网宿科技 | 网宿安全

2021年

中国互联网安全报告

CHINA INTERNET SECURITY REPORT

前言

随着世界多极化与经济全球化发展，国际竞争与博弈延伸至网络空间，面向产业链、政府等大规模针对性网络攻击频发，加上疫情的叠加与催化，网络安全形式越发严峻。

2021年发生了多起震惊全球的大规模勒索攻击、数据泄露、供应链攻击事件。如美国最大的保险公司CNA金融遭遇了安全漏洞勒索攻击，在发生两周后支付了4000万美元赎金才恢复文件访问权限；全球知名社交平台Facebook、领英等相继被曝发生涉及数亿用户的大规模数据泄露事件；年末更是爆出了被称作“核弹级”的Apache Log4j2漏洞，引发全球软件供应链安全灾难。

网络安全成为数字时代的重大课题，我国在2021年相继颁布了一系列网络安全法律法规，包括《数据安全法》、《关键信息基础设施安全保护条例》、《网络产品安全漏洞管理规定》、《个人信息保护法》等，将数据安全上升至国家安全层面，也使企业与组织在数据处理与网络安全方面，进入了有法可依、有法必依的新时代。

网宿科技作为全球领先的信息基础设施平台服务提供商和智能边缘安全领导者，深度关注互联网安全态势，并积极探索网络安全防御技术，不断提升安全防御能力，自2016年起持续发布《中国互联网安全报告》。

在本期报告中，网宿将基于2021年间网宿安全平台监测到的网络攻击行为与事件，结合网宿安全实验室积累的威胁情报技术和自身攻防经验，为企业提供防御技术、网络体系、数据安全、合规、安全管理等多方面的信息与建议，应对日益高发的网络安全威胁。

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。虽然网宿业务自身的调整作为一种客观存在的变量，会对数据所呈现出的趋势产生一定的影响，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。
- 报告根据2020年和2021年的攻防数据综合对比，分析了攻击趋势并做出判断。
- 本期报告重点发现了应用层攻击持续高发的态势，尤其是针对API业务的攻击呈爆发式增长；供应链漏洞更是显现出横扫级别的影响面。

1.1. 2021年DDoS攻击概览与趋势

- 2021年网宿安全平台监测到网络层、应用层DDoS攻击事件数量均增长了约60%；DDoS攻击带宽峰值显著上升。
- 传统重灾区——游戏行业遭受的网络层DDoS攻击数量、攻击峰值均位列第一。

1.2. 2021年Web应用攻击概览与趋势

- 2021年，网宿安全平台共监测并拦截Web应用攻击229.82亿次，为2020年同期的2.41倍，涨幅惊人。
- Web应用攻击方式分布较为分散，非法请求方法、SQL注入是攻击者使用最多的手段。
- Web应用攻击的聚焦度有所分散，除政府机构外，软件信息服务、房地产、金融等行业也成为了Web攻击主要目标。

1.3. 2021年恶意爬虫攻击概览与趋势

- 2021年，网宿安全平台共监测并拦截了超847.71亿次爬虫攻击，平均每秒发生2688次攻击，与2020年相比呈翻倍增长态势。
- 从攻击源分布来看，境外攻击源占比大幅增长，推测与后疫情时代，代购、海淘行业业务恢复有关。
- 软件信息服务是遭受恶意爬虫攻击最严重的行业，其次是房地产、交通运输、零售业。

1.4. 2021年API攻击概览与趋势

- 2021年，网宿安全平台共监测并拦截近150亿次针对API业务的攻击，攻击量已达到2020全年的3倍有余，呈爆发式增长。
- 恶意爬虫依然是针对API业务最主要的攻击方式，约占攻击总量的50%，但同比有所下降，攻击手段类型“一家独大”的状况趋于减弱。
- 零售与金融行业集中了将近七成的API攻击，分别占比34.99%和31.27%。

1.5. 2021年主机安全概览与趋势

- 2021年网宿安全平台探测到，超过60%的企业主机已应用了容器技术，可以预见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，同时对主机入侵检测能力提出更高要求。

第二章 DDoS攻击数据解读

2.1. DDoS攻击数量一路走高，而后持续在高位浮动

2021年，网宿安全平台日均监测并拦截网络层DDoS攻击事件21.55万次，同比增长62.96%；日均拦截应用层DDoS攻击请求14.90亿次，同比增长61.39%。

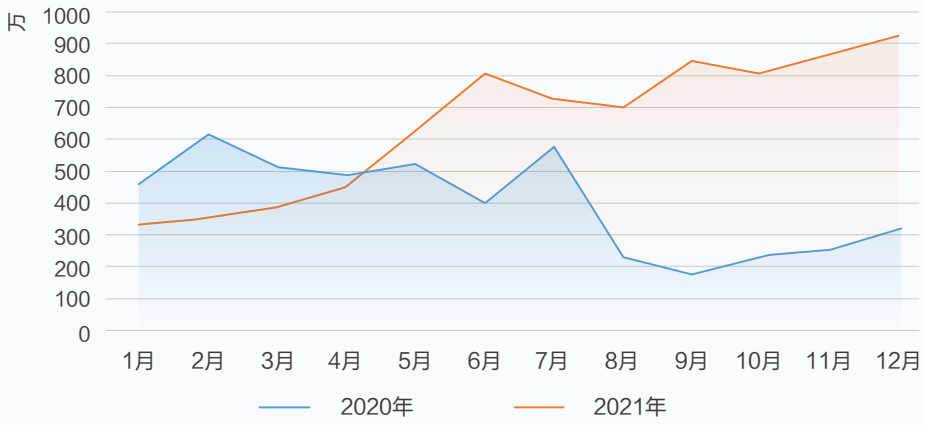


图2-1 2020/2021年网络层DDoS攻击事件月份分布

从月份走势来看，2021全年网络层DDoS攻击数量呈现持续增长态势，4月-6月增幅最大，之后趋于平稳。

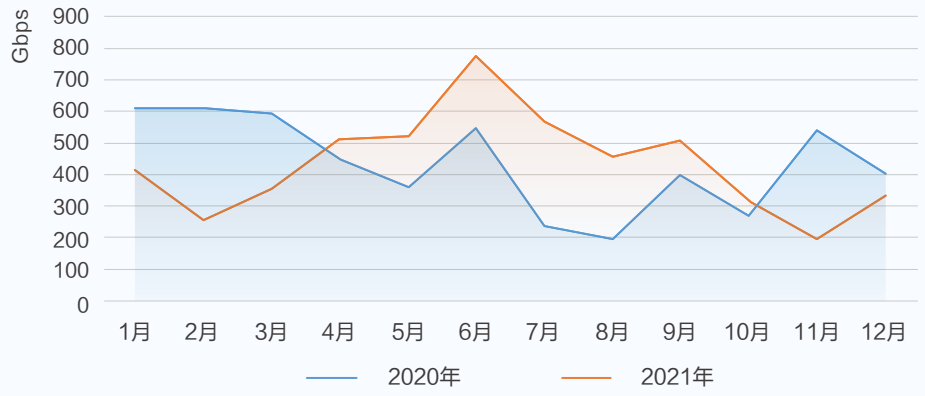


图2-2 2020/2021年网络层DDoS攻击峰值月份分布

2021年DDoS攻击带宽峰值出现在6月，达到774.58Gbps，比2020年峰值612.67Gpbs高出26.42%。峰值出现的月份也与往年不同，以往攻击峰值均出现在1月，而21年月度攻击峰值则是从2月开始一路上涨，到6月达到最高。

