2019
全球互联网安全态势报告

白山云科技 BAISHANCLOUD YUNDUN

声明

本报告为北京数字世界咨询有限公司（下称 " 数世咨询 "）、贵州白山云科技股份有限公司（下称 " 白山云科技 "）、上海云盾信息技术有限公司（下称 "YUNDUN"）联合研究成果。

报告中涉及数据来自白山云科技全球节点攻击流量采集和蜜罐监控、白山云科技全网 IP 威胁情报、YUNDUN 云安全平台、YUNDUN 安全运营中心黑灰产研究成果及 CNCERT 等互联网公开数据，或通过合法技术手段、调研考察等方式获取。由于统计方法不同、视角和数据观察维度不同，与市场实情可能存在一定误差。

本报告仅从学术角度做分析研究，任何非法行为都将受到法律严惩。

名词解释：

ATD：深度威胁识别（Advanced Threat Detection）

DDoS：分布式拒绝服务攻击（Distributed denial of service attack）。

CC 攻击：挑战黑洞（Challenge Collapsar Attack），DDoS 攻击的一种类型。

关于数世咨询

北京数字世界咨询有限公司，中国数字安全领域中立的第三方调研机构，以数字时代为背景，提供网络安全行业的调查、研究与咨询服务。

关于白山云科技

贵州白山云科技股份有限公司是国内专业的专注于数据服务的云计算服务提供商。公司坚持技术创新，运用边缘计算、大数据和人工智能等技术，搭建数据、应用、系统、网络之间相互链接的创新型云计算服务平台。

关于 YUNDUN

上海云盾信息技术有限公司（YUNDUN），是专注于提供新一代安全产品和服务的创新创业企业。以纵深安全加速的产品理念，运用零信任安全思想，融合全球智能边缘安全平台，一站式解决数字业务的应用漏洞、黑客渗透、爬虫 bot、DDoS 等安全威胁，满足合规要求，提高用户体验。

- **YUNDUN 安全运营中心：**基于多年互联网 NOC 和 SOC 的实战经验，在资源、技术、能力的深度整合下形成的产品服务和内部职能。
- **YUNDUN 盾眼实验室：**以攻促防，持续进行互联网攻防对抗策略的研究升级的内部机构。

目录

01 报告摘要

02 2019 攻击趋势分析

03 典型攻击事件案例

04 洞见未来安全技术发展，迎接未知挑战

01 报告摘要

- 2019年，YUNDUN云安全平台日均阻断上亿次的Web漏洞威胁，日均拦截数十亿次Bot请求，日均清洗DDoS峰值600Gbps以上，YUNDUN安全运营中心复盘各类攻击事件数百起，并联动白山云科技ATD平台庞大的全网威胁情报储备与大数据分析能力，全方位剖析2019年全球互联网安全态势，以及展望5G、IPv6、AI等高新技术的发展将对安全产业带来的冲击。

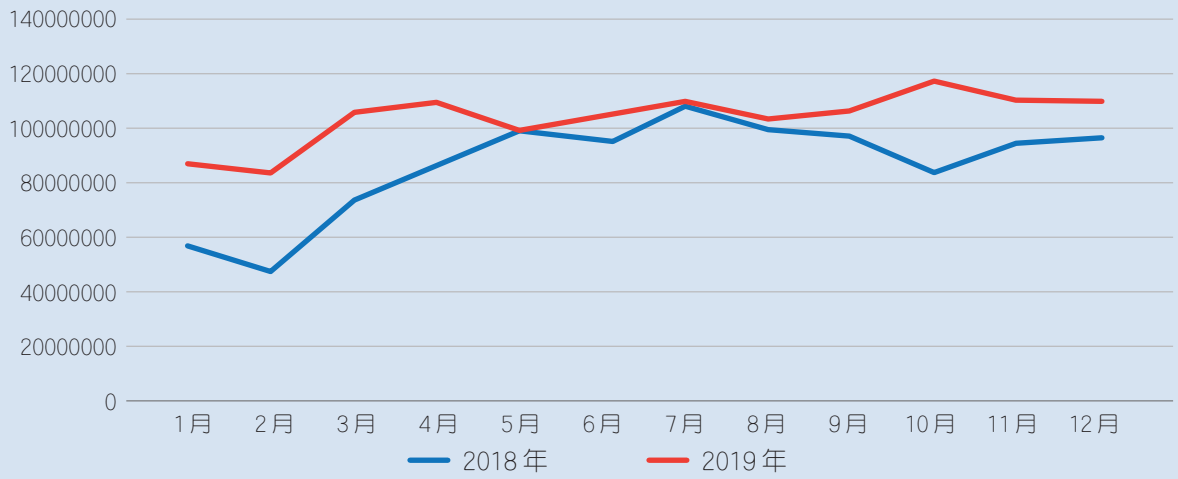
- 本报告将从Web应用攻击态势、DDoS攻击态势、业务层攻击态势三个方面，结合六个典型的安全事件的复盘，为读者解析2019年全球互联网安全态势，力求为网络安全相关从业人员提供参考，助力企业安全防御体系的完善与建设。

- 核心观点提炼：
  - 网络攻击威胁倍增，数据及敏感文件的安全性将成为企业的核心关注对象
  - 大流量 DDoS 攻击已成常态化，T 级时代来临，游戏行业备受攻击者青睐
  - 业务层威胁两极化分明，爬虫攻击稳步上升，资讯行业需保持警惕
  - 黑客攻击一改往日 " 傻大黑粗 " 的攻击模式，" 变种 " 攻击不断显露
  - 挑战与机遇并存，AI、IPv6、5G 引领未来安全技术创新发展

