网宿科技 | 网宿安全

2022 上半年

中国互联网安全报告

CHINA INTERNET SECURITY REPORT

前言

进入2022年，在国际冲突与疫情的叠加影响下，全球网络空间对抗升级，大规模针对性网络攻击有增无减，中国互联网持续承受境外网络攻击压力。世界经济论坛在年初发布的《2022年全球风险报告》将网络风险加剧列为2022年全球面临的的主要风险之一。

数据安全与合规成为今年上半年网络安全态势最突出的关键词。上半年全球范围内已发生多起大型组织数据泄露事件，数据安全问题愈演愈烈；同时，世界主要国家和地区也在不断完善数据安全、个人信息保护、关键信息基础设施保护、供应链安全等方面的政策法规。我国继《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规后，今年2月修订版《网络安全审查办法》正式施行，通过规范网络平台运营者开展数据处理活动，进一步确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全。

网宿科技作为全球领先的边缘计算及安全服务商，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2022上半年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、自身攻防经验和网络安全产业趋势洞察，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。

关于报告

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2022上半年及往年同期的攻防数据综合对比，分析了攻击趋势并做出判断。

目录

第一章
核心发现

1.1. DDoS攻击强度步入新量级

上半年网宿安全平台日均监测网络层DDoS攻击（流量攻击）事件42.90万件，应用层DDoS攻击（CC攻击）事件1170件。攻击强度上，网宿安全平台成功拦截的网络层攻击峰值达2.09Tbps，应用层攻击峰值更是达到创当时全球纪录的3470万QPS。结合目前更新的业内已知DDoS攻击峰值纪录，2Tbps（网络层）、3000万QPS（应用层）的量级已不是个例。攻击强度步入新量级，对DDoS防御能力提出了更高的要求。

1.2. 供应链攻击威胁显著提升

在本次报告的统计周期中，利用第三方组件漏洞的Web攻击量达到了2021年同期的6.2倍，在Web攻击手段中的排位也从第12位跃升至第3位。在主机安全数据中，也显现出高危漏洞几乎都来自于开源的第三方组件，并且以Log4j2为代表的主流底层组件历史漏洞，修复效率不容乐观。随着企业对于第三方开源组件的依赖也日益提升，针对第三方组件的攻击还将持续高发，影响面广大且深远。

1.3. 黑产攻击手段自动化、智能化程度进一步提升

上半年网宿安全平台监测到攻击数据中，自动化的爬虫攻击相比2021年同期增长了1倍以上，继续保持了翻倍增长的态势，并且大量见于垃圾注册、批量登录、撞库、作弊套利等营销业务风控场景。其中具有高度伪装能力的智能化爬虫数量增长了约3.5倍。爬虫的智能化，给人机识别带来了更大的挑战。

1.4. API安全威胁爆发式上升，业务逻辑漏洞易遭攻击

作为一种流转着大量数据的特殊Web 业务，API接口在如今的API经济下成为了网络攻击的重点目标，甚至已经是数据泄露的主要风险敞口之一。2022上半年，针对API业务的攻击量继续高速增长，相比去年同期翻了约1.7倍，且绝大部分都集中在电商、影视及传媒资讯、交通运输、软件信息服务、政府机构这几个行业领域。

不同于传统Web业务，大量API攻击针对的是API业务设计层面上的漏洞，实现未授权、越权访问，尤以恶意构造请求参数的攻击行为为最。这类攻击难以通过传统Web防护规则进行识别，需要通过专业的API安全监测管理手段进行防护。

1.5. IPv6攻击源呈指数级增长，安全问题显现

随着我国步入“IPv6流量时代”，大量 IPv6 网络和业务上线和应用，IPv6网络安全问题凸显。今年上半年网宿安全平台捕获的IPv6攻击IP数量已比2年前翻了10倍。在IPv6攻击中，爬虫攻击数量最多，达到18.97亿次，约占总量的八成，攻击行业重灾区则是互联网服务供应商、金融机构、政府机构，建议重点防护。

1.6. 大规模远程办公暴露出大量安全问题

新冠疫情的长期影响，客观上带动了全球范围内远程办公的普及。在网宿安全服务的企业用户中，已有接近89%使用远程接入技术，并且远程接入终端中员工自带设备（BYOD）的占比已达到近三成。但大规模远程办公也暴露出了大量的安全问题，如：终端用户安全意识薄弱导致终端设备安全基线低；内网应用易被网络钓鱼、漏洞利用、凭证窃取等方式攻陷；内部数据多通过即时通信和电子邮件等工具被泄露；针对办公网络的APT攻击持续上升，等等。

1.7. 容器普及率超七成，“安全左移”理念接受度显著提升

在网宿安全服务的企业主机中，容器软件安装率已超过70%，增长迅速。尽管容器的大量应用暴露出了业务开发人员在权限管控等环节上还存在安全意识不足的问题，导致容器逃逸等重大安全风险，但同时也有越来越多开发人员接受了“安全左移”理念，在容器构建阶段就开展安全扫描，从而提早发现安全风险，避免深层安全问题留存到生产环境，造成更大的损失。

第二章
DDoS攻击数据解读

2.1. 攻击量大幅增长，攻击强度创历史新高

2022年上半年网宿安全平台日均监测并拦截网络层DDoS攻击事件42.90万件，同比大幅度增长161.02%；日均监测并拦截应用层DDoS攻击事件约1170件，秒均拦截应用层DDoS攻击请求1.21万次。

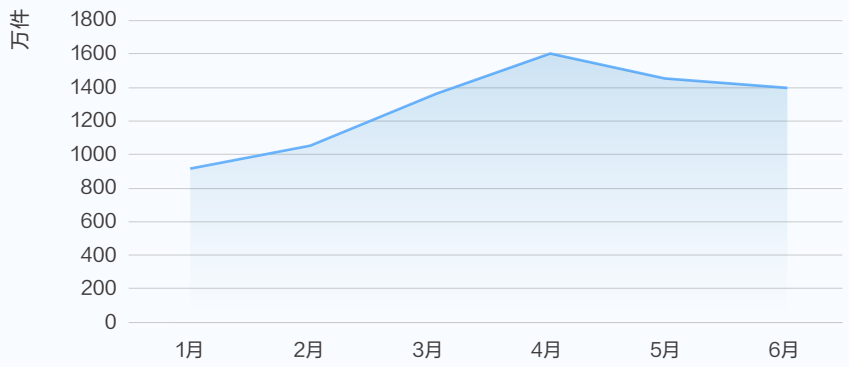


图2-1 2022上半年网络层DDoS攻击事件数量走势

图2-2 2022上半年应用层DDoS攻击事件数量走势

从攻击事件数量的月份分布来看，网络层DDoS攻击从1月至4月逐渐走高，而后略有回落；应用层DDoS攻击则在1月达到4.67万件的高峰，之后的5个月走势都较平稳地落在3~3.5万件之间。

在攻击规模上，上半年网络层和应用层攻击规模均创新高。1月16日，网宿平台遭遇并清洗了峰值达2.09Tbps的超大流量DDoS攻击。4月24日，网宿平台成功防御峰值高达3470万QPS的应用层CC攻击，规模之大超越了当时全球已知最高CC峰值纪录。

2.2. 近七成DDoS攻击以游戏、电商行业为目标

对DDoS攻击发生时段进行统计分析，无论是网络层攻击还是应用层攻击，都基本遵循凌晨攻击量下降，白天攻击量回升，晚上20:00-22:00达到高峰的规律，体现出攻击者为了使破坏效果最大化，攻击发起时间和网民上网峰谷时间段基本一致。

