网宿科技
WANGSU.COM

2021 上半年

中国互联网安全报告

CHINA INTERNET SECURITY REPORT

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。
- 报告中所使用的所有安全数据均来自于网宿安全平台，与网宿自身的安全业务规模、客户类型等有一定的关联，并会根据网宿安全业务自身的调整呈现出一些变化，这些变化对于数据所呈现出的趋势会有一定的影响，但我们还是可以从这些数据中对于安全趋势的发展进行相应的解读，进一步加深对安全攻防态势的理解，加强对安全攻防趋势的认识。
- 报告综合对比了2019年、2020年、2021年的上半年的攻防数据来进行攻击趋势的解读和判断。
- 本期报告中最值得关注的发现是，Web攻击、恶意爬虫攻击量连年成倍增长，显示出应用层攻击和针对客户业务本身所进行的攻击已呈现出愈演愈烈的态势。

1.1. 2021年上半年DDoS攻击概览与趋势

- 2021年上半年网宿安全平台监测到DDoS攻击事件近3000万起，与2020年同期几近持平；DDoS攻击峰值则略有上升。
- 传统重灾区——游戏行业在上半年遭受的DDoS攻击数量、攻击峰值均位列第一。
- 反射放大攻击中，NTP协议攻击“异军突起”，强势占据了87.55%的攻击量。

1.2. 2021年上半年Web应用攻击概览与趋势

- 2021年上半年，网宿云安全平台共监测并拦截Web应用攻击101.13亿次，为2020年同期的2.39倍、2019年同期的21.66倍，涨幅惊人。
- 政府行业不再是Web应用攻击的主要目标，软件信息服务、房地产、金融等成为Web攻击集中的行业。

1.3. 2021年上半年恶意爬虫攻击概览与趋势

- 2021年上半年，网宿安全平台共监测并拦截了超341.47亿次爬虫攻击，平均每秒发生2183.52次攻击，与往年相比亦呈翻倍增长之势。
- 从攻击源分布来看，境外攻击源占比略有上升，推测与后疫情时代，代购、海淘行业有所恢复有关。
- 软件信息服务为遭受恶意爬虫攻击最严重的行业，其次是房地产、交通运输、电子商务。

1.4. 2021年上半年API攻击概览与趋势

- 2021年上半年网宿安全平台共监测并拦截42.53亿次针对API业务的攻击，是2020年同期的2倍，增长明显。
- 针对API的攻击手段集中度降低，显示出多样化趋势。
- 绝大多数的API攻击集中在软件信息服务和金融行业，占比分别为41.62%和28.41%。

1.5. 2021上半年主机安全概览与趋势

- 2021上半年网宿探测发现过半数的企业主机已应用了容器技术，将产生越来越普遍的容器安全需求。
- 得益于规律性的网络攻防演练，企业对端口的管理规范度显著提升，公网开放端口数量大幅下降。
- 攻击者大量使用了隐藏进程、伪装恶意定时任务、Rootkit等技术规避异常行为检测，主机安全威胁隐匿度提升，要求更强大的主机入侵检测能力支撑。

第二章
DDoS攻击数据解读

2.1. 上半年DDoS攻击事件数同比几近持平，攻击峰值略有上涨

2021年上半年，网宿安全平台所监测到的DDoS攻击事件数量与去年同期相比几近持平，略微下降了1.63%。从月份走势来看，2021上半年的攻击数量呈现持续增长态势，5月、6月增幅最大。

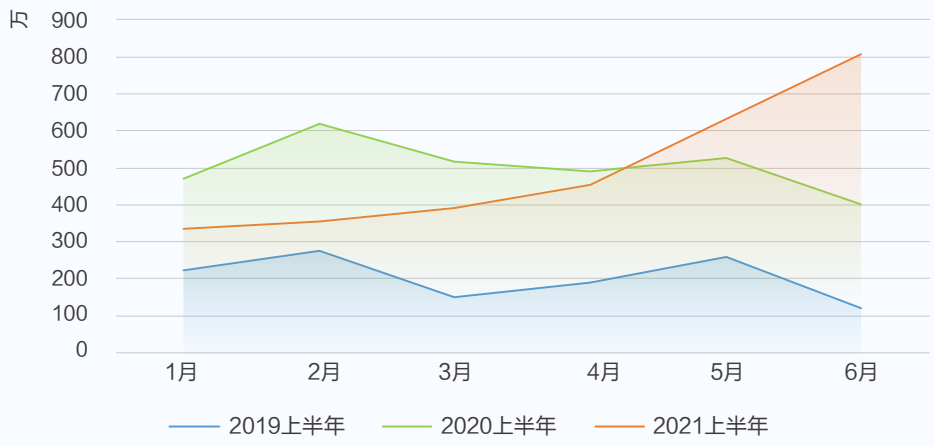


图2-1 2019/2020/2021上半年DDoS攻击事件数量趋势

上半年DDoS攻击峰值出现在6月，达到774.58Gbps，比2020上半年峰值611.73Gpbs高出26.62%，低于2019上半年的982.47Gpbs。今年峰值出现的月份也与往年不同，19及20上半年，攻击峰值均出现在1月，而今年每月的攻击峰值则是从2月开始一路上涨，到6月达到最高。