02 2019 攻击趋势分析

2.1 Web 应用攻击趋势分析

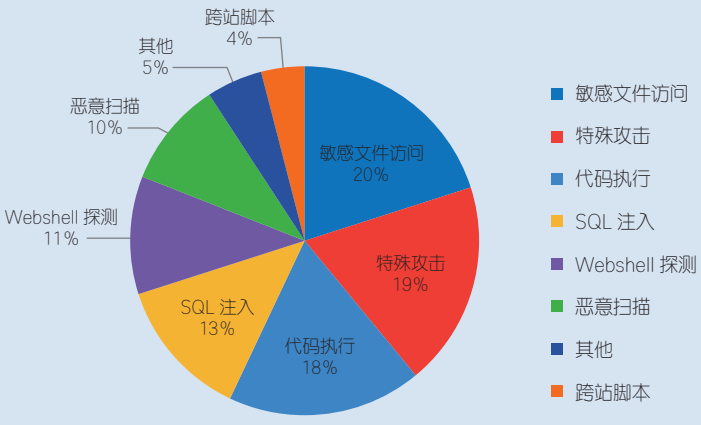
2019 年，YUNDUN 安全运营中心共计监测 Web 应用攻击 12.6 亿次，整体呈上升趋势，伴随着 9 月末 phpStudy 隐藏后门漏洞的爆出，2019 年攻击量于 10 月份达到峰值，相较于 2018 年同比上升 20%。



2019 年 v.s 2018 年 Web 应用攻击趋势图

企业需特别关注敏感文件的安全性

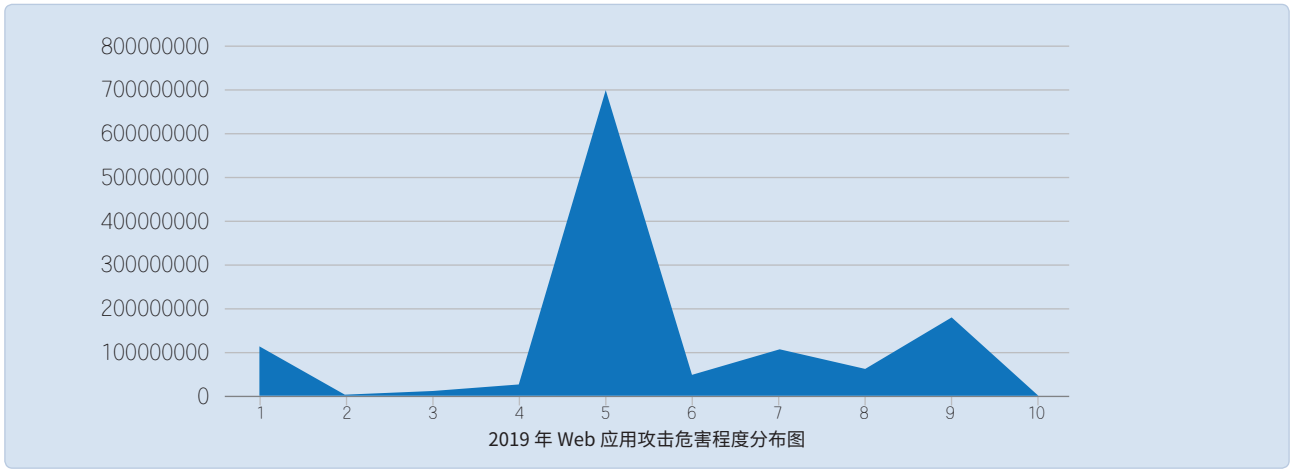
总攻击量的 20% 来源于敏感文件访问，意味着攻击者更青睐于扫描获取网站开发过程中因疏忽而对外开放的敏感文件 URL，进而直接取得网站的数据库文件、配置文件等。受 ThinkPHP、WebLogic 等 Web 应用开发框架的漏洞公布影响，基于特殊 Web 应用发起的特殊攻击量相较于 2018 年，攻击量大幅上涨，2019 年占比达 19%。



2019 年 Web 应用攻击类型分布

中高危攻击常态化，危害程度有向高危转移的趋势

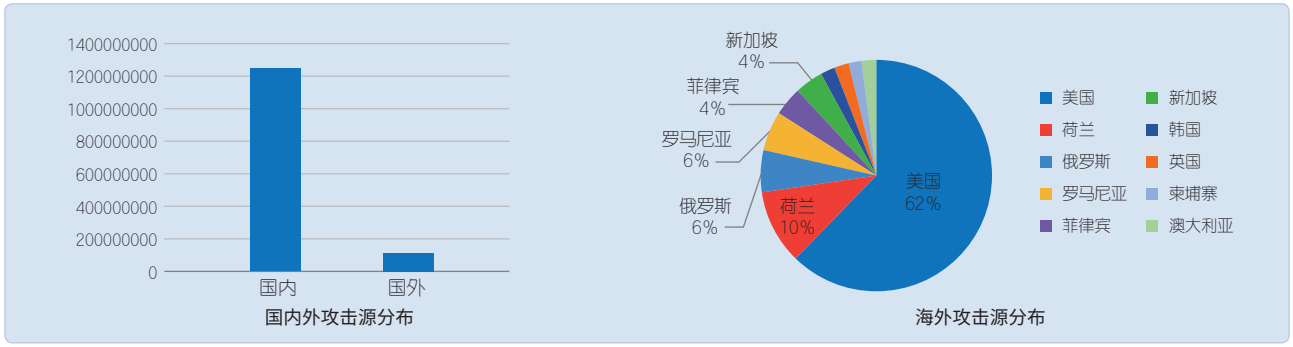
YUNDUN 安全运营中心针对监测拦截的 Web 应用攻击，针对应用遭受攻击可能的影响程度，从无明显影响 (1 档) 至无法正常运行 (10 档) 划分 10 个等级。2019 年危害程度分布与 2018 年相仿，大多数攻击可能的影响集中在造成业务波动 (5 档)，但造成业务无法运行的攻击依旧存在，需专注防护。



