网宿科技 | 网宿安全

2022年 Web安全观察报告

目录 CONTENTS

第一章 核心发现

第二章 主要安全威胁发展趋势

第三章 攻击手段解读

安全建议

第一章 核心发现

1.1. 高危Web漏洞持续爆发

2021年底核弹级Log4shell漏洞爆发之后，2022年持续爆发了多个变种漏洞。2022年网宿安全平台共检测到2700万次针对Log4shell各个变种漏洞的利用。此外，2022年又持续爆发了大量新的高危漏洞，包括Apache Fineract路径遍历漏洞、OpenSSL安全漏洞、SQLite输入验证错误漏洞、Atlassian Bitbucket Server和Bitbucket Data Center命令注入漏洞、Apache Commons BCEL缓冲区错误漏洞等热点漏洞。截至2022年底，CNVD披露的2022年新增漏洞数量为23900个，总漏洞数量相比2021年下降了10.01%，但高危数量相比2021年反而增加了13.07%，说明Web漏洞更加趋向高危级别，威胁态势越来越严峻。

1.2. API已成为黑产攻击的头号目标

互联网数字化时代，越来越多的企业已经在利用API的技术和经济模式来保证竞争力的延续。2022年在网宿CDN平台流通的API请求占全平台请求量的61.3%，随之而来的API攻击也呈现出明显增长趋势，全年针对API的攻击占比首次突破50%，达到了58.4%。Gartner曾预测，“到2022年，API将成为网络攻击者利用最频繁的载体”，现如今已得到验证。

1.3. 传统WAF防护无法覆盖多样化的安全威胁

随着企业数字化进程不断推进，企业核心业务在Web、APP、H5、微信等多渠道上，依托于开放API灵活开展，随之而来的Web业务攻击面不断增大，DDoS、漏洞利用、数据爬取、业务欺诈等安全威胁层出不穷，传统WAF难以覆盖如此多样化的威胁。根据网宿安全平台2022年数据显示，同时遇到2种以上威胁的Web业务占比达87%，3种以上占比仍高达65%。

1.4. WAAP是全面保护Web应用的有效手段

2021年，Gartner将多年来发布的WAF魔力象限改为了WAAP魔力象限，将WAAP定义为在提供传统Web安全防御能力的WAF之上扩展为集DDoS防护、Bot流量管理、WAF、API防护于一体的下一代WEB安全防护解决方案。

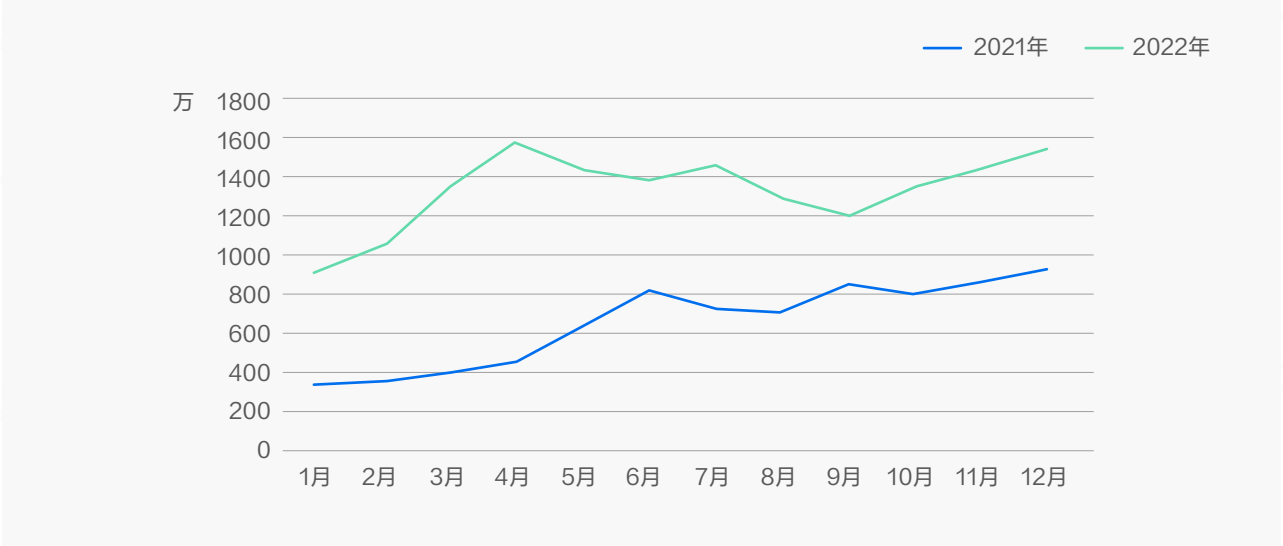
2023年，OWASP API Security Top 10新增了“API缺少对自动化威胁的保护”，也说明由自动化Bot发起的数据爬取、业务欺诈等威胁必须得到企业重视。

