网宿科技
WANGSU.COM

2020 上半年

CHINA INTERNET SECURITY REPORT

中国互联网安全报告

目录

第一章
本期报告概览与要点

- 本期报告将从攻击量、攻击方式、攻击来源、行业分布等维度对各类攻击进行详细解读。
- 从相关的数据中可以看出，2020年的新冠疫情对网络攻击趋势产生了一定影响，很多攻击数据呈现出与疫情发展趋势相匹配的特征。

1.1. 2020年上半年Web应用攻击概览与趋势

- 今年上半年，网宿云安全平台共监测并拦截Web应用攻击42.24亿次，同比增长异常显著，为去年同期的9倍。
- Web攻击手段自动化趋势显著，超90%攻击流量来源于自动化的扫描器。暴力破解依然为最主要的Web应用攻击手段，SQL注入紧随其后。
- 政府机构成为Web应用攻击的最主要目标，上半年遭受Web应用攻击超过10亿次，占比26.29%，安全形势严峻。

1.2. 2020年上半年DDoS攻击概览与趋势

- 今年上半年，网宿云安全平台监测并拦截的DDoS攻击事件次数同比剧增147.63%，但攻击规模有所下降。
- 反射放大攻击依然是最常用的DDoS攻击方式之一。
- 由于疫情期间网上课堂的大规模应用，上半年教育行业紧随零售和游戏，共同成为遭受DDoS攻击峰值最大的三个行业。

1.3. 2020年上半年恶意爬虫攻击概览与趋势

- 今年上半年，网宿云安全平台共监测并拦截了103.77多亿次恶意爬虫攻击，平均每秒发生660起攻击，比起2019年同期数据几乎翻了一番。
- 从攻击源分布来看，恶意爬虫流量绝大多数来自国内；来自海外的攻击同比减少；海外攻击源主要分布于美国、英国、韩国等国家。
- 从国内爬虫流量的区域分布看，主要来自云南、江苏、浙江等地。
- 电子制造与软件信息服务为遭受恶意爬虫攻击最严重的行业，其次是电子商务、零售、政府机构、游戏。受疫情影响，交通运输业遭受的爬虫攻击量大幅下降。

1.4. 2020年上半年API攻击概览与趋势

- 今年上半年，网宿云安全平台共监测并拦截21.20亿次针对API业务的攻击，为2019年同期的1.28倍，增长明显。
- 恶意爬虫依然是API攻击中最主要的攻击方式，占整体攻击数量的74.82%，这一占比较去年同期有所下降；其次是SQL注入（10.94%）、非法请求（5.97%）、暴力破解（5.69%）。其中SQL注入攻击相比去年同期增长了近10个百分点，增长显著。
- 绝大多数的API攻击集中在政府机构和电子商务行业，占比分别为60.94%和26.44%。

1.5. 2020年上半年企业主机安全概览与趋势

- 开放端口易遭暴力破解攻击，Web服务端口、管理端口、数据库端口、存在高危漏洞的组件及流行应用端口均是频繁遭受网络攻击的端口类型。其中，超过7成的攻击集中在80端口和1433端口。
- 安全基线检测显示，企业用户几乎不修改操作系统默认的安全设置，导致存在大量不安全配置；只有少数用户会对不合规项进行安全加固，企业用户总体的安全意识薄弱。
- 因挖矿产业变现快、难追踪，挖矿病毒已成为最主要的主机安全威胁之一，86.73%的入侵主机中检测出挖矿病毒。
- 超95%的入侵主机中发现持久化攻击手段，包括定时任务、植入后门、隐藏进程等，多种方式结合使用，达到保障恶意进程持久运行、维持控制权限的目的。

第二章
Web应用攻击数据解读

2.1. 上半年Web应用攻击次数同比激增超800%

2020年上半年，网宿平台共监测并拦截Web应用攻击42.24亿次，为2019年同期的9倍，攻击数量呈爆发式增长。

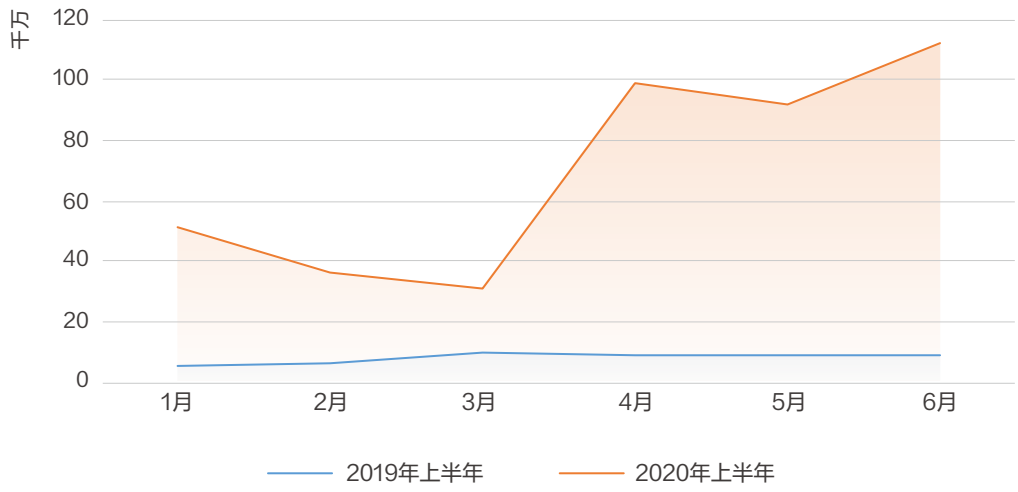

图2-1 2019与2020上半年Web应用攻击次数月份分布

从每月的攻击量分布来看，从4月份起，攻击数量有了非常明显的增长。这与国内新冠疫情得到控制，正常的生产生活逐步恢复的时间点一致。

2.2. Web攻击手段更加自动化，超90%攻击流量来自扫描器

根据网宿平台所构建的Web攻击防护体系，针对不同的攻击手段有不同的防护方式来应对，这一数据直观反映出Web应用攻击分布情况。

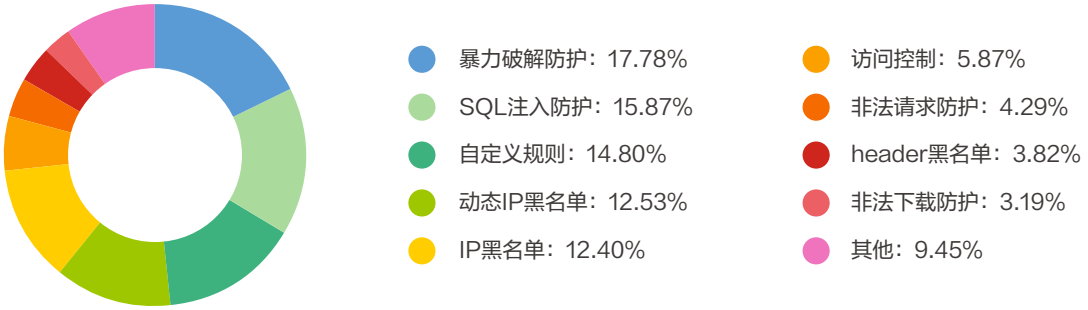

图2-2 2020上半年Web应用攻防手段分布

2020年上半年，暴力破解、SQL注入攻击依然是最主要的攻击方式，暴力破解攻击事件占据全网Web应用攻击的17.78%，排行第一；SQL注入攻击事件占比15.87%，以不到2%之差排名第二。

