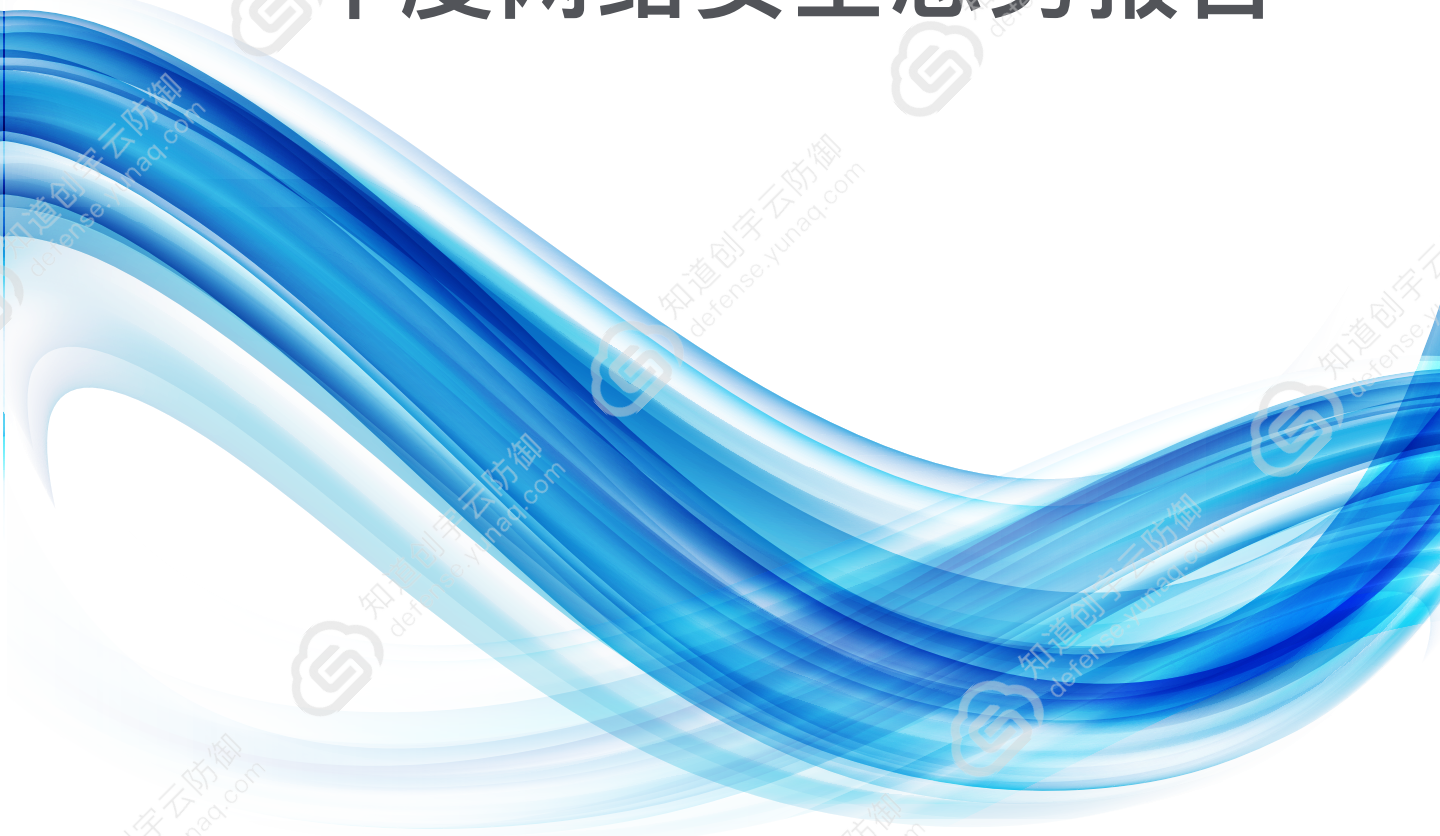
中关村网络安全与信息化产业联盟 × 知道创宇

2020
年度网络安全态势报告



中关村网络安全与信息化部产业联盟

北京知道创宇信息技术股份有限公司

联合出品

知道创宇成立于2007年，由数位资深的安全专家创办，并拥有近百位国内一线安全人才组成的核心安全研究团队。知道创宇是国内较早提出云监测与云防御理念的网络安全公司之一，经过多年的积累，利用在云计算及大数据处理方面的行业先进能力，可为客户提供具备国际先进安全技术标准的可视化解决方案，提升客户网络安全监测、预警及防御能力。凭借在行业中先进的技术实力及影响力，知道创宇创始人及CEO赵伟入选2012年《福布斯》30位30岁以下创业者之一，公司还被CIO杂志评选为2009年度国内除阿里巴巴之外唯一一家入选亚洲最具价值企业1/20名单。

“知道创宇云防御”是一个为客户提供一站式安全服务的SaaS安全边界防御平台。通过简单DNS域名指向修改，业务数据流量先经过云替身，再到达服务器，并获得军工级安全保护服务。创宇云防在全球拥有超过50个大型数据中心，高达4TB的带宽储备，为全球超过110万业务系统提供安全保障，获得一致赞誉。

概述

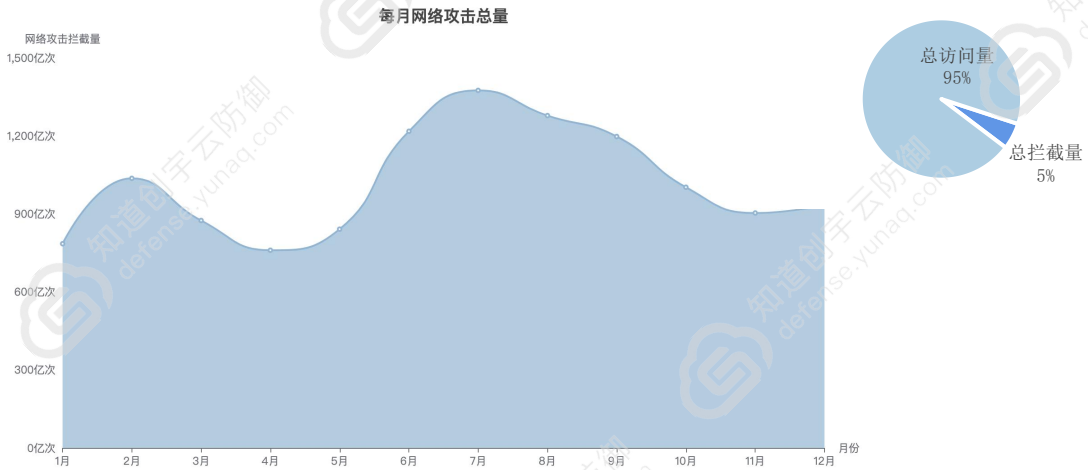
知道创宇云防御平台在2020年全年共检测到229,600+亿次网络请求，识别阻断12,180+亿次网络攻击行为。并根据漏洞利用难度、影响面、危害程度列举出10大热点漏洞。

本报告采样2020年知道创宇云防御平台的网络攻防数据，从DDoS攻击态势、Web应用攻击态势和威胁情报等，对2020年网络云安全态势进行展示与分析，为各网站运营者提供网络安全态势、优化安全防御方案等方面的参考。

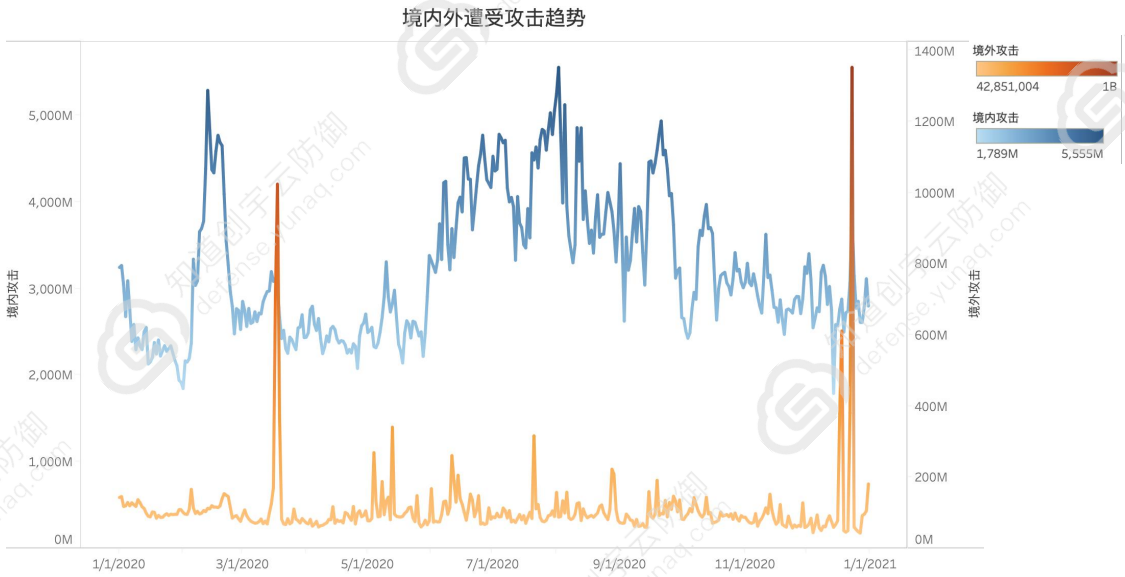
目录

1. 年度网络攻击趋势

1.1 总述



知道创宇云防御平台（以下简称云防御）在2020年全年共检测到229,600+亿次网络请求，其中5.31%为非法攻击请求，这也是云防御全部拦截量，为12,180+亿次，境内外分别占比96.74%和3.26%。