2019 年 Web 应用攻击危害程度分布图

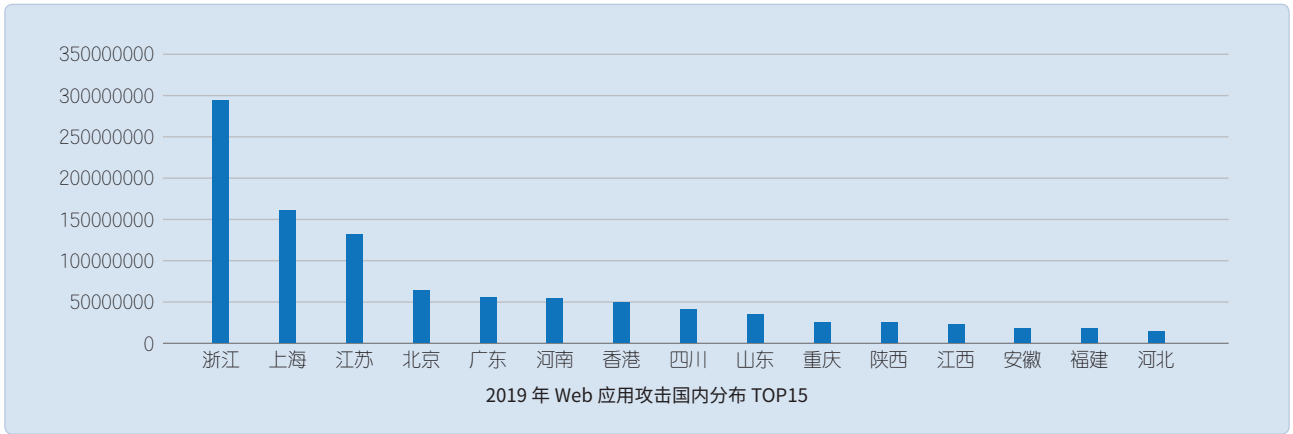
Web攻击源绝大多数分布于国内，海外分布以美国为主

鉴于云上业务的分布仍以国内用户为主，绝大部分 Web 应用攻击量依旧来源于国内。放大分析海外攻击源分布，美国以 57% 的占比居海外攻击来源榜首。



国内外攻击源分布　　海外攻击源分布

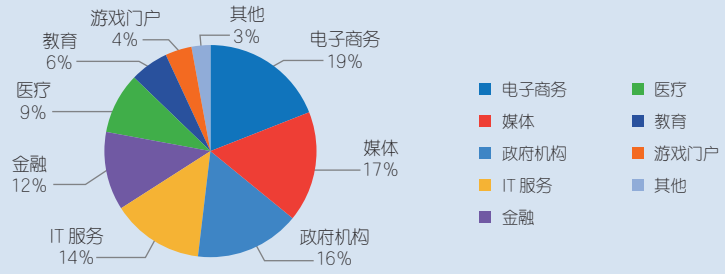
进一步分析国内攻击源分布情况，攻击源集中在浙江、上海以及苏州等南方城市。



2019 年 Web 应用攻击国内分布 TOP15

用户基数大，数据敏感度高的行业更易遭受攻击者青睐

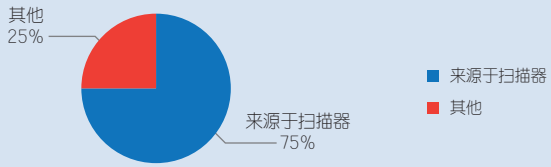
电子支付承载着大量用户的支付信息、个人敏感信息等也大量存储于各个电子商务平台，使得不法之徒趋之若鹜，攻击量占比高达 19%。媒体行业因其用户基数大、群体广，网站权重高，受到以 " 盗取 " 访问流量为目的的攻击者所青睐，攻击量占比 17%。



2019 年 Web 应用攻击行业分布

攻击流量来源多以扫描器为主

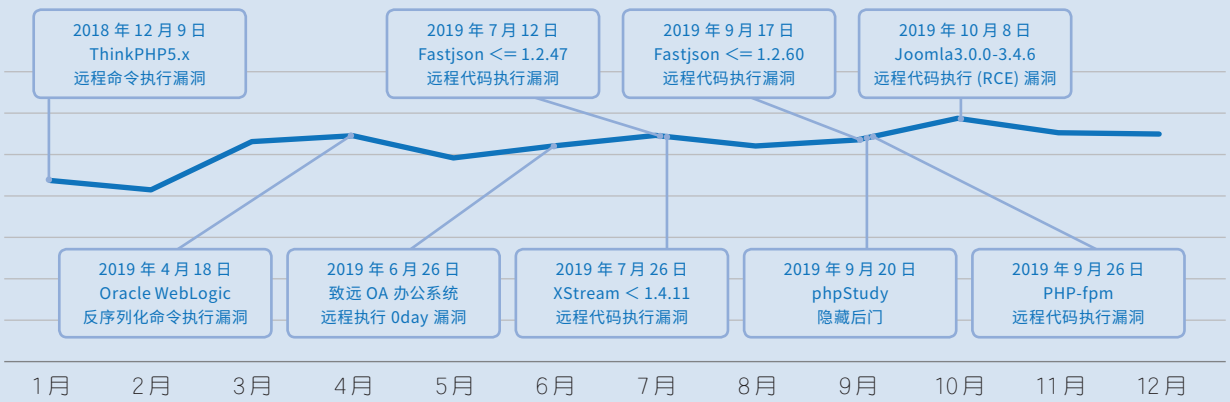
超过 75% 的攻击流量均来源于扫描器，伴随着攻击自动化的趋势，多数 Web 应用攻击的发生均来源于前期扫描器针对性的对站点 URL 扫描抓取漏洞。每一次扫描事件均伴随着数以万计的请求产生，推荐通过特征、行为、设备指纹等维度标识扫描器请求，有效防治扫描事件的发生，降低网站因扫描而暴露隐藏漏洞的可能。