网宿云安全平台识别到，超过90%的Web攻击流量均来源于自动化的扫描器。攻击者通过扫描器嗅探出Web网站存在的漏洞，从而针对漏洞发起攻击，被扫描出存在大量漏洞的网站则更容易成为攻击者的目标。

网宿云安全平台通过对攻击源的特征分析、行为模式识别、AI模型检测、威胁情报等方式识别Web扫描器，继而通过动态IP黑名单（12.53%）、访问控制（5.87%）等方式直接过滤掉大量攻击，能够有效降低网站被针对性攻击的概率，同时降低自动化扫描器对网站的负载压力。

2.3. 超9成攻击源来自中国大陆地区

通过对攻击IP的地理位置分析发现，2020年上半年全球攻击来源主要集中在中国大陆，占比高达90.91%，较2019年同期有明显的增长。

进一步分析攻击来源在中国大陆的省份分布，2020年上半年，广东、江苏、浙江依然是国内攻击源分布较为集中的省份，分别占比为9.96%、9.68%、9.39%。

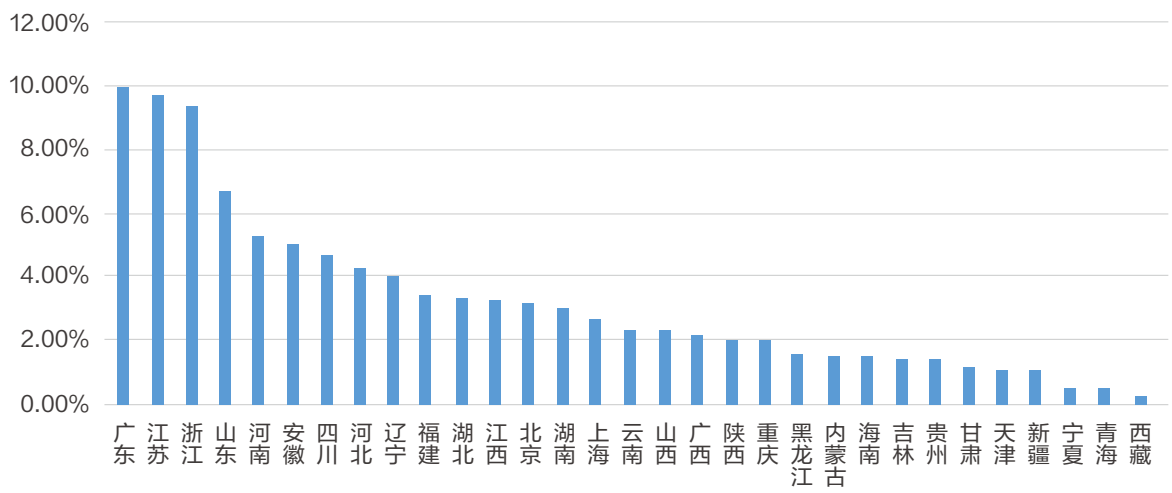

图2-3 2020上半年来自中国大陆的Web应用攻击来源分布

从海外地区攻击来源的分布情况看，前三位是印度、英国、菲律宾，分别占比35.46%、22.87%、15.83%。

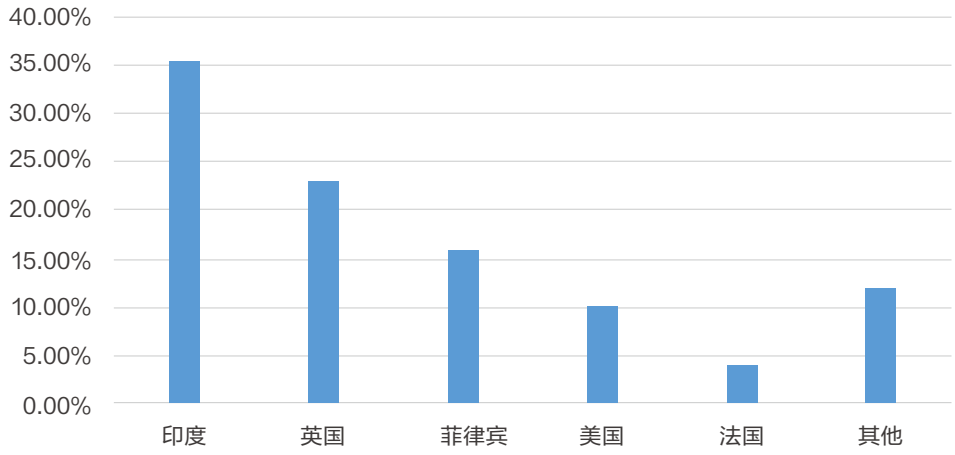

图2-4 2020上半年来自海外地区的Web应用攻击来源分布

2.4. 上半年政府机构遭受Web应用攻击超10亿次

2020年上半年，近50%的Web应用攻击集中在政府机构和零售业。其中，政府机构成为2020年遭受Web攻击最多的行业，占比26.29%；零售业位居第二，占比23.23%。

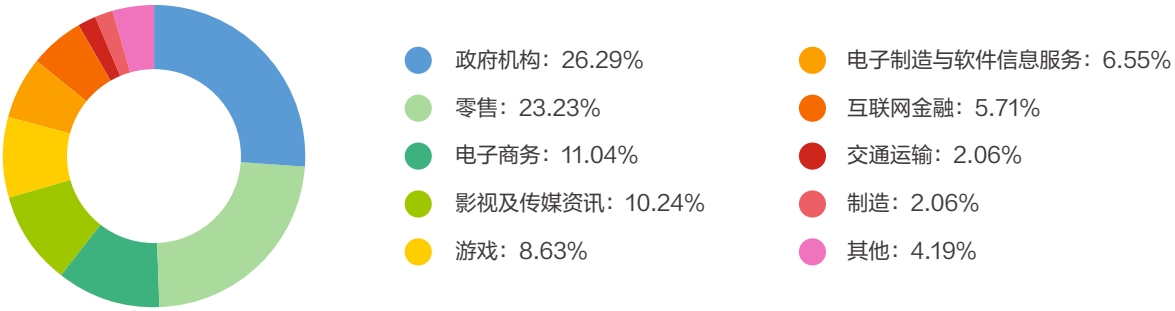

图2-5 2020上半年Web应用攻击行业分布

除了政府机构、零售行业外，电商、影视及传媒资讯也排名居前，从近几年数据看，这些行业持续成为Web攻击的重点。

其中，政府机构已经连续多年位列遭受Web应用攻击最多的行业。伴随着政府数字化转型升级、政务上云成为大趋势，越来越多的政府机构将系统从内网迁移到公网，各地政务云也呈快速发展之势，由此让黑客有了更多的攻击目标。

与此同时，随着网络安全法的实施，政府机构对安全的重视也不断提升，但由于政务上云的速度仍然快于政府机构安全体系建设的步伐，并且电子政务系统往往包含着诸多重要敏感数据，因此针对政府机构的网络攻击未来还将持续。

从攻击次数来看，上半年政府机构所承受的Web攻击次数超过10亿次，也是受攻击次数唯一超过10亿次的行业，这意味着政府机构所面临的Web应用攻击形势异常严峻，需加大安全防护力度，避免网络安全事故的出现。