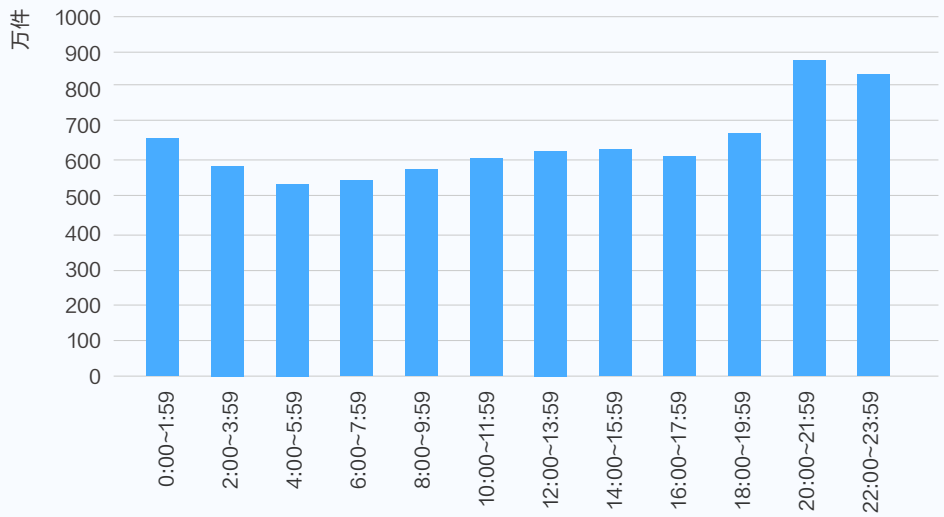


图2-3 2022上半年网络层DDoS攻击发生时段分布

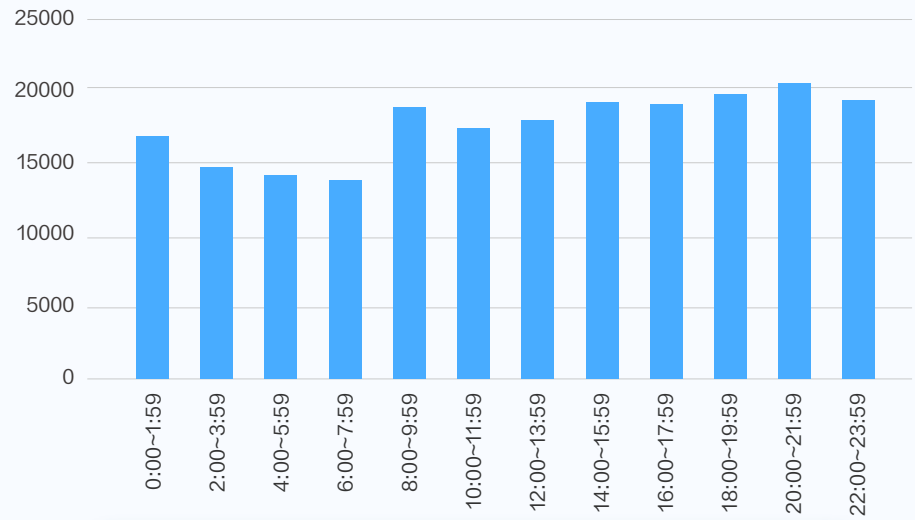


图2-4 2022上半年应用层DDoS攻击发生时段分布

2.3. 75%的攻击流量来自能产生反射放大的UDP攻击

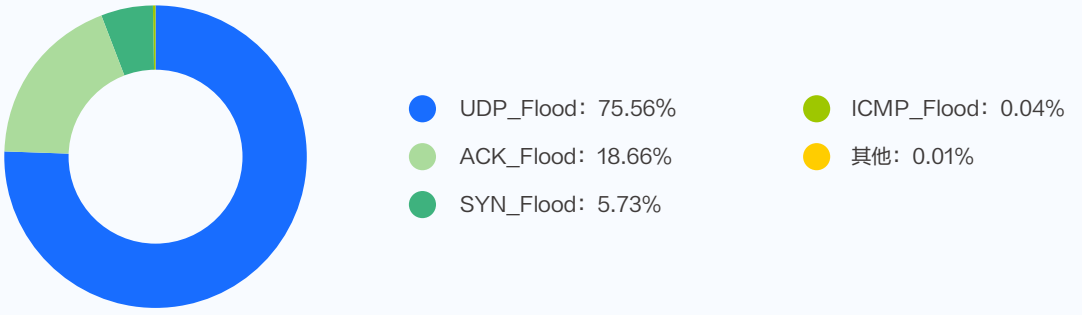


图2-5 2022上半年网络层DDoS攻击类型分布

从攻击手段上看，网络层攻击中，75.56%的流量都来自于实现简单、效果好的UDP_Flood攻击，其次是ACK_Flood攻击（18.66%）和SYN_Flood攻击（5.73%）。

目前比较普遍的UDP_Flood攻击都是反射放大攻击，能够以低成本产生巨大攻击力。网宿安全平台在2022上半年捕获到的反射放大攻击中，NTP、SSDP、Memcache这三种协议就占据了超90%的比例。

2.4. 游戏业依然是DDoS重灾区

上半年，游戏行业依旧遭遇了DDoS攻击“集火”。以游戏行业为目标的网络层攻击占到了总量的72.5%，比去年同期的占比还增长了13个百分点。同时，游戏行业遭受的应用层攻击量也排进了前三位。

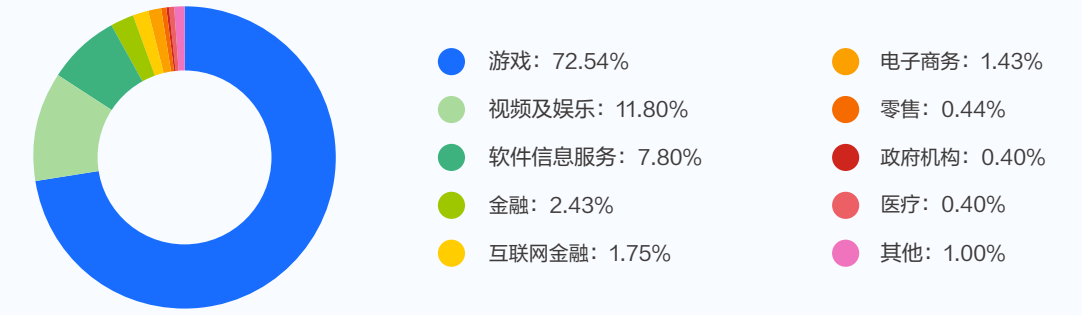


图2-6 2022上半年网络层DDoS攻击目标行业分布

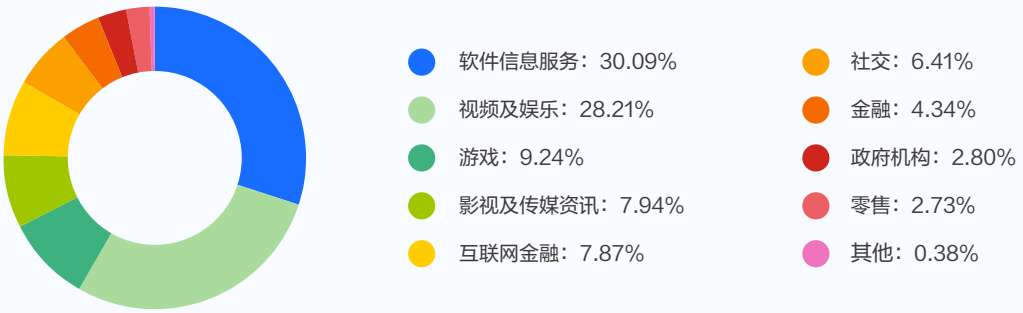


图2-7 2022上半年应用层DDoS攻击目标行业分布

游戏行业具有高竞争、高收益的特性，而DDoS攻击能够以较低成本打瘫游戏业务，造成巨大损失，使得游戏行业一直以来都是DDoS攻击的重灾区。DDoS攻击1月份的2.09Tbps攻击峰值的纪录，也正是发生在游戏相关产业链——游戏应用下载市场。