云WAAP方案价值在海外市场和企业中已得到充分验证，网宿安全最早于2017年发布了契合WAAP核心理念的一体化安全加速解决方案，我们认为WAAP是API驱动的数字时代下全面保护Web应用的有效手段。

第二章 主要安全威胁发展趋势

2.1. DDoS攻击规模足以突破大部分防御手段

随着互联网不断发展，知名的XorDDoS、Mirai、Gafgyt、Fodchas等僵尸网络的规模也在不断扩张，DDoS攻击规模也随之逐年上升。网宿安全平台2022年数据显示，网宿平台遭遇的DDoS攻击峰值达到2.09Tbps，全年T级以上攻击出现8次，T级攻击已成为家常便饭。同时，攻击发生频率也有明显增长，网宿安全平台日均监测并拦截DDoS攻击事件43.92万次，同比增长103.8%。



DDos攻击事件数量

在如此频繁且大规模的攻击面前，基于单一数据中心边界的传统防护手段已无法应对，只有运营商、CDN、云计算这类提供互联网基础设施的厂商具备应对超大规模攻击的清洗能力。

另外，网宿安全团队对僵尸网络持续跟踪发现，多个僵尸网络混合攻击已成为主流的攻击方式，攻击平台可以迅速调动多个僵尸网络的资源，瞬间操控数十万甚至更多的肉鸡IP同时发起攻击，尤其是以此方式发起的极其分散低频的七层DDoS攻击，防护难度极大。

2.2. 0day漏洞扩散难以及时控制

0day漏洞公开后，其传播扩散正在变得越来越难以控制。

从漏洞传播速度来看，当前互联网信息传播极快，0day漏洞爆发后第一时间就会出现大量黑客使用批量扫描工具在互联网上进行大规模嗅探，此时如若WAF等设备还未更新防御规则，Web业务则会面临极高的失陷风险。

从漏洞应对效率来看，面对组件0day漏洞防护，传统防御模式依赖在WAF防护设备上更新规则插件来进行防护。层出不穷的新漏洞和影响持续的旧漏洞，使安全防御规则更新频次越来越高，企业安全运营人员同时要考虑安全性和业务的稳定性，很可能无法决策合理的规则库更新时机；另外，因业务扩展IT体系越来越复杂，防御体系缺乏统一的中心管理，也容易造成部分安全设备游离在边缘，无法及时更新防御规则库，从而带来巨大的安全隐患。

2.3. API缺乏安全管理体系，成为攻击主要突破口

API作为核心业务载体，当前缺乏完善的安全管理体系，成为攻击主要突破口。攻击者可以通过API接口获取敏感数据、篡改数据、甚至直接攻击后端系统，从而对企业造成严重的损失。