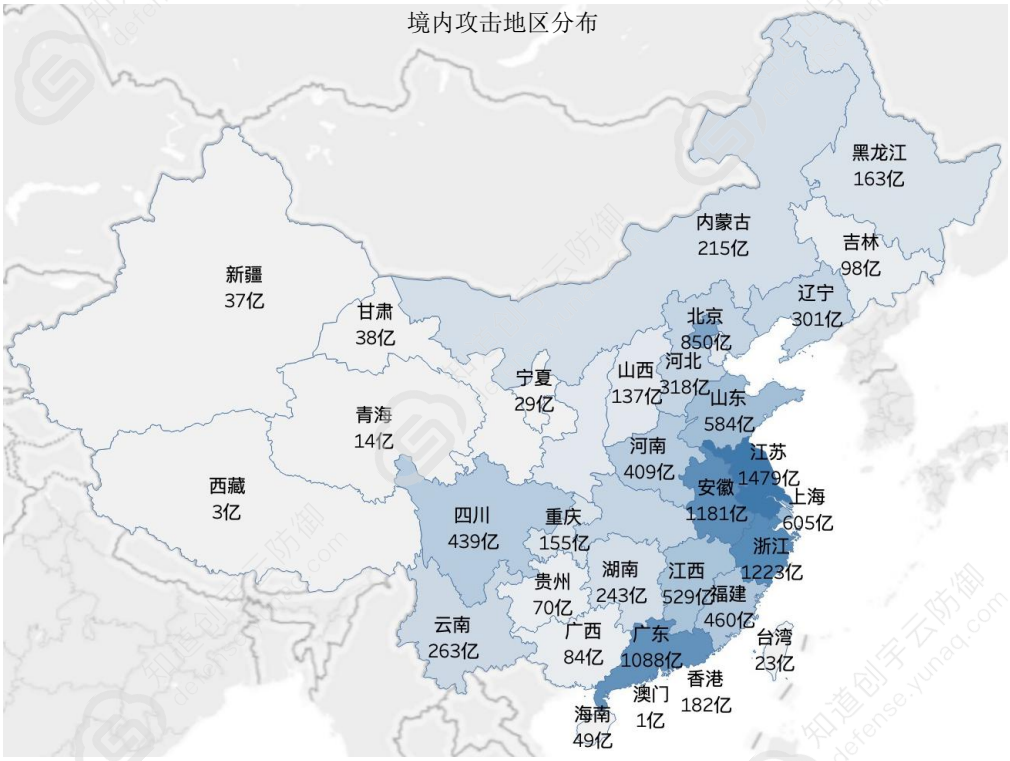
2020年月平均拦截网络攻击量为1,015+亿次；其中7月拦截量最多，为1,372+亿次。据相关行业报告显示，2020年7月为高危漏洞最为频发月份，单月新增79种高危漏洞，或成为网络攻击增加原因。同比2019年的双十一电商活动期间攻击量暴涨形式，2020年全年攻击均趋于缓和。

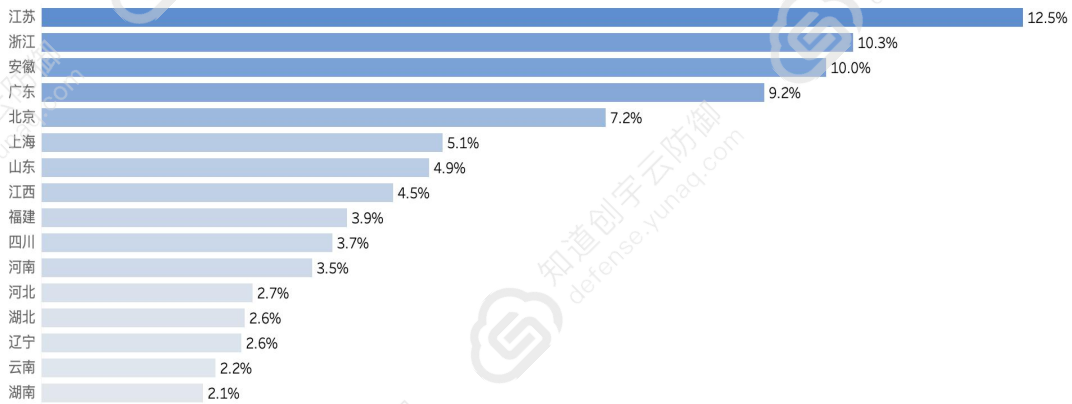
2. 全球攻击态势

2.1 境内攻击解析

2020年，江苏省、浙江省和安徽省是发动网络攻击总量最多的境内区域，分别制造了1,479亿、1,223 亿、1,181 亿次网络攻击。主要因为这些省份的数字政务日益发达，导致攻击也有着明显的线性同步增加。

另外，由于香港云计算市场较为发达，攻击者们都倾向于租用香港VPS进行网络攻击，故此香港也是一个不可忽视的攻击源，在这一年共制造了182亿网络攻击。





2. 全球攻击态势

2.2 境内攻击Top IP详解

攻击 IP Top 10 详情

序号	IP	地理位置	IP 属性	安全大脑标签
1	182.**.***.18	广东广州	IDC	-
2	183.***.***.27	湖北武汉	-	爬虫|DDoS
3	106.***.**.234	北京	IDC	-
4	39.**.***.56	北京	IDC	-
5	203.***.**.156	广东广州	IDC	-
6	113.*.***.198	广东广州	IDC	恶意扫描
7	223.***.*.37	四川成都	-	爬虫|恶意扫描|APPScan|DDoS|WVS
8	152.*.***.15	北京	IDC	恶意扫描
9	39.***.***.252	北京	IDC	爬虫|恶意扫描
10	59.***.**.159	江西南昌	IDC	爬虫|恶意扫描

以上为2020年全年攻击最多的IP Top 10。显而易见，数据类型IP是攻击者们更青睐的攻击目标，其缘由也不外乎变现方便，更有利可图。

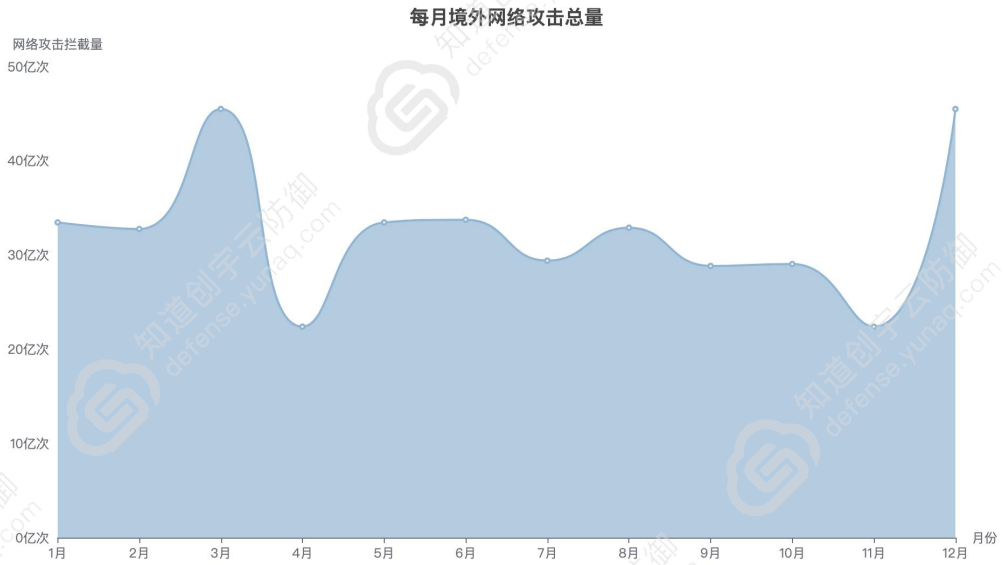
其中，广东和北京地区的Top 攻击量鏖战榜首，也说明一线城市的黑客攻击力仍然遥遥领先。