相对于网络层攻击，应用层攻击的目标行业分布得更为均匀、分散，排行前两位的软件信息服务业和视频及娱乐行业均占比约30%，远小于游戏行业网络层攻击的集中度。

另外，随着“双减”政策的施行，在线教育业务规模收缩，受到的攻击量也从去年的全行业第四，下降到前十名以外。

第三章
Web应用攻击数据解读

3.1. Web应用攻击量增速趋缓

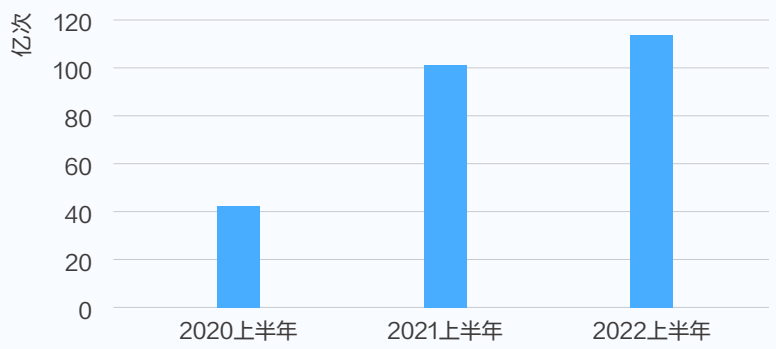


图3-1 Web应用攻击量变化趋势

2022年上半年，网宿安全平台日均监测并拦截Web应用攻击6288.75万次，同比2021上半年的攻击量小幅增长了12.56%，增速趋于减缓。

3.2. HTTP协议违背成为压倒性的攻击手段

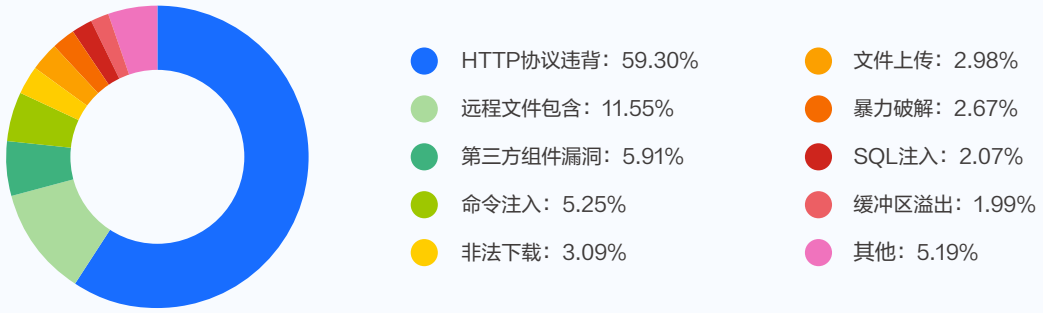


图3-2 2022上半年Web应用攻击手段分布

对Web应用攻击手段进行分析，HTTP协议违背所占比重急剧上升，占到了压倒性的59.30%，相比去年同期上升了约25个百分点。

排在第二、三位的远程文件包含攻击（11.55%）和第三方组件漏洞攻击（5.91%），在排位上也大幅提升，去年同期两者还仅排在第10和第12位。

随着全球产业的数字化升级，企业对于第三方开源组件的依赖也日益提升，针对第三方组件的攻击态势也日益加剧。第三方组件大量存在于商业应用和企业内部开发的业务中， 任何一个较底层的组件出现漏洞，都将造成“攻其一点，伤及一片”的巨大影响。

3.3. 互联网金融行业成为最大攻击目标

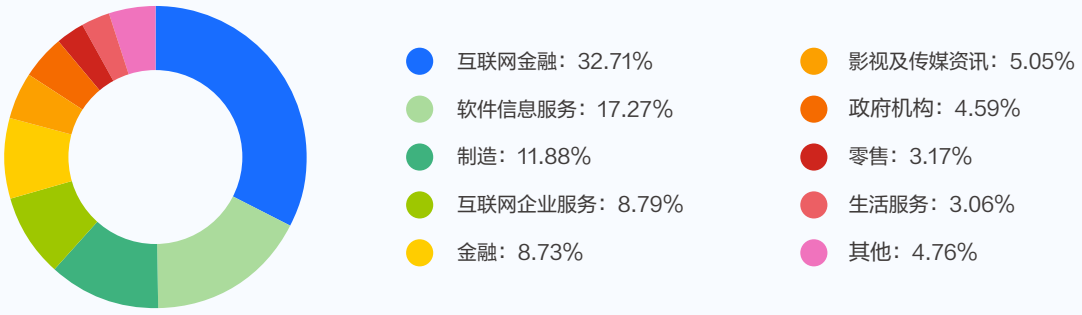


图3-3 2022上半年Web应用攻击目标行业分布

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. 爬虫攻击继续保持翻倍增长趋势

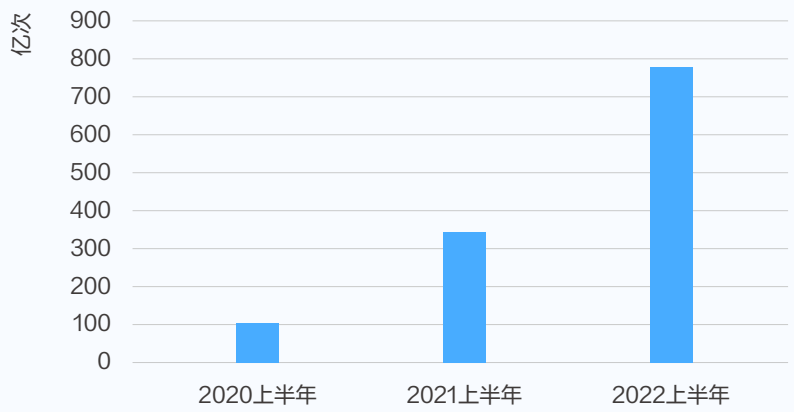


图4-1 爬虫攻击量变化趋势

2022年上半年网宿安全平台共监测并拦截了超773.66亿次爬虫攻击，平均每秒拦截攻击4947次，攻击量达到2021年同期的2.27倍，更是2020年同期的7.46倍，爬虫威胁持续高速增长。

4.2. 高度伪装的智能爬虫威胁上升

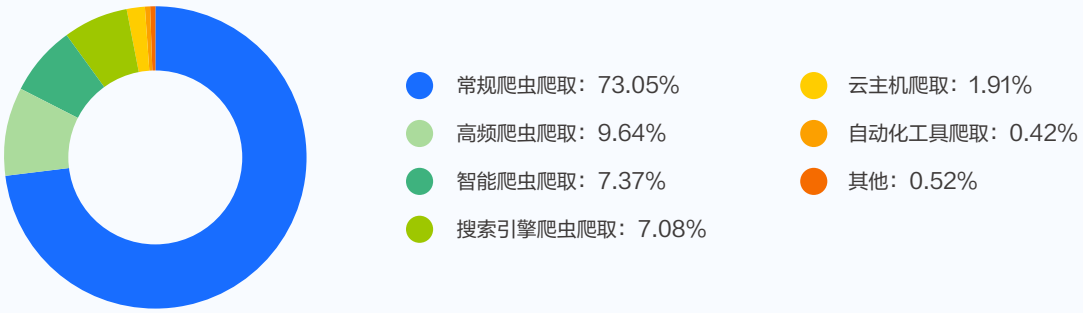


图4-2 2022上半年捕获的爬虫类型分布

从上半年网宿安全平台捕获到的爬虫类型来看，较为简单的常规爬虫仍然占据了绝大部分，占比达到73.05%，相比去年同期略微下降了约4个百分比。同时，与真人访问行为更加相似的智能爬虫，数量同比增长了348.17%，占比也从去年同期的3.73%上涨至7.37%。可见更难以辨别的智能爬虫威胁在上升，爬虫一直在对抗进化，变得越来越贴近真实世界的访问行为。