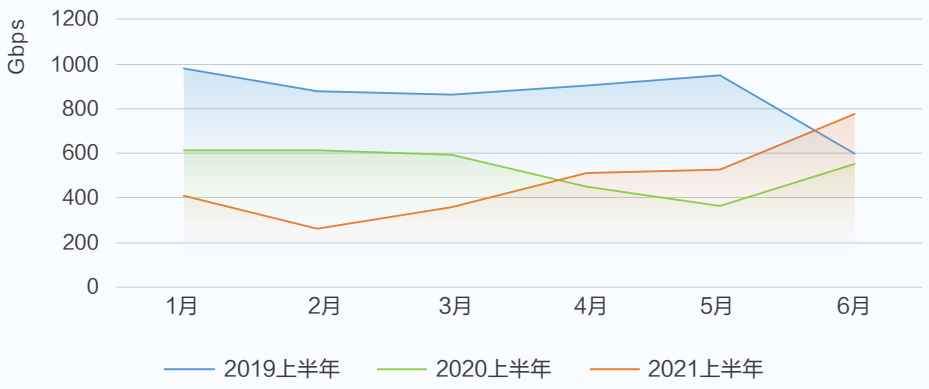


图2-2 2019/2020/2021上半年DDoS攻击峰值月份分布情况

2.2. 游戏、电商行业集中了超八成DDoS攻击

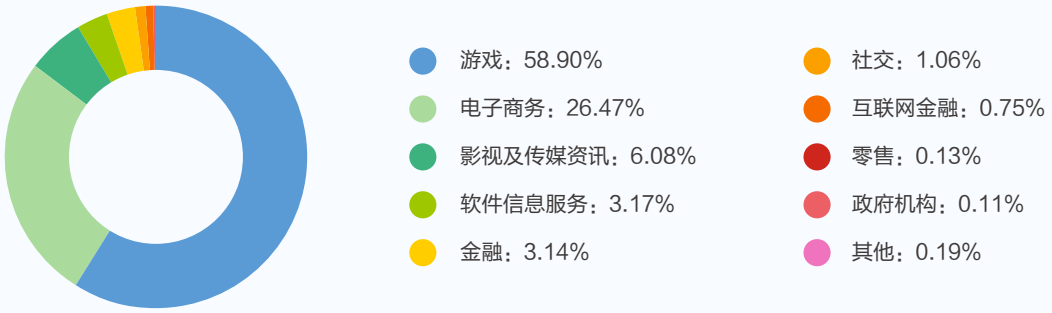


图2-3 2021上半年DDoS攻击行业分布

从DDoS攻击事件的行业分布来看，游戏业成为2020上半年受DDoS攻击次数最多的行业，占比达到58.90%，远超其他行业。电子商务以26.47%百分比占据第二位。两者遭受的攻击数量已超过全行业的85%。位于第三、第四的则是影视及传媒资讯（6.08%）和软件信息服务行业（3.17%）。

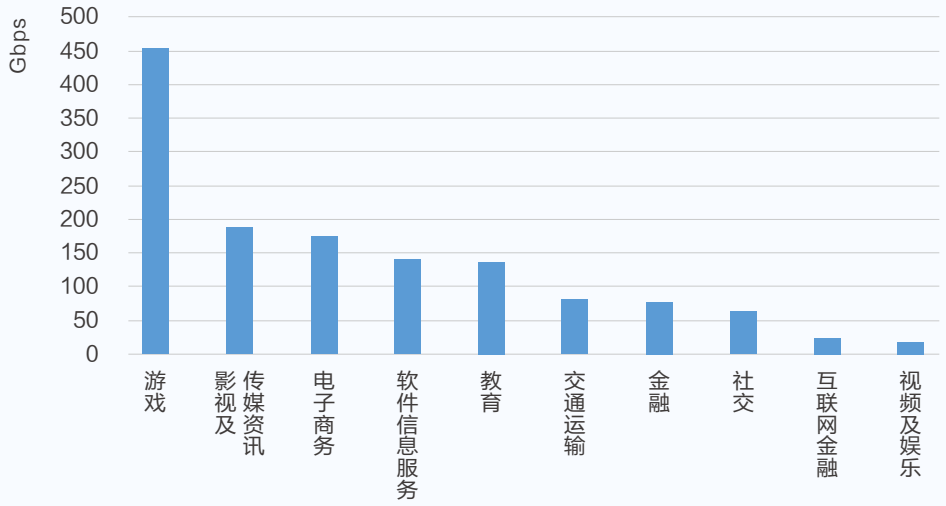


图2-4 2021上半年DDoS攻击峰值Top 10行业

从各行业遭受的攻击峰值统计来看，同样是游戏、影视及传媒资讯、电子商务、软件信息服务行业位居前四，且游戏行业的峰值同样“一骑绝尘”，超过450Gbps。攻击数量及攻击峰值的行业分布，共同反映出了明显的行业集中趋势。

2.3. NTP反射放大攻击异军突起

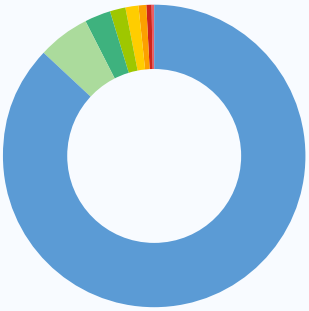


图2-5 2021年上半年反射放大攻击协议分布

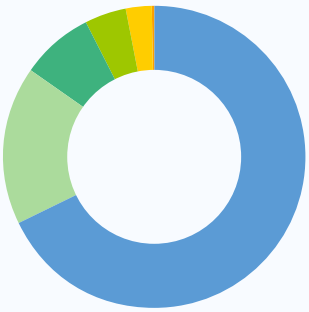


图2-6 2020上半年反射放大攻击协议分布

反射放大攻击依然是攻击者最常用的DDoS攻击方式之一，但今年上半年反射放大攻击的主流协议发生了“大洗牌”，NTP反射放大攻击异军突起，反超往年占绝对优势的SSDP协议，跃升至第一位，且占比由去年同期的7.78%暴涨至惊人的87.55%。这说明该协议被广泛用于攻击，也表明还有大量的存在配置错误的NTP服务器依然被暴露在公网上，导致被黑客利用来进行攻击。SSDP攻击的占比则从68.01%骤降至5.72%。

第三章
Web应用攻击数据解读

3.1. 上半年Web应用攻击量已超过去年全年

2021年上半年，网宿安全平台共监测并拦截Web应用攻击101.13亿次，已超过2020年全年攻击次数，同比增长139.39%，呈翻倍增长态势，显示出此类攻击的威胁持续增大。