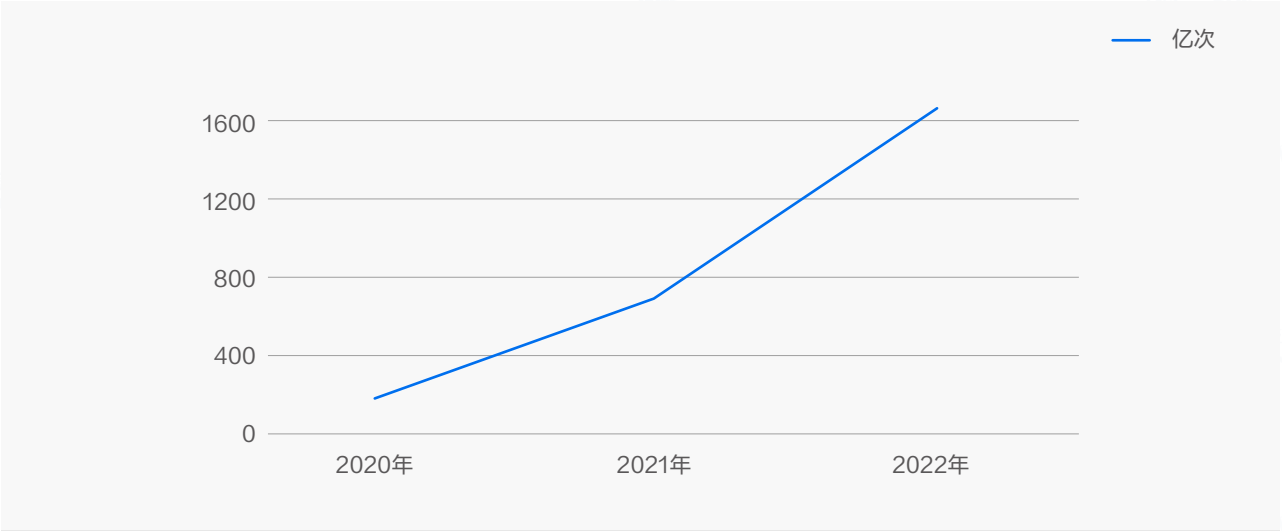
首先，API的攻击成本更低。攻击者只需要找到API的接口地址，就可以通过简单的网络请求获取数据或者进行攻击。相比之下，攻击整个网站需要攻击者具备更高的技术水平和更多的时间成本。举例来说，攻击者可以通过API接口获取用户的个人信息、账户余额等敏感数据，从而进行钓鱼诈骗或者直接盗取用户的资金。另外，攻击者还可以通过篡改API返回的数据，对企业的业务造成影响，比如篡改商品价格、库存等信息，导致企业损失惨重。

其次，企业对自己的API资产现状不清，更难保护全量API资产的安全，给业务留下了突破口。数据显示在受访者最关心的API安全问题中，僵尸API以43%占比高居第一,远超过以22%的占比位居第二的账户接管/滥用；还有83%的受访者对组织API资产清单是否完整没有信心。为何企业对僵尸API及API清单完整度有如此大的担忧？安全隐患往往藏于“未知”，未知的僵尸API、未知的影子API、未知的敏感数据暴露等，根源都在于企业对API资产全貌的未知。安全的管理与防护始于“已知”和“可见”，人们难以掌控那些被遗忘的、看不见摸不着的资产安全状况。然而正是这些被人遗忘、不可管控的API，因其往往潜藏着未被修复的漏洞，备受攻击者青睐。

正因企业缺乏对API安全的全面管理，给攻击者留下了可乘之机。例如，2022年6月，持续集成开发工具Travis CI被曝其API允许任何人访问明文历史日志，导致超过 7.7 亿条用户日志数据泄露，内含73000份令牌、访问密钥和其它云服务凭据；2021年6月，职场社交巨头LinkedIn超7亿用户数据在暗网被公开售卖，数据为黑客利用其API漏洞所得；2020年，美国在线教育平台Chegg遭受黑客攻击，攻击者通过攻击Chegg的API接口获取了4000万客户的个人信息，造成数百万美元的损失。