2019 年流量来源占比

大型漏洞的爆出与攻击量趋势呈现正相关

将有巨大影响的漏洞爆出事件与 2019 年攻击量趋势进行对比发现，伴随着大型漏洞爆出，当月及次月的攻击量均有明显的上升。特别是上半年 Oracle WebLogic 反序列化命令执行漏洞，与下半年 phpStudy 隐藏后门的爆出，分别将攻击量推向了半年峰值。比起漏洞产出源本身，攻击者对于漏洞的关注与利用程度也是极其的高。因此作为安全厂商需更加密切的关注互联网漏洞爆出情况，提前制定应对策略，实施相应的应急防护，方能有效帮助客户业务有效抑制风险的出现。



2019 年漏洞爆出与攻击量对应图

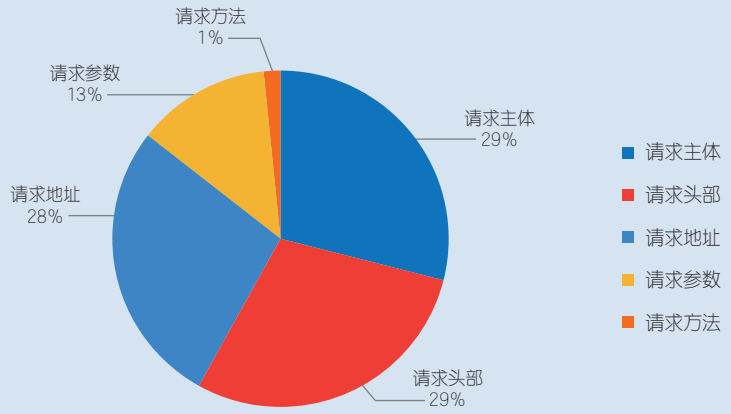
攻击者更偏向于在请求地址、请求头部、请求主体中插入攻击点

分析2019年Web应用攻击payload在报文中的分布情况，相较于请求参数、请求方法，攻击者更倾向于将payload置于请求地址、请求头部以及请求主体中。

请求地址： 进行信息收集时，扫描探测文件、目录的攻击行为较多。

请求头部： 通常网站开发者比较关注的是参数和主体中的安全问题，可能比较忽视头部字段安全。特别是诸如 user-agent、referer、cookie 等字段中；今年爆出的 phpStudy 后门，也是针对头部字段 Accept-Charset 的利用，这也是请求头部攻击较多的原因之一。

请求主体： 当前网站倾向于把向网站提交的数据内存通过主体进行提交，所以针对主体的攻击比较多；值得关注的是诸如文件上传、尝试上传 Webshell 依旧是较为严峻的攻击类型。

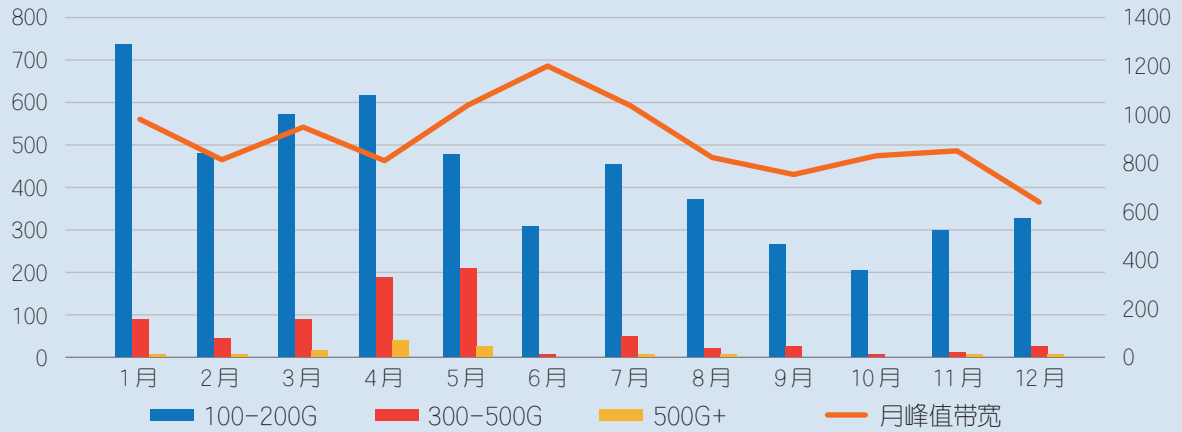


payload 在报文中的分布情况

2.2 DDoS 攻击趋势分析

300G以上大流量DDoS攻击已成常态，T级攻击不断涌现

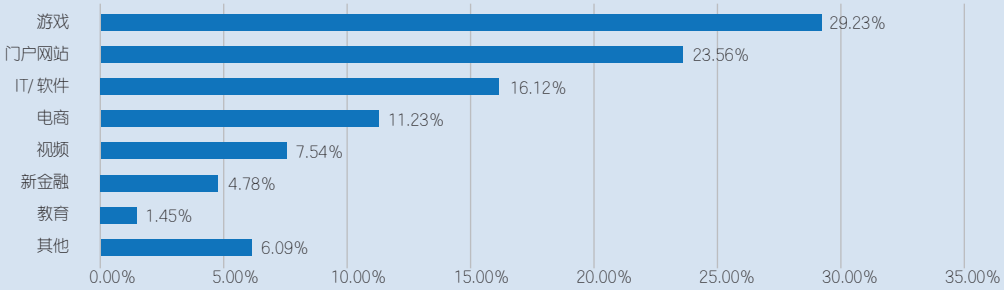
伴随着物联网时代的来临，大批量的 IoT 设备沦为黑客肉鸡，大于 300Gbps 的攻击占比整体已超 15%，大规模的 DDoS 攻击已成为常态，同时统计各月的 DDoS 攻击峰值带宽，月平均峰值带宽已接近 1Tbps，预示着 T 级攻击的时代已经来临。