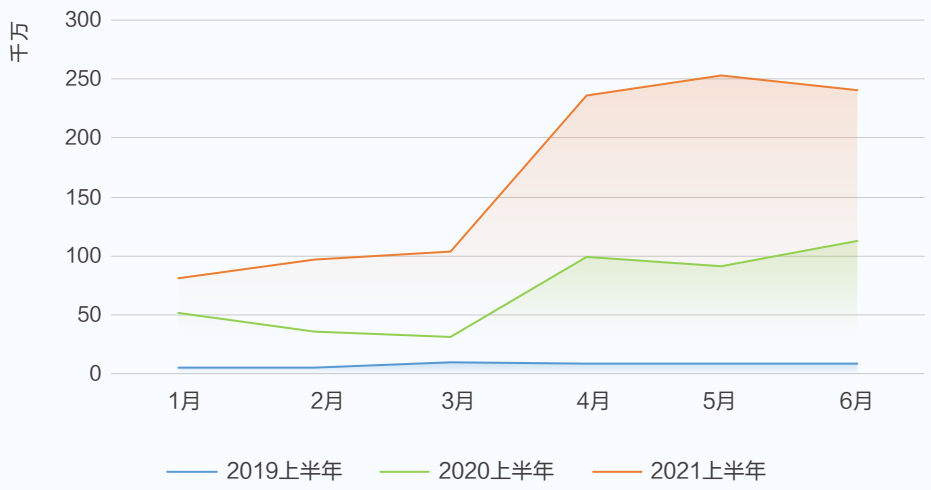


图3-1 2019/2020/2021上半年Web应用攻击次数趋势

3.2. Web攻击手段呈现多样化趋势

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进行应对，从中也能看出攻击手段的分布情况。

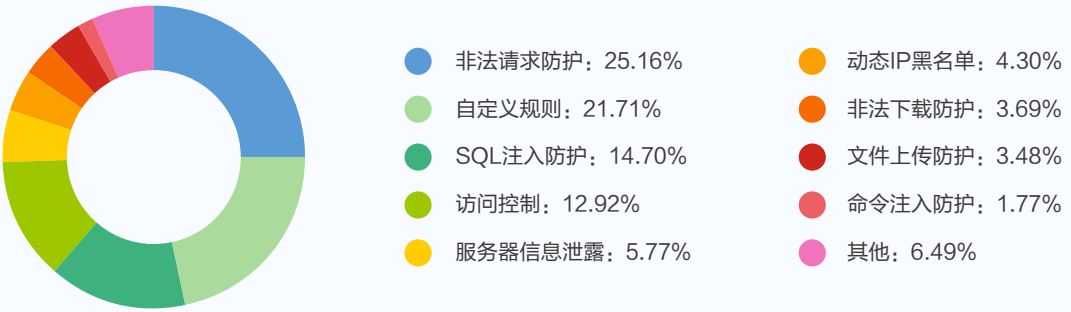


图3-2 2021年上半年Web应用攻防手段分布情况

从上图可见，Web应用攻防手段仍然保持了较为分散的分布态势。排位前三的分别是非法请求防护（25.16%）、自定义规则（21.71%）、SQL注入防护（14.70%）。与往年相比，除了SQL注入防护依旧位于高位外，此前始终没跌出过Top3的暴力破解防护，在本周期已跌出前十，仅占比0.53%。

值得注意的是，本次统计中，客户自定义规则所占的比重比之前增大不少，说明在Web攻击防护领域，针对客户自身的业务情况和特定的攻击情况，制定特定的防护规则也是非常有效的手段。

越来越多的攻击流量来源于自动化的扫描器，网宿安全防护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，能够通过访问控制（12.92%）、动态IP黑名单（4.30%）等方式直接过滤掉大部分扫描器攻击，有效降低网站被针对性攻击的概览，同时降低自动化扫描器对网站的负载压力。

3.3. 境外攻击源占比有所上升

通过对攻击IP的地理位置分析发现，2021年上半年全球攻击源有64.98%来自中国大陆，来自境外的攻击源占35.02%，比去年同期上涨了近26个百分点。

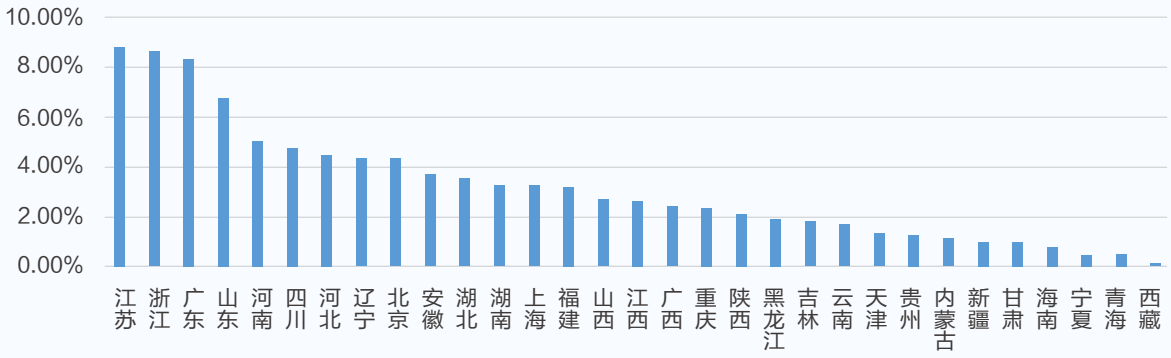


图3-3 2021上半年来自中国大陆的Web应用攻击来源分布

统计攻击来源在中国大陆的省份分布发现，2021年上半年TOP15的省份所占的攻击源比例超过75%。江苏、浙江、广东依然是国内攻击源分布的前三，分别占比为8.95%、8.78%、8.46%。这三个经济比较发达的省份由于IT资源发达，近两年一直占据着国内攻击来源的前三名。

3.4. 软件信息服务遭受超40亿次攻击

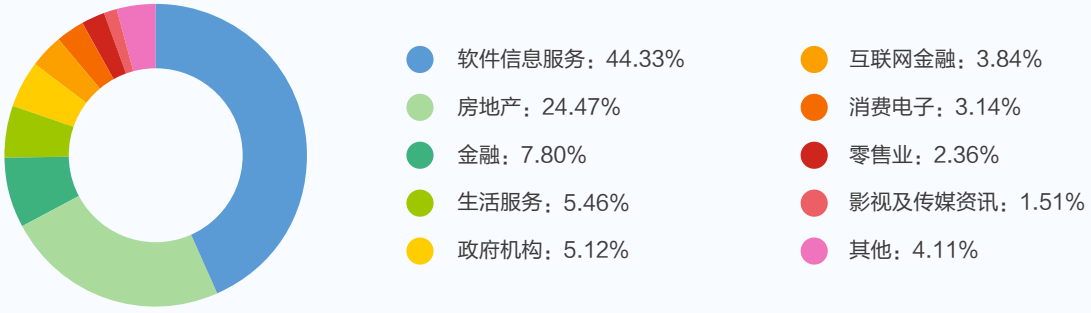


图3-4 2021上半年Web应用攻击行业分布

从2021年上半年的数据来看，软件信息服务和房地产业成为受Web攻击最多的行业，两者集中了上半年近七成的Web应用攻击，将近70亿次。金融业（7.80%）、生活服务业（5.46%）、政府机构（5.12%）分别占据第三至第五的位次。