2.4. 越来越多攻击从自动化Bot发起

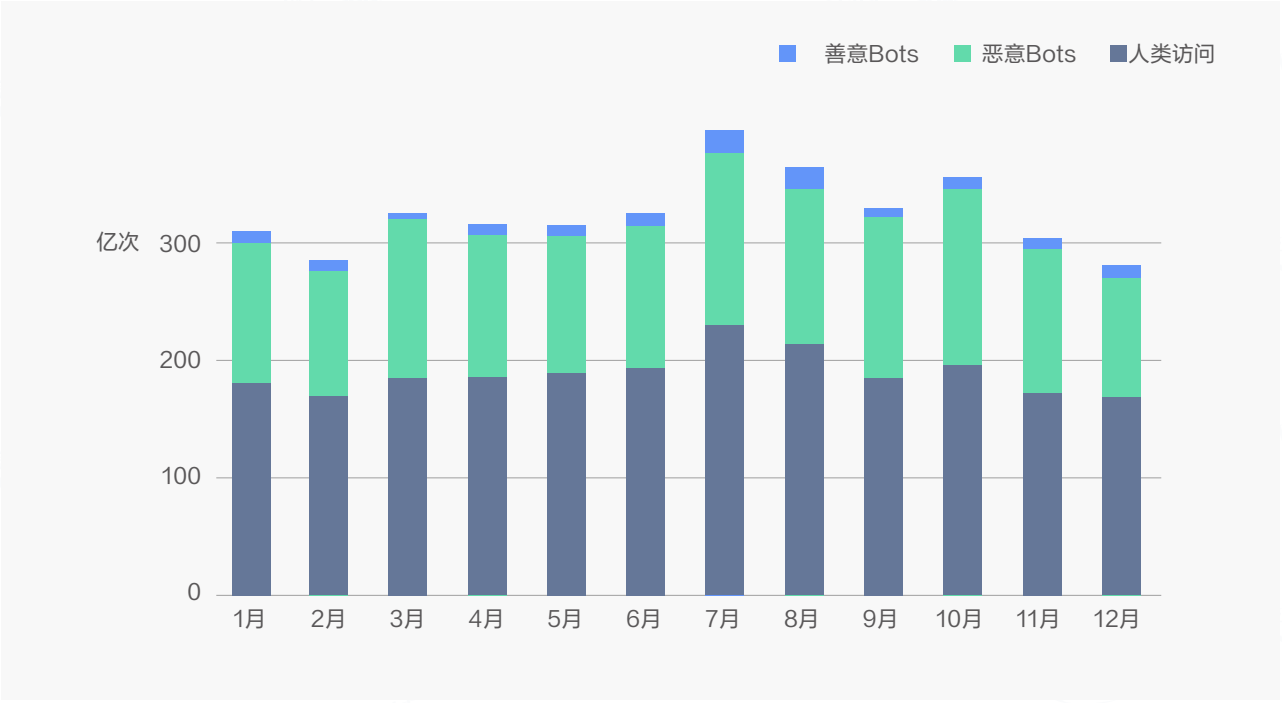
2022年全年网宿安全平台共监测到1631.85亿次Bot攻击，即平均每秒发生约5175次Bot攻击。与往年相比，攻击量是2021年的1.93倍，2020年的4.55倍。



Bot攻击次数

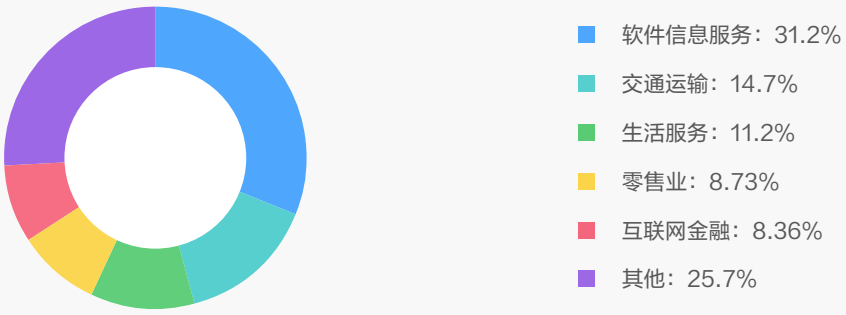
每月的恶意Bots访问量居高不下

Web业务的非人类访问量一直保持在40%左右，而其中绝大部分来自恶意Bots。



软件信息服务、交通运输、生活服务是Bot攻击的三大重灾区

从细分行业来看，受Bot攻击最严重的三大行业为软件信息服务、交通运输、生活服务，都是与当代人们生活息息相关的行业。排名前三的行业受Bot攻击总量超过一半。



Bot攻击目标行业分布

Bot攻击更隐蔽

对海量的Bot攻击数据进行汇总分析，我们发现Bot攻击手段越来越来隐蔽。比如：通过伪造正常的User-Agent和使用模拟正常浏览器的自动化框架发起攻击。另外，Bot更偏向于伪造一个看似合法的User-Agent值或者伪装成善意搜索引擎爬虫，来迷惑固定规则类的检测方案，以绕过传统防护方案的“重重围堵”。