第三章
DDoS攻击数据解读

3.1. 上半年DDoS攻击事件相比去年同期呈翻倍增长态势

2020年上半年，网宿云安全平台所监测到的DDoS攻击事件数量呈现翻倍增长态势，同比增长了147.63%，可见DDoS攻击并没有因为今年疫情的发生而减少。

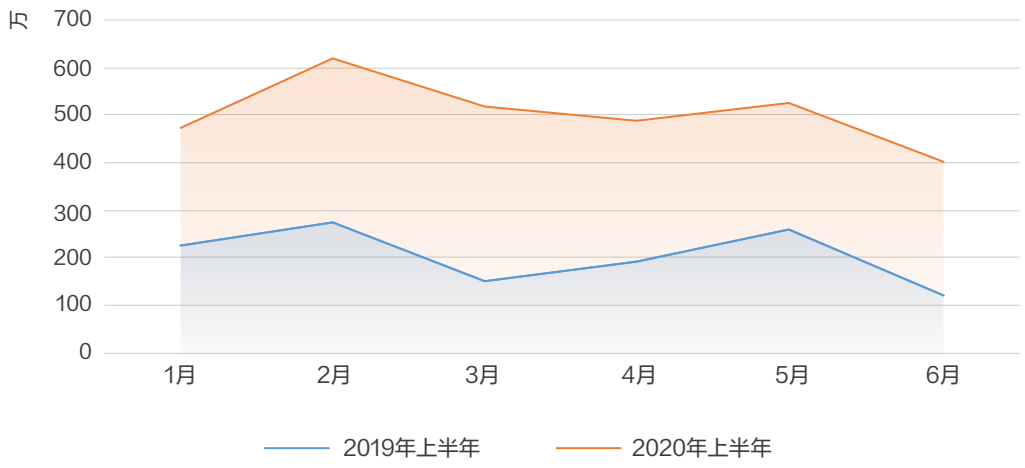

图3-1 2019与2020上半年DDoS攻击事件次数月份分布

3.2. 受疫情影响，上半年DDoS攻击规模有所下降

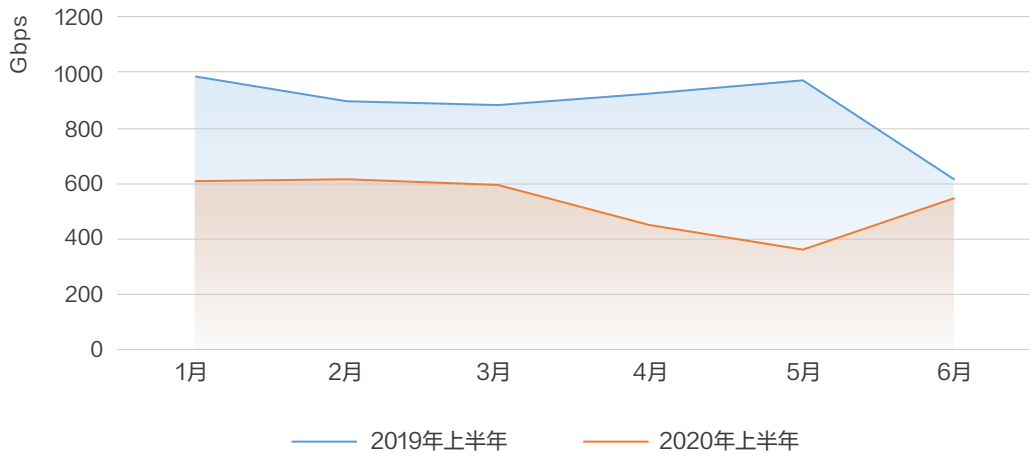

图3-2 2019与2020上半年DDoS攻击峰值月份分布

与去年同期相比，今年上半年每月的攻击峰值有所下降，主要有两方面原因：

- 一方面，疫情期间有些“肉鸡”没有上线，对攻击者而言可利用的攻击源数量有所下降。
- 另一方面，今年上半年在线教育、远程办公在疫情背景下高速发展，大量公司与资本涌入。这些公司的业务在高速增长的同时，网络安全防护没有及时跟上。加上这些行业本身流量负载高，对流量攻击较为敏感，较低强度的攻击即可产生巨大的攻击效果，也使得攻击规模有所减小。

3.3. 影视及传媒资讯、零售、游戏是上半年DDoS攻击重灾区

从DDoS攻击事件的行业分布来看，影视及传媒资讯行业成为2020上半年受DDoS攻击数量占比最多的行业，达41.78%。零售（26.63%）和游戏行业（15.22%）紧随其后，分别占据第二、三位。

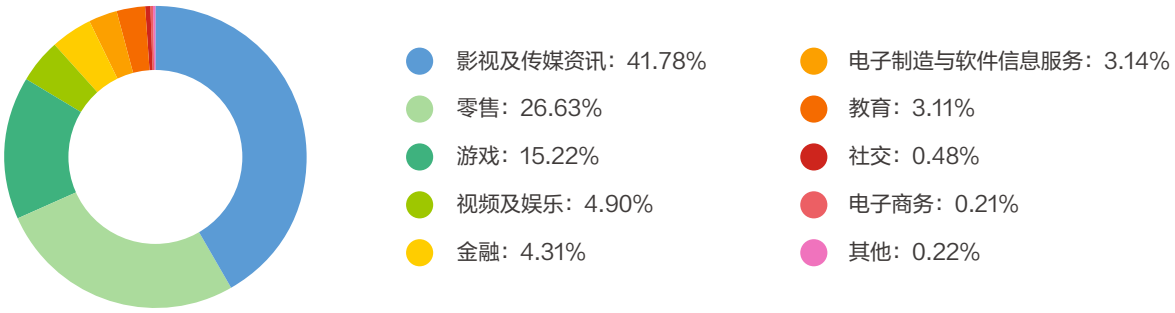

图3-3 2020上半年DDoS攻击行业分布

从各行业遭受的攻击峰值来看，零售、游戏、教育是峰值最大的三个行业，均在500Gbps左右。紧随其后的是影视及传媒资讯、视频及娱乐行业。

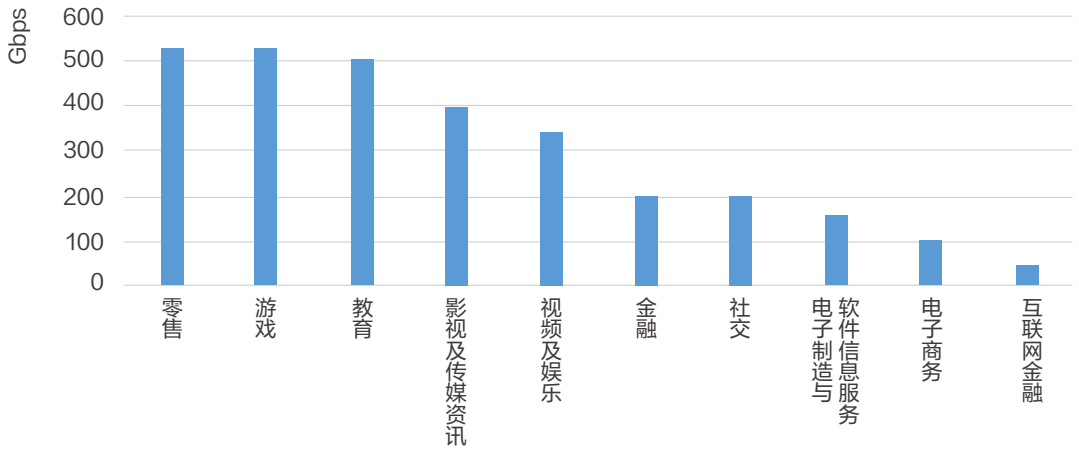

图3-4 2020上半年DDoS攻击峰值Top 10行业

与往年情况相同，零售、游戏行业在今年上半年依然遭受了高强度的DDoS攻击。而在线教育行业因疫情原因，迎来爆发式增长，针对教育行业的DDoS攻击峰值也随之迅速上升至第三位。