值得一提的是，在随后的2022年1月，网宿平台迎来了带宽峰值达到2.09Tbps的超大流量DDoS攻击并成功防御，攻击规模创历史新高。

2.2. 近七成DDoS攻击以游戏、电商行业为目标

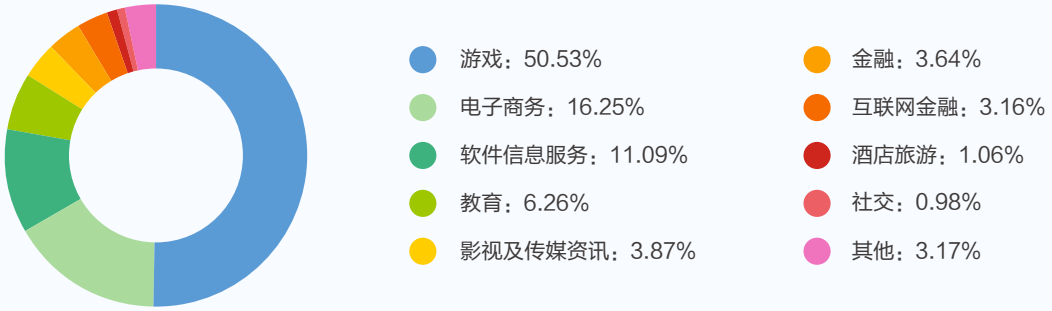


图2-3 2021全年DDoS攻击行业分布

从DDoS攻击事件的行业分布来看，游戏业成为2021年受DDoS攻击最多的行业，占比达到50.53%，远超其他行业。电子商务以16.25%的百分比占据第二位。两者遭受的攻击数量已接近总量的七成。位于第三、第四的则是软件信息服务（11.09%）和教育行业（6.26%）。

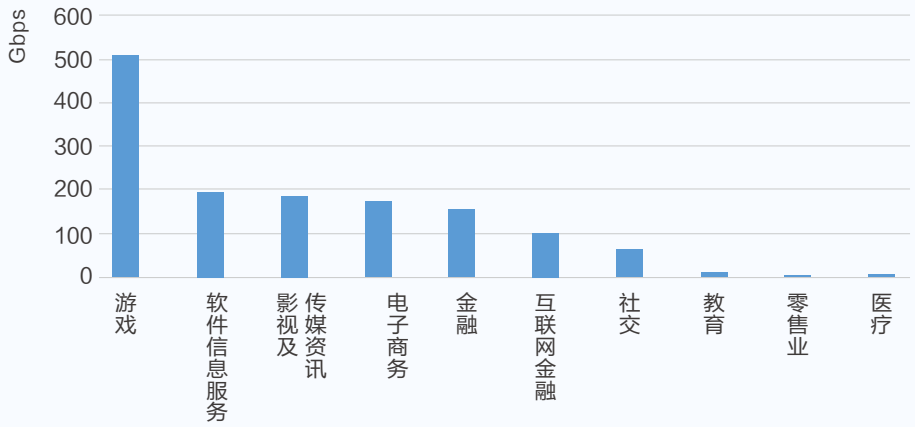


图2-4 2021全年DDoS攻击峰值Top 10行业

从各行业遭受的攻击带宽峰值统计来看，游戏、软件信息服务、影视及传媒资讯、电子商务行业位居前四，且游戏行业在攻击峰值上同样远超其他行业，达到508Gbps。受教育行业“双减”政策影响，2021年在线教育的业务规模和投资双双下降，受到的攻击规模也相应地有所下降。攻击数量及攻击峰值的行业分布，共同体现出DDoS攻击手段向多行业覆盖的趋势发展。

2.3. NTP反射放大攻击异军突起

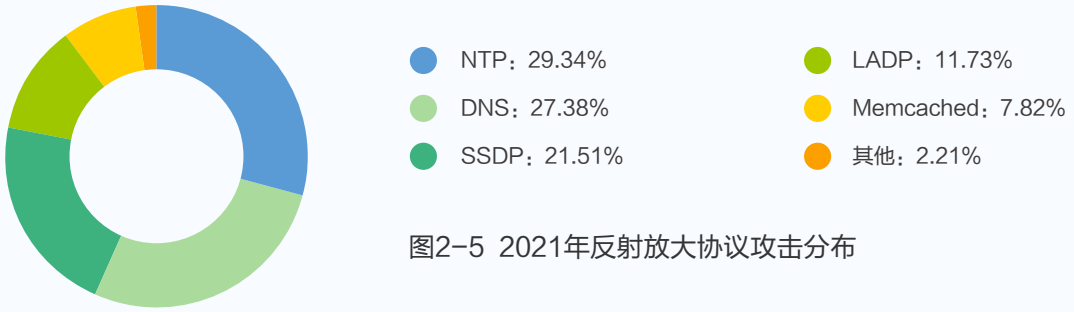


图2-5 2021年反射放大协议攻击分布

作为一种以较低成本即可产生巨大攻击力的DDoS攻击类型，反射放大攻击深受攻击者青睐。对网宿安全平台在2021年捕获到的反射放大攻击请求进行分析，发现SSDP、NTP、Memcache、DNS和LADP依旧是最为活跃的5种反射攻击协议。

与上一年不同的是，NTP反射放大攻击异军突起，反超以往占绝对优势的SSDP协议，跃升至第一位。NTP是网络时间协议（Network Time Protocol），攻击者利用可公开访问的NTP服务器，以及UDP协议无需前期建连即可发送数据的特点，对目标站点服务器发起大流量攻击。NTP反射放大攻击的活跃，表明还有大量配置不当的NTP服务器被暴露在公网上，为黑客所利用。

