、跳板或挂暗链广告等用途。

网宿科技的网络安全防护

对于上述统计到的攻击事件， 网宿科技可通过在 CDN 基础上建设的安全系统对 SYN Flood、ACK Flood、UDP Flood等 DDoS 攻击以及SQL注入、XSS、命令注入、会话劫持等Web应用层攻击进行有效的检测与防护。 在进行的安全防护中，网宿科技已经为网站规避了最高持续342小时因DDoS攻击导致的服务不可用时间，相当于一个月内将可能因攻击导致的46.7%的可用性提升到99.9%以上，大幅减少了网站可能因此造成的损失。

3.1 大规模DDoS攻击方式

2016年上半年的DDoS攻击带宽整体呈现上升趋势，其中6月份在网宿科技平台上监测到针对某游戏站点产生了峰值最大为495Gbps的DDoS攻击，并成功进行了防护。整个攻击过程自6月24日（周五）凌晨开始，总共持续了五天，攻击早期的平均攻击带宽在250Gbps上下浮动。

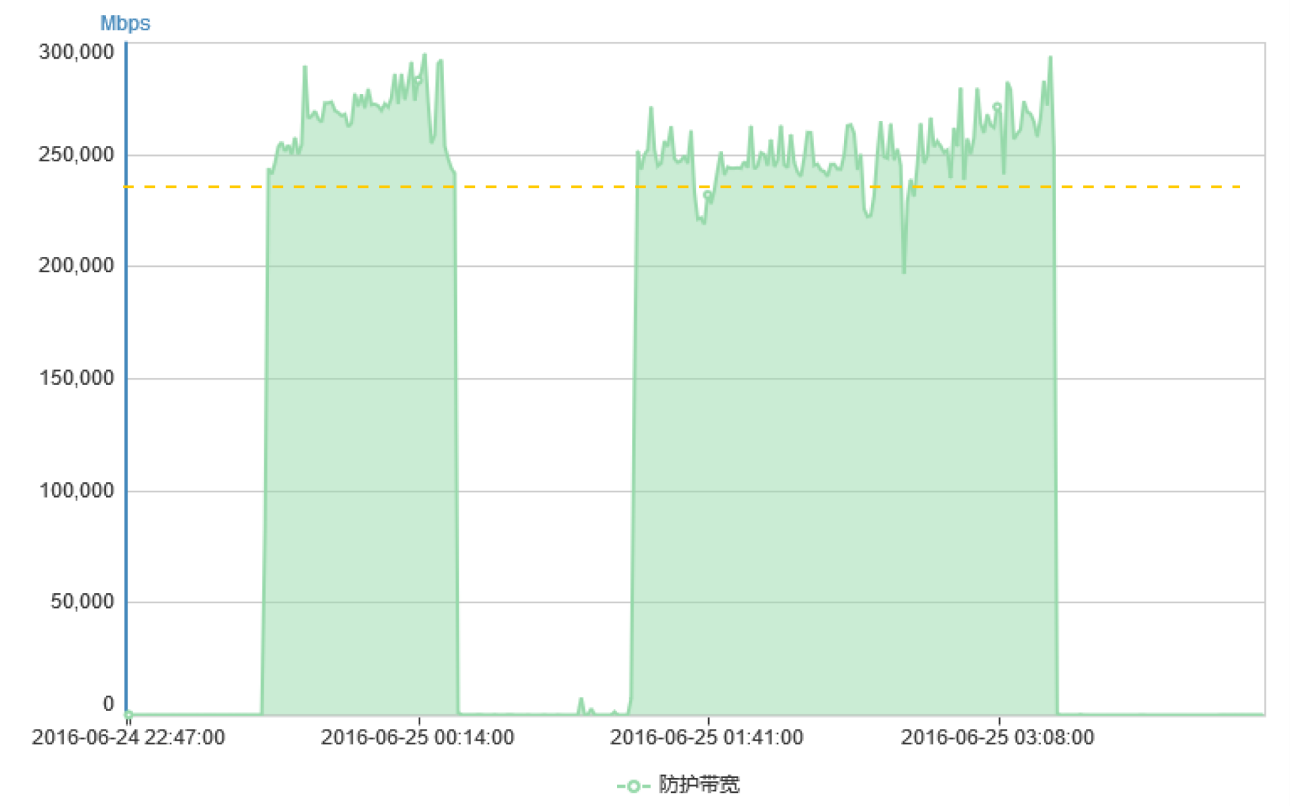


图24：6月24-25日DDoS攻击走势分布图

网宿科技的网络安全防护

3.1 大规模DDoS攻击方式

约250Gbps的带宽攻击断断续续地持续到24日中午，随后攻击方式产生了变化，攻击带宽暂时下降到了100G并持续维持在这个水平。在25日凌晨时安全平台监控到攻击量突然增加了一倍，攻击方式变化为以真实客户端 IP 模拟正常用户访问进行攻击，与此同时，安全平台上监控到了大量的攻击 IP 在交替地发起攻击，安全系统的自动防护机制启动并成功进行了防护，最终，攻击方未能对网站正常访问造成影响。

自25日中午12:38 伊始，监测到的攻击方式再次发生变化，攻击带宽瞬间飙升至421Gbps随后攻击带宽开始上下浮动，最终在28日下午达到495Gbps的上半年攻击带宽峰值。