2019 年 100Gbps 以上 DDoS 攻击事件分布

游戏行业依旧是最需警惕DDoS攻击的行业

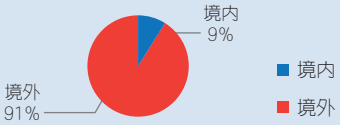
游戏行业由于其行业竞争激烈，对用户体验和实时交互的高质量要求，新游上线关键保障的业务特性。2019 年上半年依旧作为最受黑客青睐的攻击对象，占比达 29%，恶意竞争、敲诈勒索仍为主要动机门户网站与 IT/ 软件占据着大体部分，各占 23% 和 16%。 YUNDUN 安全运营中心建议以上行业注重 DDoS 预防工作。同时伴随着用户流量由网页端向移动端的转移，APP 应用相较于 Web 和 API 更易遭受攻击。



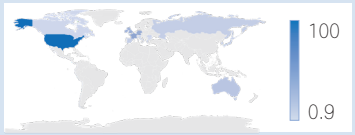
2019 年上半年 DDoS 攻击行业分布

控制端仍以境外为主，且有向第三世界转移的趋势

鉴于我国近年对网络资源的监管力度与日俱进，针对 DDoS 攻击的整治效果愈发显著，控制端（以下简称 C2）服务器主要集中在境外，境外分布以美国为主。但鉴于某些第三世界国家对于网络检查较为宽松，易于伪造源 IP 实施 DDoS 攻击，荷兰、希腊等第三世界国家 C2 服务器占比较 2018 年上升趋势。



2019 年控制端境内 / 外分布



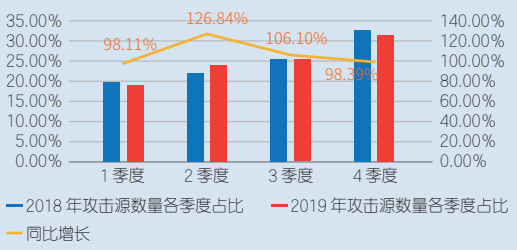
2019 年控制端境外分布

2.3 业务层攻击趋势

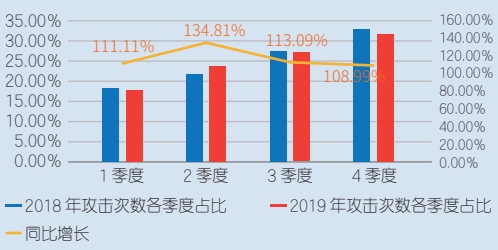
2019年网络攻击威胁总数增长翻番

2019 年，从白山云科技 ATD 平台上识别到的攻击数据来看，一共有网络攻击 9566.5 亿次，同比 2018 年增长 116.11%，攻击源有 24.5 亿个，同比 2018 年增长 106.53%，这表明，在 2019 年，整体互联网上的攻击次数和攻击源数量都保持着高速增长，整体安全态势并没有缓解，而是更严峻了。

在 2019 年第二季度，攻击源数同比增长 126.84%，攻击次数同比增长 134.81%，这和往年一样，3 月份开始是攻击高峰的开始，其中攻击次数增速尤其迅猛，攻击源环比增长 25.67%，攻击次数环比增长 32.61%。



