网宿科技
WANGSU.COM

2020年

CHINA INTERNET SECURITY REPORT

中国互联网安全报告

目录

第一章
报告概览与要点

- 《2020年中国互联网安全报告》由网宿科技与数世咨询联合发布。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。
- 从全年数据看，2020年爆发的新冠疫情对网络攻击的走势产生了明显影响，相关数据变化趋势与疫情发展情况相吻合。

1.1. 2020年DDoS攻击概览与趋势

2020年，网宿安全平台监测并拦截的DDoS攻击事件同比增长78.79%，但攻击规模有所下降，全年攻击走势与疫情发展态势较匹配。

- 零售和游戏行业依然是DDoS攻击重灾区，遭受的攻击事件数量与攻击峰值均位于前三。
- 由于疫情对网课模式的推动，在线教育行业迎来爆发式增长。这也招致黑产对其高度关注，在线教育行业成为遭受攻击峰值第三高的行业。
- 与物联网和智能设备相关的SSDP协议，成为攻击者发起DDoS反射放大攻击最常用的协议。

1.2. 2020年Web应用攻击概览与趋势

- 2020年，网宿安全平台所监测并拦截的Web应用攻击数量暴增，达95.24亿次，是2019年的7.4倍。其中，上半年的攻击量是上一年同期的9倍。
- 从攻击手段上看，SQL注入和暴力破解依然为主要攻击手段，二者长期占据攻击手段的前两名。
- 不论从半年的数据还是全年数据来看，政府机构都是Web应用攻击的主要目标，安全形势严峻。

1.3. 2020年恶意爬虫攻击概览与趋势

- 2020年，网宿安全平台共监测并拦截了358.54亿次爬虫攻击，平均每秒发生约1134起，攻击量是2019年攻击量的3倍。
- 从攻击源分布来看，恶意爬虫流量90%来自境内，来自海外的攻击同比减少，主要分布于韩国、英国、美国等国家。
- 境内恶意爬虫请求中，江苏、浙江、广东三省最多。
- 电子制造与软件信息服务是遭到最多恶意爬虫攻击的行业，紧随其后的分别是影视传媒资讯、电子商务、游戏行业。

1.4. 2020年API攻击概览与趋势

- 2020年，网宿安全平台一共监测并拦截47.32亿次针对API业务的攻击，为2019年同期数据的1.56倍，增长明显。
- 恶意爬虫是API攻击中最主要的攻击方式，占攻击总量的76.39%，与2019年的占比77.85%基本持平；其次是非法请求、SQL注入、暴力破解，其中SQL注入的占比相比2019年增长明显，而暴力破解有所下降。
- 过半的API攻击集中在政府机构和电子商务行业，占比分别为32.79%和21.16%。

1.5. 2020年企业主机安全概览与趋势

- 主机开放端口中，22端口、3389端口等管理端口是黑客最主要的攻击目标，从全年数据看，二者集中了46%的攻击量。
- 高危漏洞攻击越来越趋向于利用简单漏洞，未授权访问、远程代码执行类漏洞的自动化程度、工具集成程度越来越高。
- 安全基线检测显示，企业用户总体的安全意识仍然薄弱，只有少数用户会对不合规项进行安全加固。
- 与2019年相比，2020年来自境内的异常登录IP数量大幅上升，这与国际形势及国家收紧对境外IP的使用有关。

第二章
DDoS攻击数据解读

2.1. 全年DDoS攻击事件数量保持上升态势，攻击峰值整体回落

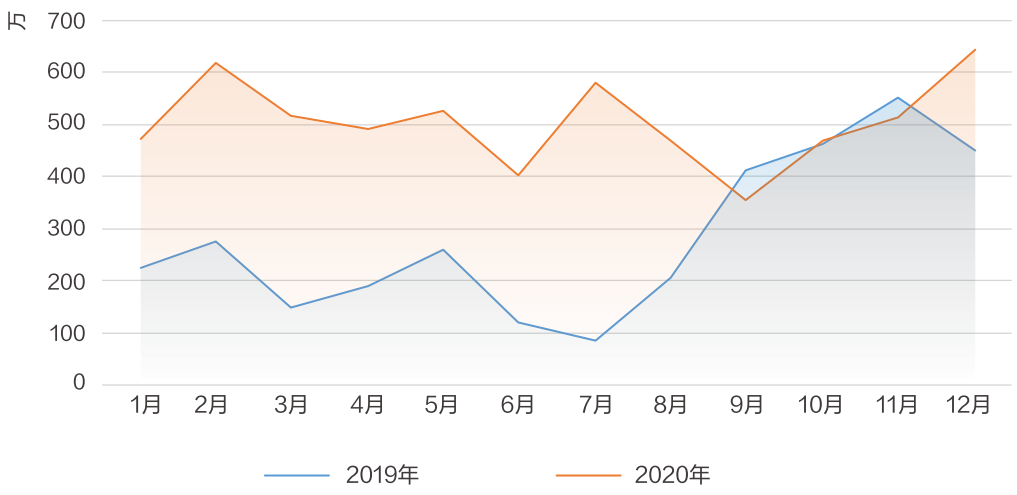

图2-1 2019与2020全年DDoS攻击事件数量趋势

2020年，网宿安全平台监测到的DDoS攻击事件数量相比往年保持了增长的态势，同比增长78.79%，相比2019年的25.76%，提升了约53个百分点，增速明显上扬。