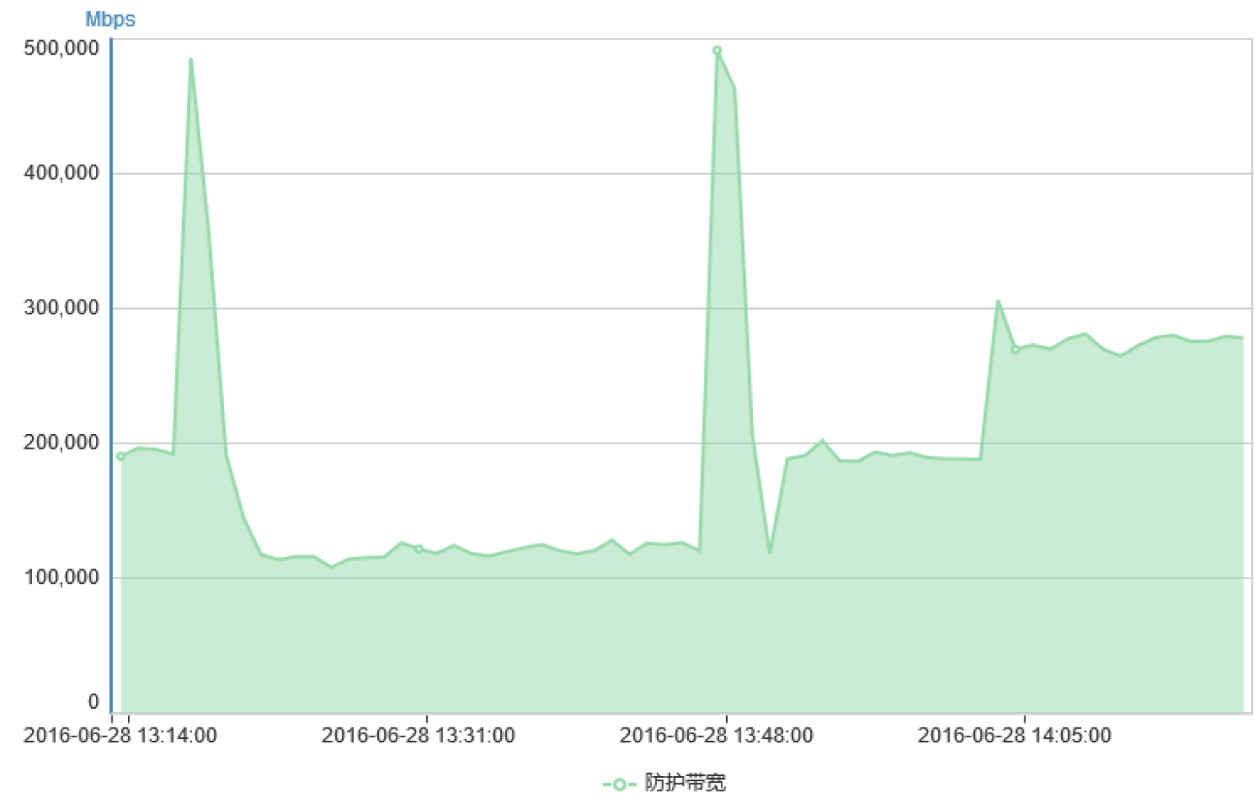


图25：2016年6月28日DDoS攻击走势分布图

网宿科技的网络安全防护

3.1 大规模DDoS攻击方式

此次攻击中，多轮大规模的攻击均被网宿科技的安全系统的防护及调度机制化解， 在整个攻击期间，客户网站始终维持正常访问，丝毫未受到攻击影响。

通过对攻击类型进行分析，此次DDoS攻击达到峰值时攻击流量以SYN大包为主，同时混合有ACK Flood、UDP Flood、ICMP Flood等多种类型的混合DDoS攻击。

众所周知， 游戏官网由于为游戏提供开服宣传、服务器信息获取、客户端下载、账号充值等核心服务，往往备受黑客青睐。黑客的目标明确：只有严重阻碍此类站点的正常使用，才能最大程度形成游戏用户的流失，最终造成游戏公司名誉和经济的双重损失。 正因如此，拒绝服务攻击防护成为了各大游戏站点的刚需。

由于在线游戏对延时的敏感度高，DDoS攻击干扰效果相对明显，并且随着发起DDoS攻击的技术门槛降低，游戏行业沦为了大规模DDoS攻击的优先目标。

从整体报告看来，网络攻击将会沿着资源消耗更大以及攻击手段更丰富的方向进行演变。随着互联网规模的继续扩增， 从2016上半年的流量攻击带宽增长趋势来看，往后平均每年的最大攻击带宽将以100Gbps为单位逐年上升。 攻击规模在一定程度上与运营商骨干、省出口带宽资源有一定关联性。 过大的攻击带宽可能导致运营商局部地区的网络服务质量下降，形成高级别的网络安全事件，从而引起公安、 政府部门的高度关注， 最终造成攻击发起者所面临的各种风险将大幅增加。由此预见，基于经济利益（竞争、勒索等）因素发起的DDoS攻击规模不会过快的增长。