4.3. 过半爬虫工具使用Chrome内核

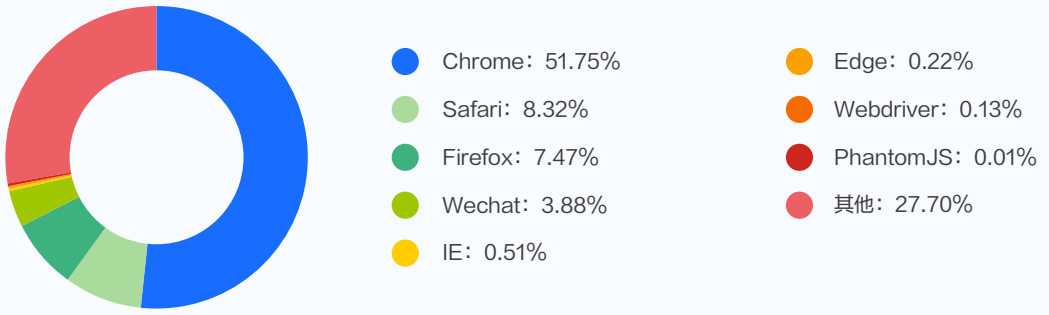


图4-3 2022上半年爬虫工具内核分布

随着攻防对抗升级，爬虫工具会隐藏自己的真实身份，工具特征伪装得越来越像真实浏览器，越来越贴近真实用户访问行为。

通过对网安全平台监测到的爬虫工具的浏览器内核进行分析，发现Chrome家族依旧是霸主地位，使用Chrome内核进行开发的爬虫工具占比达到51.75%，占据半壁江山。

使用Safari和Firefox内核的位居第二、三位，占比分别达到8.32%、7.47%。随着人们对移动端公众号、小程序等应用的高频使用，Wechat内核排到了第四位，占比3.88%。

4.4. 重灾区：软件信息服务、交通运输、零售行业

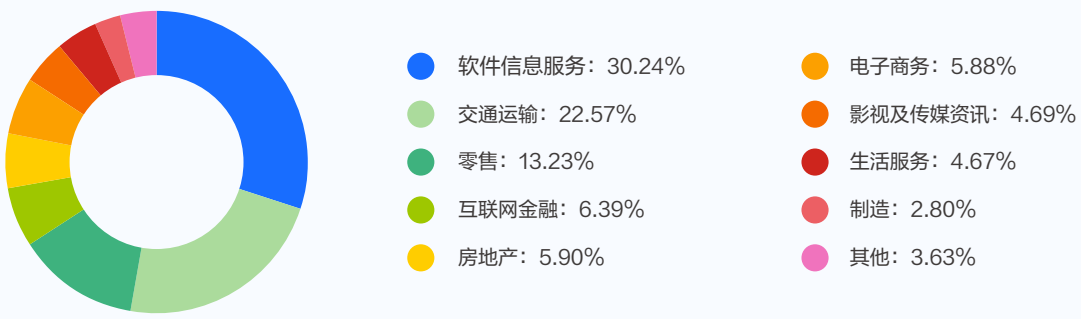


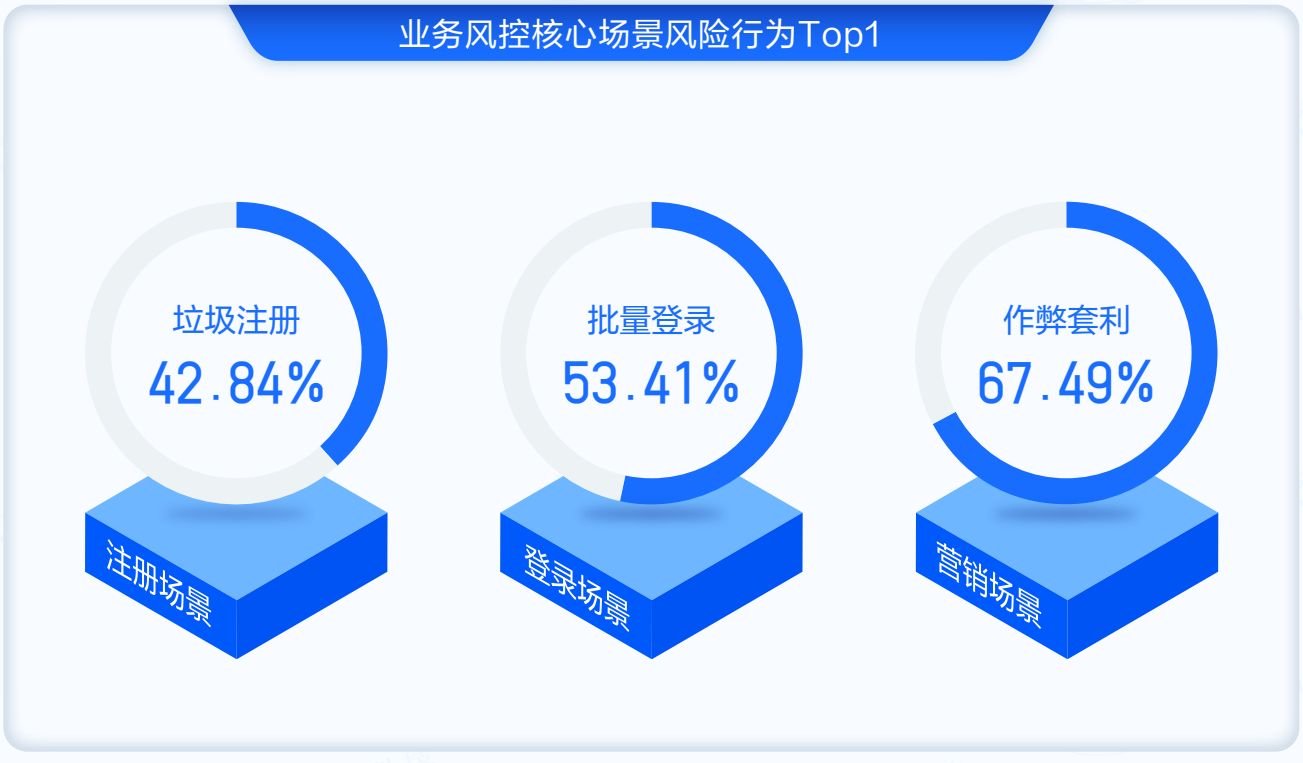
图4-4 2022上半年爬虫攻击目标行业分布

2022上半年，恶意爬虫攻击的目标行业分布继续呈现出较为分散情况，集中度相对较低。软件信息服务（30.24%）、交通运输（22.57%）、零售业（13.23%）依旧是爬虫攻击的重灾区。线上业务中大量含有基金、理财产品行情等高价值信息的互联网金融业，排位从去年同期的第十位大幅上升至第四位，建议互联网金融企业引起重视。

4.5. 黑灰产已大量应用高度伪装的爬虫进行业务欺诈

在疫情影响下，2020年后，大量线下业务加速转移到线上，尤其是金融、营销领域。黑灰产团队盯上了这一契机，利用高度拟人的爬虫进行账号与身份创建、刷量、薅羊毛等自动化批量操作，进行业务欺诈。业务欺诈已形成分工精细的产业链，对风控识别已知和未知自动化攻击的能力提出了更高的要求。

2022年上半年，网宿安全平台共监测到多种业务风控场景。其中，注册场景中，最多的风险类型是垃圾注册（42.84%）和流量欺诈(32.65%)；在登录场景中，监测到批量登录（53.41%）、异地登录（15.88%）、撞库（9.12%）等多种风险行为；在营销场景中，最严重则是作弊套利（67.49%）。



第五章
API攻击数据解读

5.1. API安全威胁爆发式上升

在API经济下，企业线上业务大量使用API共享数据、算法、交易、流程等业务功能，其价值水涨船高，因此API成为了网络攻击的重点目标。

2022上半年，针对API业务的攻击继续呈现高速增长态势。网宿安全平台平均每日监测并拦截针对API业务的攻击908.65万次，相比去年同期大幅增长168.80%。