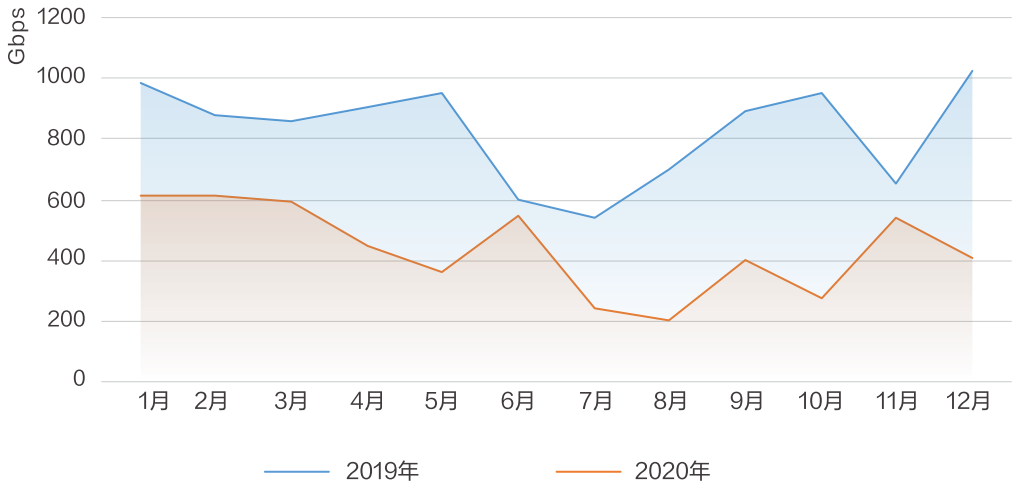

图2-2 2019与2020全年DDoS攻击峰值月份分布

全年DDoS攻击规模整体有所下降，各月份的攻击峰值均低于上年同期。

2020年DDoS攻击事件数量上升、攻击峰值却下降的原因有两个：一方面，受2020年上半年新冠疫情的爆发，下半年海外疫情的持续蔓延，全球企业工作生产受到影响，有些“肉鸡”没有上线，攻击者可利用的攻击源数量有所减少，导致打出的攻击流量下降；

另一方面，2020上半年，受新冠疫情影响，在线教育、远程办公高速发展，大量资本涌入。许多公司的IT聚焦于满足业务快速增长的要求，网络安防建设没有及时跟上。同时，在线教育、远程办公这类业务本身的用户流量就已占用了大量带宽资源，较低强度的攻击便能将其打垮，因此，攻击者无需通过发起大流量攻击即可达成目的。

2.2. 90%的DDoS攻击事件集中在视频娱乐、零售、游戏行业

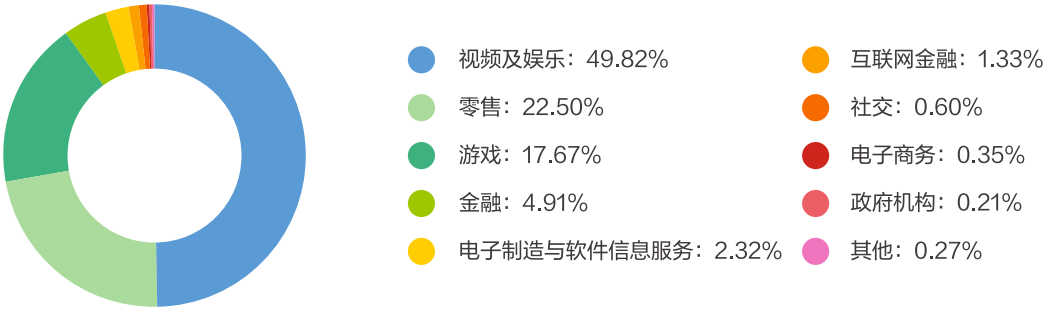

图2-3 2020年DDoS攻击事件行业分布

统计DDoS攻击事件在各行业的分布，排行前三位的视频及娱乐（49.82%）、零售（22.50%）、游戏（17.67%）所承受的攻击量占比近九成。零售和游戏行业在往年也一直都是DDoS攻击的重灾区，而视频及娱乐则在2020年吸引了约半数的DDoS攻击，位居第一。受疫情影响，线下活动受限，网民的各种云娱乐方式需求凸显，视频及娱乐领域受冲击较小，甚至迎来利好发展机会。

2.3. 各行业DDoS攻击峰值受疫情影响明显

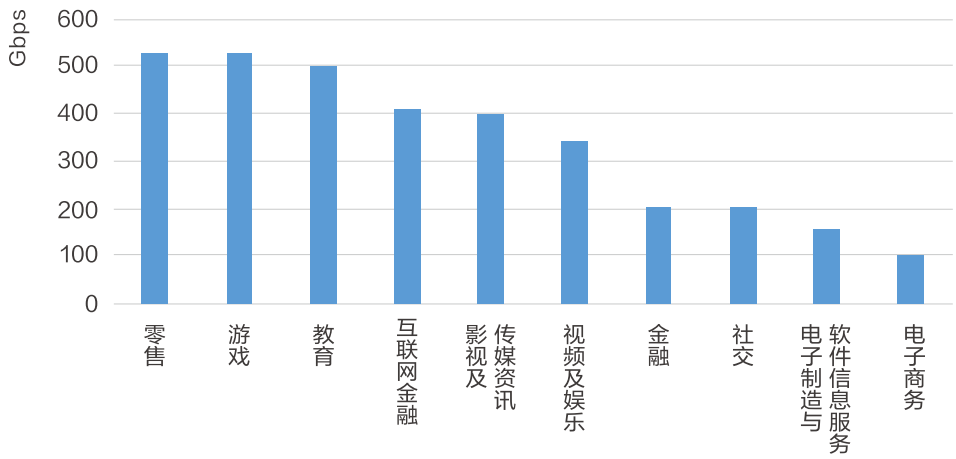

图2-4 2020年DDoS攻击峰值Top 10行业

从各行业遭受的攻击峰值来看，零售、游戏、教育行业峰值均超过了500Gbps，且均发生在上半年。

2020年，受疫情影响，在线教育行业迎来爆发式增长，针对教育行业的DDoS攻击也随之而来。虽然数量不多，但单次攻击事件的规模很大。可以预测的是，后疫情时代，在线教育模式还将继续流行普及，推动教育生态体系的变革，后期也将吸引更多的资本和服务提供商。利益驱使下，教育行业可能会出现越来越多的攻击事件。

2.4. 黑客最常利用物联网设备发起DDoS放大反射攻击

在DDoS攻击方式中，反射放大攻击只需要非常少的带宽，就可以对攻击目标产生上百倍甚至数万倍的巨大流量。这种成本低、攻击力极强且难溯源的攻击方式，极受黑客的青睐。从网宿安全平台的数据来看，反射放大攻击依然是常用的攻击方式之一，全年捕获到了大量的反射放大攻击请求。