第三章 Web应用攻击数据解读

3.1. Web应用攻击量同比翻倍增长

2021年，网宿安全平台共监测并拦截Web应用攻击229.83亿次，同比2020年增长141.30%，呈翻倍增长态势，显示出此类攻击的威胁持续增大。

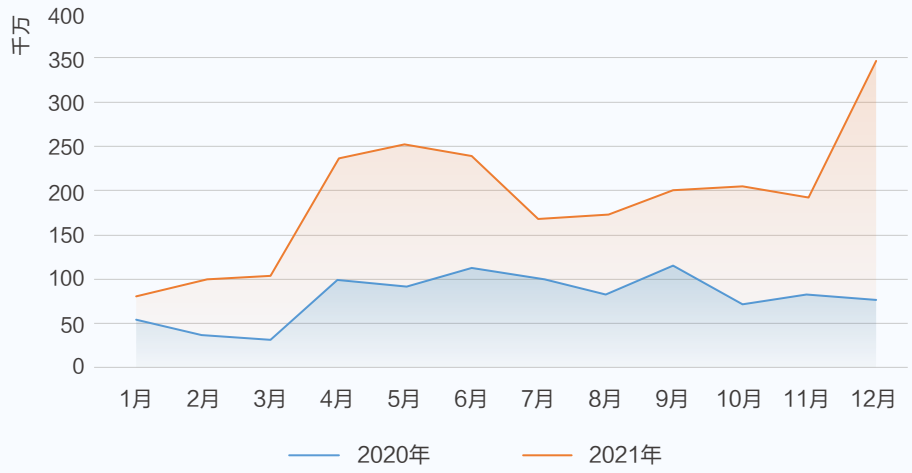


图3-1 2020与2021年Web应用攻击次数趋势

企业数据资产价值上升、Web漏洞高发、当前国际环境下出于政治目的发起的攻击行为增加，以上种种因素共同推动了Web应用攻击持续高速增长。从攻击行为来看，Web应用攻击的目标以窃取数据为主，随着2021年《数据安全法》、《个人信息保护法》等相关法规的实施，企业或组织若未能建立起有效的网络安全防线，不仅将面临数据泄露的经济风险，还将面临法律风险。

3.2. Web攻击手段呈现多样化趋势

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，从中也能看出攻击手段的分布情况。

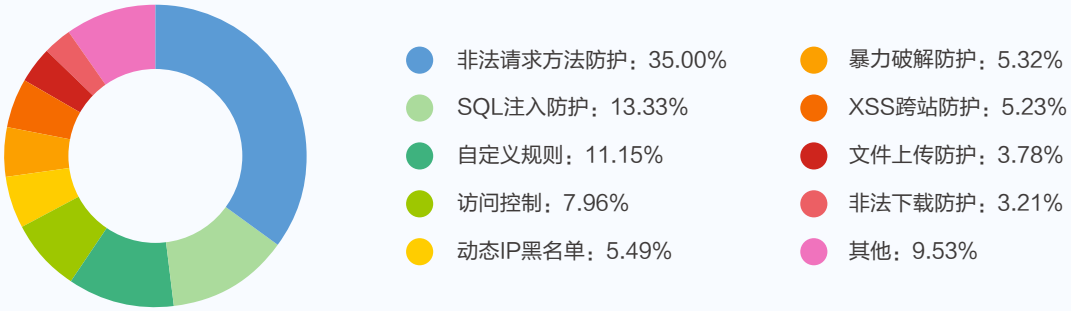


图3-2 2021全年Web应用攻防手段分布

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方法防护（35.00%）、SQL注入防护（13.33%）、自定义规则（11.15%）。

值得注意的是，本次统计中，业务端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，针对业务自身情况和特定的攻击方法制定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。网宿安全平台基于对攻击源的特征分析、行为模式识别、AI离线检测、威胁情报等多种方式识别Web扫描器行为后，能够通过非法请求方法防护、访问控制（7.96%）、动态IP黑名单（5.49%）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扫描的威胁，同时降低自动化扫描器对网站的负载压力。

3.3. 来自境外的攻击大幅上升

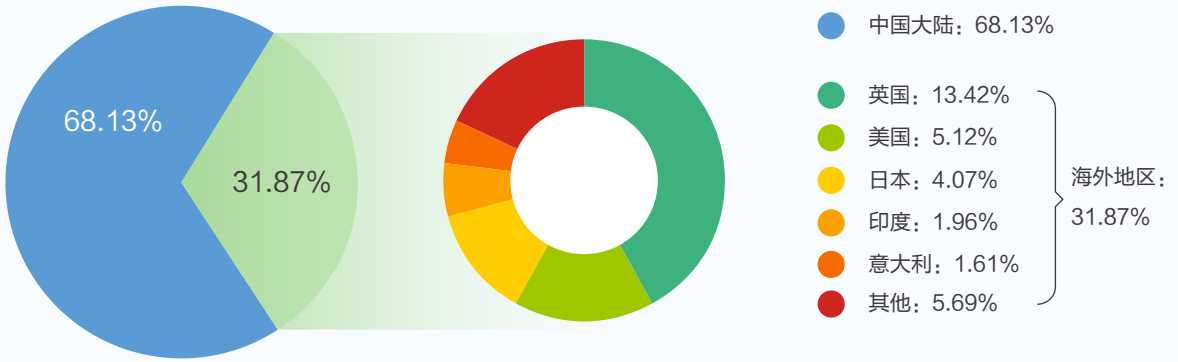


图3-3 2021年Web应用攻击全球来源分布

通过对攻击IP的地理位置进行统计，发现2021年来自境外的Web应用攻击IP数量同比2020年暴涨了357.16%，在全球攻击源中的占比也由2020年的13.30%上升至31.87%，增长了约19个百分点。境外Web攻击源的大幅上升，推测与日趋紧张的地缘政治局势有关。

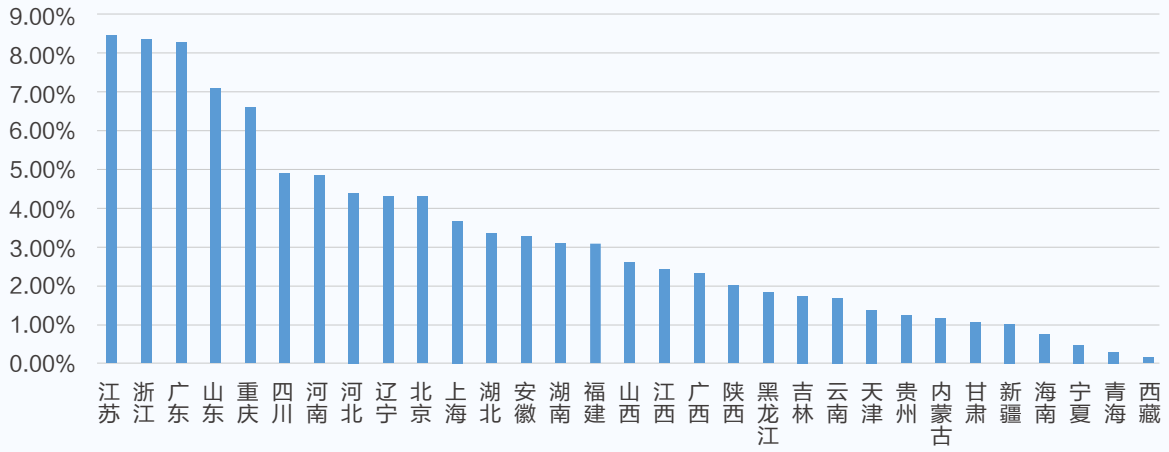


图3-4 2021全年来自中国大陆的Web应用攻击来源分布

统计攻击来源在中国大陆的省份分布发现，2021年前15位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10.64%、8.62%、7.77%。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前三名的位置。