图5-1 2022上半年API业务攻击量月份走势

具体到月度攻击走势，数据显示出上半年API攻击高峰出现在3月和6月。

5.2. 恶意利用API参数风险极其突出

针对API业务的攻击可以分为两大类型。一类是传统Web攻击。由于API也是承载Web业务的一种形态，并且调用的多是高价值的动态数据，本身就是Web攻击的重灾区，这类攻击往往带有明显区分与正常请求的恶意特征。另一类是针对API弱点的攻击，并不携带恶意特征，只是利用API业务逻辑缺陷实现未授权、越权访问。这类攻击难以通过传统Web防护规则进行识别。

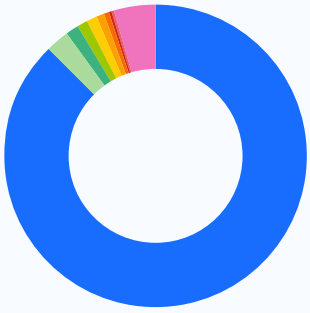


图5-2 2022上半年API业务攻击手段（传统Web攻击类）分布

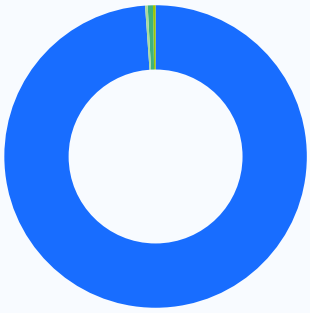


图5-3 2022上半年API业务攻击行为（针对业务逻辑缺陷）分布

通过对网宿安全平台拦截的API攻击手段进行分析，显示出今年上半年在针对API业务的传统Web攻击中，爬虫攻击依旧强势，占据了87.7%的绝大多数，同比去年的53.44%也有较大幅度的上升。

在针对API业务逻辑的攻击行为，则以恶意利用API请求参数为主，占比达到98.9%。当API业务在参数合规校验上不够严密时，攻击者可以通过掌握的参数特征，构造请求参数进行遍历，获取全量数据，成本低、效率高。

5.3. 重灾区：电商、影视及传媒资讯、交通运输行业

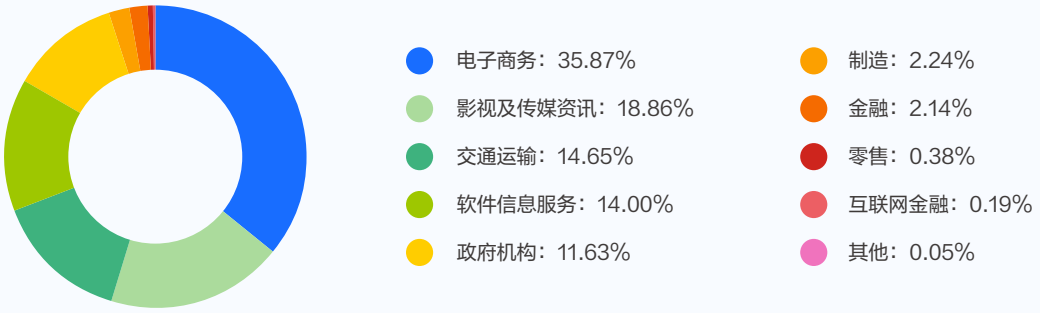


图5-4 2022上半年API攻击目标行业分布

从API攻击的目标行业来看，富含商品和用户隐私信息的电子商务行业成为最大的攻击目标，占比达到35.87%。第二至五位的影视及传媒资讯业（18.86%）、交通运输业（14.65%）、软件信息服务业（14.00%）、政府机构（11.63%）占比较为相近。95%的API攻击量都集中在了这五个行业。

第六章
IPv6安全数据解读

6.1. IPv6攻击IP呈指数级增长

自2021年起，我国IPv6规模部署进入“流量提升”新阶段，网站和应用IPv6升级改造提速，支持IPv6的终端设备规模也快速扩大。就在IPv6日渐普及的同时， IPv6安全威胁也日益显现。

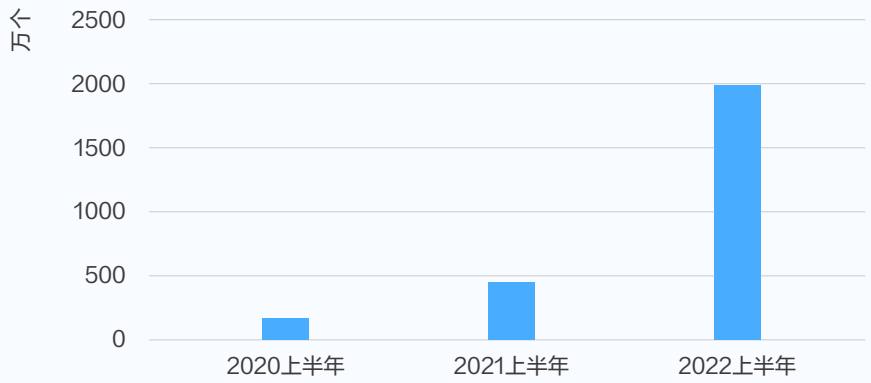


图6-1 IPv6攻击IP数量变化趋势

2022上半年，网宿安全平台捕获IPv6地址的攻击IP 1983万个，同比增长341.18%，相比2020年上半年的数据更是已经翻了10倍，呈指数级增长。

图6-2 2022上半年IPv6境内外攻击源分布

其中，99.60%的IPv6攻击IP均来自大陆境内，来自境外的仅占到0.40%，说明IPv6几乎都来自境内。

6.2. 针对IPv6业务的攻击中，爬虫攻击最为突出

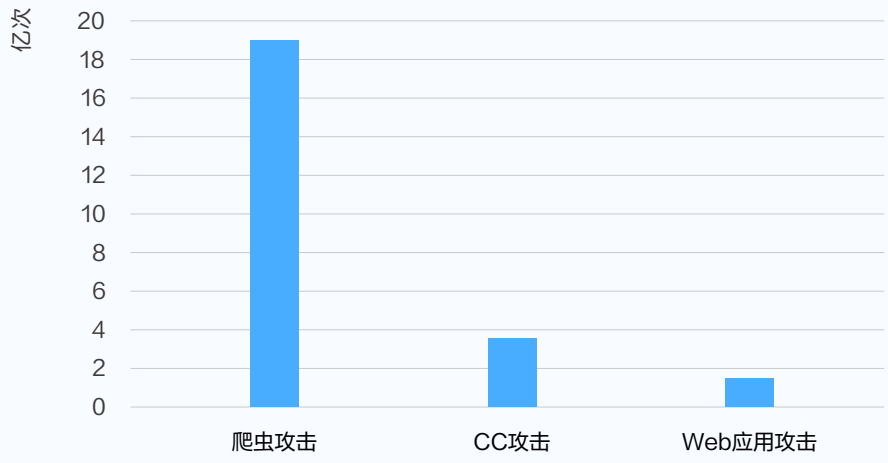


图6-3 2022上半年IPv6应用层攻击量

上半年，网宿安全平台共拦截针对IPv6业务系统的应用层攻击23.93亿次。其中以爬虫攻击为最，达到18.97亿次，占总量的79.26%，建议重点防护。CC攻击数量次之，达3.52亿次。