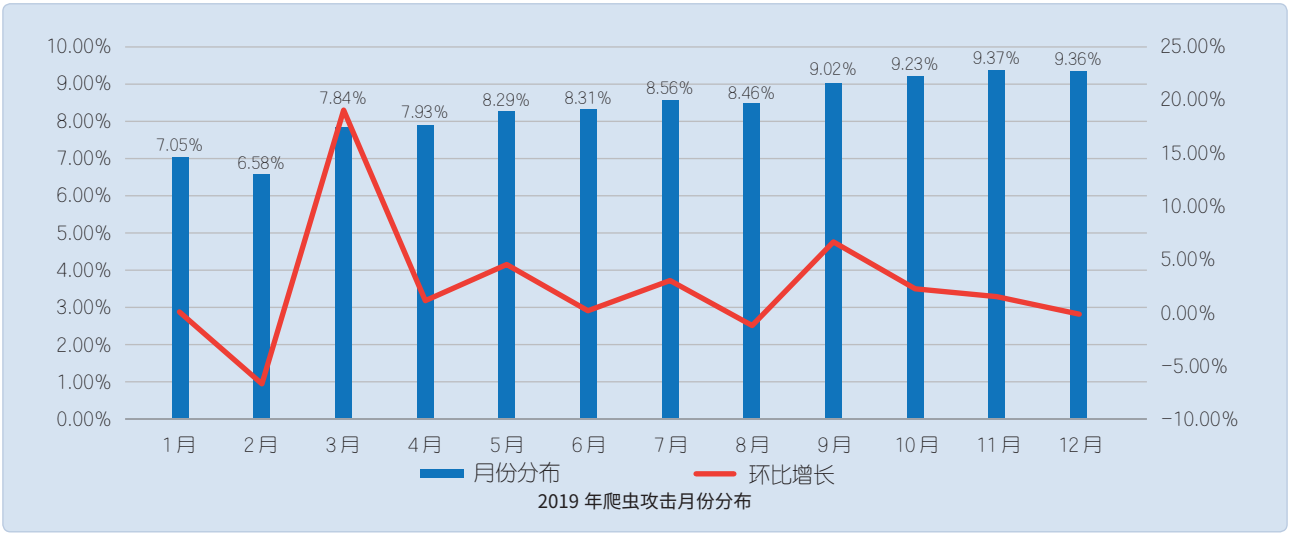
2018 年和 2019 年攻击源增长态势



2018 年和 2019 年攻击次数增长态势

爬虫攻击增长趋势稳定

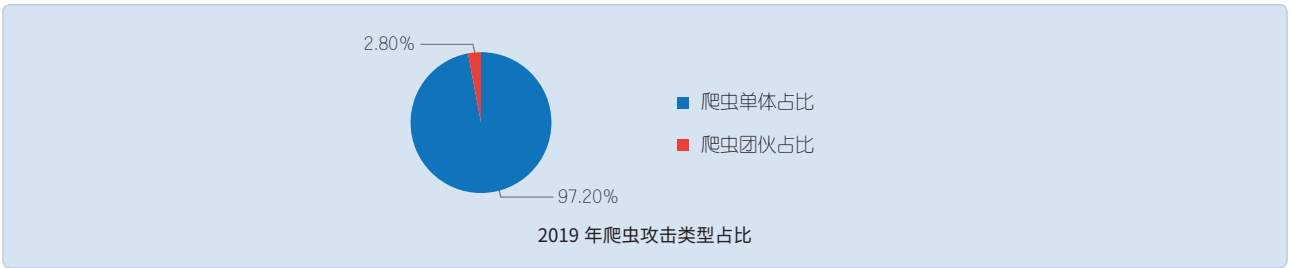
2019 年，爬虫攻击次数每月的增长趋势较为稳定，尤其 2019 年 2 月、3 月环比增长趋势变动较大，可能受春节影响。



2019 年爬虫攻击月份分布

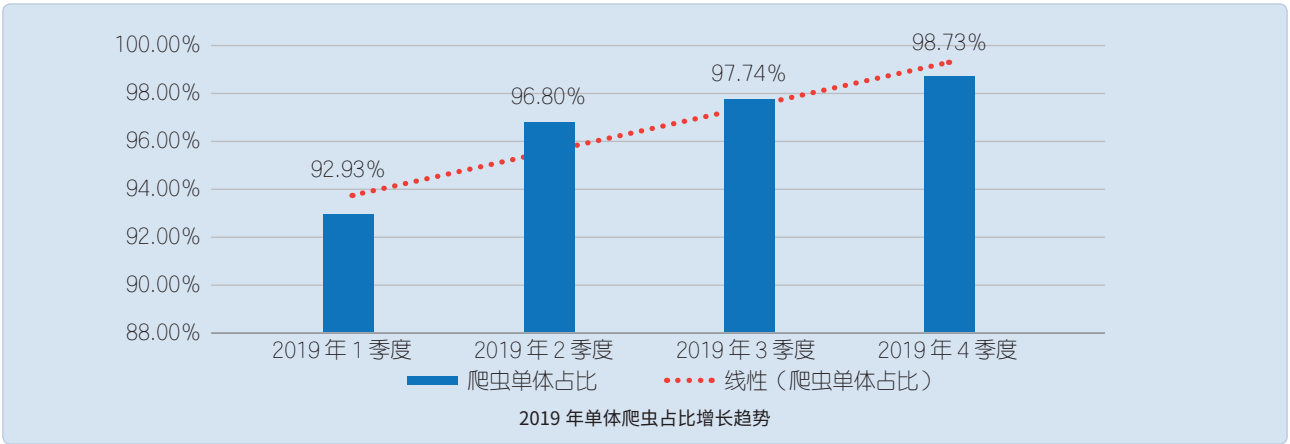
爬虫攻击者存在爬虫团伙，但更偏向于单体作案

在白山云科技 ATD 平台识别到的爬虫中，单体爬虫占据了绝大多数比例，而爬虫团伙占到了大概 2.8% 的比例，这说明在所有爬虫中，相对简单的个体爬虫还是绝大多数。虽然爬虫团伙占比不大，但由于其大量的使用代理池和批量化程序，相比单体爬虫往往可以爬取更多的数据。



2019 年爬虫攻击类型占比

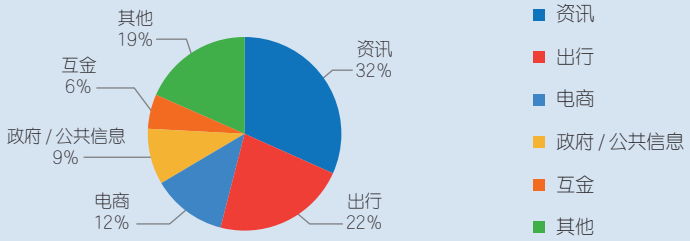
爬虫攻击总数的不断增加，2019 年第 1 季度到第 4 季度，爬虫单体占比也逐渐上升，这也从另一方面印证了爬虫攻击中单体爬虫相比团伙爬虫更易实施，基数占比更大。



2019 年单体爬虫占比增长趋势

资讯行业是爬虫攻击的主要目标

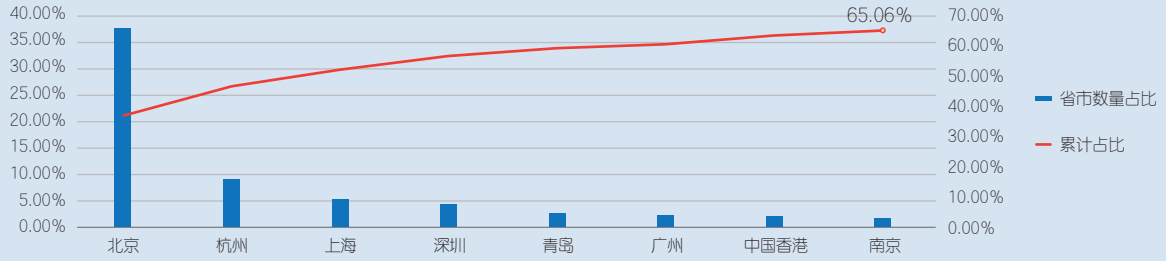
通过对 2019 年各个行业的恶意爬虫数据统计分析，可以看出资讯、出行、电商、政府 / 公共信息、互金等成为 2019 年受爬虫攻击最严重的 5 个行业。由于资讯行业中的内容信息直接影响着互联网用户流量的留存转化，资讯行业更看重暴露在网络中的数据价值，所以资讯行业的内容信息更受恶意爬虫的 " 青睐 "，占比最高达到 32%。