这也解释了为何在上半年全民在线上课期间，不少在线教育平台发生掉线、卡顿等现象：除了瞬间增长的用户量以外，DDoS攻击也是造成在线教育平台崩溃的一大原因。

与直播行业类似，在线教育行业对DDoS攻击比较敏感，该行业本身流量负载较高，用户对卡顿、延时的容忍度低。因此，在平台业务迅速增长期间，DDoS攻击更容易以较小的攻击体量对平台造成较强的破坏，成为影响在线教育平台使用体验的主要原因。

3.4. 反射放大攻击是最常用的攻击方式之一

反射放大攻击依然是攻击者发起DDoS攻击常用的方式之一。其中，绝大多数反射放大攻击是利用SSDP协议发起的，占比达到68.01%。

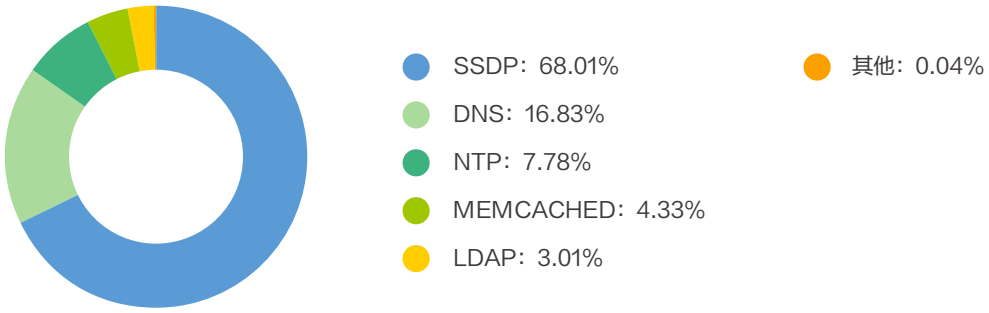

图3-5 2020上半年反射放大攻击协议分布

SSDP反射放大攻击的崛起，与物联网和智能设备的快速发展和普及有关。越来越多的智能设备联入了互联网，但这些设备的安全情况却不容乐观。很多设备将不必要的服务端口直接暴露在公网，没有做任何的访问控制。因此，当SSDP等相关的协议漏洞被曝光之后，就有攻击者利用这些协议来发起反射放大攻击，对攻击目标造成严重伤害。

DNS和NTP作为常用的反射放大攻击协议，分别排在第二位和第三位，占比分别为16.83%以及7.78%。而前几年曝光的Memcached反射放大攻击漏洞也依然被不少攻击者使用。

第四章
恶意爬虫攻击数据解读

4.1. 恶意爬虫攻击次数几近翻番

2020年上半年网宿云安全平台共监测并拦截了103.77亿次爬虫攻击，平均每秒发生660起攻击，为2019年同期的1.97倍，增长明显。

恶意爬虫攻击的月份分布数据，则直接地反映出疫情对生产生活的影响。从3月份开始，复工复产逐步推进，爬虫攻击数量呈现出非常明显的上升趋势。

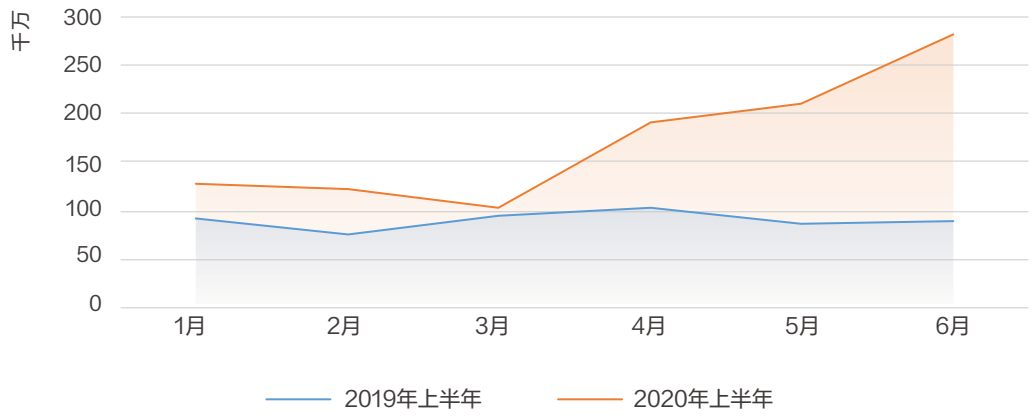

图4-1 2019与2020上半年恶意爬虫攻击次数月份分布

4.2. 合法性验证有效拦截超半数攻击

网宿云安全平台集成各种防护算法来构建恶意爬虫防护体系，从攻防数据中可以直观评估恶意爬虫攻击方式的演进趋势与防护效果。

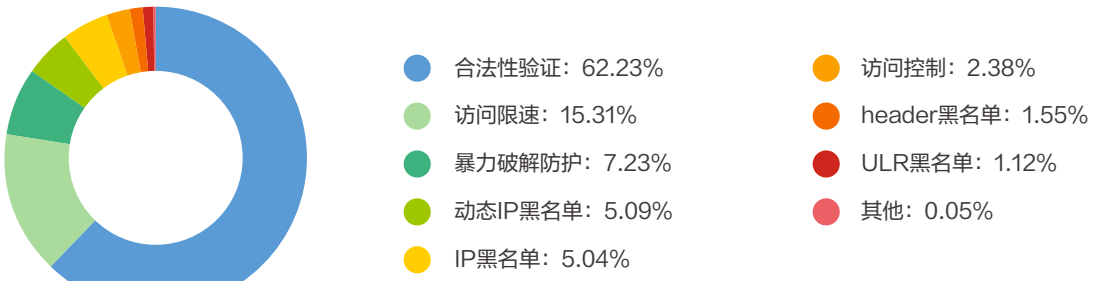

图4-2 2020上半年恶意爬虫攻防类型分布

从上半年的攻防数据中可以看出，客户端及其请求的合法性验证依然是对付恶意爬虫的最有效手段，能够过滤掉超过60%的攻击。

其次，访问限速拦截了15.31%的恶意爬虫攻击，占比第二。

4.3. 恶意爬虫攻击源超9成来自国内

从网宿云安全平台监测并拦截的源IP分布来看，2020年上半年的恶意爬虫攻击中超过九成来自于国内，来源于海外的攻击有所减少，只占到7.08%，同比下降6个百分点。

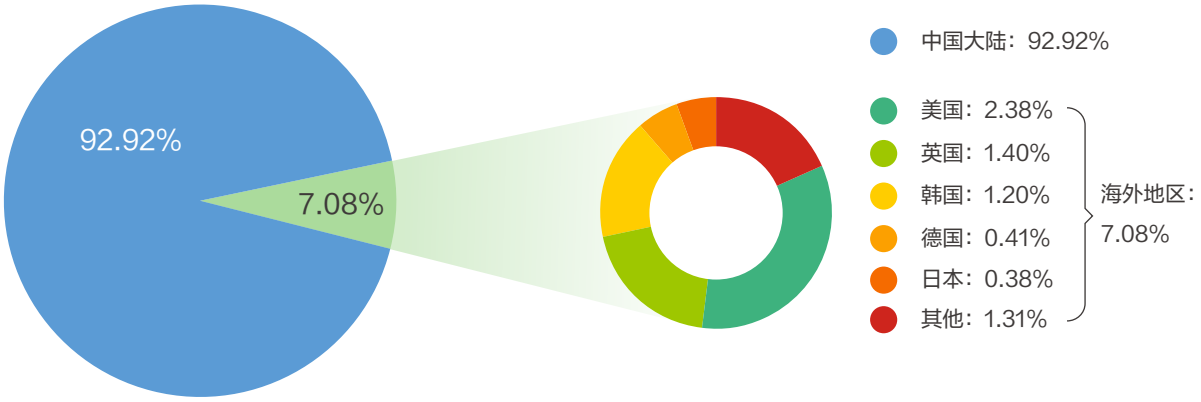

图4-3 2020上半年恶意爬虫攻击全球来源分布

海外爬虫攻击占比下降与疫情、国际关系变化、信息管制更为严格等多方面因素有关。受疫情、国际关系、政策法规影响，代购、海淘等行业遭受巨大的冲击，许多商品流通周期变长，甚至无法过关，海外商家通过爬取竞争对手的商品、价格等信息进行销售策略分析的需求降低，因此源于海外的爬虫攻击相应的减少。