3.4. 软件信息服务遭受超60亿次攻击

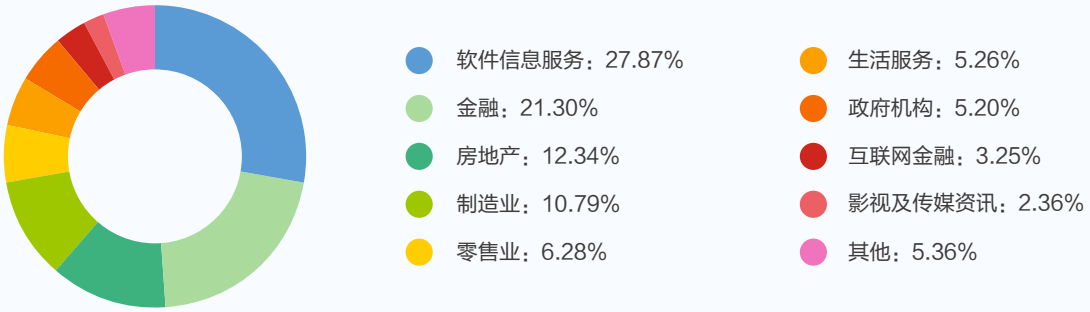


图3-5 2021全年Web应用攻击行业分布

从2021年的攻击数据来看，软件信息服务和金融成为Web应用攻击最多的行业，针对两者的Web攻击量达到近112亿次，几乎占了全年的一半。房地产（12.34%）、制造业（10.79%）、零售业（6.28%）分别排列第三、第四和第五位。

第四章 恶意爬虫攻击数据解读

4.1. 平均每秒发生2688次爬虫攻击，攻击量连年翻倍增长

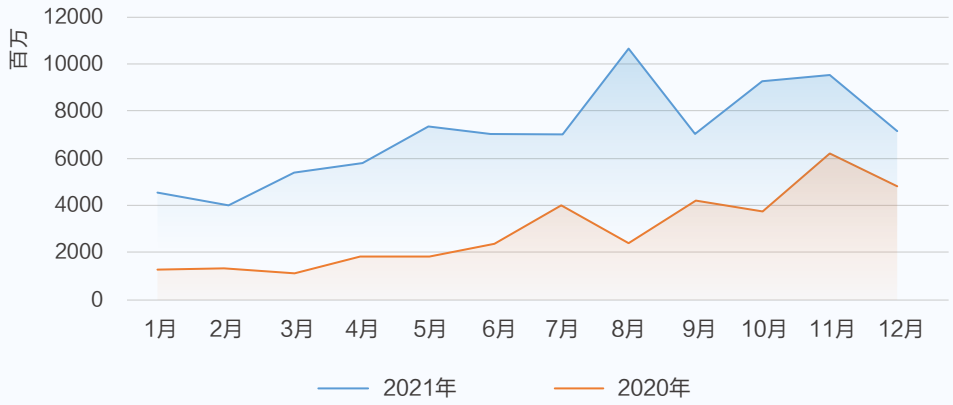


图4-1 2020/2021年恶意爬虫攻击数量趋势

2021年网宿安全平台共监测并拦截了847.71亿次恶意爬虫攻击，平均每秒拦截攻击2688次，攻击量达到了2020全年的2.36倍。近三年恶意爬虫攻击量连年成倍增长，安全威胁日益明显。

4.2. 恶意爬虫境外攻击源比重明显回升

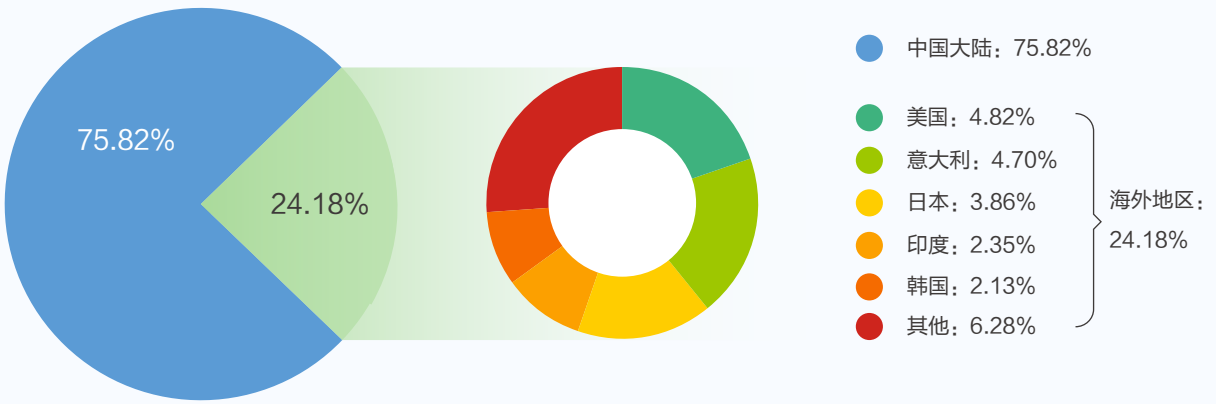


图4-2 2021年恶意爬虫攻击全球来源分布

从网宿安全平台监测并拦截的源IP分布来看，2021年全年的恶意爬虫攻击超七成来自于境内。境外攻击源占比从去年同期的7.08%上升至24.18%。

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有关。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回升。

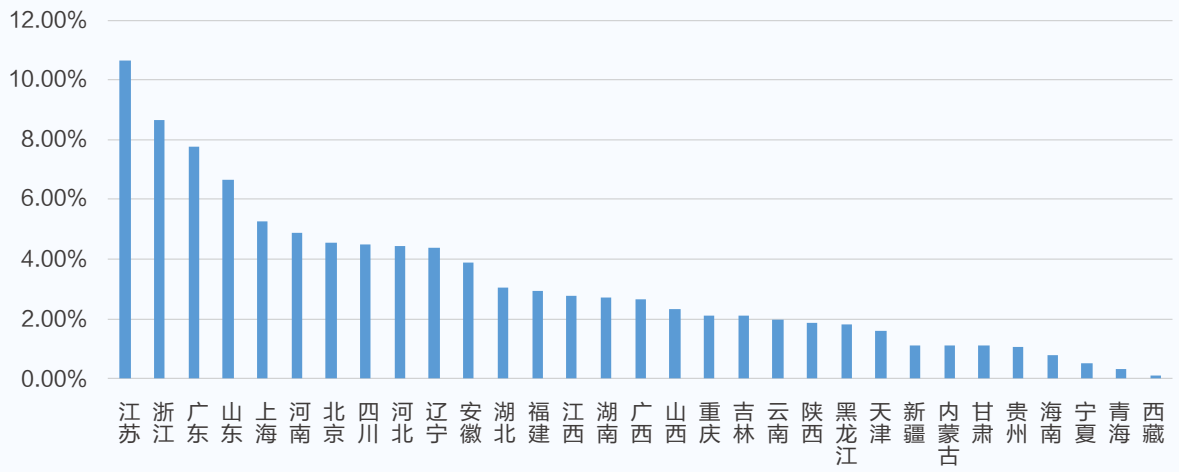


图4-3 2021全年来自中国大陆的恶意爬虫攻击来源分布

江苏、浙江、广东的恶意爬虫攻击分别在境内攻击源中占比10.64%、8.63%、7.77%，成为来源数量最多的三个省份。整体上看，境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。