第四章
恶意爬虫攻击数据解读

4.1. 恶意爬虫攻击量连年翻倍增长

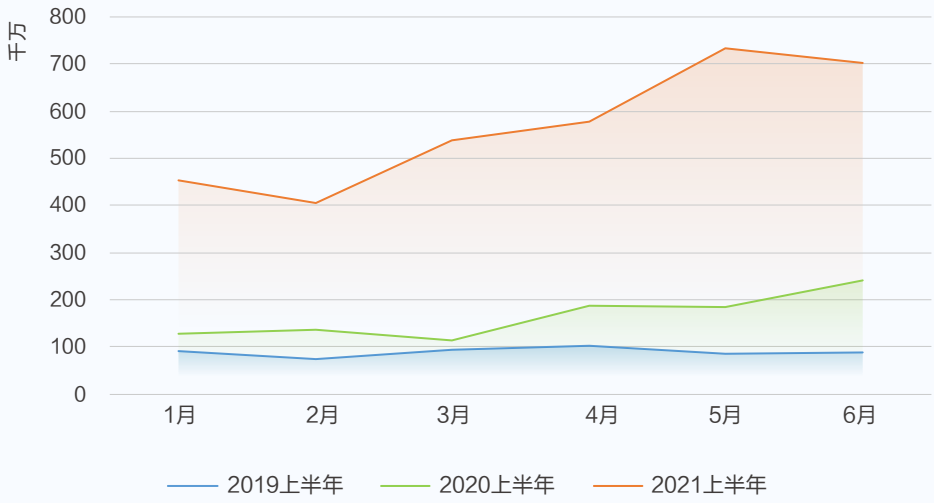


图4-1 2019/2020/2021上半年恶意爬虫攻击数量趋势

2021年上半年网宿云安全平台共监测并拦截了超341.47亿次恶意爬虫攻击，平均每秒发生2183.52次攻击，攻击量已接近2020年全年总量，是2020年同期的3.29倍，2019年同期的6.34倍，呈连年成倍增长趋势，安全威胁日益突出。

4.2. 合法性验证有效拦截超七成攻击

网宿平台集成了各种防护算法来构建恶意爬虫的防护体系，从线上的攻防数据中可以评估攻击方式的趋势以及防护效果。

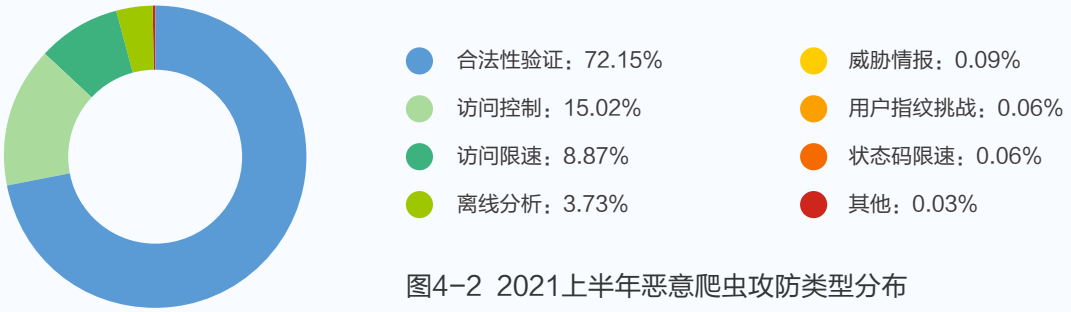


图4-2 2021上半年恶意爬虫攻防类型分布

从2021年上半年的攻防数据中可以看出，使用客户端及其请求的合法性验证的各类恶意爬虫防护方法依然是对付恶意爬虫的最有效手段，能够过滤掉超过七成的攻击。

其次，访问控制（15.02%）、访问限速（8.87%）等手段也有非常明显的防护效果。

4.3. 恶意爬虫境外攻击源比重略有回升

图4-3 2021上半年恶意爬虫攻击全球来源分布vv

从网宿安全平台监测并拦截的源IP分布来看，2021年上半年全年的恶意爬虫攻击超八成来自于国内。境外攻击源比重从去年同期的7.08%上升至18.04%。

境外攻击源比重上升，可能与全球新冠疫情趋于稳定，代购、海淘等行业有所恢复，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回升有关。

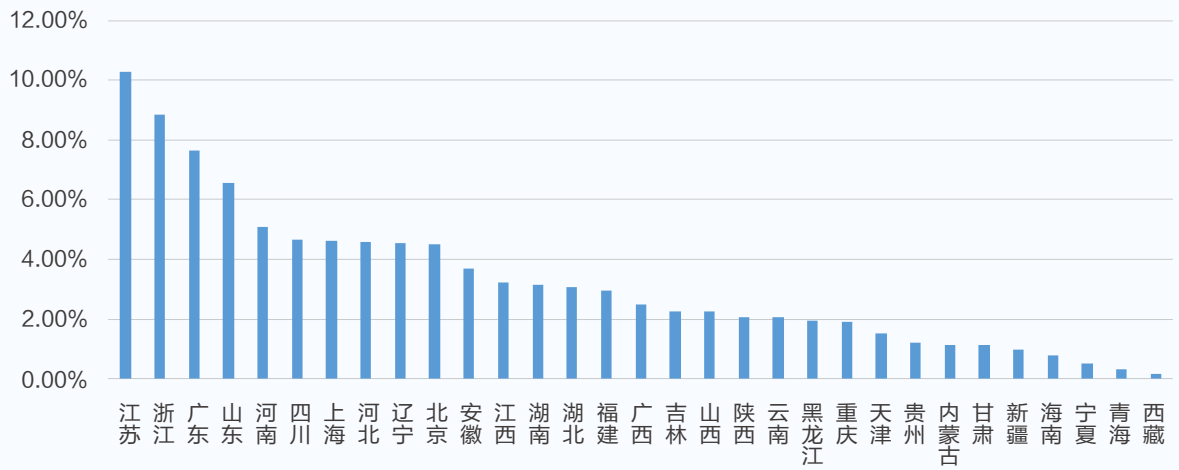


图4-4 2021上半年来自中国大陆的恶意爬虫攻击来源分布

江苏、浙江、广东的恶意爬虫攻击分别为10.29%、8.83%、7.65%，成为来源数量最多的三个省份。整体上看，国内攻击源分布相较往年同期更加趋于平均，这与各地IDC、网络、云计算等IT基础设施建设水平提升，区域间服务器、IP资源差异缩小有一定关系。