同时国家政策法规对代理软件的管制更为严格，海外代理速度下降、稳定性降低且随时面临被禁封的风险，爬虫使用海外代理的成本大幅度上升。成本高、速度慢导致国内的爬虫攻击者更多地使用国内IP池。

从国内的数据来看，来自云南、江苏、浙江的恶意爬虫攻击分别为10.19%、9.03%、8.62%，成为攻击来源IP最多的三个省份。

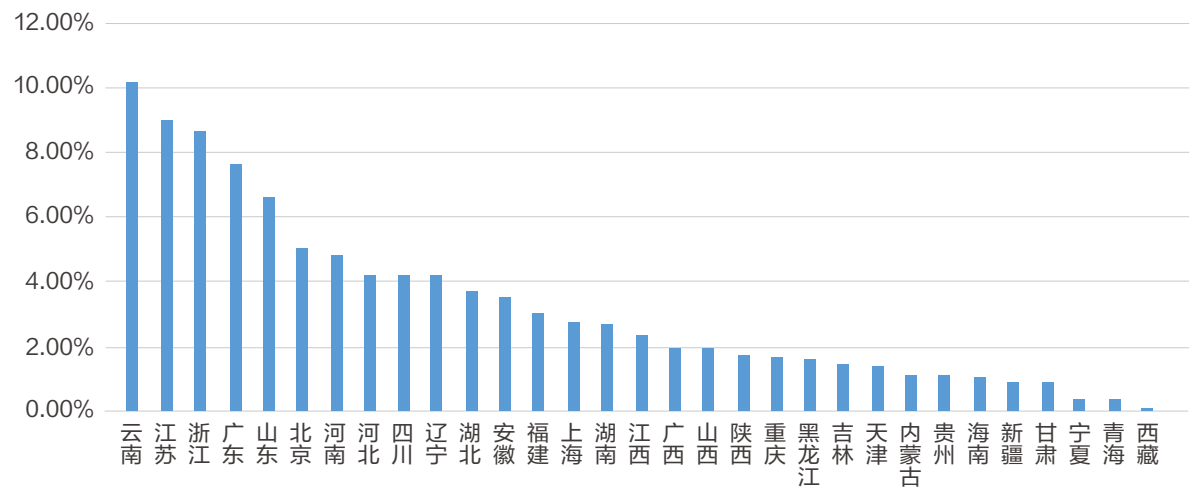

图4-4 2020上半年来自中国大陆的恶意爬虫攻击来源分布

4.4. 受疫情影响，交通运输业受爬虫攻击量显著下降

今年上半年，电子制造与软件信息服务行业成为受恶意爬虫攻击最严重的行业，其受到的爬虫攻击占到总数的29.28%。其次是电子商务（17.43%）、零售（13.12%）、政府机构（12.42%）、游戏（12.19%），这些行业的占比都超过了10%。

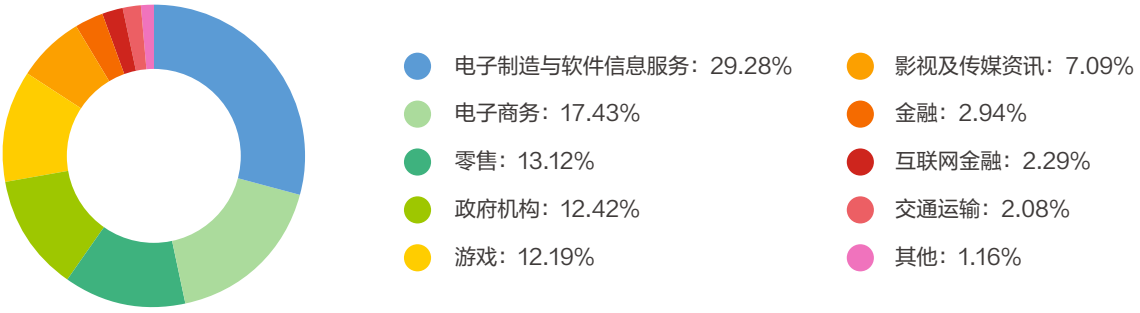

图4-5 2020上半年恶意爬虫攻击行业分布

爬虫攻击与经济利益密切相关，各行业的爬虫攻击强度与行业发展呈正相关关系，行业发展越蓬勃，相关爬虫攻击越频繁。

往年1-4月份是返乡、旅游出行、返工的高峰期，全国在短时间内面临着几亿人次的人员流动。今年受疫情影响，各省市执行严格的交通管制与居家隔离措施，冻结了大部分的人员流动，因此旅游、出行等交通运输相关行业业务断崖式下滑，今年1-4月份交通运输行业爬虫数量下降明显；复工复产阶段，全国各地区采取逐步开放的方式，出行时间分布相对均匀，与往年相比缺少高峰期，票源没有出现紧张的情况，因此抢票类爬虫攻击与往年相比也大幅度下降。

与交通运输行业相反的是，在疫情期间，电商、零售行业的线上业务受冲击较小，民众的依赖性较大。因此从数据上看，这些行业所遭受的恶意爬虫攻击较为集中。

第五章
API攻击数据解读

5.1. 上半年API攻击超20亿次，同比增长近3成

在互联网、大数据浪潮下，API的应用已经十分广泛，开放式的API虽然为各类互联网产品的发展提供了便利，但也极易成为被攻击的目标。

2020年上半年，网宿云安全平台共监测并拦截21.20亿次针对API业务的攻击，同比增长28.23%。从每个月的攻击量分布情况看，3月到4月期间API攻击出现飙升，同样与复产复工的节奏同步。