6.3. 互联网服务供应商、金融机构、政府是IPv6攻击重灾区

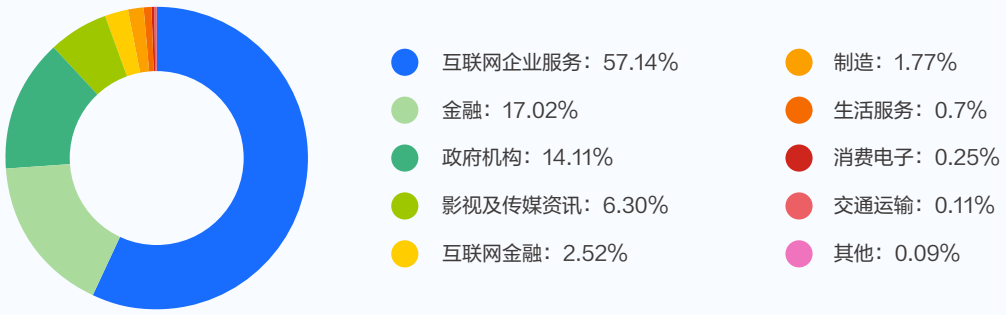


图6-4 2022上半年IPv6 Web攻击目标行业分布

与IPv6+IPv4全体的Web攻击数据相比，IPv6 Web攻击在目标行业上的分布情况有所不同。互联网企业服务业（57.14%）、金融业（17.02%）、政府机构（14.11%）、影视及传媒资讯业（6.30%）的排位从4~7位前进至Top 4。这几个行业均是优先开展IPv6改造升级的领域，因此受到IPv6安全威胁也是首当其冲。

第七章
企业远程办公安全数据解读

自2020年以来，在新冠疫情的催化下，全球范围内远程办公需求激增。在网宿服务的企业用户中，就有接近89%使用远程接入技术，将外网终端设备接入企业办公内网进行访问。远程办公的大规模引入，也暴露出了大量的安全问题。

7.1. 安全措施薄弱的BYOD使用比例达到近三成

图7-1 2022上半年远程办公终端设备类型分布

对网宿企业用户使用的远程接入终端设备类型进行统计，BYOD（Bring Your Own Device，即员工自带设备）占比已经达到约27.07%，并且还在上升中。相比得到统一管控的公司设备，BYOD普遍缺乏明确的安全管理政策进行约束，安全措施薄弱，经常成为黑客攻击的入口。

7.2. 终端用户安全加固意识十分薄弱

通过对终端设备安全基线中的核心项目进行检测发现，终端用户几乎没有修改操作系统原有的安全配置。合规性最高的两个项目分别为：是否开启操作系统防火墙（99.21%）、密码复杂度（98.3%），这些正好是终端设备操作系统在原始配置中已经进行了规范的项目。

合规性最低的三个项目分别为：是否开启远程桌面（20.14%）、杀毒软件版本检测（26.7%）、是否存在共享目录（30.61%）。考虑到终端用户使用过程中的便利性，大部分情况下管理员对这些项目没有做强制性的规范，而用户自身也不会主动去设置，造成安全隐患。

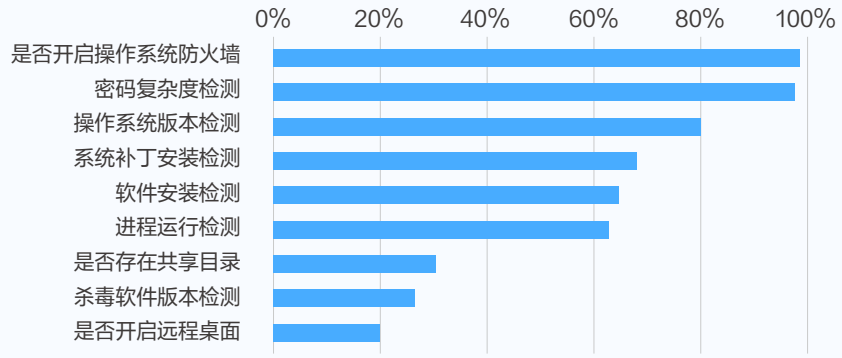


图7-2 2022上半年远程办公终端设备安全基线重要检测项通过率

7.3. 钓鱼、漏洞利用是网络攻击的重要手段

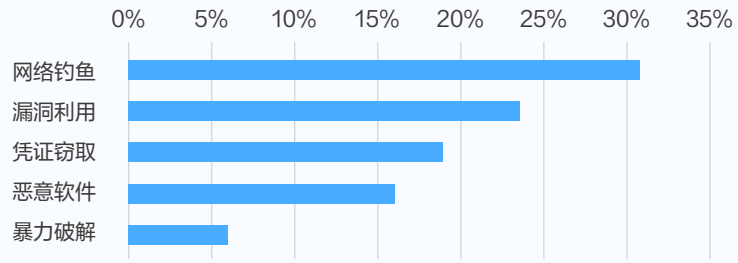


图7-3 2022上半年远程办公攻击手段Top 5

黑客通常将失陷的终端设备作为跳板对办公网络内应用进行攻击。由于内网的应用通常安全性较差，比如Web应用很多还未从HTTP协议升级成HTTPS、应用的系统漏洞没有及时升级等。因此黑客一旦进入内网，就可以较为轻松地攻陷内网应用。

在针对办公网络的攻击中，网络钓鱼是最多见的攻击手段，其中钓鱼邮件被攻击者广泛应用。漏洞利用、凭证获取、恶意软件、暴力破解也是需要重点防护的攻击手段。

7.4. 企业数据泄露途径：即时通信位居第一

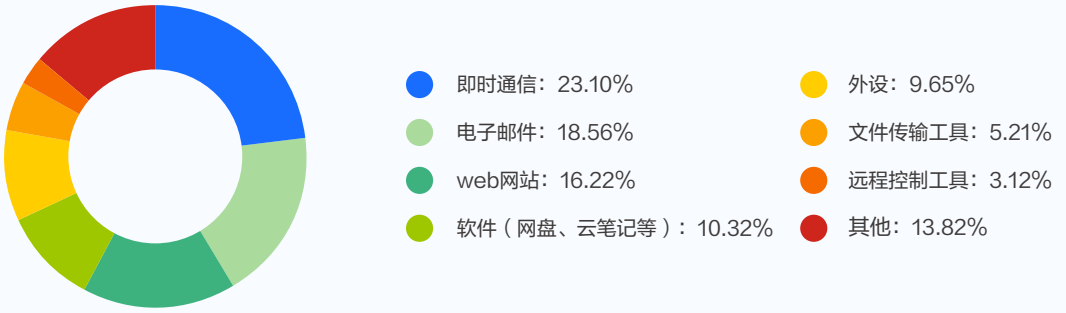


图7-4 2022上半年企业数据泄露途径分布

来自内部的数据泄露，已成为企业急需解决的安全问题。互联网在提升员工办公效率的同时，也使员工可以通过多种途径将企业的数据泄露出去。在数据泄露的途径中，排名前三的为：即时通信（23.1%）、电子邮件（18.56%）、Web网站（16.22%）。

7.5. 警惕越权访问、IP扫描等异常行为背后的隐蔽性攻击

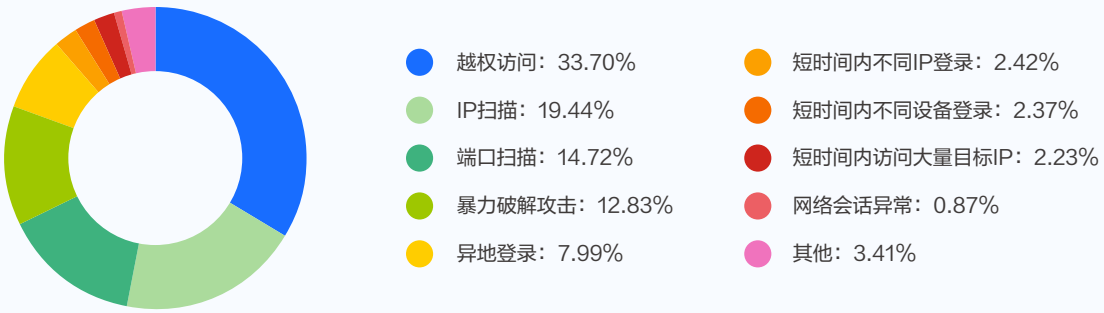


图7-5 2022上半年远程办公异常行为分布情况

随着远程办公的爆发，针对办公网络的APT（Advanced Persistent Threat高级持续性威胁）攻击持续上升。APT攻击作为一种具有组织性、特定目标以及长时间持续性的网络攻击，其特征在于，攻击者往往选择“放长线钓大鱼”，利用失陷的终端设备持续、隐蔽地收集企业核心信息，或破坏网络基础设备，而非谋取短期利益。因此能够绕开传统网络防御系统。