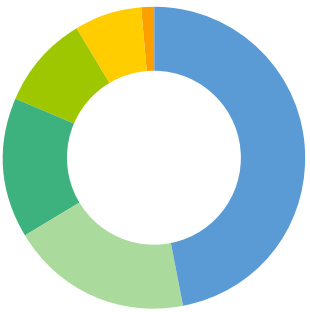

图2-5 2020年反射放大攻击协议分布

从网宿安全平台在2020年捕获到的反射放大攻击请求来看，SSDP反射放大（47.07%）仍然占据着第一位。SSDP协议主要用于感知家用路由器、网络摄像头、打印机、智能家电等物联网设备。可以预测，随着物联网和智能设备的快速发展和普及，利用智能设备展开DDoS反射放大攻击会越来越普遍。

与上半年相比，涨势明显的是LDAP反射放大攻击（15.19%），下半年的攻击次数环比上半年翻了近30倍。 Memcached反射放大攻击因其以万为单位的放大倍数，被攻击者使用的比例也在上升。

第三章
Web应用攻击数据解读

3.1. Web应用攻击量暴增，达2019年的7.4倍

2020全年网宿安全平台共监测并拦截Web应用攻击95.24亿次，为2019年的7.4倍，攻击量呈爆发式增长。其中上半年的攻击量甚至达到了2019年同期的9倍之多。

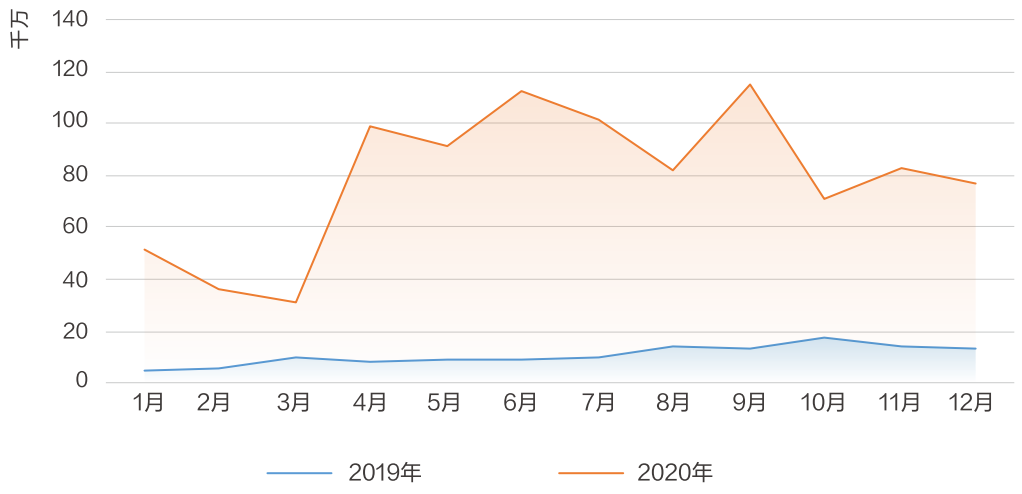

图3-1 2019与2020年Web应用攻击次数趋势

分析全年Web应用攻击数量走势，不难看出，攻击量变化态势与社会生产生活的恢复出现一定吻合。2020年3月疫情初步得到控制后，攻击量也骤然暴涨。

与Web攻击量爆发式增长相呼应，2020年全球敏感数据泄露事件数量持续高频发生，且规模及造成的影响都有明显增长。随着各行业加速数字化转型，数据的价值在进一步凸显。可以预见的是，未来以敏感数据为目标的攻击将持续增长，必然会要求各行业不断加强相关业务系统的防护。

3.2. SQL注入、暴力破解连年进入Web攻击手段Top 3

根据网宿安全平台所构建的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进行应对，从中可反映出Web应用攻击手段的分布情况。

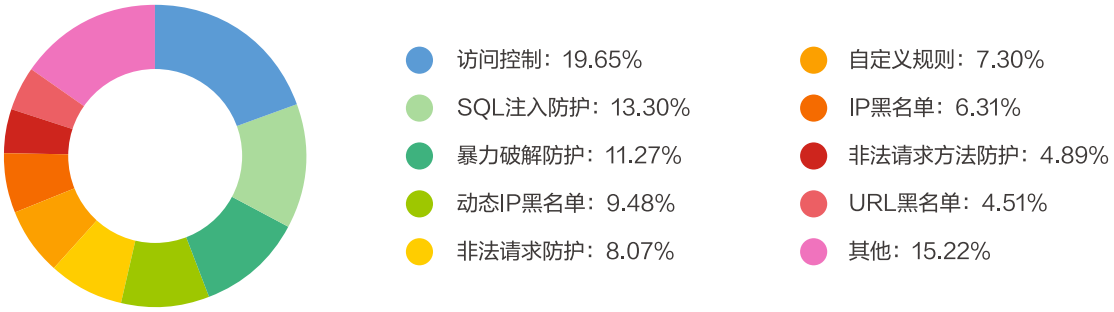

图3-2 2020年Web应用攻防手段分布情况

总体来说，Web应用攻防手段分布相对较平均。SQL注入（13.30%）和暴力破解（11.27%）在近几年的数据中始终位于Top 3之内，是较高频的攻击方式。

网宿安全平台识别到，有超过90%的Web攻击流量来源于自动化的扫描器。扫描器嗅探出Web网站存在的漏洞后，攻击者针对漏洞发起攻击。被扫描出存在大量漏洞的网站更容易成为攻击者的目标。

网宿安全平台通过攻击源的特征分析、行为模式识别、AI模型检测、威胁情报等方式识别Web扫描器，继而以访问控制（19.65%）、动态IP黑名单（9.48%）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。

3.3. Web攻击源地理分布向境内集中

分析攻击IP的地理位置，2020年全球攻击源主要集中在中国大陆，占比高达86.7%。对比2019年，源自中国大陆的攻击占比刚刚过半。可见，攻击源向境内集中的趋势显著。

这一趋势变化与近年来国家对境外IP访问控制趋严有关。境外代理成本上升，黑产团队倾向于改以境外IP作为控制源，只需少量IP，即可向境内大量攻击机器下发攻击指令，由境内机器发起直接攻击，在加大追踪难度的同时，降低成本。