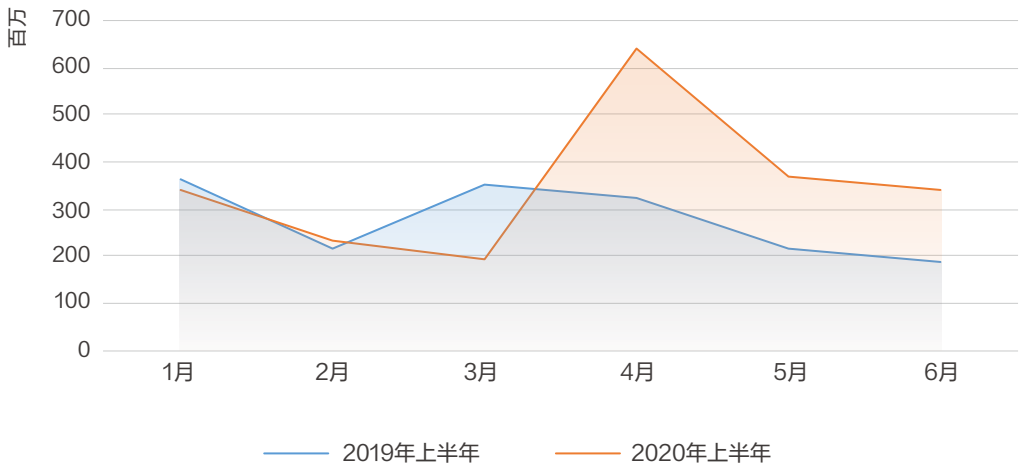

图5-1 2019与2020上半年API业务攻击次数月份分布

5.2. 恶意爬虫攻击占比有所下降，SQL注入攻击增长显著

在2020年上半年的API攻击数据中，恶意爬虫攻击占整体攻击数量的74.82%，虽与去年同期相比下降约16个百分点，仍牢牢占据统治地位。分列二、三位的是SQL注入（10.94%）和非法请求（5.97%）。其中，SQL注入较去年同期（1.55%）增长显著。

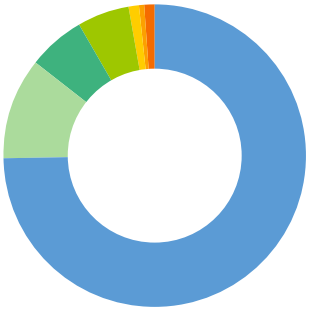

图5-2 2020上半年API攻击方式分布

5.3. 近9成攻击聚焦在政府机构和电商行业

2020年上半年，政府机构承受的API攻击占比达到了60.94%，较2019年同期的47.00%增长约14个百分点；其次，电子商务占比为26.44%，排名窜升至第二。去年同期以35.84%的占比位列第二位的交通运输行业，因今年疫情原因，数据呈断崖式下降，仅占3.56%。

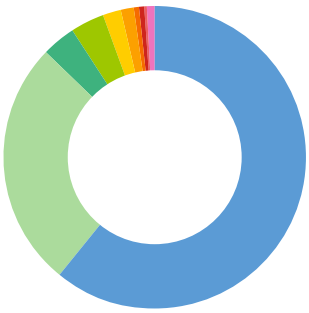

图5-3 2020上半年API攻击行业分布

政府机构及电子商务聚集了超过85%的API攻击，这与今年上半年抗疫期间，政务信息发布与在线购物在人们的生产和生活过程中起到了重要作用密不可分。

第六章
主机安全数据解读

6.1. 近90%的企业主机使用Linux系统

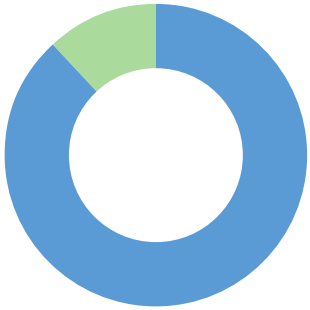

图6-1 2020上半年企业服务器系统分布

Windows和Linux是当前企业主机使用的主流系统。网宿主机安全平台统计，使用Linux系统的企业主机占88.15%，使用Windows系统的占11.85%。

Linux系统由于具有更好的兼容性与稳定性、更低的资源消耗，深受企业用户青睐。而使用Windows系统的企业，主机数量规模大多较小。在运维管理上，Linux更适合于大批量自动化管理。

6.2. 80端口、1433端口遭受攻击最为频繁

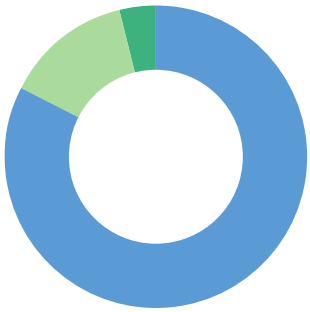

图6-2 2020上半年Linux服务器端口开放情况

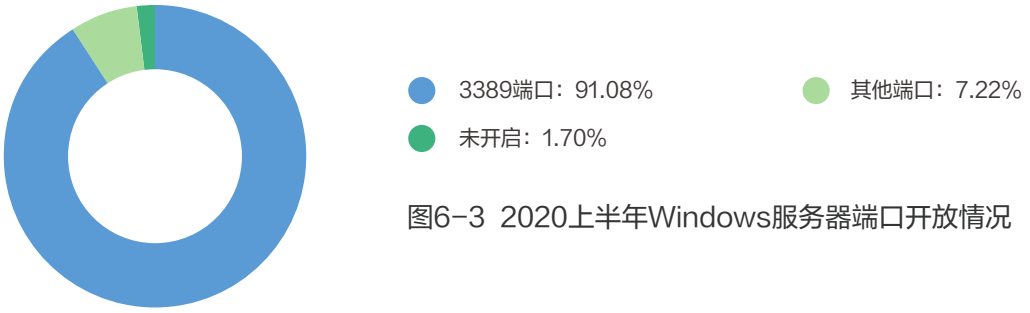

图6-3 2020上半年Windows服务器端口开放情况

基于网宿主机探针采集到的本地端口数据分析，Linux系统下82.71%的主机开启了SSHD远程管理，并且使用默认的22端口，对外提供服务。Windows系统下91.08%的主机开启了RDP远程管理，并使用默认的3389端口，对外提供服务。开放管理端口容易遭受暴力破解攻击，通过修改默认端口，限制访问IP等方式能够有效缓解暴力破解攻击。

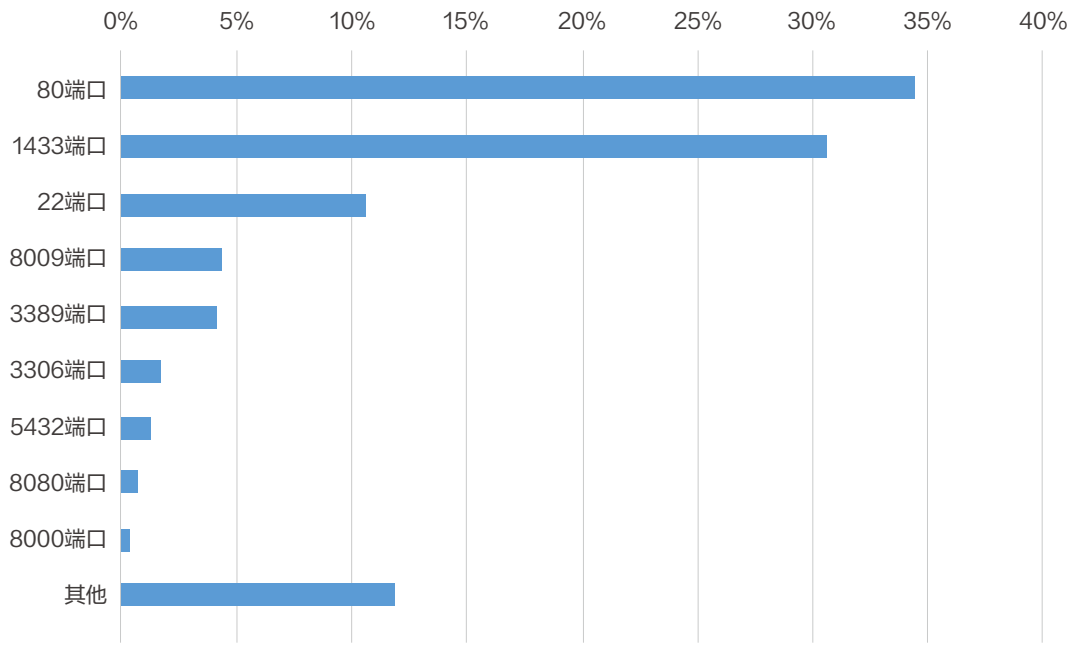

图6-4 2020上半年主机开放端口受攻击次数占比分布

企业网络环境下，主机开放端口通常需要再经过一层NAT映射，才能在公网进行访问。通过对一段时间内端口遭受网络攻击进行分析，发现频繁遭受攻击的主要有以下几种类型：

Web服务端口：如80端口、8080端口、8008端口等。因为Web服务需要开放到公网，并且攻击类型众多，所以这类端口遭受攻击特别频繁。

管理端口：如22端口、3389端口。这类端口一旦通过暴力破解方式入侵成功，即可直接获取控制权限。并且暴力破解自动化程度高，攻击成本低。管理端口攻击的特征是攻击类型单一、攻击频率快。