以APT攻击为代表的隐蔽性攻击，还是可以通过异常行为或异常流量分析发现其端倪。网宿零信任安全平台对异常访问行为进行分析后发现，越权访问行为数量最多（占比达33.70%）。攻击者为了最大程度收集数据，会尝试对其无权限的应用进行访问。

IP扫描（19.44%）、端口扫描（14.72%）分列二、三位，则是由于攻击者通常通过这些方式来对企业网络进行探测感知。

第八章
主机安全数据解读

8.1. 高危漏洞多来自开源生态组件

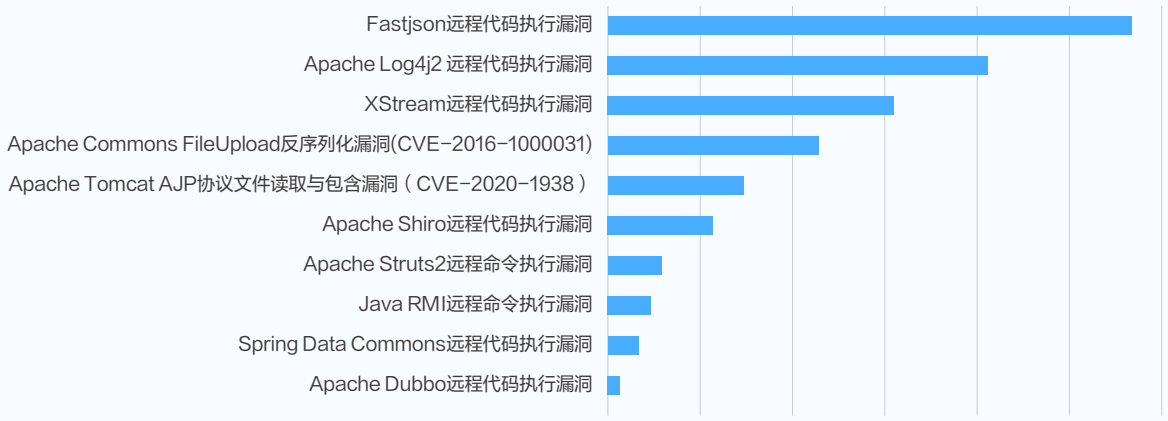


图8-1 2022上半年网宿主机安全平台捕获的高危漏洞Top 10

攻击者入侵利用的高危漏洞类型依然是以应用、组件漏洞为主，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。

上半年网宿主机安全平台捕获到的高危漏洞中，开源生态组件漏洞占比非常高。其中，占据第一位的是Fastjson远程代码执行漏洞。作为国内Java生态常用的基础库，Fastjson在今年5月份再度爆出高危漏洞，数据显示出其影响之广泛。

位居第二的则是去年底爆发的历史漏洞Log4j2，其捕获数量到今年上半年依然占据了高危漏洞Top 2的位置，可见该漏洞在主机中仍然普遍存在，并造成持续影响。

8.2. 无文件进程在异常进程中占比大幅度提升

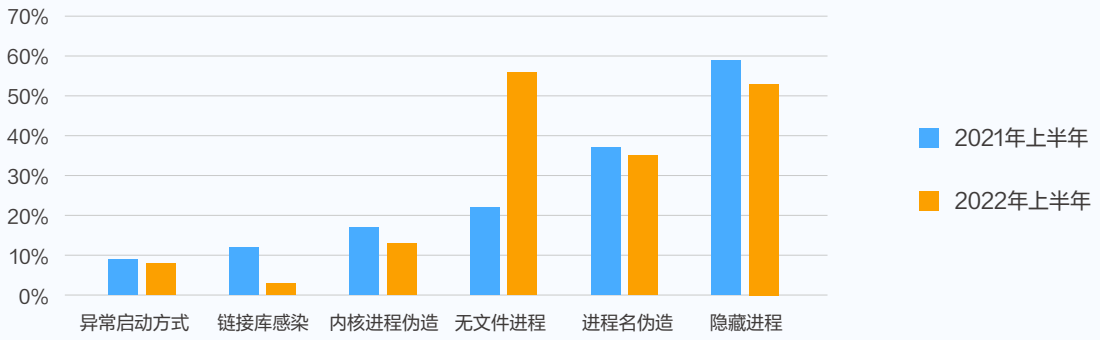


图8-2 进程异常行为检出率对比

从网宿主机探针识别到的异常进程数据可看出，隐藏进程、进程名伪造等手段出现比例略有下降。而无文件进程在异常进程中占比大幅度提升，达到56.44%，比去年同期增加33.86%。

使用无文件进程技术能够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，从而规避杀毒软件的检测。具体来说，无文件进程通常有两种创建方式：其一是由其他进程生成可执行病毒文件，拉起进程后立即将病毒文件删除；其二是通过mem_fd技术在内存中直接创建无文件进程。两种方式都能使传统杀毒软件无法查找到病毒文件，从而导致安全研究人员的入侵分析工作变得困难。

8.3. 超80%的入侵事件利用定时任务实施权限维持

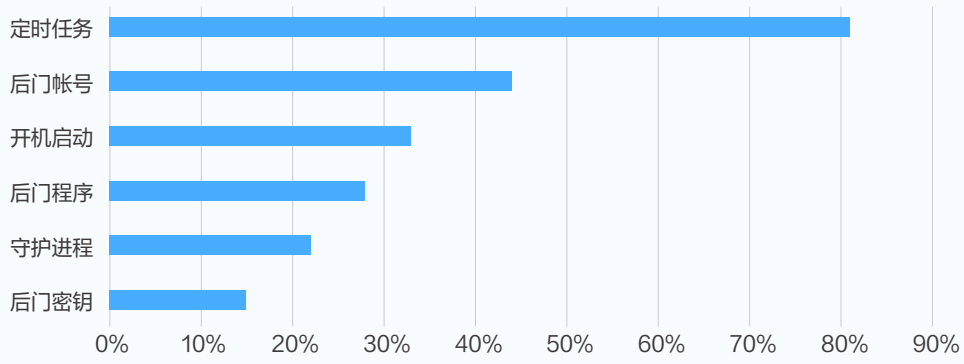


图8-3 2022上半年权限维持行为占比

超过95%的主机入侵事件中都存在权限维持手段。在上半年网宿主机探针识别到的权限维持行为中，定时任务、后门账号、开机启动位居前三，占比分别达到81.29%、44.13%、33.46%。

恶意定时任务通常通过恶意脚本的形式，执行病毒木马、恶意指令等恶意行为。与传统的PC病毒相比，服务器主机病毒更多地使用定时任务进行持久化。由于服务器主机很少进行重启，利用定时任务进行持久化要比排第三位的开机启动配置有效得多。

8.4. 容器应用率飞速提升，容器安全问题不容忽视

图8-4 2022上半年企业主机容器软件安装情况

网宿主机安全探针检测发现，已有73.14%的企业主机有安装容器相关软件，相较于去年同期的安装率提升了近20个百分点。在容器技术得到广泛应用，为应用程序的开发和迁移带来极大便利的同时，容器安全问题也日益凸显。