2. 全球攻击态势

2.3 境外攻击解析

2020 年境外网络攻击拦截总量为392+亿次，平均境外网络攻击月拦截量为33亿次。全年境外攻击中有2次攻击高点，均与新冠疫情相关：

- 3月，“海莲花”组织以“湖南省家禽 H5N1 亚型高致病性禽流感疫情情况”、“冠状病毒实时更新：中国正在追踪来自湖北的旅行者”等新冠疫情相关的时事热点为诱饵，对我国数字政府网站进行鱼叉攻击。
- 12月，攻击者瞄准 COVID-19 疫苗冷链组织，对其相关的储存和运输公司发起网络钓鱼邮件攻击。IBM 网络安全部门表示，其目的在于试图收集攻击目标的内部电子邮件和应用程序的凭据。

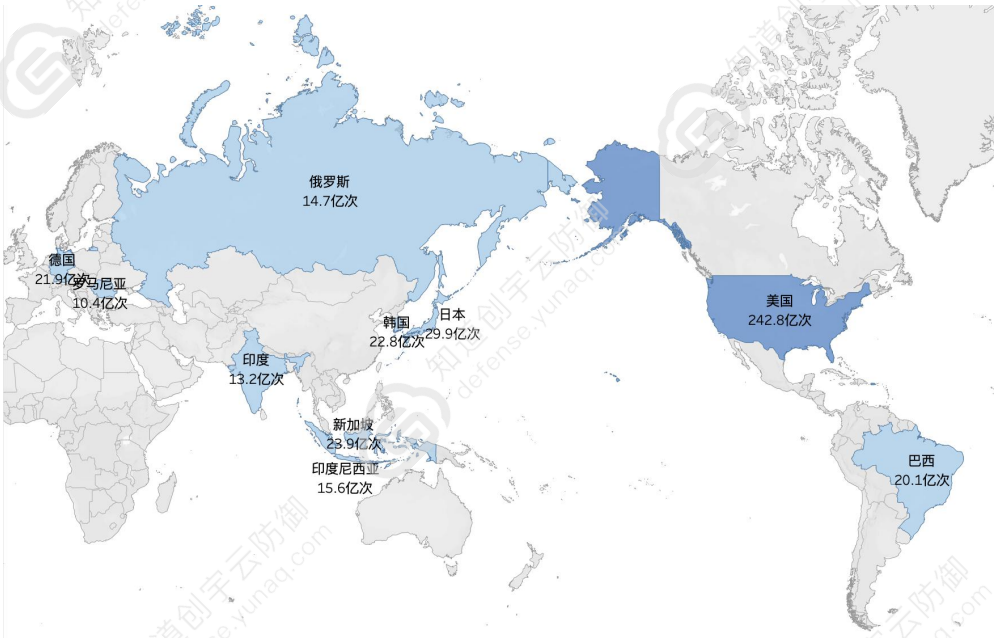


2. 全球攻击态势

2.3 境外攻击解析

美国依然是最大的境外攻击源，在2020年境外地区对我国网站及业务系统的网络攻击总量中占据了 58.46% 的份额。其原因是美国国家网络安全发展水平较高，网络渗透能力较强，对我国网络空间的威胁程度远超其它任何国家或地区。

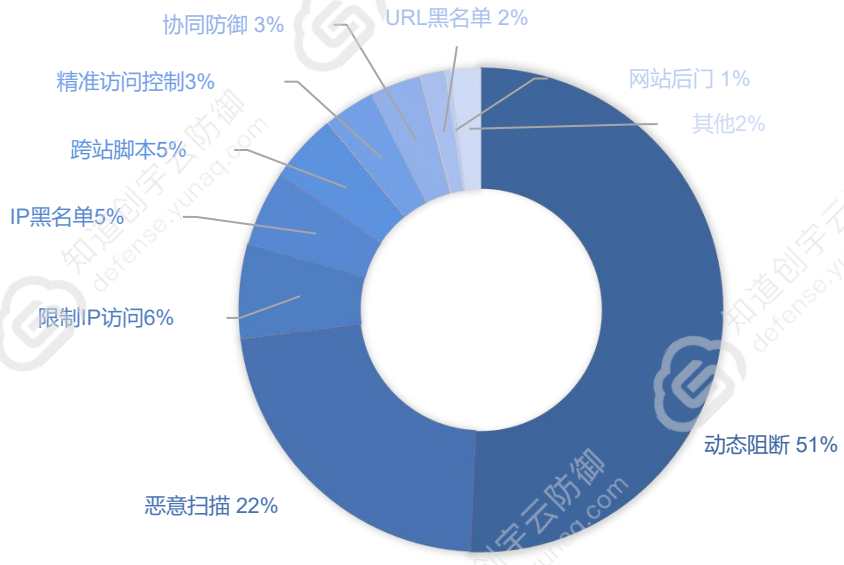
境外攻击地区分布

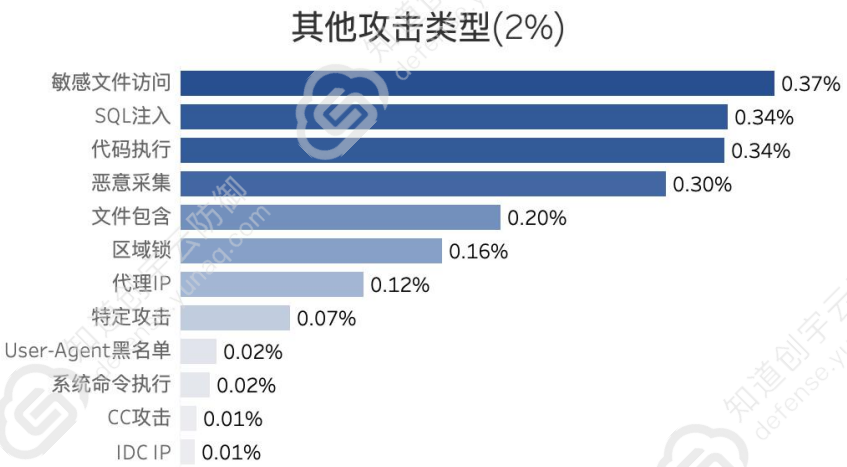


攻击来源国家Top10

3. 攻击详情解读

3.1 Web攻击拦截详情





从以上2020年Web攻击情况来看，大部分攻击被动态阻断，也从侧面说明企/事业单位使用了有效的安全防御工具，需要警惕的是更细化的攻击方式也在逐步渗透安全圈。

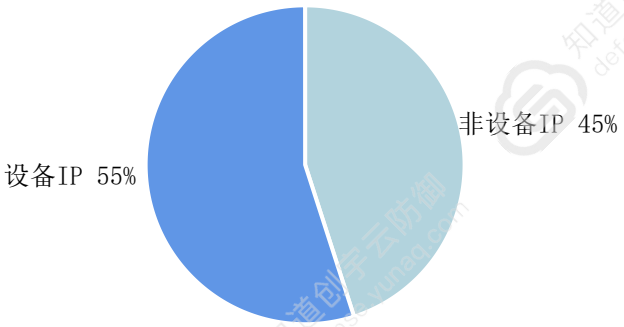
除动态阻断攻击外，恶意扫描是占比最高的网络攻击类型。根据后台数据显示，AWVS、IBM AppScan 等知名漏洞扫描产品的使用率相对较高，某些伪造成搜索引擎爬虫User-Agent的自动化扫描器也制造了大量的恶意扫描流量。

3. 攻击详情解读

3.2 DDoS攻击-形势解读

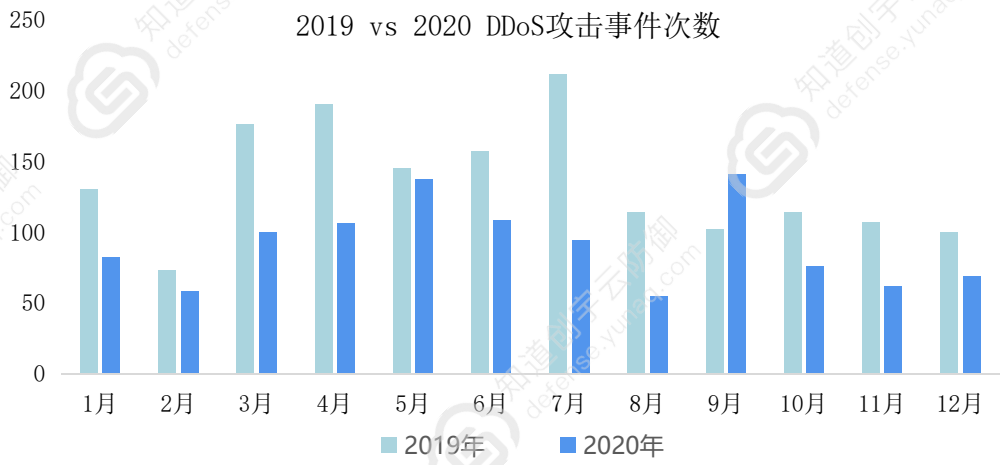
2020年全年共拦截了6,448万+ DDoS 攻击IP，结合知道创宇旗下的产品ZoomEye（钟馗之眼）内的数据交叉分析，发现其中有3,544万+IP来自路由、监控等硬件设备，占比高达55%；