4.3. 恶意爬虫攻击行业分布较分散

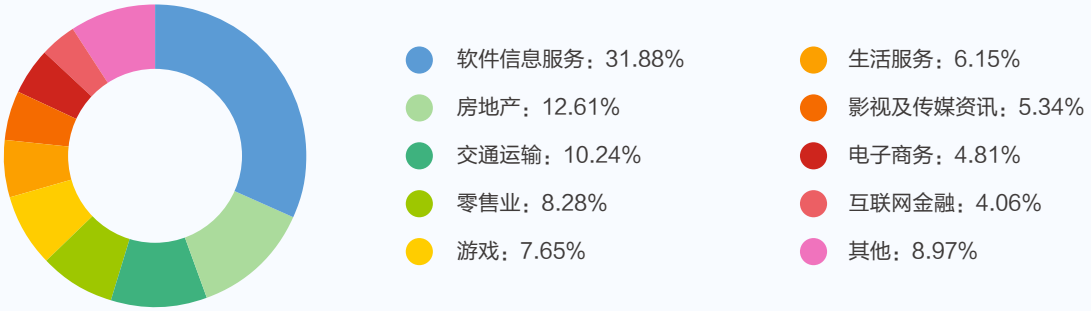


图4-4 2021全年恶意爬虫攻击行业分布

恶意爬虫攻击的行业分布，呈现出集中度低，“多点开花”的态势。遭受攻击最多的是软件信息服务行业（31.88%），其次是房地产行业（12.61%），交通运输（10.24%）、零售业（8.28%）、游戏（7.65%）分别排列第三位至第五位。

其中，交通运输行业的排位从2020年的第六，重新回到前三位，体现出疫情对交通运输业的负面影响逐渐消除，抢票类爬虫攻击态势有所恢复。

第五章 API攻击数据解读

5.1. API威胁进入爆发期，攻击量同比增长超200%

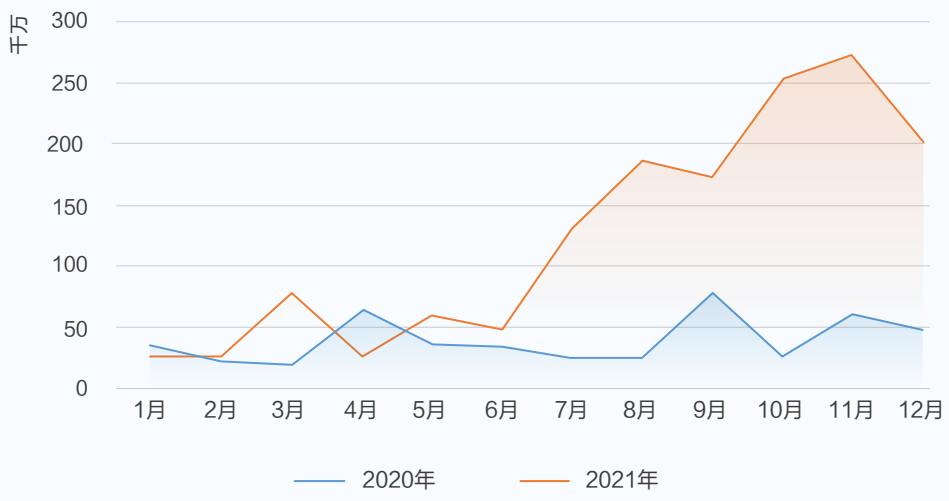


图5-1 2020与2021年API攻击次数趋势

2021年全年，网宿安全平台共监测并拦截147.98亿次针对API业务的攻击，平均每秒发生攻击469次，全年攻击量是2020年的3倍有余，呈爆发式增长。尤其是下半年，攻击量大幅跃升。

数字化转型的背景下，企业开放的API越来越多，面临的风险也越来越高，API业务逐渐成为众多黑客的攻击目标。

5.2. API攻击手段显示出多样化趋势

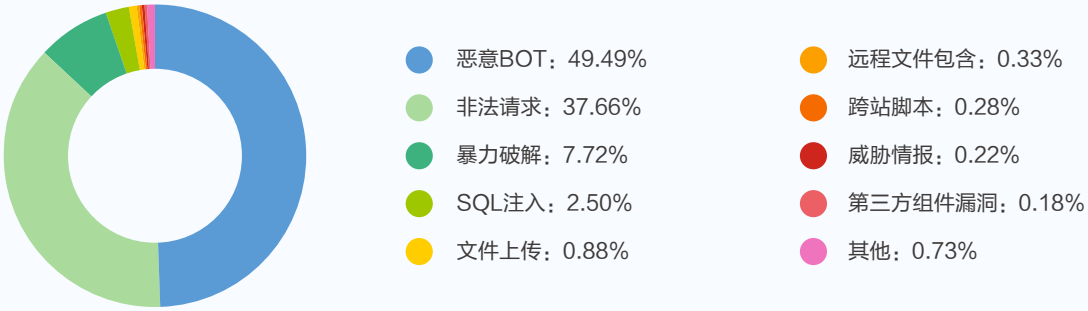


图5-2 2021年API攻击方式分布

在针对API业务发起的攻击中，恶意爬虫依旧是最主要的攻击方式。在2021年的API攻击数据中，恶意爬虫攻击占整体攻击数量的49.49%，同比有所下降。

排第二、三位的分别是非法请求（37.66%）和暴力破解（7.72%）。其中暴力破解攻击手段多用于账户API，严重威胁到个人资产安全。整体来看，针对API业务的攻击手段类型趋于多样化。

5.3. 零售业、金融业成为API攻击重灾区

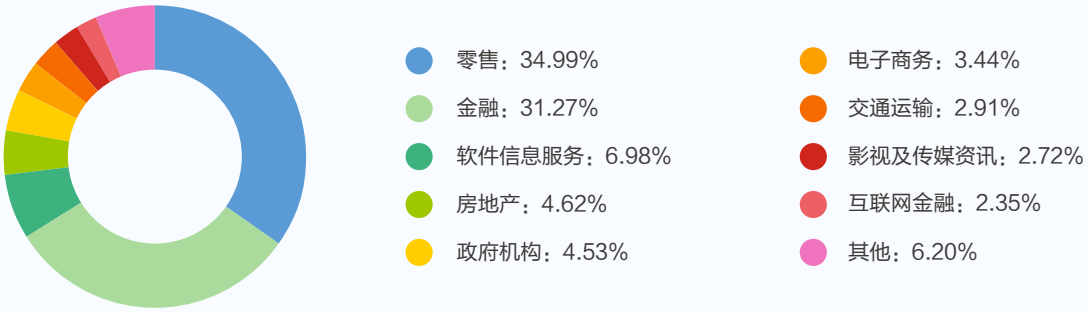


图5-3 2021年API攻击行业分布

2021年，零售行业成为受API攻击最多的行业，攻击量占整体比重的34.99%。金融行业占31.27%，排在第二。

零售与金融行业集中了将近七成的API攻击，体现出这两个数字化转型程度较深的行业，在面临API攻击时，也首当其冲。交通运输占比有小幅增长，与疫情较2020年有所缓解带来的跨区域和跨境客流增长有直接关系。