2.5. 在线业务欺诈风险骤升

随着企业的数字化转型，大量线下业务加速转移到线上，流量模式成为大势所趋，H5、小程序愈加普及，同时，企业开展线上业务，需要大量使用API共享数据、算法、交易、流程等业务功能，由此成为了网络攻击的重点目标，攻击所导致的数据泄露，同时为黑产提供了大量的账号、手机号、身份信息、银行卡号等基础物料资源。在大量的黑产资源下，超200万的黑产从业人员通过批量的高度拟人的自动化攻击技术、伪造设备信息的各类改机工具，使得欺诈手段进一步升级，随之而来的便是在线业务欺诈风险骤升。

网宿安全团队结合黑灰产跟踪和2022年网宿平台流量分析发现，大量企业正在遭受恶意注册、恶意登录、营销作弊等业务欺诈行为。疫情时代下，越来越多企业通过线上开展及推广业务，因此通过业务欺诈获利生存的黑灰产正将黑手伸向品牌零售、在线电商、数字藏品等各行各业。

第三章 攻击手段解读

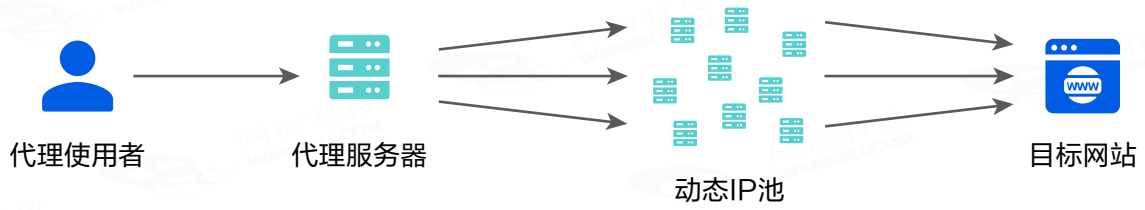
3.1. 利用API安全缺陷攻击

攻击者常常利用API缺陷进而发起的一系列针对API业务的破坏：

身份验证和访问控制不当	身份验证和访问控制是API安全的第一道防线，若实现不当，攻击者可以通过绕过或突破这些机制，获取对API的非法访问权限。例如，某社交平台的API在身份验证中未验证请求的来源，攻击者可以使用被盗的凭证进行未授权的访问。
盗取敏感信息	攻击者通过在未加密传输或未加密存储的数据中查找机密信息，例如用户名、密码和API密钥等。据APIsecurity.io统计，数据泄露是API安全风险中的第二大问题。 一些API暴露了过多的数据，包括用户的私人信息和系统配置信息。攻击者可以利用这些信息来发起更有针对性的攻击。因此，API应该实现最小化原则，仅向需要数据的应用程序提供所需的最少信息。 攻击者还可以通过不安全的数据存储可能导致攻击者轻松地窃取和篡改数据。例如，某社交平台的API在存储用户个人信息时，没有对密码进行哈希或加密，导致攻击者可以直接访问并窃取用户的密码。根据Verizon的数据泄露调查报告，2019年有22%的数据泄露涉及未加密的数据存储。
暴力攻击和暴力破解	攻击者可以通过大量尝试不同的用户名和密码组合的方式，进行暴力攻击和暴力破解。这种攻击方式可以利用API的弱点，从而导致帐户被封锁或者被完全控制。例如，2020年3月份，Zoom视频通信平台遭受了大规模暴力攻击，攻击者使用了大量的凭证进行尝试，并成功获取了一些凭证，从而导致了安全漏洞。
API参数污染	攻击者通过修改API的参数来修改API返回的结果。这种攻击通常发生在API的查询字符串、POST数据或者HTTP标头中，通过修改这些参数，攻击者可以绕过API的访问控制或者欺骗API的返回结果。
重放攻击	攻击者可能会利用API服务中的重放攻击漏洞来重复执行之前的请求，从而绕过身份验证或执行未经授权的操作。例如，攻击者可能会重复发送之前的请求来执行恶意操作或窃取数据。 应对此类攻击的关键在于如何有效管控API安全风险，通常需要至少覆盖以下几方面： ①避免出现API安全缺陷：如借助API网关等管理工实现API的规划、设计、实施、测试、发布、运营、调用、版本管理和下线等API各个生命周期阶段的闭环管理。 ②保障核心数据安全：通过敏感数据发现、脆弱性评估、脱敏、审计、数据安全态势运营等手段保障核心数据安全。 ③威胁防护：如借助专业的API安全工具或Web应用防护产品，基于内容检查、流量管理、AI业务模型分析等手段，保护API免遭自身缺陷导致的滥用、非授权访问和拒绝服务攻击。