随着IoT设备的迅速增长，且这些安全设备的安全性相对较低、无法升级或升级频率太低，即更容易受黑客的大规模控制，进一步成为DDoS攻击的源头。



2020年整体大环境萧条，以及金融客行业-尤其是 P2P 企业势头走低，导致DDoS攻击肉眼可见的减少。

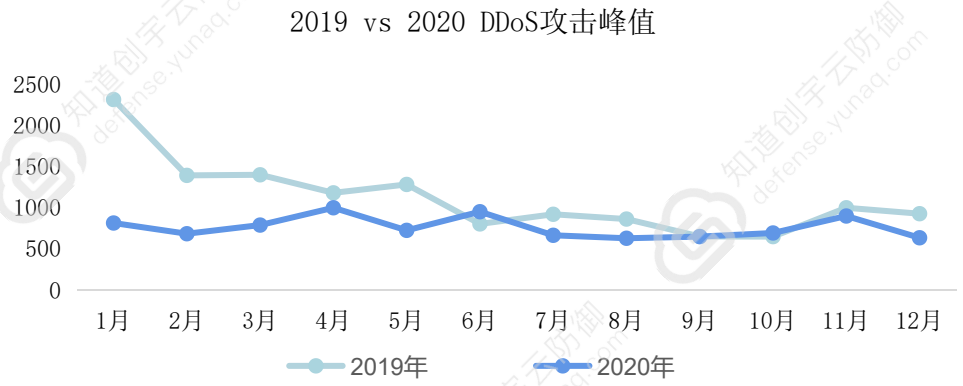
相比2019年，2020年全年攻击量较于整体下降33%；从各维度的DDoS 统计数据来看，2020年数据均有不同幅度的下降。



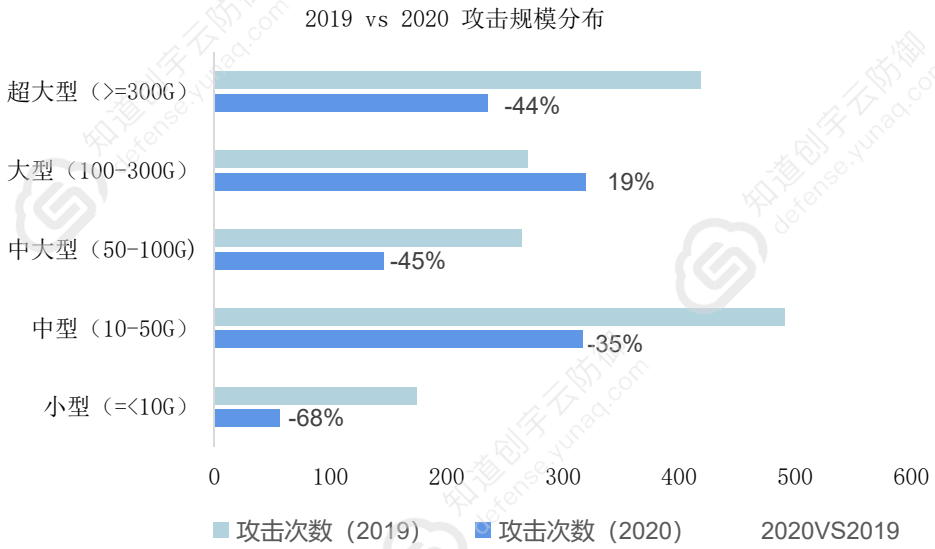
3. 攻击详情解读

3.3 DDoS攻击-峰值规律解析

2020年每月的攻击峰值相对平均，平均峰值为180 Gbps，较2019年均值下降了16%；其中最高攻击峰值达到1000 Gbps，近两年下半年攻击趋势基本拟合。



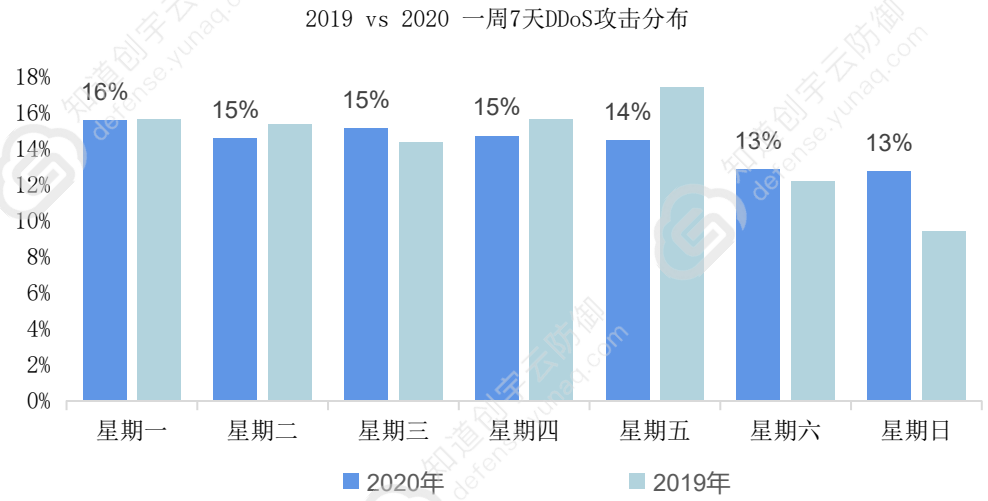
从攻击规模来看，2020年的大型攻击（100~300G）和中型攻击（10~50G）分别占比为全年的30%和29%，超大型攻击（≥300G）占比下降到22%。对比2019年，2020年仅大型攻击增加19%，其他类型的攻击均有大幅下降。



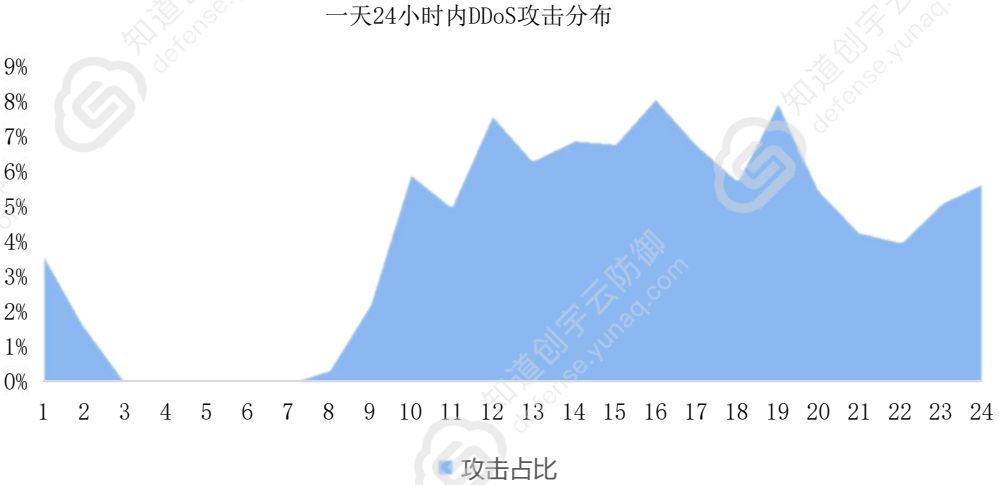
3. 攻击详情解读

3.3 DDoS攻击-峰值规律解析

DDoS攻击在一周中的分布差异较小。此现象不仅与云防御的7*24小时服务模式有关，也由互联网“996”工作模式导致。网络攻击份子和网络安全守护者同样一周无休，且攻击力度分布均匀。



在全天攻击分布中，网络攻击分子也有着“上班族”作息，但较于2019年凌晨1~2点的攻击是其他时段的20倍+，2020年此时段的攻击力度明显减小，甚至低于其他时段。由此可见，利益空间的压缩也极大的降低了攻击者们的攻击力度。



3. 攻击详情解读

3.4 DDoS攻击-手法解读说明

从攻击手法角度来分析，2020年仍然以反射型DDoS和CC攻击为主，而攻击手法也不断在更新迭代，我们整理了2020年公布的主要新型攻击手段：

- 5月，以色列的研究人员公布了一种新的DNS漏洞攻击——NXNSAttack。该漏洞与往常针对IP的DDoS攻击不同，NXNSAttack主要针对DNS服务器，该漏洞利用DNS协议的递归解析器指向恶意的DNS服务器，然后返回特定的响应体，导致中间交换过程中的DNS数据包产生大量的请求而产生拒绝服务。