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

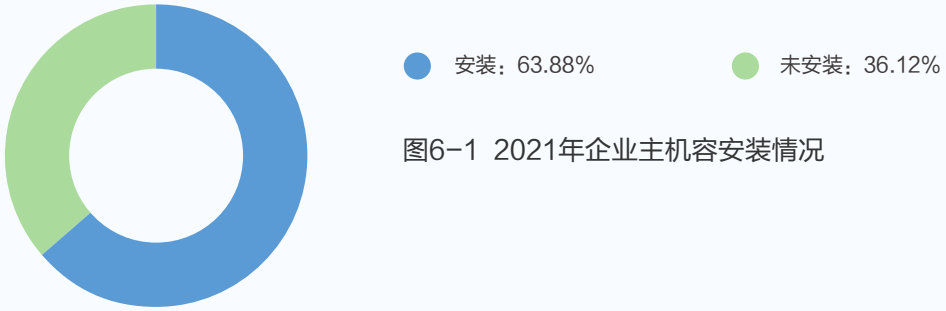


图6-1 2021年企业主机容安装情况

网宿主机安全探针检测发现，63.88%的企业主机有安装容器相关软件，相较于2020年同期的占比40.27%，增长了约24个百分点。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

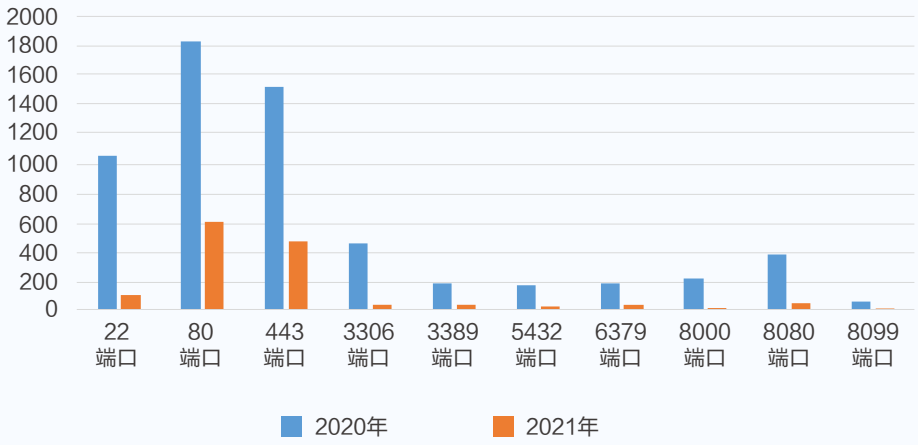


图6-2 2020与2021全年公网开放端口数量对比

与2020年相比，2021年网宿主机探针采集到的数据显示，公网开放端口数量大规模下降。

公网开放端口数量下降主要源于规律性的网络攻防演练，有效提升了管理端口的使用规范。 在攻防演练结束后，公网开放端口数量依然保持在较低的值，说明攻防演练对企业安全管理及安全意识有较高的提升作用，端口管理也更为常态化，使攻击面大幅缩减。

6.3. “核弹”级漏洞Log4j2影响面一骑绝尘

图6-3 2021年网宿主机安全平台捕获的高危漏洞Top 10

针对高危漏洞的入侵依然是以利用应用组件漏洞为主，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。

值得注意的是Apache Log4j2远程代码执行漏洞（CVE-2021-44832）影响面巨大。截至2021年12月31日，即本次报告统计周期结束，该漏洞被公布仅半个月时间，引起的入侵事件数量就超过了第2-9名高危漏洞引起的入侵事件数量总和。并且Log4j2漏洞的利用方式还在不断变形，使得官方发布的升级版本不断被发现新的绕过方式。该漏洞信息还需持续追踪，才能准确掌握可能受其影响的资产范围。

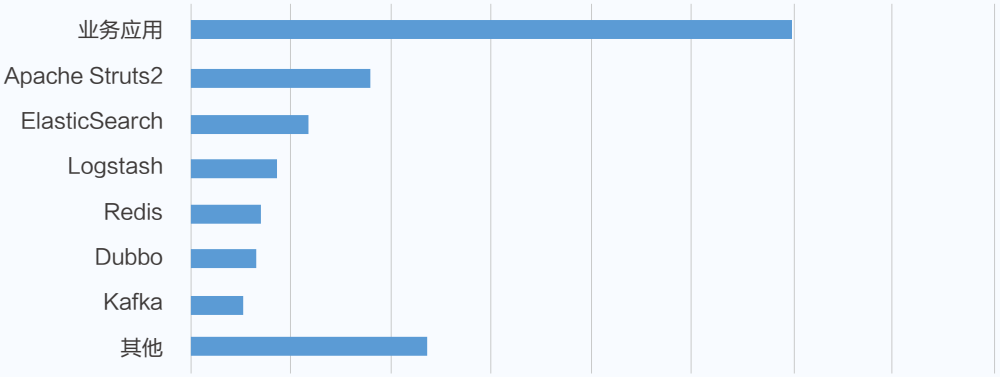


图6-4 2021年受Log4j2漏洞影响的中间件的影响面情况

通过网宿主机探针的资产采集模块对受Log4j2远程代码执行漏洞影响的中间件所造成的影响面进行分析，发现Log4j2组件在业务应用中被大量使用，影响的主机范围最广；Log4j2也常见于Struts2、ElasticSearch、Logstash、Redis、Dubbo、Kafka等流行的中间件，受这些中间件影响的主机合计约占36.13%。

6.4. 进程隐匿技术使人工入侵排查变得困难

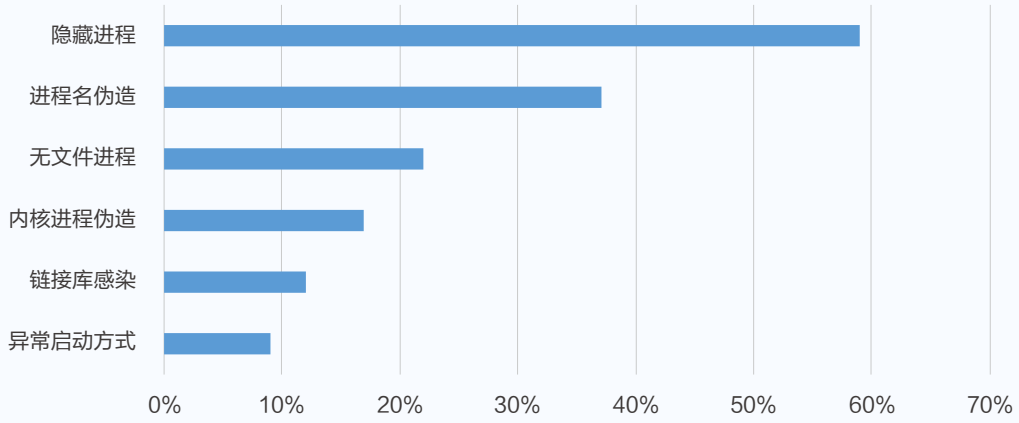


图6-5 2021年进程异常行为检出率

从网宿主机探针识别到的异常进程数据中可看出，主机上出现的异常进程大量使用了规避检测的技术，以达到干扰杀毒软件检测及人工入侵排查的目的。

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。隐藏进程技术可以使应急响应人员无法查看到恶意进程，加大入侵分析的难度。