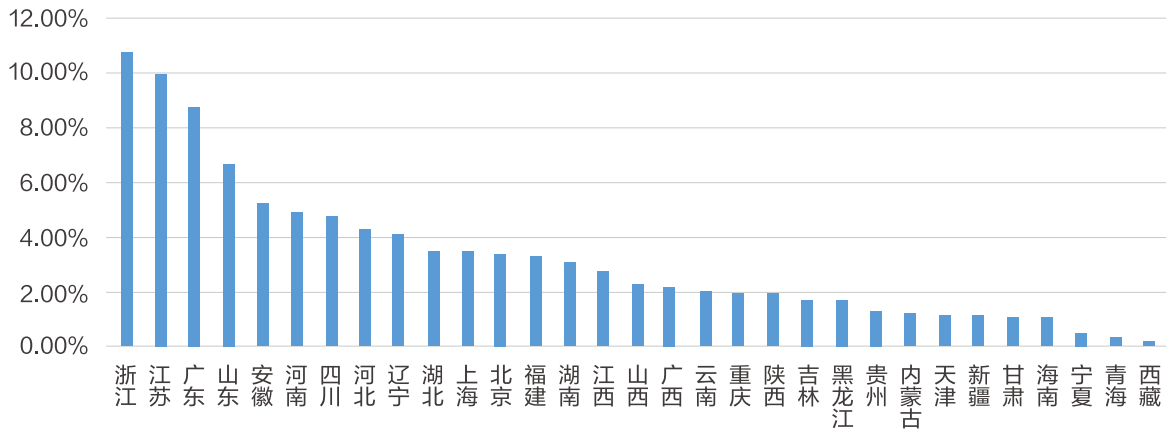

图3-3 2020年来自中国大陆的Web应用攻击来源分布

进一步分析境内攻击源，前三名依旧由浙江、江苏、广东三省占据，分别占比为10.75%、9.91%、8.71%。由于经济较为发达，这三个省份拥有更丰富的IT资源为攻击者所利用。

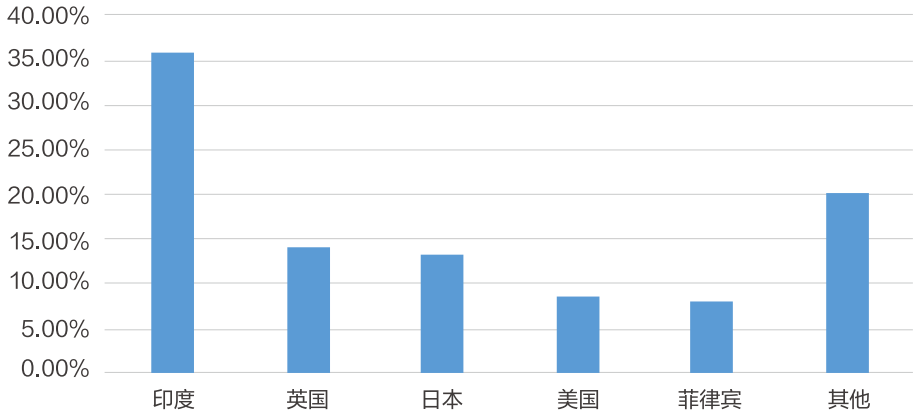

图3-4 2020年来自海外地区的Web应用攻击来源分布

统计海外攻击来源，印度、英国、日本位列前三，分别占比35.86%、14.08%、13.26%。

3.4. Web应用攻击在各个行业普遍存在

统计Web攻击的行业，不难发现分布较为平均。排行第一的政府机构占比16.36%，从排行第二的零售行业到第八的游戏行业，两两相差均只在1%左右，显示出Web攻击已经渗透于各个行业的局面。

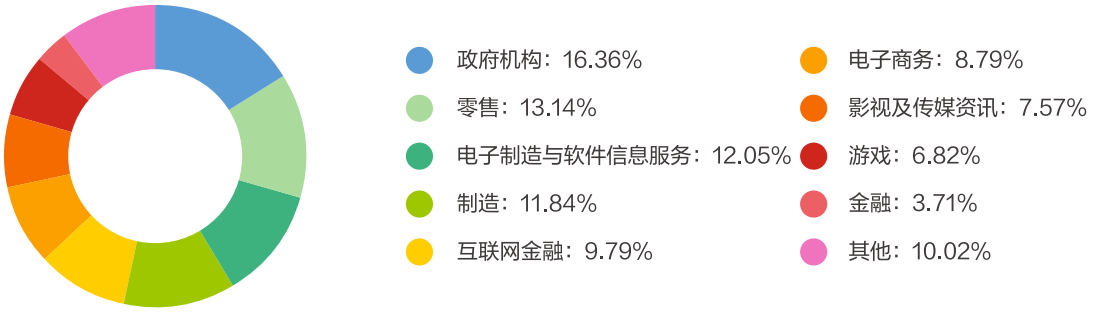

图3-5 2020年Web应用攻击行业分布

对比2019年的数据，政府机构的排行从第三升到了第一，结合2020年Web攻击数量是2019年的7.4倍，不难看出，政府机构所承受的攻击压力极大。随着政务上云，全面推进全国政务服务“一网通办”进入加速期，政务平台所保存的公民及企业的海量数据，受到黑客的垂涎。