- 同为5月，中国研究人员公布了一种新的攻击手法——RangeAmp。利用修改HTTP协议的Range字段导致CDN与源站之间需要交换大量流量，从而消耗了源站出口带宽，产生拒绝服务。

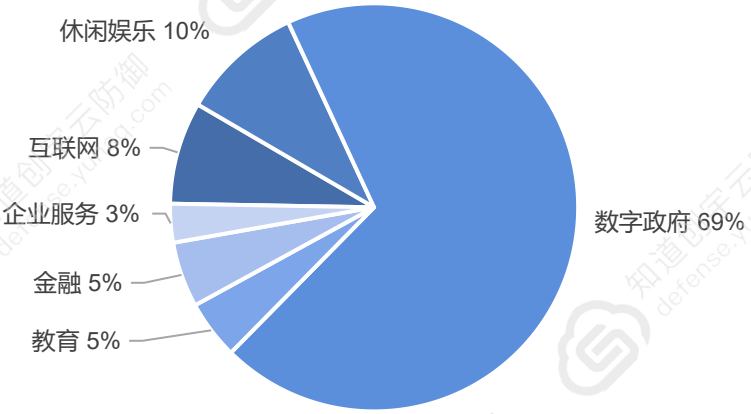
- 7月，基于WS-DD、CoAP、ARMS协议的新型UDP反射型攻击也反复出现。来自外媒7月27日的报道，美国联邦调查局（FBI）也针对这三类协议发出正被不法份子作为DDoS滥用的警告。

参考链接：

- https://www.usenix.org/conference/usenixsecurity20/presentation/afek
- https://netsec.ccert.edu.cn/files/papers/cdn-backfire-dsn2020.pdf
- https://www.zdnet.com/article/fbi-warns-of-new-ddos-attack-vectors-coap-ws-dd-arms-and-jenkins/

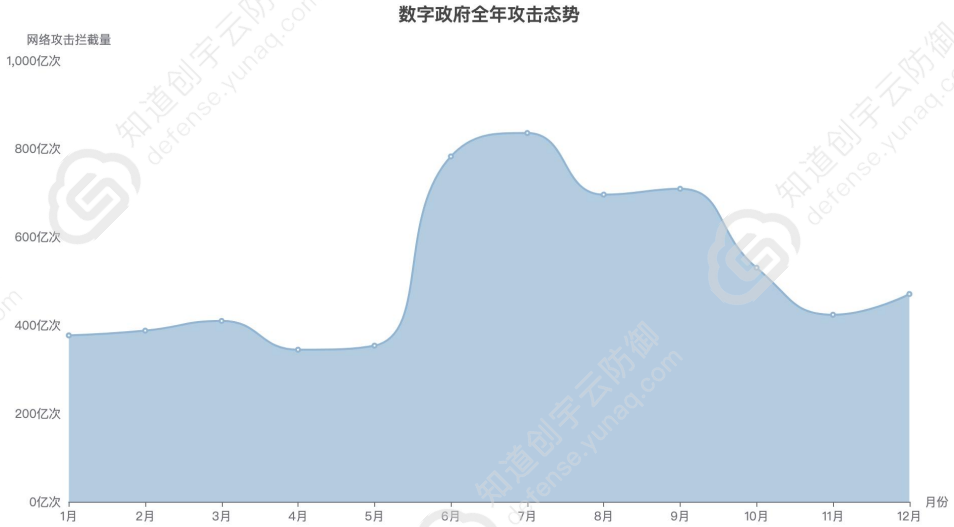
4. 重点受攻击行业

4.1 数字政府 “首当其冲”



2020年全年攻击拦截量中，数字政府类网站占比极大，其中包含政企、国企和央企等；受新冠疫情影响，金融、互联网和资本市场缩水，更多攻击者将攻击矛头调向数字政府类网站，数字化覆盖面增加，其访问流量呈线性同步增加，黑灰产团伙纷纷盯上了这块流量蛋糕。据不完全统计，云防御通告数字政府网站的恶性SEO被黑事件高达200+起，几乎每天都有该类被黑事件发生。

数字政府类网站作为云防御的主力客户群体，其攻击趋势和云防御全年攻击趋势基本拟合。



4. 重点受攻击行业

4.2 境外攻击者也“偏爱”中国数字政府

境外黑客首选攻击对象也是数字政府类网站 ，更多目的旨在抹黑中国政府形象。

知道创宇安全大脑在2020年年底监测到土耳其黑客组织“图兰军”攻击活动频繁，攻击量呈上升趋势。该组织是2019年12月22日成立的土耳其反华黑客组织，并大力支持东突分裂势力，同时针对中国境内政府、教育等类别网站进行攻击。经过长期跟踪分析，发现多数被黑的站点均属于安全防护较差、长期处于无人维护的网站。

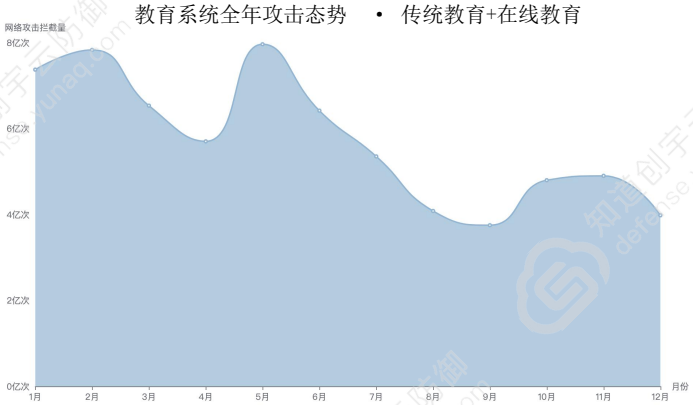
该黑客组织组织共计入侵中国境内网站达百余个，其中不乏高等院校和科研单位的官方网站，并将“战果”贴在Twitter上：

4. 重点受攻击行业

4.3 互联网行业 也非“黑”外之地

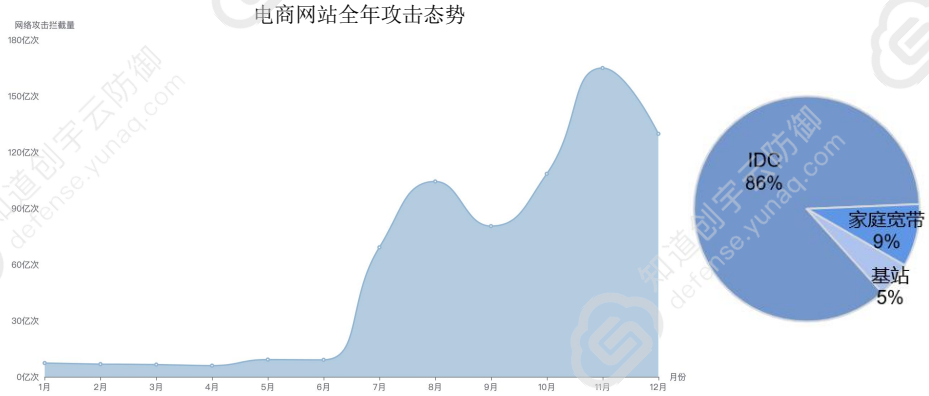
2020年全年都被疫情笼罩的情况下，教育行业和电商行业的被迅速催化进而高度发展，必然也成为了黑客们的“眼中钉”，其攻击态势也突破了往年的极值，呈现出新形态。

教育系统全年攻击态势 • 传统教育+在线教育



教育系统在全年都面临着极为严峻的网络安全态势，在5月达到攻击高点后，6月开始呈下降趋势，这主要是是因为学校开始正常开学授课，学生并非全部依赖线上教学系统；而之后的平缓趋势也和教育行业开始实行了“线下+线上”的并生教学模式有关，该类型网站系统仍无法脱离攻击者的目标。

电商网站全年攻击态势



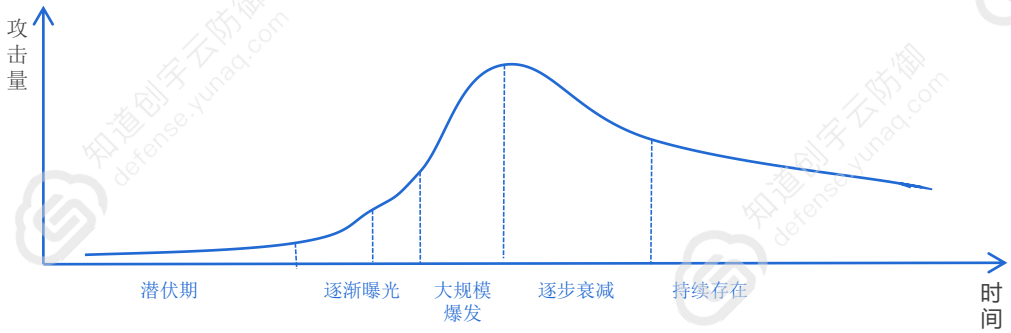
2020年全民经济收缩，直到Q2复工、Q3经济复苏，各大电商网站的购买力（直播除外）逐渐恢复，再有618、双十一等促销活动的加持，从6月开始电商网站的攻击量和正常访问流量同比大幅上涨。