无文件进程、异常启动方式、链接库感染等行为在入侵事件中的占比在10%~30%之间。这些技术能够规避杀毒软件的检测，使杀毒软件无法获取到进程文件内容，无法与病毒特征库进行匹配。

6.5. 超70%的入侵事件利用定时任务实施权限维持

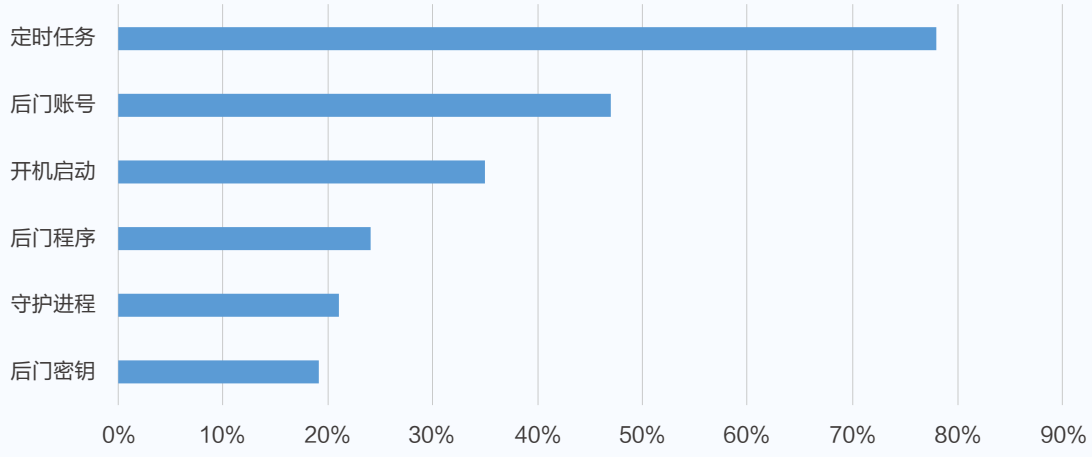


图6-6 2021 年权限维持行为检出率

通过对网宿主机探针识别到的恶意行为进行检测分析，95%的入侵事件中都使用了权限维持攻击方法。其中通过定时任务维持恶意脚本、程序运行的占比最多，高达78.12%，其次是后门帐号（46.58%）、开机启动（35.35%）。

恶意定时任务通常通过以恶意脚本执行恶意行为的方式来实现，例如执行病毒木马、恶意指令等。通过使用恶意脚本，攻击者更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. 兼容性强、对系统影响小的Rootkit更受攻击者青睐

Rootkit是隐匿能力最强的恶意软件，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。

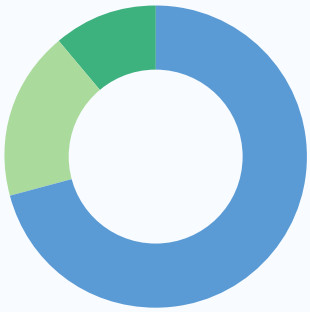


图6-7 2021年Rootkit类型分布

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70.87%，其次分别为预加载链接库（18.08%）、LKM内核模块加载（11.05%）。

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。常见被替换的可执行文件如ps、top、sshd等，替换后能够实现进程隐藏、后门等功能。

LKM内核Rootkit虽然隐蔽性高、功能强大，能够灵活地对进程、网络、Rootkit自身、文件进行隐藏。但其存在内核兼容性问题及破坏系统稳定性的风险，因此使用占比较低。

当前，在入侵主机后通过植入挖矿木马进行牟利，已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规避会对系统造成破坏的入侵行为，以便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

网络威胁与攻击始终在不断变化。从前述报告中可以看出，2021年的数据所显示出的攻防态势相比2020年，呈现出了一些不同的特点。可见企业在建设网络安全防御体系时，需要根据攻击技术发展趋势随时调整防护思路和策略，才能对攻击进行有效防御。

一、软件供应链安全风险加剧，企业迫切需要建立有效应对手段

网宿安全平台在本期报告周期内统计到，由席卷全球的Log4j2漏洞所产生的入侵事件已经占到全部主机安全入侵事件总数的近一半，攻击目标包括依赖该组件的开源软件及企业内部开发的软件平台。作为被大量业务框架使用的开源工具，Apache Log4j2漏洞的危害可以说是“核弹”级。在漏洞曝光不久之后，针对该漏洞的利用行为很快就在网络上广泛流传，引起大规模入侵。至今该漏洞的影响还在发酵，预计负面影响还会长期持续。

全球最大的开源组件中央仓提供商Sonatype在《2021年软件供应链现状报告》中统计，2021年世界上的软件供应链攻击增加了650%。Gartner也预测，到2025年，全球45%的企业将遭遇软件供应链攻击，比2021年增长三倍。现代企业软件大部分是混合代码，由于开源软件开放共享的特性，很多组织都会利用高质量且免费的开源组件来组成他们的软件产品。随着全球产业的数字化升级，企业对于开源软件的依赖也日益提升，任何一个比较底层的开源组件出现漏洞，都将造成“攻其一点，伤及一片”的广泛影响。

企业该如何有效应对开源软件供应链漏洞带来的巨大安全风险？网宿安全实验室建议打组合拳，以综合手段防护。在漏洞曝光初期，可以通过主机安全产品进行资产采集和漏洞检测，快速定位软件漏洞，尽快推进漏洞应用升级；同时结合Web应用防护产品提供的虚拟补丁来拦截针对该漏洞的攻击利用行为。在应用开发阶段，可以使用软件成分分析(SCA)技术手段，加强应用上线前的安全管控，避免应用带病上线。

二、数据安全上升到国家战略高度，API数据安全风险突出，亟需强化综合防控体系

2021上半年报告中所指出的业务安全威胁持续升级现象，在2021全年数据中仍然延续。其中API攻击的爆发式涨幅尤为引人注目，同比增长超过200%。攻击者的主要目标是获取企业数据。API经济下，API数量井喷。API访问环境越发开放、通过API流转的数据价值水涨船高，使得API攻击趋势走高。

越来越多的企业和组织通过向合作伙伴、客户开放API，与商业生态共享数据、算法、交易、流程和其他业务功能，以挖掘新的价值源泉，构建新的核心能力。例如银行业的“开放银行”战略，即是以向各行业开放金融服务接口，推动业态变革的典型代表。但开放API也加聚了数据隐私与安全的风险，金融业居高不下的API攻击量就是直观体现。