3.2. 利用海量秒拨IP发起低频应用层DDoS攻击

由于应用层流量更贴近业务逻辑，在应用层发起DDoS攻击可以同时对目标网络与目标服务器的稳定性造成威胁，应用层DDoS攻击的攻击方式与手法在也在不断演进升级。从集中式高频请求逐步演进为分布式低频请求，从请求报文中携带显著恶意特征变化为重放合法请求流量、伪造搜索引擎爬虫流量等手段规避常见的频率限制或访问控制策略。而秒拨作为在2014年就成熟的IP资源解决方案，被大量应用于黑灰产网络攻击场景。



秒拨的底层思路是利用家用宽带拨号上网（PPPoE）的原理，每一次断线重连就会获取一个新的IP，主要涉及到以下几点技术：

IP地址池管理	NAT技术	VPN技术	负载均衡技术	高可用性技术
通过管理IP地址池来实现IP地址的动态分配和回收。当用户需要使用IP时，从IP地址池中分配一个可用的IP地址给用户，用户使用完毕后，则将该IP地址回收到IP地址池中，以便下一次分配使用。	使用NAT技术来实现多个用户共享一个公网IP地址的功能。当用户使用秒拨IP地址进行网络访问时，将用户的私有IP地址转换成公网IP地址，从而实现用户与外部网络的通信。	使用VPN技术来保证用户数据的安全性和隐私性。用户使用秒拨IP时基于VPN连接在公共网络上建立一个安全的隧道，将用户的数据加密传输，从而保证用户数据的安全性和隐私性。	使用负载均衡技术来实现多个服务器之间的负载均衡。当用户请求访问秒拨IP服务时，会被分发到多个服务器上，从而实现服务器资源的合理利用和负载均衡。	使用高可用性技术来保证服务的可靠性和稳定性。当某个服务器出现故障时，会自动将请求转发到其他可用的服务器上，从而保证服务的连续性和可靠性。

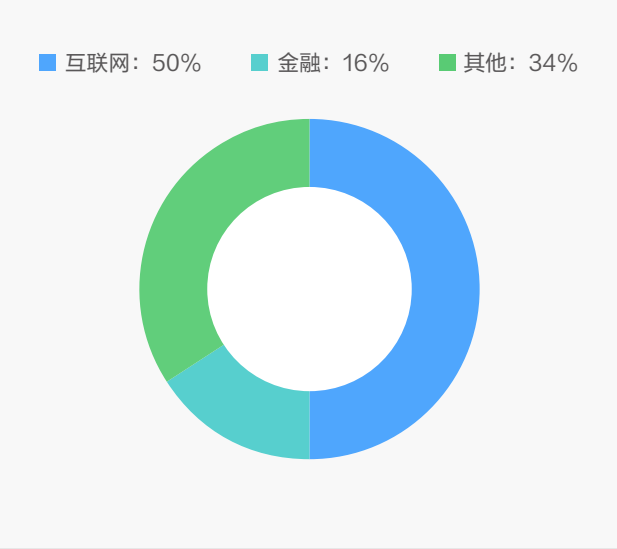
利用大规模秒拨IP发起对于Web业务站点合法且低频的请求发起攻击，在对抗防护策略有两个天然的优势：
①资源池巨大，少则十万多则百万的秒拨IP，轻松绕过基于频率的传统防护手段；
②难以识别，秒拨IP与正常用户来源同一个池子，并且秒拨IP存活周期短，被释放后大概率会分配到正常用户手中，因此在实际研判难以区分正常用户IP与秒拨IP。防守方如果还想以积累IP池的传统方式与攻击者对抗，必然会引入大量误报。

识别风险IP的核心依据应该是，该IP是否当下被黑产持有。IP的黑产使用周期和时间有效性这两个指标尤为重要，尤其是对于像家庭宽带IP、数据中心主机IP这种“非共享型”的IP。针对基站、专用出口等“共享型”的IP，由于单个IP背后会有大量用户，防控阈值应该相对更宽松，但是如果能准确识别IP是否当下被黑产使用，也能提供很重要的参考价值。这往往需要投入大量精力进行情报数据挖掘、清洗、生产，最终形成数据驱动的防护能力。