通过对电商网站的访问流量深度分析后发现，“羊毛党”成为了电商流量的主力军，其原因不外乎限量的促销活动让“羊毛党”们有利可图。

5. 热点漏洞及趋势

5.1 黑客仍爱经典“主使原料”

通常来看，一个漏洞的利用情况都会经历一个完整的生命周期：长期潜伏、公开曝光、热度升温、规模爆发、逐步衰减、持续存在。



不同的漏洞属性、受影响组件特征或爆发的特定时间背景，每一个漏洞都可能呈现出一种独特的利用趋势。

总的来说，反序列化漏洞和远程命令执行漏洞依然为黑客们主要使用原料，正所谓万变不离其宗。

2020年知道创宇云防御十大热点漏洞

序号	漏洞名称	公开编号	公开情况
1	通达OA任意用户登录漏洞	CNVD-2020-25050	2020年4月17日官方发布补丁
2	用友NC JNDI远程代码执行漏洞	CNVD-2020-32435	2020年6月4日第三方发布漏洞公告
3	F5 BIG-IP TMUI 远程代码执行漏洞	CVE-2020-5902	2020年7月1日官方发布漏洞公告
4	Citrix ADC 远程代码执行漏洞	CVE-2020-8193	2020年7月7日官方发布漏洞公告
5	宝塔面板数据库管理页面未授权访问漏洞	-	2020年8月23日官方发布漏洞公告
6	用友NC monitorservlet反序列化漏洞	-	2020年10月27日互联网首次出现漏洞分析文章
7	Weblogic 管理控制台未授权远程命令执行漏洞	CVE-2020-14882 CVE-2020-14883	2020年10月20日官方发布漏洞公告
8	泛微云桥e-bridge任意文件读取漏洞	CNVD-2020-59520	2020年10月30日官方发布补丁
9	XXL-JOB API 接口未授权访问致远程命令执行漏洞	-	2020年10月27日第三方发布漏洞公告
10	TerraMaster TOS未授权命令执行漏洞	CVE-2020-28188	2020年12月12日第三方发布漏洞公告

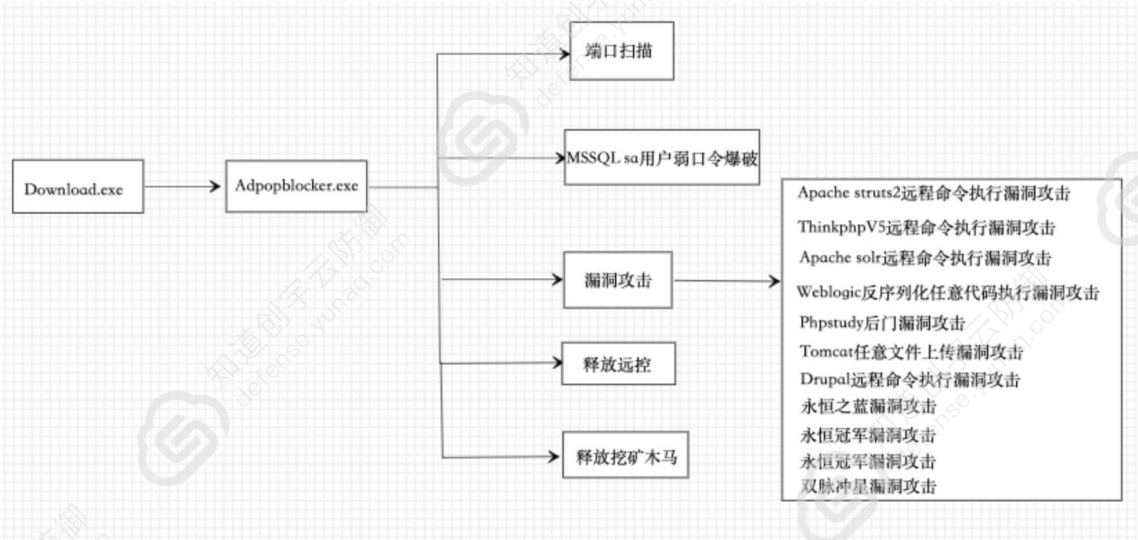
5. 热点漏洞及趋势

5.2 漏洞利用趋势详解

从另外一个角度看热门漏洞：

热门漏洞更偏向于远程代码和远程命令执行这两类漏洞。这两类漏洞使得从漏洞利用到控制主机系统两个步骤能更加自动化，从而更受黑产组织青睐。

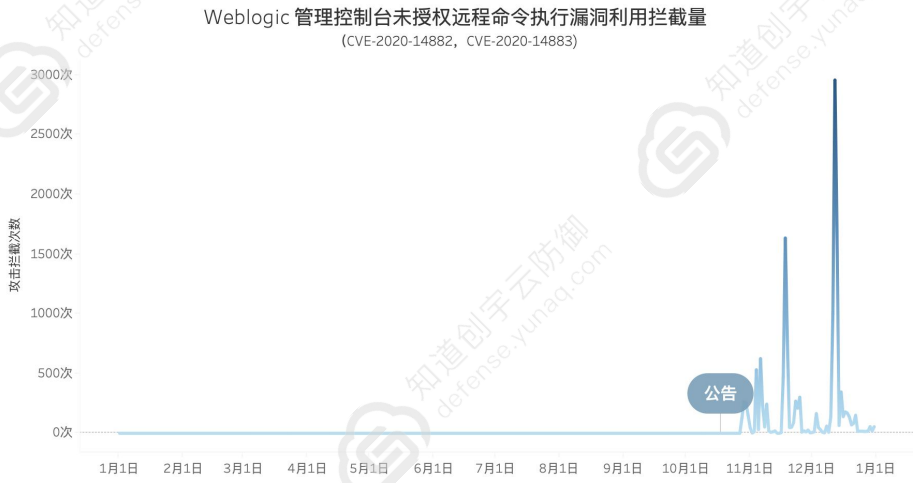
例如，在7月26日，404积极防御团队监测到47.92.**.**、119.23.**.**、117.89.**.**等多个IP大量利用Struts2、Weblogic等多个Web组件漏洞进行的组合攻击，这些攻击请求中主要夹带了远程代码和远程命令执行漏洞的利用代码，试图通过漏洞去下载执行远程的恶意文件Download.exe，而被确认为Bulehero蠕虫病毒；恶意文件会进一步在内网传播自身，以及攻击其他网站。



5. 热点漏洞及趋势

5.2 漏洞利用趋势详解

对于 Oracle 之类的国际巨头公司，如其产品Weblogic，全球装机量巨大且影响范围广泛，一直都是安全研究人员和黑客的关注焦点。一旦官方修复了某个高危漏洞并发布公告，攻防双方都会第一时间进行 PoC 探测，1月之期内大规模的扫描器流量就会出现，并在之后呈现逐步爆发的态势，其原因通常是由于安全研究人员或黑客逐步将该漏洞的PoC嵌入到了自动化扫描器程序中。不过云防御在1～2天内即可监测到较小规模的利用流量。

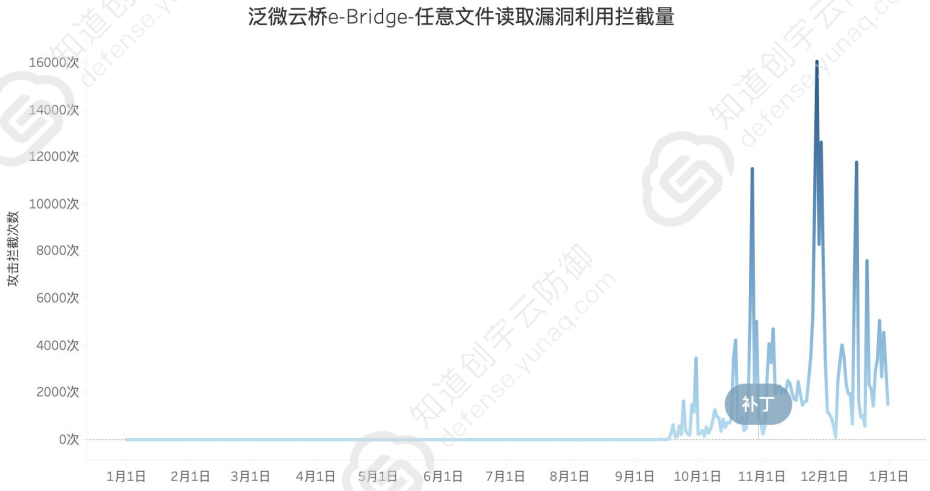


F5 Big-IP 组件在国内的应用场景较少，其漏洞的爆发也不会受到的业界很高的关注度。这种情况下，安全研究机构会降低应急响应的优先级，针对漏洞的PoC检测或扫描器集成工作可能会出现一些滞后。