报告中2月份的DDoS攻击事件及攻击带宽均有下降趋势，可能与下列因素有一定关系：

1）春节假期中，办公主机、非重要系统长时间关机，被感染的傀儡机无法参与到DDoS攻击中；

2）春节假期中多种业务的外部需求量下降，攻击导致的损失大幅减少，发动攻击的动力随之减少。

网宿科技的网络安全防护

3.2 Web应用攻击防护

上半年的Web应用攻击事件统计中， 告警类型以敏感信息下载为主，此类攻击多为互联网上对各种网站撒网式的简单漏洞探测行为。下文将通过实际案例来介绍这种攻击。

案例涉及的攻击事件持续时间为 8 分钟， 主要攻击告警由敏感信息下载与扫描器扫描为主，部分攻击样本如下图所示：

请求方式	URL	攻击类型	状态码	处理动作
GET	/www.zip	敏感信息下载防护	403	拦截
GET	/wwwroot.rar	敏感信息下载防护	403	拦截
GET	/wwwroot.zip	敏感信息下载防护	403	拦截
GET	/1.zip	敏感信息下载防护	403	拦截
GET	/1.rar	敏感信息下载防护	403	拦截
GET	/web.rar	敏感信息下载防护	403	拦截
GET	/web.zip	敏感信息下载防护	403	拦截
HEAD	/e/e.rar	敏感信息下载防护	403	拦截
HEAD	/data.rar	敏感信息下载防护	403	拦截
HEAD	/data.zip	敏感信息下载防护	403	拦截

图26：Web应用攻击案例（源码）

敏感信息下载行为根据事前准备好的测试列表对各种敏感文件尝试进行下载，上图所示的文件多为一些可能保存网站源码的文件名称，如果站点上存在相应的文件则攻击者将有可能获得站点的源代码。获取源代码后，可能进行人工或者工具审计，从而让攻击者更详细的了解站点结构及一些比较隐避的漏洞。