第四章
恶意爬虫攻击数据解读

4.1. 平均每秒发生约1134次爬虫攻击

2020年网宿安全平台共监测并拦截了358.54亿次爬虫攻击请求，平均每秒1133.81次，是2019年的3倍，呈翻倍增长态势。

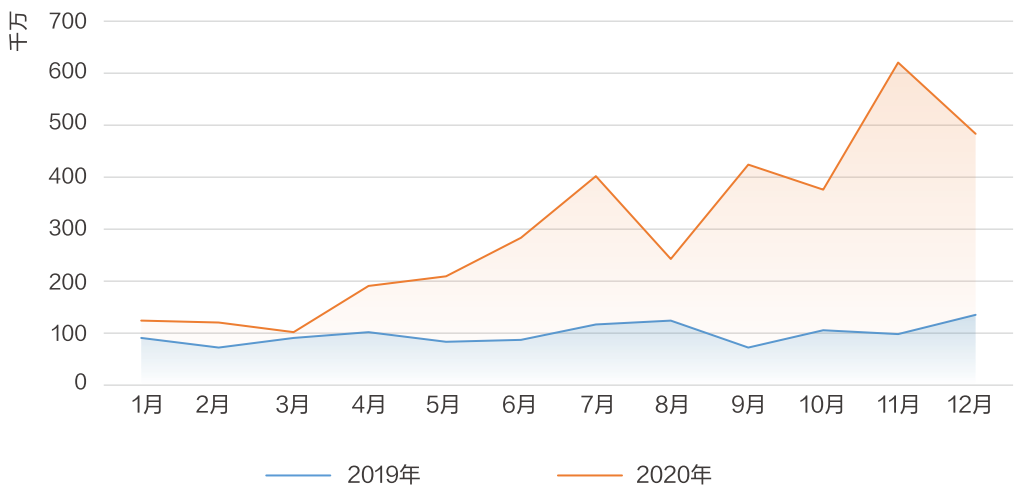

图4-1 2019与2020年恶意爬虫攻击数量趋势

从2020年间走势来看，从3月份开始，恶意爬虫攻击一路飙升。这一转折的出现几乎与复产复工逐步推进同步。

4.2. 来自海外的恶意爬虫攻击大幅下降

从网宿安全平台监测并拦截的源IP分布来看，2020年全年的恶意爬虫攻击有超过九成来自于国内，来源于海外的攻击仅占9.99%，相比2019年的占比35.28%下降了超25个百分点。

图4-2 2020年恶意爬虫攻击全球来源分布

海外爬虫数据大规模下降受新冠疫情、国际关系变化、信息管制更为严格等多种因素影响。受新冠疫情、国际关系、政策法规影响，代购、海淘等行业受到巨大冲击，许多商品流通周期变长，甚至无法过关，海外商家的数据分析需求降低，源于海外的爬虫攻击相应的减少。同时国家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，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的更换为国内IP池。

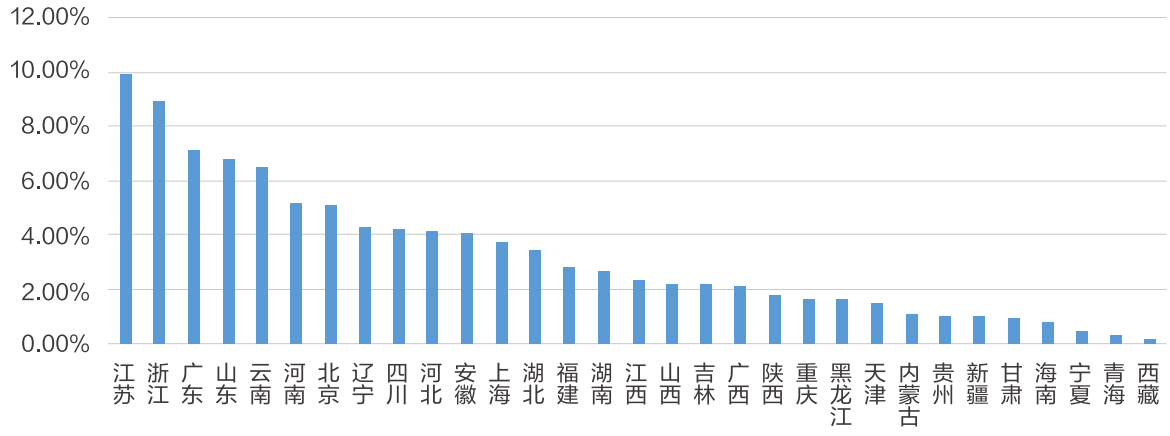

图4-3 2020年来自中国大陆的恶意爬虫攻击来源分布

从境内的数据来看，来自江苏省（9.92%）的爬虫攻击源IP超过了700万个，紧随其后的浙江（8.97%）、广东（7.15%）、山东（6.83%）三省的爬虫攻击源IP均超过了500万个。

4.3. 电子制造与软件信息服务业遭到最多爬虫攻击

从行业分布看，延续了2020上半年的情况，电子制造与软件信息服务行业继续占据第一的位置，成为全年恶意爬虫攻击最严重的行业（23.87%）。其次是影视及传媒资讯（13.26%）、电子商务（12.46%）、游戏（11.05%）、零售业（9.64%）、交通运输（8.98%）等，占比均在10%左右。

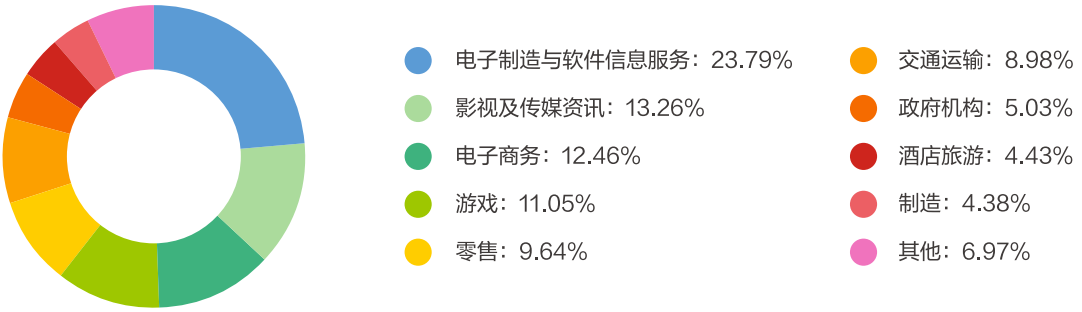

图4-4 2020年恶意爬虫攻击行业分布

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。同时，攻击强度也与目标行业公开信息数据的价值及其反爬能力有较大关系。

与往年相比，2020年1-4月份交通运输行业爬虫数量下降明显。往年1-4月份是返乡、旅游出行、返工的高峰期，短时间内全国面临着几亿人次的人员流动，车票、机票极度紧张，抢票爬虫工具盛行。而2020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，旅游、出行等交通运输相关行业业务断崖式下滑，相关爬虫也失去了攻击的意义。

但按全年数据，针对交通运输业的恶意爬虫攻击次数反倒是2019年的2.16倍，显示出在疫情得到控制，解除交通管制后，抢票类爬虫攻击迅速复苏，甚至加倍活跃的态势。

第五章
API攻击数据解读

5.1. 全年API攻击达47亿次，同比增长56%

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作为数据传输流转通道虽然为各类互联网产品的发展提供了便利，但也极容易被攻击。近年来，国内外曝出多起与API相关的数据安全事件，严重损害了相关企业、用户的合法权益。我国通信、金融、交通等多个行业已出台涉及API安全的相关规范性文件。