4.4. 恶意爬虫攻击行业分布较分散

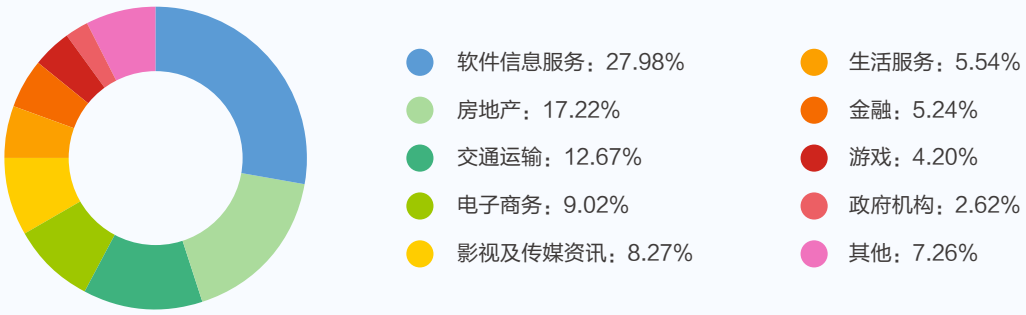


图4-5 2021上半年恶意爬虫攻击行业分布

恶意爬虫攻击的行业分布，呈现出集中度低，“雨露均沾”的态势。遭受攻击最多的软件信息服务行业（27.98%），占比也未超过30%。攻击量第二到第五的分别是房地产（17.22%）、交通运输（12.67%）、电子商务（9.02%）、影视传媒资讯（8.27%）。

其中，交通运输的排位从去年同期的第九（2.08%），重新回到前三位，也体现了交通运输业已从疫情的负面影响中逐渐恢复，抢票类爬虫攻击死灰复燃。

第五章
API攻击数据解读

5.1. 上半年平均每秒发生272次针对API业务的攻击

在互联网、大数据、微服务浪潮下，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，但也极容易被攻击。

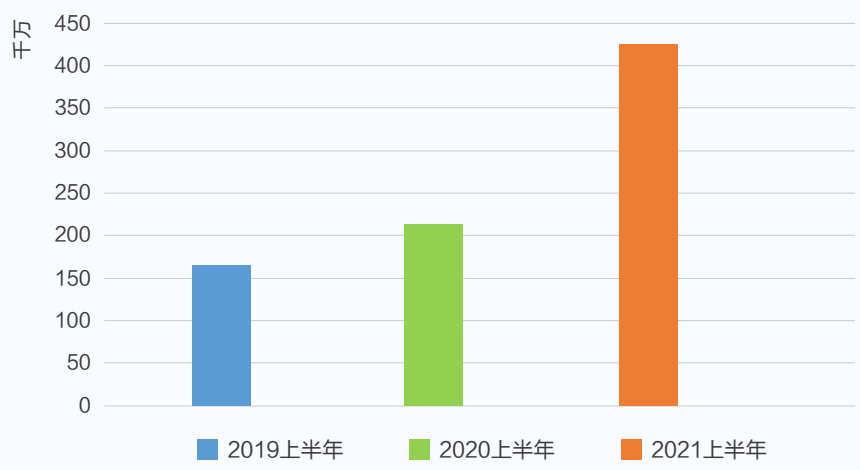


图5-1 2019/2020/2021上半年API业务攻击次数

2021年上半年，网宿安全平台共监测并拦截42.53亿次针对API业务的攻击，平均每秒发生攻击271.96次，攻击量已达到去年同期的2.01倍，增长速度逐年上升，显示了API业务面临的严峻的安全形势。

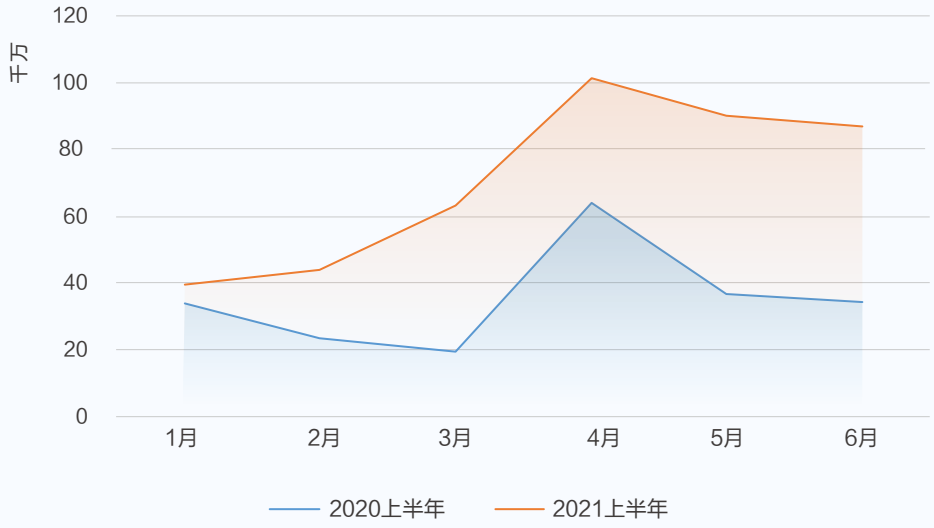


图5-2 2020与2021上半年API业务攻击次数月份分布

从每月走势来看，上半年API业务攻击从1月份开始就一路走高，在4月份迎来一个小高峰，走势与2020年同期大体相近。

5.2. API攻击手段显示出多样化趋势

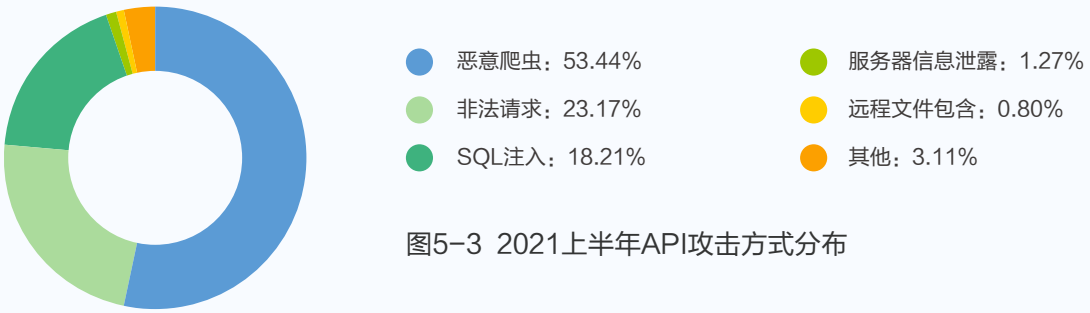


图5-3 2021上半年API攻击方式分布

在针对API业务发起的攻击中，恶意爬虫是最主要的攻击方式，这一趋势依然继续保持。在2021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53.44%，比去年同期的74.82%明显下降。

排第二、三位的分别是非法请求（23.17%）和SQL注入（18.21%），占比相比去年同期的5.97%、10.94%均有大幅增长。攻击手段分布的集中性减弱，显示出针对API的攻击手段逐渐呈现出多样性发展的态势，而不是仅依赖于某一种。