2019 年恶意爬虫流量目标行业分布

威胁攻击IP国内来源的主要区域分布在发达地域，北京最多

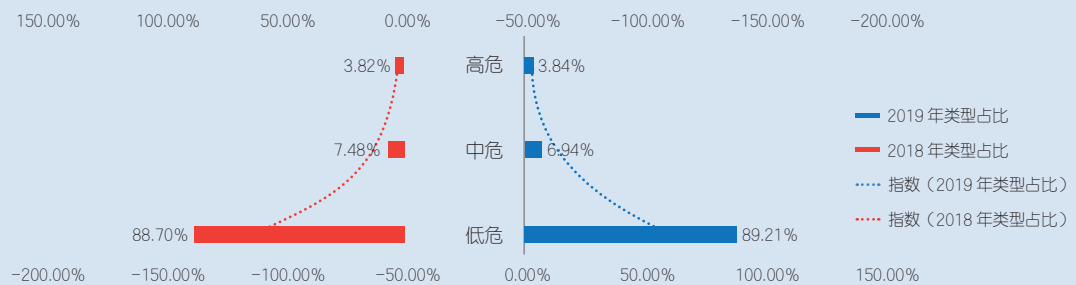
2019 年通过对威胁攻击 IP 来源的分析，主要来自北京、杭州、上海、深圳、青岛、广州、中国香港、南京等地区，以上 8 个地区所占威胁攻击流量超 65%。IP 来源不代表威胁攻击的背后指示者，是因为爬虫攻击大多部署在租用的 IDC 机房中，而上述发达地域的 IDC 机房较多。



威胁攻击 IP 来源省市分布

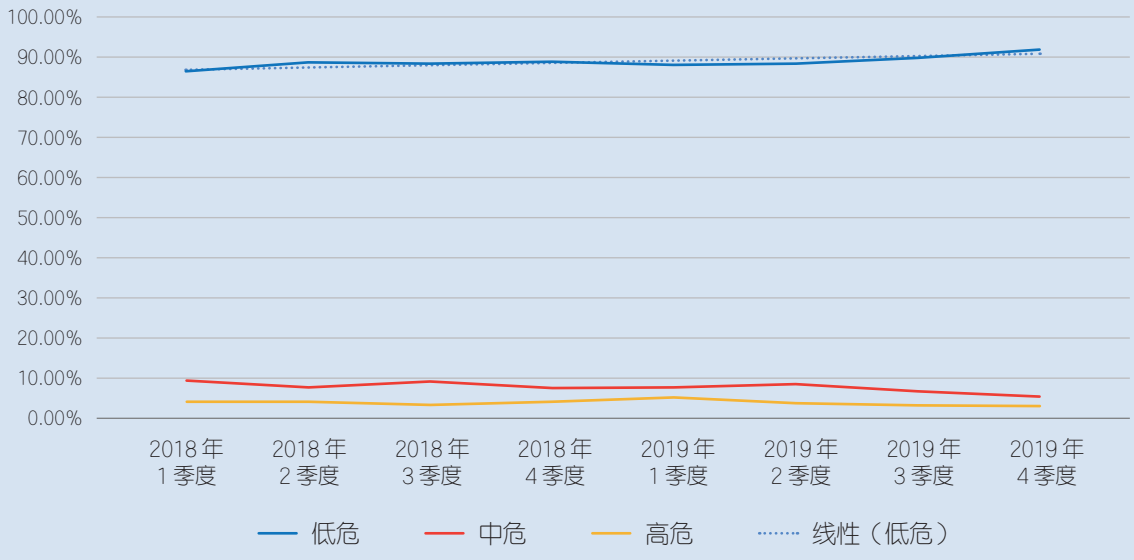
低风险威胁常态化，高占比态势稳定

白山云科技 ATD 平台针对监测拦截的攻击威胁，对应业务网络遭受攻击可能的影响程度，从无明显影响（低风险威胁）至无法正常运行（高风险威胁）划分 3 个梯度等级。2019 年业务攻击威胁程度分布与 2018 年分布相似，成金字塔分布。虽然威胁攻击次数总量巨大，但通过对不同等级的威胁攻击划分不同的响应机制，能大幅降低安全运维的工作量。



2018 年和 2019 年业务攻击威胁程度分布对比

各级别威胁数量占比较为稳定，其中低风险威胁总数量约占比 90%，从 2018 年 1 季度至 2019 年 4 季度，有轻微增长趋势，增长 4.93%。



2018 年至 2019 年各级别攻击威胁占比

03 典型攻击事件案例

3.1 漏洞应急响应实践

2019 年 4 月 17 日 20:59:17，国家信息安全漏洞共享平台（CNVD）公开了 Weblogic 反序列化远程代码执行漏洞（CNVD-C-2019-48814）。攻击者利用反序列化处理输入信息的过程中存在的缺陷，发送恶意 HTTP 请求，以此获取服务器权限，最终实现远程代码执行。官方补丁未发布，漏洞细节未公开，归属 0Day 漏洞，此时漏洞所能带来的危害将无从防范。结合潜在威胁挖掘数据中心中观测到的大量异常行为，YUNDUN 安全运营中心判定该漏洞风险评级为 " 高危 "，并迅速进入应急响应状态，力求第一时间制定抵御该漏洞攻击的防护策略，保障平台客户业务的安全运行。

AI数据挖掘，助力捕获漏洞攻击行为

为加速漏洞攻击行为的采集流程，并最终实现漏洞的自动发现，YUNDUN 安全运营中心基于深度学习等技术，构建了一套用以挖掘潜在威胁的 AI 模型，通过 " 学习 " 大量的威胁情报、事件类型、来源和结果等威胁情报数据，现阶段，AI 模型已经具备对网络威胁的发现识别能力，可以自动化地执行威胁情报数据的采集流程，并进行低层次的处理，显著降低 YUNDUN 安全运营中心对漏洞攻击行为特征的分析成本。