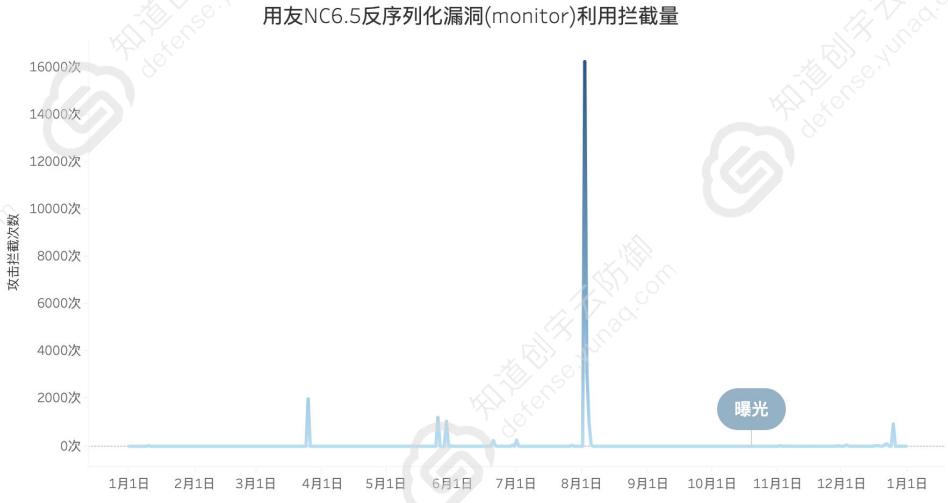
5. 热点漏洞及趋势

5.2 漏洞利用趋势详解

用友、泛微等国内各类知名商业软件是安全行业关注的另一个焦点，同时，这类软件往往也是黑客利用0day进行网络攻击的重要目标。从趋势图中可以看出，在官方公告或补丁发布之前，知道创宇云防御平台中可回溯检测到相关的漏洞利用流量。在2020年全国各省市网络安全特别行动中，这类漏洞一般都是攻击队使用的主要“武器”，在此期间相关漏洞利用拦截量呈现了爆发趋势。



对“用友NC monitorservlet 反序列化”等只在小范围内传播但并未大规模曝光的漏洞，由于信息传播的不透明，很多安全厂商在不知情的情况下亦不能支持对这类漏洞的检测和防护，这类通用产品的用户实际上就持续暴露在部分黑客的威胁之中。

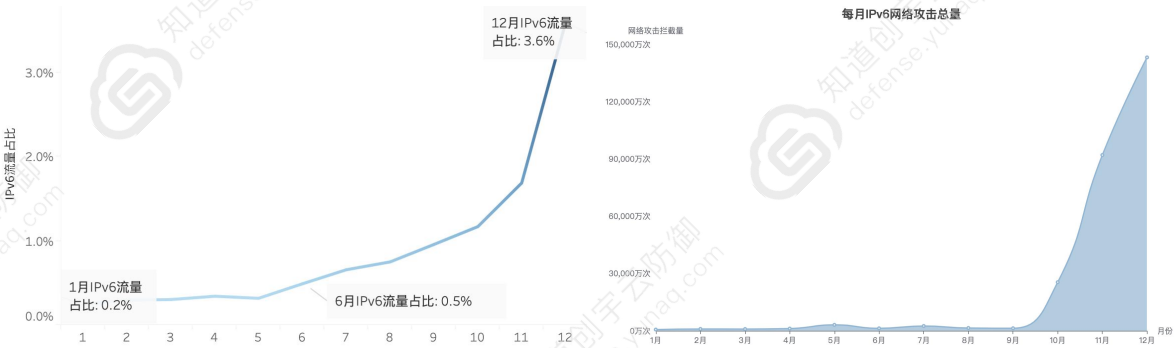


6. IPv6 形式解读

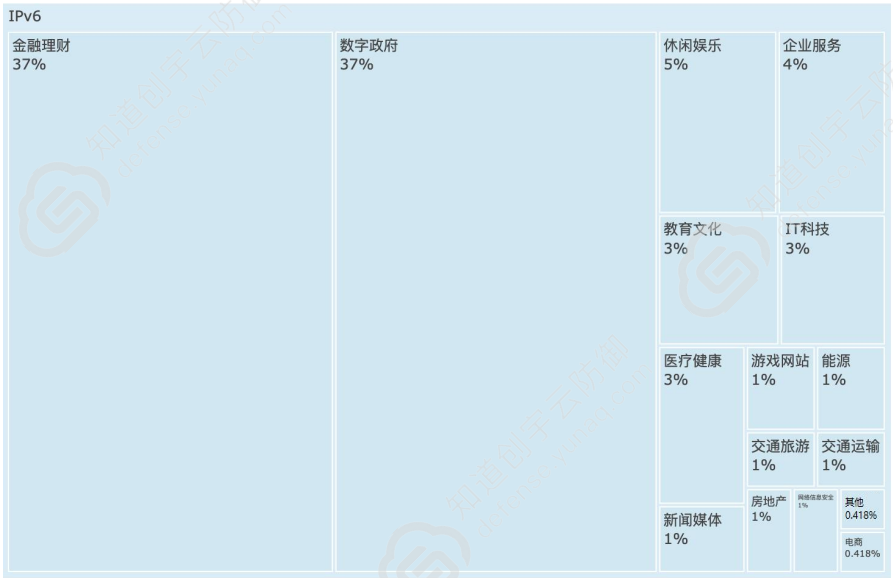
6.1 流量与趋势详解

随着《推进互联网协议第六版（IPv6）规模部署行动计划》的加快推进，越来越多企业完成了系统或网站的IPv6改造，2020年1月到12月云防御平台内 IPv6 流量增加了14倍多。

从右下图攻击趋势来看，在IPsec和更好的QoS等升级性能加持下，升级IPV6 的网站受到的攻击略有滞后，但从9月开始，攻击量即呈持续陡增趋势。



全国各行业在这一年贯彻落实推进IPv6下一代互联网建设，数字政府和金融服务机构门户网站在2020年均积极投入到 IPv6 部署中，故此在IPv6整体流量中数字政府类网站和金融两大行业的流量占比最大且不分伯仲。



6. IPv6 形式解读

6.2 安全说明

目前全网平台中，部署有IPv6代理服务的域名中“gov.cn”或“edu.cn”较多。这类域名往往在搜索引擎排名算法中具有极高的收录权重，通过这类域名收录的页面会在搜索结果列表中排名十分靠前，更容易被普通用户发现。

知道创宇安全大脑在2020年上半年监测到一种新型互联网黑产技术手段，部分黑产人员可以利用部署在公共网络的具有漏洞的IPv6代理服务实现国内外知名搜索引擎对各类违法网页的收录。

黑产人员正是凭借这种特性来滥用高权重IPv6代理域名对违法的色情或博彩网站进行伪装，提高其曝光度，从而实现敛财的目的。

由于这种配置漏洞的存在，任何人都可以通过点击一个经过特殊构造的URL 链接，使用代理服务器绑定的域名来访问其它域名下部署的网络服务。

特别故事

- **安全保障每一秒**

国家某信息公共查询平台平均每秒有 2500 次+网络爬虫请求，均被云防御成功拦截。

如果你希望了解一个公司的经营现状，最直接的方式可能就是使用企*查这类软件进行搜索查询。其实，由国家运营单位维护的某信息公共查询平台才是各类企业信用查询服务厂商的根本数据来源。

该信息公共查询平台作为一个面向公众的信息查询系统，其公开性虽然方便了普通用户的使用，但同时也使其成为滋生网络爬虫的温床。大量未经授权的个人或团体企图通过公开途径使用爬虫程序爬取海量的企业数据，将其据为己有以实现盈利的目的。假若浪潮般的恶意爬虫请求未加限制直接到达公示系统源站，轻则损耗大量带宽和计算资源，重则可使系统直接崩溃。