5.3. 软件信息服务业、金融业成为API攻击重灾区

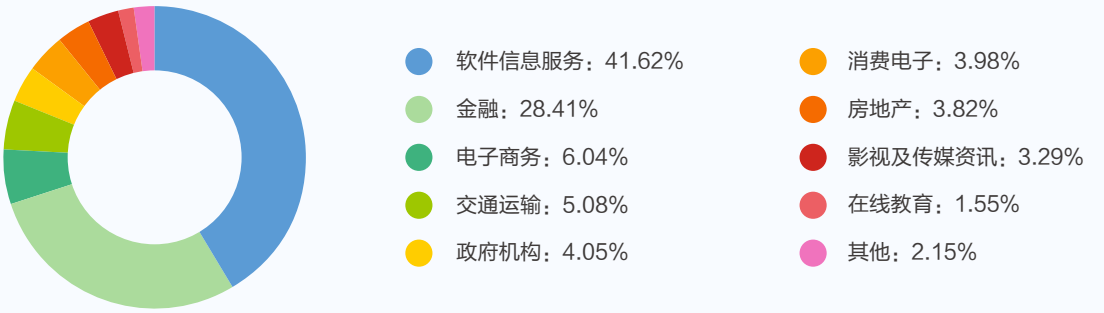


图5-4 2021上半年API攻击行业分布

2021年上半年，软件信息服务行业成为受API攻击最多的行业，攻击量占整体比重的41.62%。金融行业占28.41%，排在第二。

这两个行业所遭受的API攻击占比达到近7成，显示了这两个行业异常严峻的攻击形势。

往年聚集了绝大多数API攻击的政府机构，在今年上半年遭受的攻击量则大幅下降至去年同期的约1/10，占比也由2020上半年的60.94%降至4.05%。

第六章
主机安全数据解读

6.1. 超半数企业主机已应用容器技术

图6-1 2021上半年企业主机容器安装情况

网宿主机安全探针检测发现，55.73%的企业主机有安装容器相关软件，与去年年底时相比上升15.46%，上升速度较快，可以预见未来容器安全的需求将越来越大。

6.2. 公网开放端口数量大幅下降，攻击面收窄

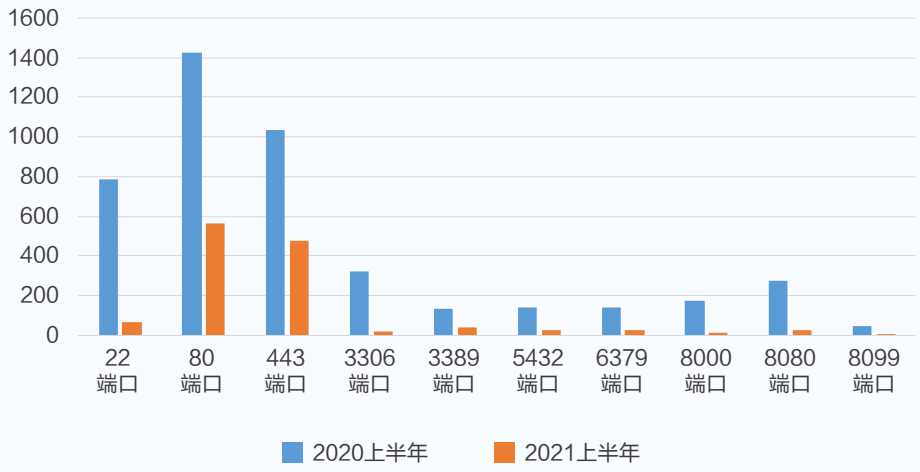


图6-2 2020与2021上半年公网开放端口数量对比

分析网宿主机探针采集到的公网开放端口情况，发现与2020年同期相比，2021上半年公网开放端口数量大规模下降。

其中管理类端口（如22端口、3389端口）、数据库端口（如3306端口、5432端口）、测试类端口（如8000端口、8099端口）降幅达到约90%，正式业务类端口（如80端口、443端口）降幅也超过了50%。

公网开放端口数量下降主要源于规律性的网络攻防演练，有效提升了网宿安全平台客户管理端口的规范度，改变了过去业务部门未严格按照安全规范使用端口，导致管理端口、临时的测试端口经常被作为黑客入侵的入口点的情况，大大缩减攻击面。

6.3. 高危漏洞中多为与Web应用相关的通用组件漏洞

2021上半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	XStream多个反序列化漏洞
No.3	Apache Tomcat AJP协议文件读取与包含漏洞
No.4	Apache Commons FileUpload反序列化漏洞
No.5	Apache Shiro远程代码执行漏洞
No.6	Apache Struts2远程代码执行漏洞
No.7	JMX远程命令执行漏洞
No.8	Druid远程代码执行漏洞
No.9	Spark远程代码执行漏洞
No.10	Apache Flink Web Dashboard远程代码执行漏洞

针对高危漏洞的入侵依然是以应用、组件漏洞为主，尤其是与Web应用相关的通用组件漏洞。应用组件漏洞比操作系统漏洞具备更容易获得的执行环境，比业务漏洞具有更强的通用性。

通常黑产团队会选择用户数量较多、漏洞利用条件简单且稳定的漏洞来开发自动化工具，以较低的成本实现“肉鸡”控制、自动化挖矿等牟利行为。

另外，从漏洞分布来看，开源组件更受安全研究人员青睐，由于更容易获取源码与分析环境，从数量上看开源软件暴露出来的漏洞往往比商业软件更多。但这并不代表商业软件比开源软件更安全，相反，开源软件由于漏洞发现得更快，有利于企业及时修复漏洞，而商业软件则存在更多的潜在漏洞未被发掘。