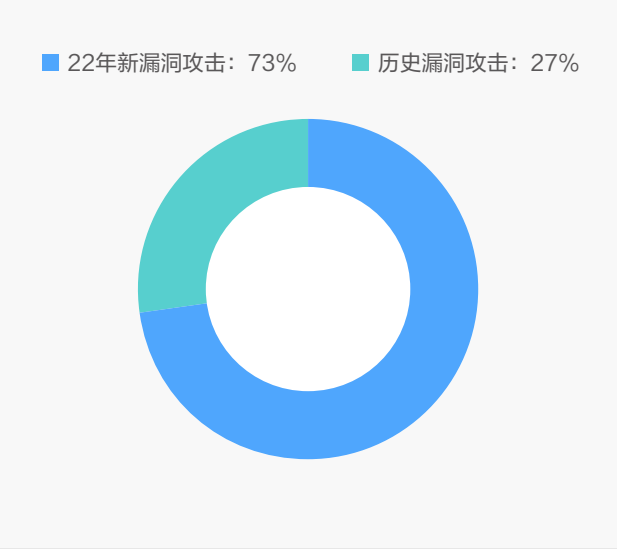
3.3. 0day漏洞自动化探测绕过WAF防护

网宿安全平台2022年WAF攻击数据发现，66%的漏洞利用攻击发生在互联网和金融行业，因为这些行业的数据更有价值。

其中，对新漏洞的攻击利用占比高达73%。



组件漏洞利用行业偏好



新旧漏洞攻击占比

网宿安全团队发现，在0day漏洞被公布前，黑客越来越多地使用自动化程序进行批量嗅探。以CVE-2022-22965 Spring Framework远程代码执行漏洞为例，该漏洞公布后，通过对网宿安全平台的历史攻击数据手段溯源发现，在漏洞公布时间之前已有大量利用此漏洞POC的探测请求被网宿Bot防护产品识别。通过分析CVE-2022-22965漏洞对应的WAF检出量和自动化Bots检出量，我们发现二者趋势具有明显的正相关。

3.4. 手段多变的Bot攻击

Bot分类

从Bot的攻击手段来看，Bot攻击可以分为如下四个级别：

简单Bot

不具备Cookie和JavaScript特性的简单自动化脚本。这些自动化脚本甚至不会通过伪造User-Agent信息来伪装自己，仅机械地对目标应用实施爬取、扫描、重复访问等。但此类访问占据Bot流量比例最大。

复杂Bot

具备Cookie和JavaScript特性的复杂自动化脚本。这些自动化脚本会模拟正常的浏览器对目标应用进行访问，基于对请求报文的检测方式已难以发现异常。

拟人Bot

不仅具备Cookie和JavaScript特性，同时还能模拟人类的鼠标移动、键盘敲击等交互事件。此类Bot一般为具备浏览器内核的自动化框架或者集成了恶意插件的真实浏览器。

持续动态Bot

类Bot不仅能达到复杂Bot或拟人Bot的级别，同时还会采用动态伪造不同的User-Agent、使用IP代理等手段躲避追踪。固定的策略或者人工分析难以追踪并及时做出阻断动作。

案例解读

Bot类型	自动化框架
攻击手段	通过自动化测试工具（自动化测试工具）进行模拟人类的点击、滚动、填写表单等操作实现页面信息的爬取。此类攻击的访问序列及行为与正常人的访问行为非常接近，通过常规的检测方式难以识别。
详情描述	以某航司遭受的自动化框架爬取页面信息的场景为例：

正常购票流程	自动化框架BOT	备注
行程查询	自动查询行程	
票价查询	自动查询票价	重点爬取对象
账号登陆	自动登录	
编辑乘机人	自动添加并勾选乘机人	
提交订单	自动提交订单	
支付订单	自动支付	