2020年，网宿安全平台共监测并拦截47.32亿次针对API业务的攻击，同比增长56.03%。攻击量的大幅增长显示了API业务面临的严峻安全形势。

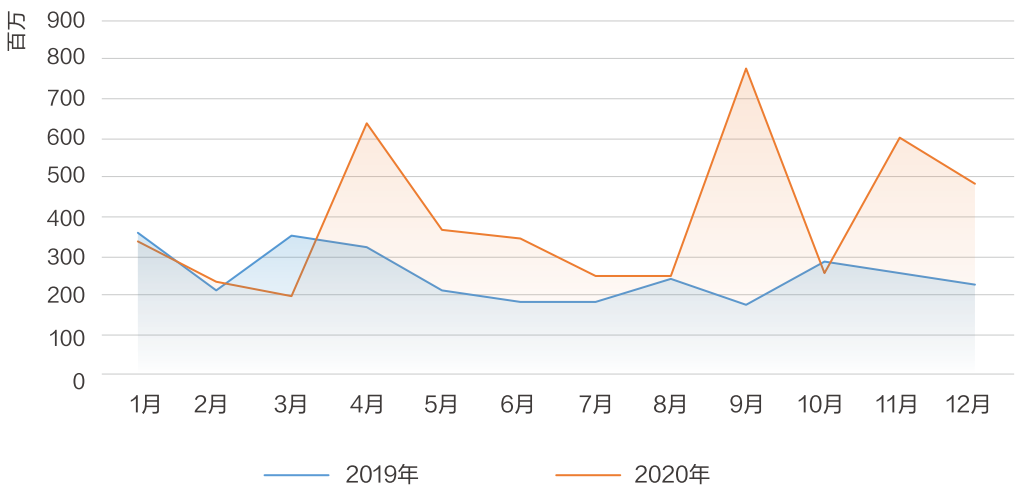

图5-1 2019与2020年API业务攻击量趋势

如图所示，2020年3-4月间及8-9月、10-11月间API攻击一度飙升。其中，3-4月的增长推测也与复工复产的展开有关。

5.2. 恶意爬虫攻击超7成，蝉联最主要API攻击方式

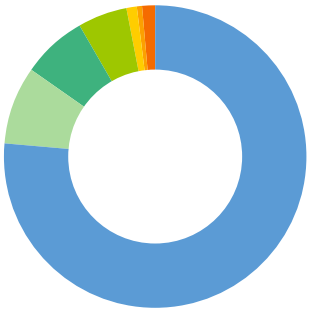

图5-2 2020年API攻击方式分布

在针对API业务发起的攻击中，恶意爬虫（76.39%）占压倒性的多数，蝉联首要攻击方式，并且占比数据与2019年基本持平。恶意爬虫能对企业开放的各类不受保护、有信息价值的API接口进行不断攻击，以达到破坏、牟利、盗取信息等目的。

位居第二、三位的是非法请求（8.36%）、SQL注入（7.10%）。暴力破解的位次从2019年的第二下降到第四，占比也从8.76%下降到5.24%。

5.3. 超5成攻击集中在政府机构和电子商务领域

图5-3 2020年API攻击行业分布

2020年，政府机构依然承受了最多的API攻击，占比达32.79%。对政府机构的攻击主要集中在上半年：上半年数据中，其攻击占比甚至超过了六成，达到了60.94%。

电子商务（21.16%）排位上升至第二。其变化与疫情期间人们的的生活方式相匹配。特别是在2020上半年，政府机构与电子商务聚集了超过85%的API攻击，这与抗疫期间政府信息发布与在线购物在人们生产生活中起到了重要作用密不可分。

2019年以近30%的占比位居第二的交通运输业，因疫情原因，在2020年数据显著下降，仅占3.38%，排行第七。

第六章
主机安全数据解读

6.1. 超90%企业主机使用Linux系统

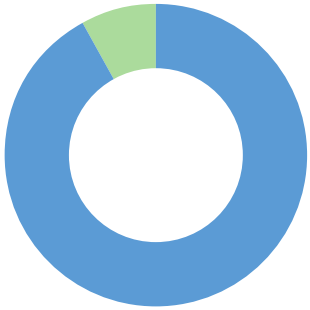

图6-1 2020企业服务器系统分布

Windows和Linux是当前企业主机使用的主流系统。网宿安全平台监测到，使用Linux系统的企业主机占91.95%，使用Windows系统的占8.05%。与2019年相比，Linux占比进一步上升。

Linux系统具有更好的兼容性与稳定性、更低的资源消耗，因而更适合大批量自动化管理。

6.2. 已有40%的企业主机使用容器技术

图6-2 2020年企业主机容器安装情况

网宿安全平台监测出，40.27%的企业主机有安装容器相关软件。容器作为一种虚拟化技术，可以让应用程序的部署和运行无视服务器是否已部署该应用程序所需的操作系统和依赖环境，大大提高部署发布效率。容器技术使用率近几年在国内快速上升，但与国外容器使用率相比，仍有较大的上升空间。

6.3. 管理端口集中了近五成攻击

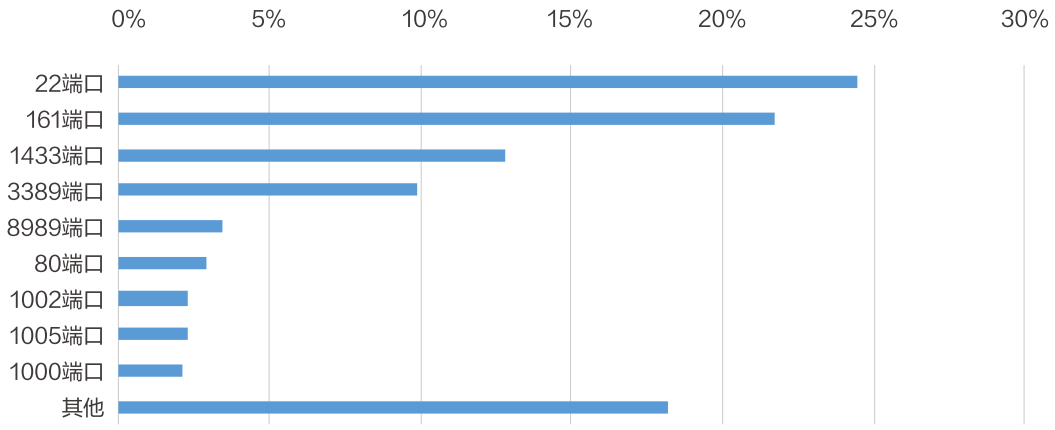

图6-3 2020年主机开放端口受攻击次数占比分布

基于网宿主机探针采集到的端口攻击数据分析，针对22、161、1433、3389端口的攻击数量最多，这些端口的主要攻击方式均为暴力破解。由于暴力破解攻击简单，自动化程度高，并且一般需要大量的尝试才能攻击成功，所以在攻击数量上遥遥领先。