6.4. 主机异常进程检测难度大大增加

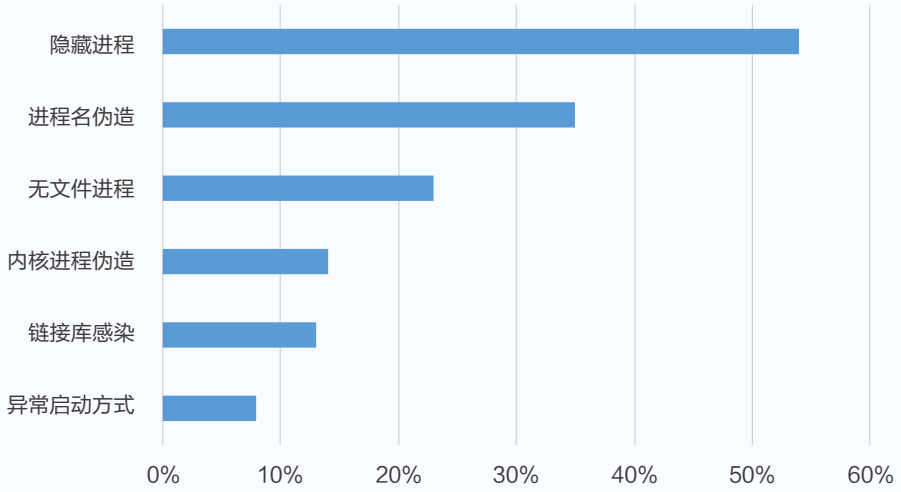


图6-3 2021上半年常见异常进程类型检出率

从网宿主机探针识别到的异常进程数据可看出，主机上出现的异常进程大量使用了规避检测的技术，以干扰安全软件检测及人工入侵分析。

规避检测的手段中，使用最多的是隐藏进程，网宿主机探针在超过50%的入侵事件中均检测到了此技术。隐藏进程可使恶意进程在进程列表中不显示。

检出率排行第二的伪造进程名，也是攻击者规避入侵检测、排查的常用方式，通过将显示出的进程名伪造成系统常用进程名或内核进程名，以达到混淆的目的。链接库感染与异常启动方式则是使用合法的进程去加载恶意代码，以绕过杀毒软件的检测。

6.5. 伪装恶意定时任务也是攻击者规避检测的常用方式

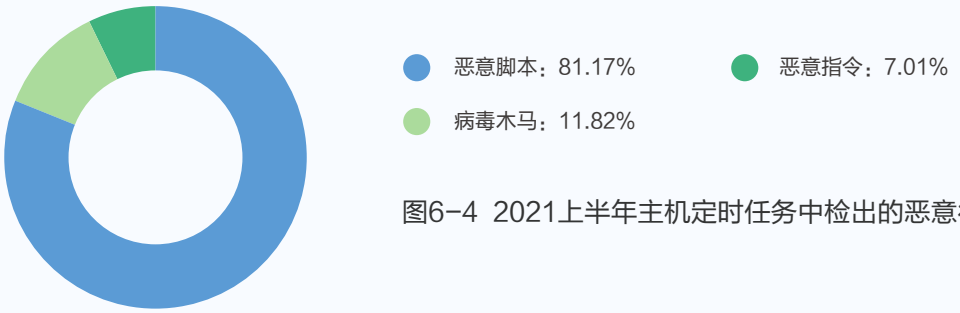


图6-4 2021上半年主机定时任务中检出的恶意行为类型分布

通过对网宿主机探针识别到的恶意定时任务进行检测分析，在定时任务封装的恶意行为中，检出恶意脚本的占比高达81.17%。其次为病毒木马（11.82%）、恶意指令（7.01%）。

恶意定时任务通常通过以恶意脚本执行恶意行为的形式来实现，例如执行病毒木马、恶意指令等。通过恶意脚本的形式，攻击者容易将恶意定时任务伪装成合法程序的路径，以规避检测。此外，恶意脚本还可以将各种恶意行为封装到一起，减少定时任务配置量，提高攻击者的配置效率。

6.6. 最隐蔽的高危威胁：对系统影响小的Rootkit行为成为主流

Rootkit是隐匿能力最强的恶意软件技术，能够获得root访问权限、完全控制目标操作系统及其底层硬件。攻击者常采用Rootkit技术隐藏自身或指定的文件、进程和网络连接等信息，达到长期潜伏于目标系统，规避入侵检测的目的，安全威胁极大。

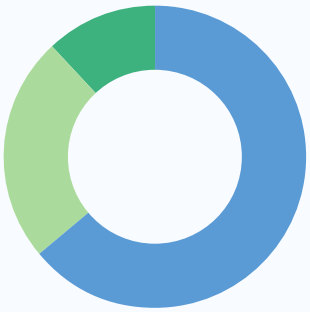


图6-5 2021上半年Rootkit行为类型分布

分析网宿主机探针识别到的Rootkit行为，发现进行文件替换的应用级Rootkit占比最高，达64.01%，其次分别为预加载链接库（24.28%）、LKM内核模块加载（11.71%）。

文件替换的方式对系统影响较小，较容易集成到自动化流程中，因此最受攻击者青睐。而LKM内核模块加载的方式虽然较难以查杀，但是存在内核兼容性问题及破坏系统稳定性的风险，因此占比较低。当前，在入侵主机后通过植入挖矿木马进行牟利，成为网络黑产的一种主流操作。这种方式需要稳定的系统以持续获取利益。因此黑产团队也逐渐尽量规避会对系统造成破坏的入侵行为，在获得稳定的系统环境的同时，也不易被管理人员发现。

第七章
趋势展望与建议

从前述报告中可以看到，网络威胁与攻击始终在不断变化，在这一阶段的安全报告中所呈现出来的数据与攻防态势与2019及2020年同期有了一些新的变化。从这个角度也看出，企业在考虑自己的业务所面临的安全威胁与防护时，也需要根据情况不断地进行调整和防护，防护思路和策略需要跟上攻击的变化，这样才能对攻击进行有效应对。

一、业务安全威胁持续升级，攻击手段更加隐蔽，安全防线亟需向综合化、纵深化建设

本期报告中**Web攻击、恶意爬虫攻击、API攻击的攻击**量都有了成倍的增长，相对地，网络层DDoS攻击增长趋于停滞，**显示出针对应用层和客户业务的攻击手段越来越受到攻击者的青睐，比重越来越大**。其攻击目的不再是简单地让客户业务无法访问，而是更直接地盯上客户的业务相关的数据等，一旦成功，不仅是对客户业务本身造成影响，这些泄露的数据也会成为获利的手段，或者被拿下的服务器会成为挖矿或者攻击其他目标的资源，从而为攻击者创造更多的利益，对企业造成更长久的损害。

同时，随着越来越多企业采用云原生架构来构建业务，业务应用的运行环境也在发生变化。**云原生所依赖的容器、微服务等技术在提升业务的敏捷性的同时，也引入了新的安全风险**，比如容器逃逸风险、镜像安全风险等，同样可直接损害业务运行、造成业务数据失窃。

从攻击手段上看，**黑客攻击已呈现出自动化程度提升、隐蔽性增强的特点**，用AI模拟人行为绕过常规安全规则匹配的手段屡见不鲜，入侵检测和防护的难度水涨船高。

在这一趋势下，**企业在提供线上服务时需要认真考虑从网络层到应用层的综合性安全防护方案**，形成纵深防御，确保在一层安全措施被攻破后，还有多层后手拦截进一步的威胁，阻止攻击者触及核心业务应用和数据，造成损失。