网宿科技的网络安全防护

3.2 Web应用攻击防护

请求方式	URL	攻击类型	状态码	处理动作
HEAD	/config.tar.gz	敏感信息下载防护	403	拦截
HEAD	/ucenter/data/config.inc.php.bak	敏感信息下载防护	403	拦截
HEAD	/uc_server/data/config.inc.php~	敏感信息下载防护	403	拦截
HEAD	/config/config_ucenter.tar.gz	敏感信息下载防护	403	拦截
HEAD	/config/config_ucenter.php.rar	敏感信息下载防护	403	拦截
HEAD	/config/config_ucenter.php.zip	敏感信息下载防护	403	拦截
HEAD	/config/config_ucenter.php.bak	敏感信息下载防护	403	拦截

图27：Web攻击案例（配置文件）

这类攻击者也会去尝试去下载各种配置文件，这些配置文件中可能包含当前系统的后台路径、帐号、密码或其它系统库（如数据库）的内网IP、帐号、密码等信息。如果相关文件存在并被攻击者获取，则会对源站形成较大的安全隐患。

除上述示例中展示的样本外，还会有对系统帐号口令文件、数据库文件/备份、存在已知漏洞的软件/应用等敏感文件的试探。

此次攻击事件中还包含少量使用扫描器进行的扫描行为，样本告警如下图所示：

请求方式	URL	攻击类型	状态码	处理动作
GET	[redacted]72_112759.html	扫描器防护	403	拦截
GET	[redacted]2_616880.html	扫描器防护	403	拦截
GET	[redacted]6_467050.html	扫描器防护	403	拦截
GET	[redacted]_118289.html	扫描器防护	403	拦截
GET	[redacted]6_894001.html	扫描器防护	403	拦截
GET	[redacted]26_693010.html	扫描器防护	403	拦截
GET	[redacted]72_145973.html	扫描器防护	403	拦截
GET	[redacted]/redirect.jsp	扫描器防护	403	拦截
GET	[redacted]/redirect.jsp	扫描器防护	403	拦截
GET	[redacted]/redirect.jsp	扫描器防护	403	拦截
GET	[redacted]/redirect.jsp	扫描器防护	403	拦截

图28：使用扫描器进行的扫描行为的告警案例

网宿科技的网络安全防护

3.2 Web应用攻击防护

网宿科技安全平台在第一时间监测到此次攻击事件并进行了响应， 对攻击请求实时进行了拦截，保证了网站的正常运行；在后续定期攻击事件分析的过程中， 没有发现漏报与误报情况，此次事件相关的攻击源信息已更新至信誉库，供后续的安全防护提供数据参考。

在互联网上有许多开源维护的安全测试用例， 上述告警中的样本也部分包含在其中，下图即为一个开源测试用例的列表：

528	ConfigBuilder	1352	ref	3583	wcf
529	ConfigBuilder.exe	1353	ucenter	3584	weblinks
530	ConfigBuilder.ini	1354	wp-icludes	3585	weekfilm
531	config.cfg	1355	Shop	3586	workshop
532	config.include.php	1356	WorkArea	3587	wpm
533	config.inc.php	1357	ct	3588	write
534	config.ini	1358	cv	3589	wwwroot
535	config.php	1359	details	3590	xgallery
536	configs	1360	exports	3591	xls
537	Configs	1361	images1	3592	coID
538	configsample.inc.php	1362	invoices	3593	111
539	Configs.php	1363	o	3594	Audio
540	Configs.txt	1364	phpadmin	3595	Back-up
541	config.tpl	1365	posts	3596	ClickTale
542	config.txt	1366	pricelist	3597	Configuration

图29：开源测试用例的列表

敏感信息下载类告警多为通过工具根据类似上述列表的测试用例对网站的各级目录进行枚举测试行为；此现象与国外网络环境中所遇到的以SQL注入/XSS为首的攻击类型有着较大区别。

而除上边的这种攻击之外，SQL注入、XSS等包含在OWASPTop10以内的Web攻击以及利用这些漏洞使用工具发起的扫描行为仍将是最为直接也最具威胁的Web应用层攻击手段。

版权声明

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属网宿科技股份有限公司所有，受到有关产权及版权法保护。任何个人、机构未经网宿科技股份有限公司的书面授权许可，不得以任何方式复制或引用本文件的任何内容。