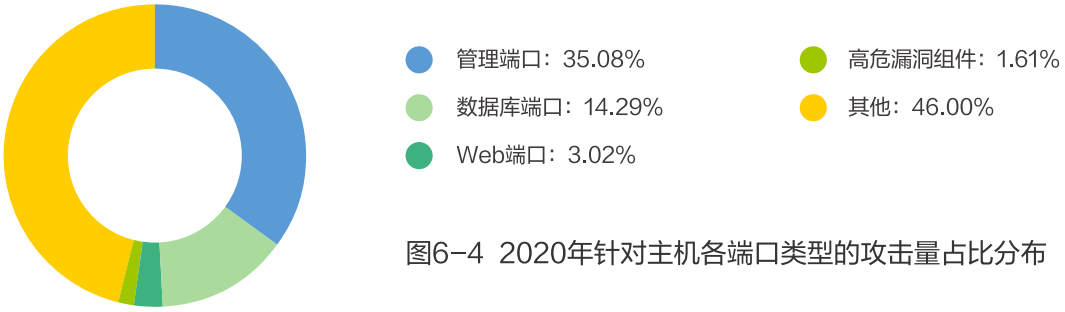

图6-4 2020年针对主机各端口类型的攻击量占比分布

按被攻击端口类型划分，管理端口被攻击的次数最多，占46.00%。其次是数据库端口（14.29%）、Web端口（3.02%）、高危漏洞组件端口（1.61%）。攻击方式越简单，自动化程度越高，并且直接获取权限越大的端口越受黑客青睐。

6.4. 高危漏洞攻击趋向于利用简单漏洞

2020年网宿主机安全平台捕获的高危漏洞Top 10

No.1	Fastjson远程代码执行漏洞
No.2	Elasticsearch未授权访问漏洞
No.3	JMX远程命令执行漏洞
No.4	Apache Struts2远程代码执行漏洞（S2-059/CVE-2019-0230）
No.5	Spark远程代码执行漏洞（CVE-2020-9480）
No.6	Druid远程代码执行漏洞
No.7	Docker Remote API未授权访问漏洞
No.8	Apache Flink Web Dashboard远程代码执行漏洞
No.9	Apache Tomcat AJP协议文件读取与包含漏洞（CVE-2020-1938）
No.10	Apache Tomcat 远程代码执行漏洞(CVE-2017-12615)

根据网宿主机探针采集的流行应用、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。

高危漏洞攻击越来越往利用简单漏洞方向增长，未授权访问、远程代码执行类漏洞的自动化程度、工具集成程度越来越高。

6.5. 企业用户的安全加固意识仍然薄弱

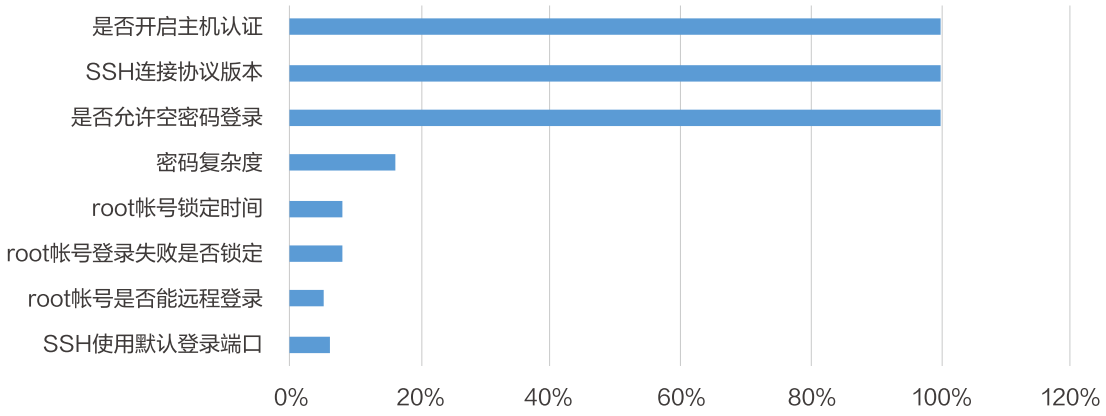

图6-5 2020年主机安全基线检测部分核心配置项合规率

基于风险程度，网宿安全平台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，如root账号是否允许远程登录、SSH是否使用默认登录端口等，只有少数用户进行了安全加固。

当前安全加固的需求主要来源于网络安全等级保护的安全加固规定，而非来源于真正内化的安全意识。大部分管理员依然为了便利而放弃一定的安全性。同时资产管理困难也是一个重要的原因，许多主机并没有在安全人员的管理范围内，一些无主的主机、测试主机通常被作为入侵的入口。

6.6. 来自境内的异常登录IP数量跃升至第一

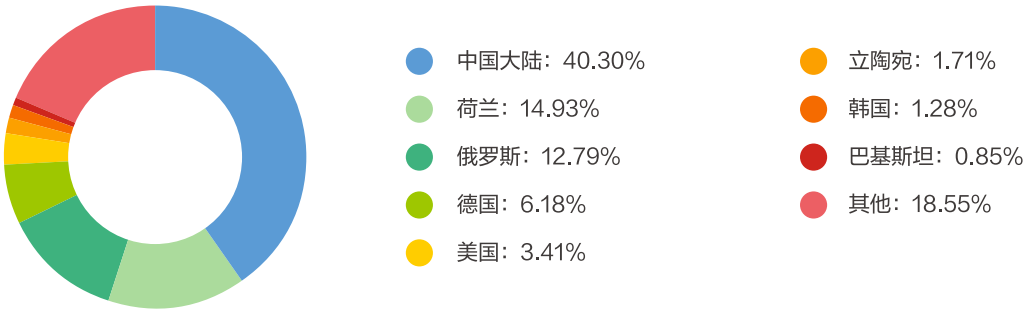

图6-6 2020年异常登录IP来源分布

与2019年相比，异常登录告警IP中境内登录IP比例大幅度上升。随着国际形势与国家政策的变化，境外代理的成本原来越高。并且近几年使用境外IP作为跳板机已不被允许，这些因素导致境内攻击IP的占比趋势明显上升。