Gartnet近年提出的WAAP（云Web应用程序和API保护）方案，即是整合了Web应用程序防火墙、DDoS防护、爬虫管理和API保护四大核心能力的一种综合性解决方案。Garner预测，到2026年，40%的组织机构将以高级API防护和Web应用安全能力，作为挑选WAAP服务商的基础。

Gartner对综合性解决方案将成为企业安全需求趋势的观点，与网宿的判断不谋而合。网宿提供的安全加速解决方案，能够在为客户提供DDoS防护、Web应用防护、恶意爬虫防护等云安全服务的基础上，同时为客户带来全网加速功能，最大限度地为客户的业务提供可用性保证。

除了分布式的云端安全防护网，网宿还提供主机安全、容器安全产品，**在主机和容器侧**为客户提供基于海量大数据样本和AI引擎，高度精准的脆弱性检测、入侵行为检测、攻击告警等能力，与云端的安全能够形成更完整的纵深防护体系。同时，网宿完善的客户服务体系和安全运维团队能够在攻击发生变化时及时关注到客户的业务情况，对新的攻击手段进行响应，确保防护策略有效性，从而更好地保证客户的业务顺畅运行。

二、SASE需求上升，下一代安全模型加速落地

受疫情催化，全球企业数字化转型加速，催生了远程办公等大量新应用，加上混合云、多云架构、大数据、物联网、边缘计算等技术普及的大趋势，使企业IT架构由以IDC为中心的星状结构向分散的网状结构演变，任何用户、任何设备，在任何位置均可访问位于IDC及云上的企业应用，打破了企业内外网的边界，攻击面大增。

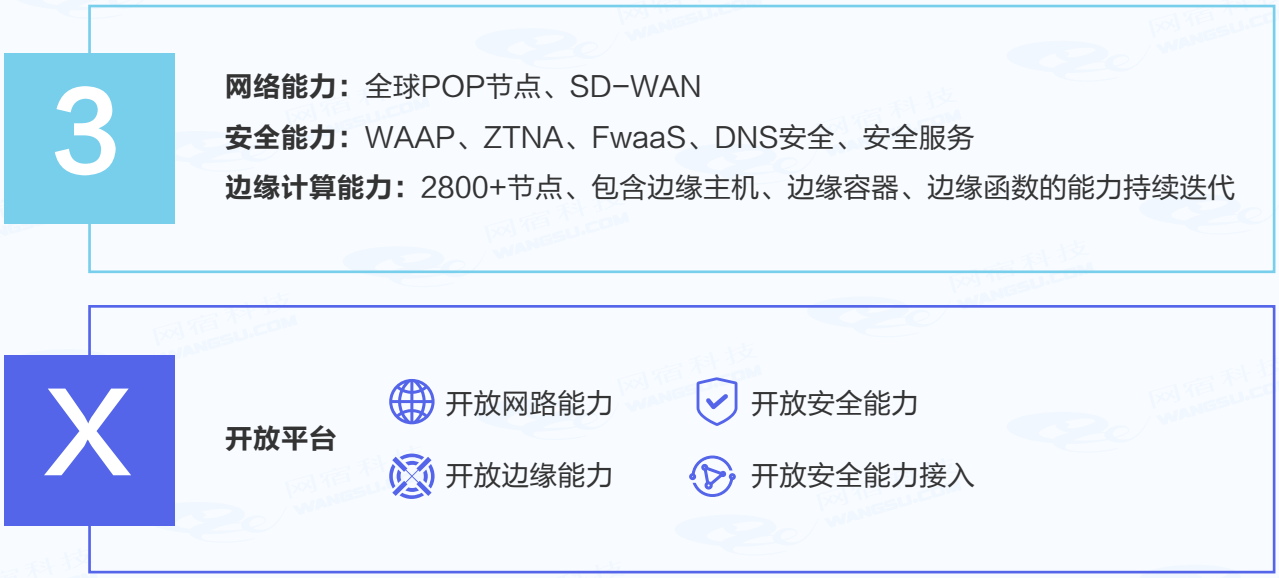
传统对内网流量即默认可信的边界信任模型和边界安全防护已无法适应新的企业IT架构，暴露出明显的安全缺陷。比如，一旦连接内网和外网的VPN网关被攻破，就没有更有力的安全措施能够阻止攻击到达企业数字资产。

传统边界安全加速失效的背景下，企业亟待构建与数字化业务融合的新型网络安全体系。由Gartner提出的全新的SASE（安全访问移动边缘）模型已经成为越来越多企业关注的技术趋势。SASE将广域网功能与全面的网络安全功能融为一体，可实现安全架构的核心从数据中心向身份的根本性转变。

Gartner在最新的报告中预测，到2024年，30%的企业将采用云交付的SWG、CASB、ZTNA和来自同一供应商的分支机构FWaaS功能，而2020年这一比例不到5%。到2025年，至少60%的企业将制定明确的SASE采用战略和时间表，包括用户、分支机构和边缘访问，高于2020年的10%。

观察到这一市场趋势，越来越多的网安厂商加速布局SASE领域，尝试推出相关方案。SASE主要的关键组件包括SD-WAN、ZTNA（零信任网络访问）、SWG（安全Web网关）、FWaaS（防火墙即服务）等，经过近些年的发展，技术成熟度也不断提高。

作为全球领先的云分发及边缘计算公司，网宿科技在SASE方案领域有着天然的优势。对于如何落地SASE，网宿提出了“3+X”能力框架。



“3”即网络能力、安全能力、边缘计算能力3项。在网络能力方面，网宿基于2800+的全球节点，及节点之间的高速网络（SD-WAN），能够较好的保证终端用户最后一公里接入体验及回数据中心（包含云平台）的体验；在安全能力方面，在今年2月推出基于零信任理念的SecureLink产品之后，网宿已具备WAAP、ZTNA、FwaaS、DNS安全能力，及成熟的安全服务；在边缘计算能力方面，网宿边缘计算平台在音视频、Web及垂直的应用场景有广泛应用和成熟的运营体系，未来将结合在边缘计算的积累，把边缘安全的能力开发出来。

“X”则指的是开放平台。开放平台将开放网络能力，通过SD-WAN和POP节点资源为安全软硬件赋能，达到全链路体验最优；开放边缘能力，通过开放容器平台，提供第三方运行环境，实现专业安全能力的分布式服务；开放安全能力，利用全球分布式安全基础设施与安全硬件、数据中心形成云网协同；开发海量云安全威胁信息情报，与同业和客户形成立体防护；开放对接安全能力，在零信任框架上接入可信终端、可信传输、可信行为能力，且全环节向合作伙伴开放安全能力接入，为企业提供一体化零信任SASE服务。

版权信息

CHINA INTERNET SECURITY REPORT