8.5. 特权容器是造成容器逃逸风险的重要原因

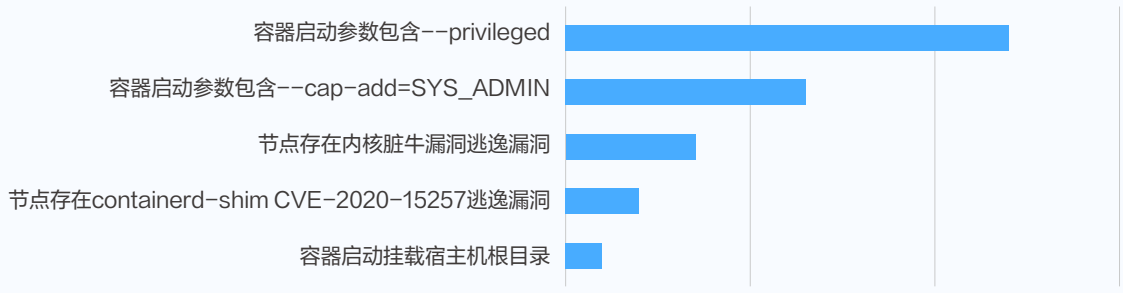


图8-5 2022上半年容器逃逸风险因素Top 5

逃逸是容器特有的，也是最为严重的安全风险之一，能够直接危害其他容器和底层宿主机的安全。

通过网宿容器安全产品对容器逃逸风险进行检测分析，得出造成容器逃逸风险原因主要有：启动参数包含“privileged” （特权容器）、启动参数包含“cap-add=SYS_ADMIN”（特权容器）、节点存在脏牛漏洞（内核漏洞）、容器软件存在安全漏洞（容器软件漏洞）、容器启动参数挂载根目录（敏感目录挂载）。

特权容器是为了方便开发人员而产生的，能够被允许访问系统内的所有设备资源，因此也存在极大的安全风险。由于特权容器的隐患更多是源自于业务相关开发人员安全意识缺乏导致滥用，难以进行统一的管控，因此成为了实际生产业务环境中造成容器逃逸的主要原因。

攻击者利用内核漏洞能够轻易地获得高权限，任意一个可利用的可执行内核代码的漏洞都可以进行容器逃逸，从而威胁整个系统。容器软件也已被发现多个漏洞能够导致容器逃逸。但由于内核漏洞、容器软件漏洞通常由运维人员统一管控，通过更新版本即可规避风险，因此实际造成逃逸风险的数量略低一筹。

利用敏感目录挂载进行逃逸，要通过将危险资源挂载进容器内比较重要的目录比如根目录、/proc目录实现，然而通常业务并无将此类敏感目录挂载进容器的需求，因此这类风险数量较低。

8.6. “安全左移”理念接受度显著提高

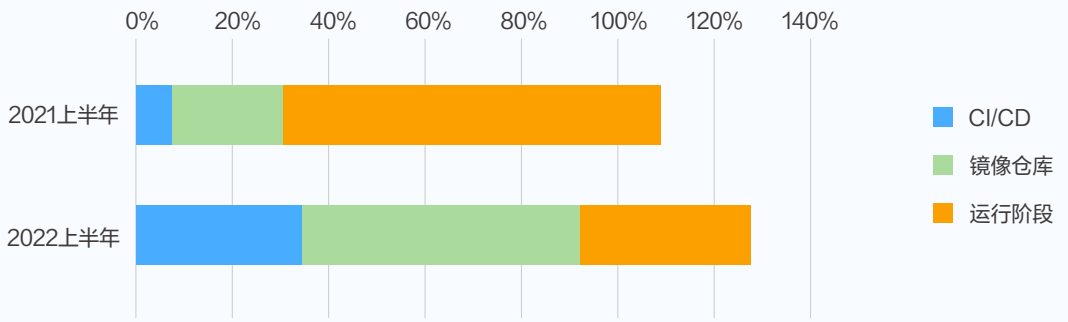


图8-6 容器生命周期各阶段安全扫描率

网宿容器安全产品在容器全生命周期（构造阶段+运输阶段+运行阶段）都能够对镜像进行安全扫描，以发现镜像中存在的病毒木马、安全漏洞、敏感信息等安全风险。越早进行安全扫描，越能够帮助用户提早发现安全风险，避免在镜像已经部署到生产环境、投入运行之后再对深层安全问题进行“回炉”修复，从而产生高昂的修复成本和对业务的负面影响。这就是“安全左移”理念。

网宿通过对各阶段的安全扫描使用率进行进行分析，发现2022上半年用户在CI/CD（构建阶段）和镜像仓库（运输阶段）的安全扫描率，分别已经达到34.33%、57.85%。相较于去年同期的扫描率，CI/CD提升了27个百分比，镜像仓库提升了35个百分比，说明这一年间容器镜像在进入生产环境（运行阶段）之前的安全扫描率出现了显著提高，“安全左移”理念随着容器技术的流行逐渐得到普及和接受。

第九章
趋势展望与建议

基于对2022上半年网宿安全平台的数据分析及产业观察，本次报告总结安全威胁趋势如下：

- 数据泄露风险进一步升级。随着数字化进程的深入，数据的价值也水涨船高，也有越来越多的数据和设备暴露于网络之中，面临来自外部攻击和内部泄露的双重威胁。可以预见数据安全风险将持续上升，且数据泄露规模恐将不断升级。另一方面，网络安全法、数据安全法、个人信息保护法等法律法规的相继出台，也使得如何规范数据处理活动、保障数据安全成为企业合规经营的重要课题。
- API安全威胁继续呈爆发式上升，其安全挑战远远超过传统的Web网页。API的使用场景丰富、迭代频繁且业务与安全存在割裂，导致大量API业务存在不同程度的安全设计缺陷和管理不当。尤其是在参数合规校验上的设计漏洞，被攻击者大量利用，批量盗取数据。只依靠基于规则的Web防护思路已无法应对如今的API安全态势。
- 针对开源生态的供应链攻击将持续高发。现代软件业已高度依赖开放共享的开源软件生态，然而这些第三方软件、组件的安全问题却容易被安全团队忽视，难发现、难溯源，且杀伤力广泛，因此利用开源生态安全漏洞的供应链攻击倍受攻击者青睐。本期报告统计到的数据也一定程度上显现出了这一趋势：针对第三方组件漏洞的Web攻击量大幅上升；影响面上，主机高危漏洞几乎都来自开源生态组件，以Apache Log4j2漏洞为代表的历史漏洞的负面影响仍在持续，不易消除。
- 随着容器技术的广泛使用，在漏洞检测方面企业将越来越多的精力放在镜像构建环节进行检测，“安全左移”的理念在容器生态下得到比较好的实践，既方便在开发构建环节及时修复安全问题，也推动着更多的开发人员参与到安全工作中来，更好地形成安全闭环。
- 基于SASE构建企业的纵深防御体系，逐渐成为企业实现信息系统安全的趋势，并且对SASE框架下各方面的安全技术成熟度也提出了更高的要求：在设备方面，要求具备全面终端环境感知和终端安全管理能力；在网络方面，对终端准入控制和网络访问控制要求更为严格和精细；在应用/数据方面，更加重视数据泄露防护和网络威胁分析；而在安全运营方面，则更注重异常行为检测和统一的安全策略管理，以实现统一、高效、准确的管理。

企业线上业务的载体正逐渐向云、容器、API等基础设施进行转移。在当前复合的网络形态下，安全工作仅仅聚焦于点和线是远远不够的，需要云、管、端的安全能力进行协同，构建全链路、体系化的安全防御架构，才能有效应对网络安全风险的持续升级。网宿安全聚焦云安全、企业安全和安全服务领域，围绕WAAP、零信任、SASE、AI、大数据等前沿理念与技术，已为企业用户构建出从主机层到网络层、应用层到数据层、业务层的纵深防御能力，并将安全防护的边界拓展到用户层，形成全链路深度融合的一体化安全体系。

未来网宿安全将继续依托自身在技术创新与服务实践上的积累，进一步打造开放效应，与上下游安全技术和企业已有安全防御体系相结合，实现SASE一体化安全服务目标，共建网络安全。

版权信息

CHINA INTERNET SECURITY REPORT