数据库端口：如1433端口、3306端口、5432端口等。数据库端口暴露在互联网上也容易遭受暴力破解攻击，并且数据库不仅类型众多，还存在许多高危漏洞，因此建议不要将数据库端口开放到互联网上。

存在高危漏洞的组件、流行应用端口：如6379端口、9001端口、7001端口等。这些端口的相关应用由于存在远程代码执行漏洞，容易结合自动化工具进行攻击，从而成为黑客攻击的重要目标。

6.3. 利用应用层组件高危漏洞是主机入侵的重要途径

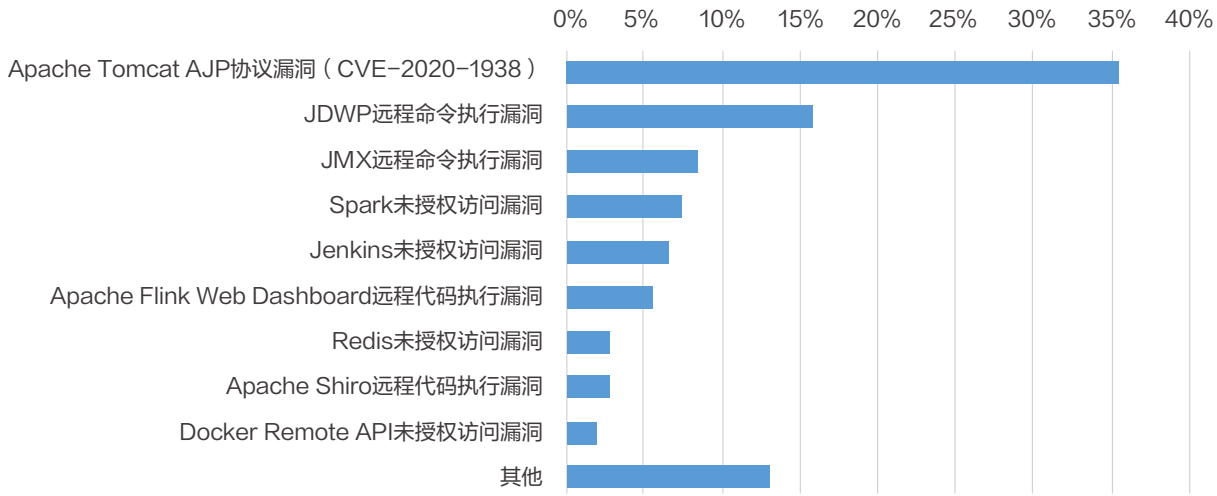

图6-5 2020上半年主机入侵主要利用的高危漏洞数量分布

根据网宿主机探针采集的流行应用、容器、组件漏洞数据，结合入侵溯源分析发现，应用层组件高危漏洞已成为主机入侵的重要途径。与操作系统漏洞相比，应用层组件更多地暴露在互联网上，能够直接被远程攻击，并且存在比操作系统更多的远程执行漏洞。与Web业务应用漏洞相比，组件漏洞的通用性更强、使用面更广泛，攻击者无需针对Web业务应用进行漏洞挖掘，组件漏洞结合自动化工具，更容易组成自动化“肉鸡”控制、自动化挖矿等黑产工具链。

随着大数据技术的发展，越来越多的企业开始应用大数据技术。许多大数据组件都提供自动化管理API，这些API提供了许多文件操作、命令执行功能，但企业在使用的过程中往往会忽视这些功能的安全使用规范，如随意地将API开放到公网、使用默认的账号密码等，造成许多接口被未授权访问入侵。在对入侵主机进行溯源分析后，发现多起由于Hadoop、Redis、Spark等组件的管理功能被利用导致的入侵事件。

6.4. 企业用户几乎不修改默认安全配置，安全加固意识薄弱

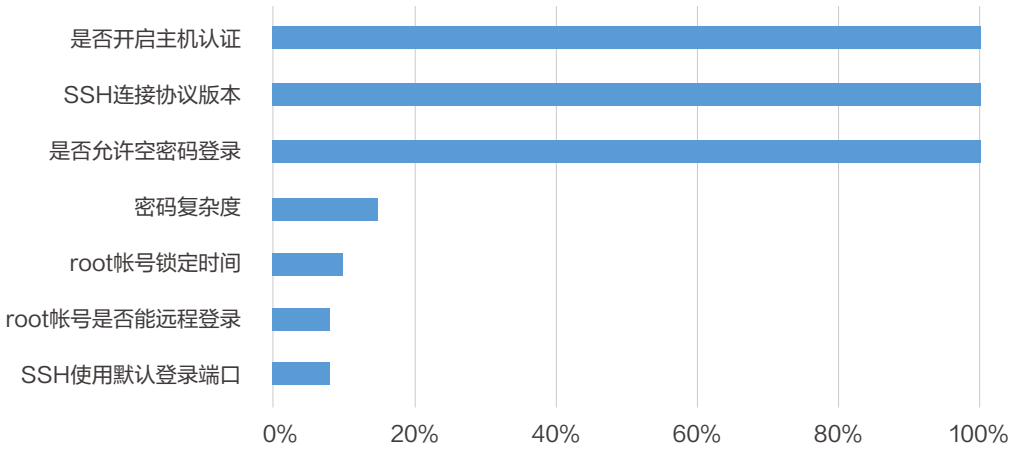

图6-6 2020上半年主机安全基线检测部分核心配置项合规率

基于风险程度，对主机安全基线的核心配置项进行抽样检测分析后发现，用户几乎没有修改操作系统默认的安全配置，合规项与不合规项的分布几乎与操作系统默认配置相同。对于操作系统默认设置的不安全配置，只有少数用户进行了安全加固。

其原因在于，其一，部分用户认为安全基线不是安全漏洞，造成入侵的可能较低。其二，也有部分用户在安全与便捷之间选择了便捷，如怕密码使用繁琐，而选择了复杂度低的密码；再比如虽然禁止root远程登录可以提高安全性，但是大部分用户依然选择直接使用root账号。除了安全意识不足意外，企业缺乏强制的安全规定也是造成主机中存在大量不安全配置的重要原因。

6.5. 异常登录IP大部分来自于海外，尤其是美国

统计数据显示，异常登录告警IP 85.42%来源于海外。但这并不代表这些入侵全部来自于境外黑客，也存在部分境内黑客为了避免被追踪溯源，会使用多层代理与海外代理服务器来登录目标主机。