实战对抗思路

自动化框架本质上还是由人类编写和维护，且由于效率与成本的双重约束，攻击行为往往在一个或多个角度与正常人类的访问存在差异。例如：

User-Agent

为了躲避检测和追踪，自动化框架通常会动态变换UA值（通常是利用随机UA生成工具或自行维护一个UA列表）；

访问间隔

为追求爬取页面信息的效率，自动化框架的访问间隔通常与正常人类的访问间隔有所区别（例如在查询机票后，真实的人类访问通常会停留较长时间以进行对比）；

相似行为

尽管自动化框架可以模拟正常人类的点击、滑动等操作行为，但是这类行为需要通过录制或编码实现，通常多个客户端存在相同或相似的操作行为；

访问序列

由于成本和效率的限制，自动化框架常常在爬取页面信息时呈现有规律的访问序列。

基于上述差异，可以采用如下防护方案：

基于情报对存在恶意攻击历史的IP、UA等标识进行更严格的校验（比如验证码或直接拦截）。

使用浏览器特性检测手段动态检测浏览器内核和浏览器指纹，对携带非法UA或关联多UA的访问say“No”。

利用大数据分析和AI检测技术持续对网站访问日志进行推理和检测，发现其中异于正常人类的访问行为，加以管控。

3.5. 欺诈背后的黑灰产业链

黑灰产已通过大量自动化、流程化的方式进行业务欺诈，并贯穿于整个在线业务场景，在黑产攻击猖獗的注册、登录、营销场景下，自动化攻击占比均在50%以上。以攻击行业的重灾区电商行业为例，我们梳理了以下主要攻击场景及风险类型：

注册	登陆	收藏/加购	下单/支付	物流	售后
渠道刷量 虚假账户 垃圾注册	撞库 暴力破解 账户盗用 批量登录	刷榜 骗取补贴	刷单 占库存 木马钓鱼 盗用盗卡 洗钱 黄牛秒杀	虚假地址 虚假运单	刷好评 恶意差评 退货套利

每个业务环节都充斥着业务欺诈行为，其背后的黑产团伙已具备高度成熟的产业化、技术化，结构现状如下图所示：

实现流程	实现方式
物料层	手机卡商、账号商人、银行卡商、接口攻击泄露的账号/密码
平台层	打码平台、接码平台、代理IP池、非法交易平台
工具层	群控软件、自动化工具、改机工具
实施层	撞库/拖库、交易欺诈、营销作弊、黄牛代下单、刷单诈骗
变现层	特惠商品转卖、套现、刷榜刷单赚取佣金、商家炒信

应对产业化的业务欺诈，当前银行、大电商平台等大型企业通常有自建风控体系，也会将部分专业风控厂商、情报厂商的能力纳入自身风控体系中。但在新零售、社区电商等“万物皆可电商”的趋势下，许多中小企业或传统零售品牌尚不具备应对此类威胁的能力和经验，部分安全厂商在其Web安全产品体系中推出了业务场景化防护能力，但目前整体还处于探索阶段，能否真正帮助企业解决业务欺诈问题还有待考证。

安全建议

基于2022年Web安全趋势观察，网宿安全团队建议企业选择能够一站式防护各类Web安全威胁的WAAP安全方案，针对多云环境下的Web业务，充分整合DDoS防护、WAF、Bot管理、API安全、威胁情报等防护能力，实现Web业务全场景、全栈防护。

选择WAAP方案时，建议特别关注以下能力：

优先选择自身安全水位高的CDN、云计算平台

CDN、云计算平台作为互联网关键基础设施，自身具备高安全水位。同时，在混合云的IT基础架构下，通过CDN/云计算+WAAP反向代理可隐藏真实业务源站，实现攻击面收敛，减少暴露风险。

支持API资产和风险盘点、一体化管理、监控和响应的完整闭环

面对日益复杂的Web安全威胁，端到端闭环的安全管理才能真正解决问题，而不是Web及相关安全产品的堆叠。选择方案时建议重点详细考量产品是否具备API资产和风险盘点、安全策略一体化管理、高度自动化的监控和响应这几个核心能力。

具备情报及AI实战化能力

对于传统被动式策略防护无法应对、高度自动化智能化的盗取敏感数据、业务欺诈等攻击，基于数据驱动的情报和AI主动对抗能力已不可或缺。建议重点考量WAAP方案中是否包含情报和AI的交付能力，以及实际检测效果。

提供安全托管服务

复杂的Web安全威胁对安全运营的综合性要求很高，建议优先选用具备持续专家安全运营和安全托管服务能力的厂商，有效发挥出WAAP方案的防护价值。

版权信息

CHINA INTERNET SECURITY REPORT