然而，企业间普遍存在着高速增长的API业务与较弱的API防控体系之间的错位，只依靠基于规则的应用漏洞攻击防护，已经无法应对攻击者通过滥刷、越权访问等方式面向正常业务接口或被遗忘的僵尸API发起攻击，达到批量窃取或篡改数据的目的。

加上2021年《数据安全法》和《个人信息保护法》的相继颁布，采取必要措施保障数据安全和个人隐私信息已经成为了企业必须履行的法律义务。网宿安全实验室建议企业采用能够自动化发现API、带有API访问行为检测功能，并支持API全生命周期管理的高级API防护产品，以消除僵尸API隐患，防止非授权调用和超额调用，确保数据安全。在此基础上，网宿安全还建议选用支持WAAP（云Web应用程序和API保护）方案的厂商，结合Web应用程序防火墙、DDoS防护、爬虫管理能力，形成应对API攻击、Web应用攻击等的综合防护能力。

网宿WAAP方案深入洞察用户场景，基于全球分布式平台，整合DDoS云清洗、WAF、BotGuard、API安全与管理能力做全栈协同和统一管控，结合业务流分析、AI模型、黑灰产情报、漏洞威胁情报、营销风控模型，提供用户视角的先进WAAP服务。

三、企业加速转向零信任，带动对安全无缝集成和SASE的需求

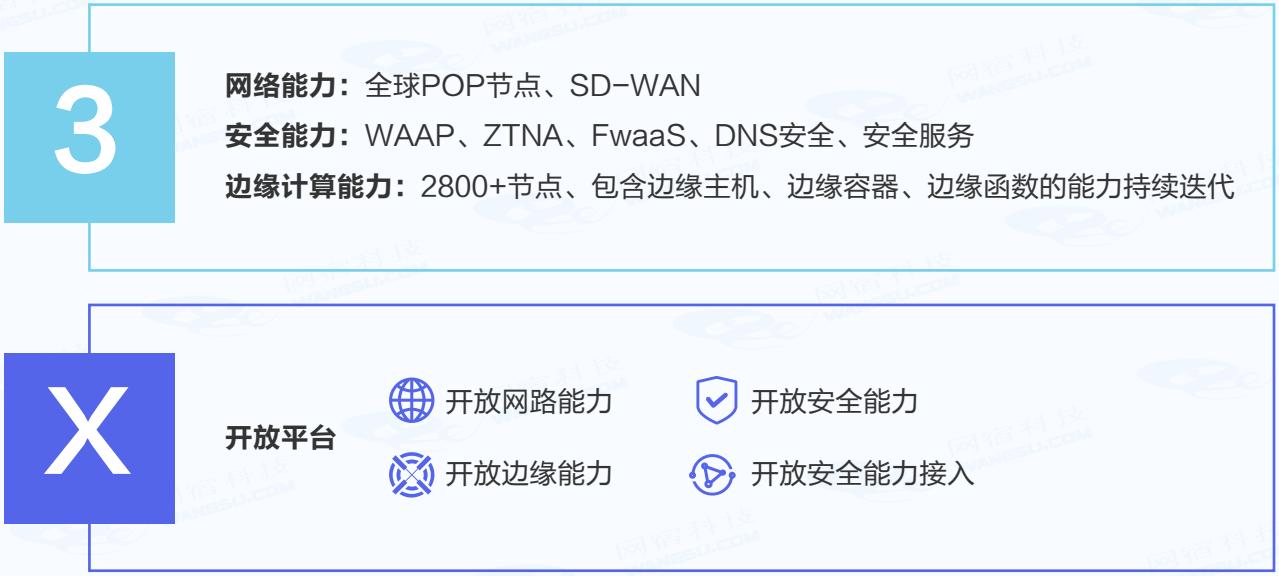
新冠疫情已持续近三年，企业在远程办公上、业务上云、攻击防御等方面的实践不断深入，越来越多的企业意识到传统网络安全防护边界在不断消解，对于当下流行的零信任防护技术一改观望态度，从以ZTNA（零信任网络访问）逐步取代VPN入手，制定战略和时间规划表，向新一代网络安全模型转变。

在安全防护技术更新换代的过程中，对接不同供应商、策略和控制台的复杂性给企业安全技术实施带来压力。企业对供应商进行整合、对策略及控制台等实现无缝集成将逐渐成为趋势。Gartner预测，到2024年，30%的企业将采用云交付的SWG(安全Web网关)、CASB（云访问安全代理）、ZTNA和FWaaS（防火墙服务）功能，而2020年这一比例不到5%。

在实现对安全功能的集成后，下一步再完成对广域网功能的集成，这就达成了SASE（安全访问服务边缘）目标，即将广域网功能与全面的网络安全功能融为一体。

SASE作为备受安全行业关注的下一代网络安全模型，能够实现基础设施、运营和安全团队以一致和集成的方式提供丰富的网络和网络安全服务，支持数字业务转型、边缘计算和移动办公等需求。观察到这一市场趋势的网安厂商相继提速布局SASE领域，尝试推出相关方案。其竞争力的关键就在于，是否能够更完整、成熟地支持上述各项SASE关键组件功能。

作为智能边缘安全领导者，网宿科技在2021年10月份创新性地提出以“3+X”能力框架落地SASE模型，“3”由安全能力、网络能力、边缘计算能力3项组成，“X”则指的是开放平台。



经过近半年的发展，网宿“3+X”能力持续进化：

在安全能力方面，继2021年2月发布ZTNA（零信任网络访问）产品网宿安达SecureLink后，网宿进一步升级产品能力，**形成“3+1”安全访问体系**，即身份可信、终端可信、行为可信的“3”个可信原则+从加密传输、边缘防护、应用隐身层面打造的“1”套平台安全能力，确保远程或本地办公人员访问企业资源的全过程安全。

而后，网宿在深耕DDoS防护、云WAF、Bot防护能力的基础上，又针对API业务特性**推出API安全与管理产品**，提供自动化API发现、API全生命周期管理及持续安全检测能力，形成管理-保护-分析服务闭环，合上WAAP（云Web应用程序和API保护）能力最后一块“拼图”。至此，**网宿已完全具备WAAP、ZTNA、FwaaS、DNS安全能力，以及多项成熟的安全专家服务。**

在网络和边缘计算能力方面，网宿分布在全球的2800+边缘节点及节点之间的高速网络（SD-WAN），不仅能够有效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，并且发展出了新一代CDN可编程能力，将原本由源站处理的业务逻辑转移到CDN边缘节点上，支持用户“搭积木”式地自有组合各类个性化边缘业务，从而快速完成新应用或新服务的全球化部署，极大缩短开发周期，进一步降低源站负载。

未来，网宿安全将基于持续进化的3大能力，进一步打造开放效应，利用全网海量数据开放云安全威胁信息情报，与上下游安全技术和企业已有安全防御体系结合，形成立体防护，**实现一体化SASE安全服务目标，共建网络安全。**

版权信息

CHINA INTERNET SECURITY REPORT