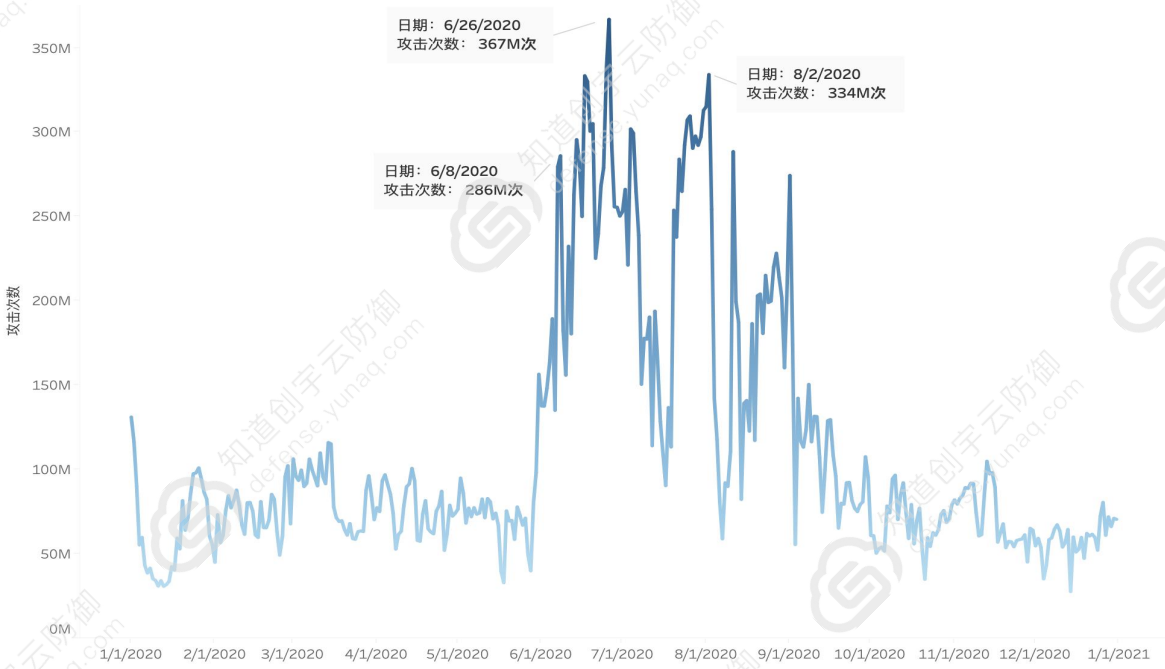
2020年全年，知道创宇成为了该系统防护网络爬虫的“守护神”，识别并拦截了来自全球范围内 6,000万 +IP地址的800亿+恶意爬虫请求，保障了公示系统的平稳运行。

特别故事

- **守护企业， 保障即可靠**

某大型信息资讯类网站www.****.cn 在前半年所受攻击较少且平缓，从6月开始到9月初，该网站所受攻击陡增，6月26日为2020年全年单日攻击最多的一天，共有366,885,622 次攻击，且有6,438 个IP在这一天内对该网站均发动了超过10,000次的网络攻击，在基于知道创宇安全大脑制定的协同防御代理IP拦截规则下，所有攻击全部被拦截。

显然，这是一次有组织有准备的恶意数据爬取事件。攻击者使用了高成本的秒拨动态IP代理池，但其恶意访问仍然没有逃脱被拦截的命运。



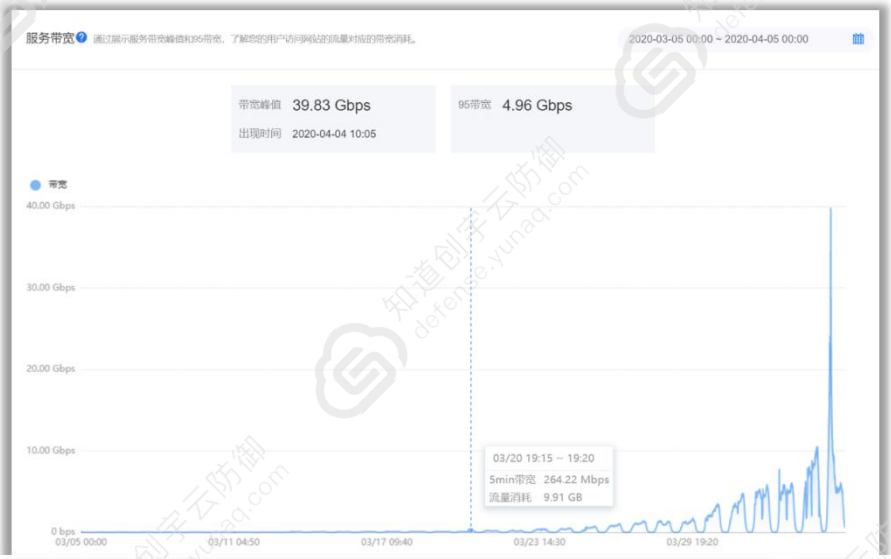
特别故事

- **守护国家网络安全，守护国泰民安**

由于疫情关系，某国家级网上祭扫平台于4月4日 - 4月6日举办线上祭扫活动，如专家组前期预估，本次活动期间网络访问量极大，伴随的网络风险也就极大。

4月4日10时00分至10时03分带宽峰值超40Gbps，超过平时访问峰值70倍，当日访问总量达到10亿次。

截至4月6日，***英烈网某页面访问量超过37 亿次，拦截各类网络攻击达到4,500 万次。



总结

2020年是极为“特别”的一年，新冠疫情在全球范围内肆虐、中美贸易对抗持续升温、2020全国“两会”如期举行、印度频繁在中印边境处挑起事端……在被称为“第五空间”的网络空间，同样也经历着难以平静的一年。年初，土耳其黑客组织“图兰军”、越南黑客组织“海莲花”、印度黑客组织“白象”等众多境外APT组织针对中国政府网站发起数波猛烈的网络攻击。3月，Github、京东等多家网站出现了 SSL 证书劫持事件，中间人攻击致使正常用户访问受阻。年中，5.38亿条微博用户信息被打包后在暗网黑市以 500 美元的价格出售。12月，网络安全公司 FireEye 发布的 APT 事件“ SolarWinds 供应链攻击”已渗透到包括五角大楼、美国财政部、白宫、国家核安全局在内的几乎所有美国关键部门。发生在虚拟网络空间中的威胁，已然波及到每个普通人的现实生活。

这一年，知道创宇云防御平台拦截了12,180+亿次全球范围内的网络攻击，对接入网站及业务系统的防护工作实现了0事故。针对政府机关门户和电子政务系统的网络攻击态势尤为猛烈，大量怀有邪恶目的黑客团伙企图破坏党政机关网站及业务系统的可用性。随着IPv6网络使用的普及，发生在IPv6网络空间的攻击态势也随之高涨，完成针对性防护升级工作刻不容缓。国产商业办公软件的高危漏洞利用情况持续活跃，是黑客团伙谋取不义之财的首选目标。2020年全国各省市“网络安全攻防演练专项行动”中，知道创宇云防御平台为全国各重点客户提供了包含实时攻击威胁情报、资产脆弱面检测、攻击队溯源等多个环节在内的一站式立体重点保障服务，客户相关网站及业务系统在攻击队的专业技术手段面前无一被攻破。

2021年是中国共产党建党100周年，知道创宇云防御平台将持续保持对境外反党反华黑客势力网络攻击行动的高度关注，确保防护各党政机关门户网站、互联网+电子政务系统、各类在线业务系统万无一失。

客户案例


中华人民共和国国家互联网信息办公室
Cyberspace Administration of China
中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China
国家信息技术安全研究中心
National Research Center for Information Technology Security
中华人民共和国司法部
中华人民共和国最高人民法院
国家市场监督管理总局
State Administration for Market Regulation
中华人民共和国工业和信息化部
中华人民共和国退役军人事务部
Ministry of Veterans Affairs of the People's Republic of China
中华人民共和国国务院新闻办公室
The State Council Information Office of the People's Republic of China
中国银行保险监督管理委员会
China Banking and Insurance Regulatory Commission
中华人民共和国国家互联网信息办公室
Cyberspace Administration of China
中国国新控股有限责任公司
CHINA REFORM HOLDINGS CORPORATION LTD.
中央政府采购网
www.zycg.gov.cn
招商局集团
CHINA MERCHANTS GROUP
中国核工业集团有限公司
China National Nuclear Corporation
中国交建
CHINA COMMUNICATIONS CONSTRUCTION
中国移动
China Mobile
中国电信
CHINA TELECOM
CEC 中国电子
南光(集团)有限公司
NAM KWONG (GROUP) COMPANY LIMITED
中国联合航空
CHINA UNITED
中国地震局
CHINA EARTHQUAKE ADMINISTRATION
信用中国
WWW.CREDITCHINA.GOV.CN
CNCERT/CC
国家互联网应急中心
中共中央统一战线工作部
The United Front Work Department of CPC Central Committee
国家统计局
国家药品监督管理局
National Medical Products Administration
中广核 CGN
中国节能环保集团有限公司
北京市人民政府
The People's Government of Beijing Municipality
国务院侨务办公室
公安部第三研究所
The Third Research Institute Of Ministry Of Public Security
中国共青团
www.gqt.org.cn

为了更好更安全的互联网

北京知道创宇信息技术股份有限公司
www.knownsec.com