6.7. 修改定时任务是最常用的主机入侵持久化手段

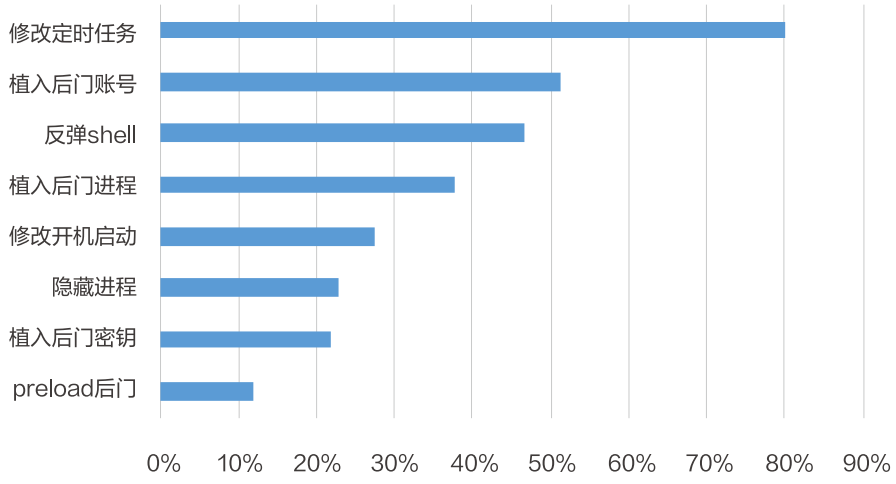

图6-7 2020上半年主机入侵持久化手段检出比例

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（80.04%）、开机启动（27.62%）等手段保障恶意进程的持久运行，并通过植入后门账号（51.42%）、植入后门进程（37.70%）等方式维持控制权限。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

世上唯一的不变，是变化本身，网络安全行业更是如此。网络威胁与攻击始终在不断变化，各个阶段体现出新的特征。因此，规划与运营线上业务时，需要充分考虑到各类潜在网络安全威胁所带来的安全隐患。

基于报告内容和网宿安全平台的运营情况，我们认为，未来网络安全态势有以下发展趋势：

一、云安全综合解决方案成为企业的刚需

从网宿科技的平台数据以及业界发生的攻击事件来看，当前的攻击方式逐渐出现融合式的趋势，企业面临的威胁不会是单一的DDoS攻击或者Web应用攻击，而通常是综合类的攻击手段，通过多种攻击方式，达到使被攻击对象服务下线或者窃取敏感数据等目的。

同时，随着云原生架构的发展，越来越多的企业采用云原生的服务来构建业务，以提升自身业务的敏捷性。云原生大量依赖容器、微服务、API等技术，在为企业业务带来便利的同时，也引入了一些新的风险，比如容器环境带来的镜像安全风险、API被滥用及攻击等风险，都容易为企业自身业务引入脆弱性风险。

面对这样的攻击趋势和业务发展趋势，企业的需求也从单一的抗D、WAF等需求逐渐发展为综合性的云安全解决方案，这样更便于企业对云安全产品和服务的使用及运维，比如企业能够在一体化的Portal系统中完成各类安全事件的综合的报表内容查看以及配置调整和下发等，能够大大提升对安全事件的响应速度以及效率，进一步降低攻击所带来的影响。

Gartner近年提出WAAP(Web应用程序和API保护)方案，也是整合了DDoS防护、Web应用攻击防护、爬虫管理、API防护等各类功能的综合性解决方案。从中我们也可以看到，Gartner也认为企业需要的是一个综合性的解决方案，这一趋势与网宿平台所看到的情况是一致的。

网宿科技的安全加速解决方案，在为企业提供DDoS防护、Web应用防护、恶意爬虫防护等云安全服务的同时，还可以提供全网加速功能。不论是否在攻击情况下，都可以最大限度地为企业的业务提供可用性保证。同时，HIDS产品能够在主机和容器侧为企业提供脆弱性检测、攻击告警等功能，与云端的安全能够形成更完整的防护体系。

二、SASE成为明显的趋势，且逐渐落地

2020年，受新冠疫情影响，远程办公的需求在全球范围内井喷式发展。经此大考，对企业而言，远程办公不再是可上可不上的“Plan B”，而是成为了必选项，这在客观上极大推动了远程协作办公模式在全球的“常态化”。

除疫情催化因素外，新的企业协作模式，如异地团队协作、外部合作伙伴协作，也在加速远程办公的应用与普及。然而，对于大部分企业来说，以VPN为代表的传统远程办公工具在解决企业员工办公需求的同时，却暴露出大量效率和安全问题。

VPN网关在公网暴露端口，很容易成为攻击目标，被攻击者使用DDoS等方式变为不可用，同时，近年来不断地有厂商的VPN系统被曝存在漏洞，也对此类系统的使用和运维带来了非常大的风险。另外，VPN网关由于部署位置比较固定，用户在远程访问时由于跨网等导致的访问质量问题也会大大影响用户体验和办公效率，很多企业不得不为VPN系统寻找额外的加速系统以提升其可用性。越来越多的企业意识到，他们需要一个更加安全、更加高效的综合解决方案来保证自身业务的顺利进行。

Gartner此前提出的SASE——安全访问服务边缘，正是应对这一场景需求的理想模型。SASE集中了SD-WAN、零信任、安全网关等各类网络及安全方案于一体，能够为远程访问、移动办公等场景提供可靠、安全的连接，从而保障不同场景下员工能够正常访问公司的办公资源且保证整个内网的安全。当前，越来越多的安全厂商尝试推出类似方案，来实现SASE的落地，未来这一领域将大有可为。

网宿科技作为全球第二大的CDN厂商，在SASE方案领域有着天然的优势。当前，基于已有的SD-WAN产品和资源，网宿科技推出了基于零信任理念的SecureLink产品，在保证企业的分支访问、远程办公等场景的需求之外，通过在端侧和边缘节点构建身份管理、访问管理、IPS、DLP等功能，为企业提供安全高效的远程访问解决方案。

版权信息

CHINA INTERNET SECURITY REPORT