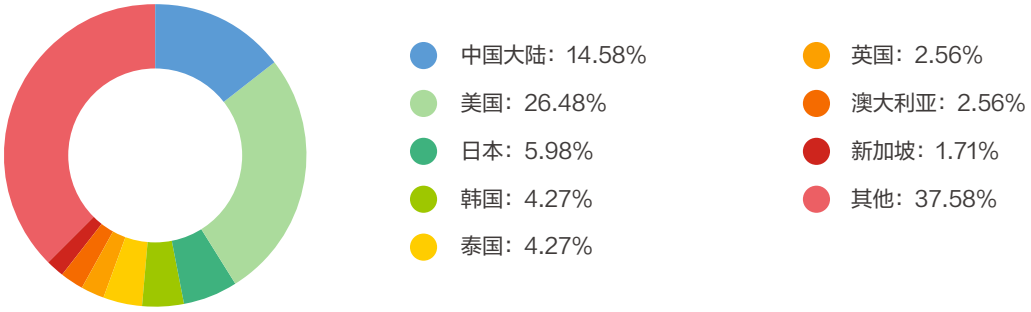

图6-7 2020上半年异常登录IP来源分布

境外异常登录IP的分布与境外代理服务器主要供应区域较为契合：从分布图中可看出，来源于美国的IP数量远超其他国家和地区，而美国恰恰拥有较多的IP资源——许多大型的云厂商、IDC厂商，这些正是代理服务器的主要来源。

6.6. 超8成入侵主机中检测出挖矿病毒

网宿主机安全平台通过对近半年入侵事件进行统计分析，发现86.73%的被入侵主机中检测出了挖矿病毒。

挖矿病毒已经成为黑客变现的主要手段。通过挖矿获取利益具有变现快、匿名化、产业链短等特点。以往黑客从入侵到变现需要较长的流程，需要成熟的团队，如DDoS需要维持大量的肉鸡，需要等待客户下单。而在区块链货币出现以后，任何一个黑客都可以通过挖矿病毒盗取他人主机的算力为自己挖矿，直接牟取利益，并且无法通过经济链路追踪入侵者的真实身份。由于挖矿病毒产业链极短，黑客能够更方便地使用工具开展自动化的入侵，包括自动化暴力破解、利用自动化远程代码执行漏洞、自动下载并执行挖矿病毒等。

网宿主机安全平台从入侵主机当中多次提取到dota家族病毒，该家族病毒已迅速发展到第3代版本，能够自动执行攻击主机、下载病毒、运行挖矿、植入后门、修改定时任务等恶意行为。

6.7. 超95%的入侵主机中发现持久化攻击手段

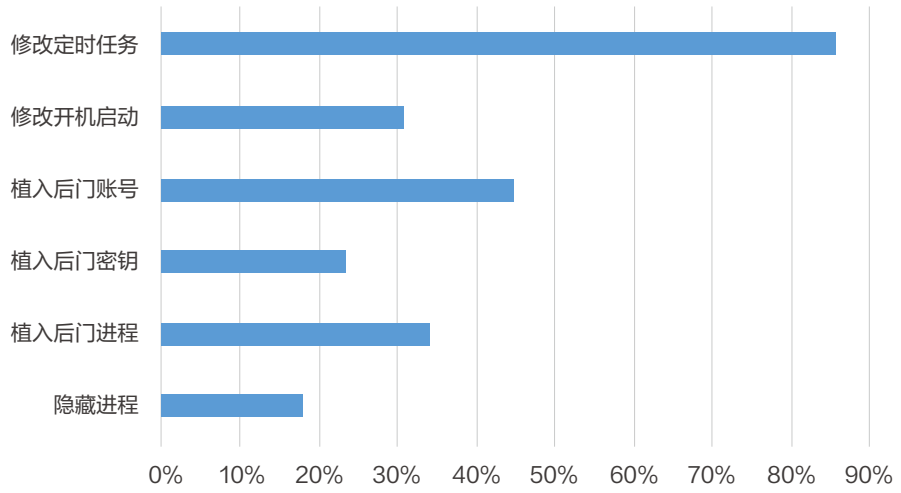

图6-8 2020上半年主机入侵持久化手段检出比例

持久化几乎是主机入侵必备的辅助手段。黑客入侵后通常会通过修改定时任务、开机启动等手段保障恶意进程的持久运行，并通过植入后门账号、后门进程等方式维持控制权限。

网宿主机安全平台在超过95%的被入侵主机中均发现了持久化行为。与传统的PC入侵相比，服务端的入侵通过修改定时任务（85.55%）维持恶意进程运行的比例要比通过修改开机启动（30.76%）的方式高得多。这是由于相比会频繁重新启动的PC，服务器为了保证业务的连续性，很少进行重启。主机入侵植入后门的方式则更为多样、更为随机，许多入侵会留下多个后门通道——后门账号、进程、密钥同时实施。普遍存在的持久化入侵行为隐蔽性强，这就要求企业提高排查分析能力，才能避免黑客通过后门再次入侵。

第七章
趋势展望及建议

基于2020年上半年网宿安全平台数据监测与安全分析，本次报告总结安全趋势如下：

- 从主机安全到网络安全，再到云安全，安全的防护边界在不断扩张，用原有安全设备和策略去应对新的安全环境难以跟上发展的脚步。5G网络、边缘计算、物联网的发展更是加速了传统安全边界被打破的速度，软件定义安全、零信任网络将是未来网络安全发展的重要趋势。
- 黑产攻击手段更加自动化、智能化，1Day漏洞、nDay漏洞、暴力破解等更为直接的攻击方式，更受黑客青睐。尤其是加密货币出现以后，自动化的攻击、入侵、挖矿工具成为最方便的牟利方式，在黑产中最为流行。
- 黑客产业链具有极高的敏感性，会快速随着目标产业景气程度的变化而变化。伴随着疫情的出现，旅游出行行业遭遇困境，线上教育、远程办公蓬勃发展，攻击流量也迅速跟着产业变化进行转移。
- 《网络安全法》实施后，安全成为企业的必选项，尤其是对拥有敏感数据的企业来说。企业可能因为没有做好安全措施，遭受攻击、入侵而被处罚；同时《网络安全法》也对一些攻击行为做了明确的定性，比如企业可以对爬虫进行溯源，进而提起诉讼，反向限制恶意攻击。《网络安全法》在要求企业加大安全投入的同时，也给企业安全防御提供了一些新思路。
- 人工智能将会在未来的网络安全中承担重要角色，黑客能够利用机器学习等技术手段掌握攻击目标的数据库规则与防护策略，从而探测网络和系统中的漏洞。同时安全厂商也逐渐将人工智能应用到策略自动化学习、实体行为分析、攻击溯源、安全检测等多个领域。未来智能对抗将会成为安全的重要战场。

针对当前的安全趋势，网宿安全团队提供一些安全建议，以供参考：

- 提升主机自身的安全性，如关闭不必要的端口，对检测到的弱口令、高危漏洞、风险配置等安全风险进行加固，做好事前防护工作，防患于未然。
- 保障安全的同时兼顾安全对服务器性能造成的影响，采用分层纵深防御原则，使用DDoS云清洗、云WAF等防护方式分担防护产生的负载，在服务器层使用轻量级检测方式作为最后一道防线。
- 针对内网业务逐渐云化，导致业务不在同一物理空间内的情况，可以考虑采用零信任网络方案，对企业网络进行合理、长期的规划。
- 企业应对《网络安全法》有更深入的了解，有助于企业在使安全建设满足法律合规要求的同时，能够应用法律武器维护自身的合法权益。

版权信息

CHINA INTERNET SECURITY REPORT