漏洞公示第一时间，为最大化的捕捉到敏感时期的未知漏洞的攻击行为，YUNDUN 安全运营中心将 AI 模型阈值调整为敏感级别。同时，根据已披露的信息，对产生漏洞的 Weblogic 版本的进行研究，结合 AI 模型捕获到的攻击行为，持续进行漏洞行为特征的研究发现。

沙箱流量回放，助力防护策略的制定与验证

YUNDUN 安全运营中心通过分析漏洞依赖的 Weblogic 版本，构建定制化的沙箱环境，并根据 AI 模型挖掘到的威胁情报数据相关字段，进行数据包的重组，组成一个接近与攻击时的 http 报文包，置于沙箱环境中进行威胁流量回放测试，根据攻击效果，标注攻击行为，最终确认有效的攻击 payload。

针对攻击行为特征的研究分析结论，YUNDUN 安全运营中心制定专有防护策略，并同步至沙箱环境中，再次进行威胁流量回放测试，用以检测安全策略的防护效果：

> 初次流量回放测试中未知漏洞 60000 个，下发防护策略后，仅存 700 个未知漏洞，其余部分均被拦截并标注为代码执行

最终，YUNDUN 安全运营中心确认策略的防护效果，并着手防护策略的下发及善后工作的准备。

防护策略的生效，与应急响应的善后

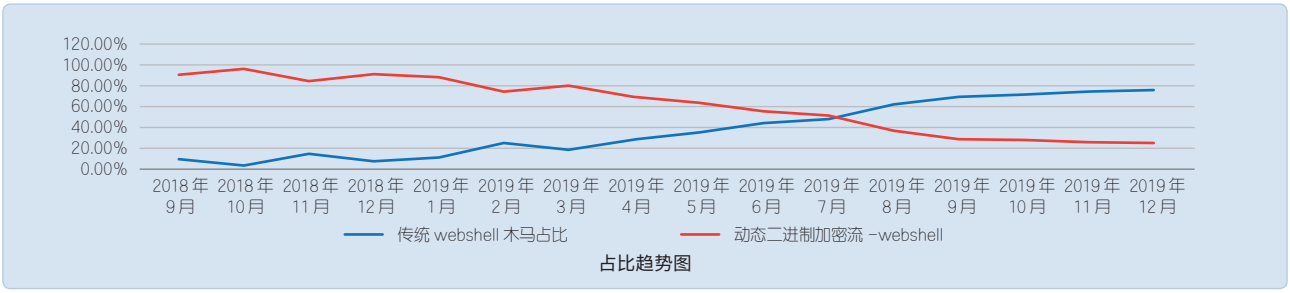
确认策略的防护效果后，YUNDUN 安全运营中心迅速在安全策略防护中心中更新防护策略，并进行全网策略的更新，得益于全网实时下发机制，可以保证更新后的防护策略于 1-2 分钟内全网生效。防护策略生效后，持续观测大数据中心中的漏洞攻击检测情况，确认针对该漏洞的攻击均被识别并阻断，做到了有效防护、及时防护。

应急响应后，YUNDUN 安全运营中心仍未放松警惕，持续关注潜在威胁挖掘数据中心，以防有遗漏或变种的绕过行为，同时，AI 安全研发人员，针对此漏洞的攻击 payload，对神经网络模型进行微调，以增强其对此类攻击的识别泛化能力，最终完成本次高危漏洞的应急响应，保障平台用户业务运行的安全稳定。

应用的开发到管理将涉及大量的第三方软件，例如应用服务中间件 Weblogic。因此漏洞的产生是难以规避的，除了漏洞产生的必然性，漏洞爆出的不确定性也是其最具风险的特性。对于 0day/1day 漏洞的爆发进行应急响应，做到及时防护、有效防护是 YUNDUN 云安全平台的核心能力体现之一。

3.2 Webshell 入侵倾向使用二进制加密流以逃避检测

2019 年，随着企业安全意识的提高，云安全防护产品的普及，仅通过传统 Webshell 木马已经很难达到预期效果。YUNDUN 安全运营中心持续监测拦截日志发现，攻击者发起 Webshell 入侵时，逐渐由使用传统 Webshell 木马转向使用动态二进制加密流技术，试图达到逃避检测的目的。



占比趋势图

为持续研究升级对抗策略，YUNDUN 安全运营中心就一起典型的结合动态二进制加密流的 Webshell 入侵事件进行了复盘剖析。

2019 年 6 月 14 日 -- 客户接入

某客户由于其网站内容屡次遭黑客恶意篡改，为保护网站内容安全，选择接入 YUNDUN 云安全平台，进行网站的安全防护。

接入当晚 18:40 -- 拦截网站 Webshell 连接行为

基于 AI 的 Webshell 实时识别模型监测到了有黑客试图连接该网站 Webshell 的行为，立即进行实时阻断，并发送告警通知 " 拦截 Webshell 入侵行为，业务无风险 "。

接入当晚 19:15 -- 黑客尝试再次上传 Webshell

YUNDUN 云安全平台检测并捕获黑客试图上传的 Webshell 文件，对比传统的菜刀一句话木马以及浏览器可直连的木马，内容组成有着明显的变形，如下图：

```
$k= "AES128";
$_= 'o'.'p'.'e'.'n'.'s'.'s'.'l'.'_'.'d'.'e'.'c'.'r'.'y'.'p'.'t';
```

对内容进行还原后，可见该攻击者在木马中引入 AES 加密算法。

```
,openssl_decrypt(file_get_contents("php://input"), "AES128", $_SESSION
```

观察本次 Webshell 入侵拦截事件，黑客在发现传统木马被识别拦截后，尝试上传使用动态二进制加密流木马来逃避检测。

随着动态二进制加密技术的普及，通过解析攻击 payload 的组成，并针对性的更新防御规则。传统防御思路已经失效，为保证防护效果，提高防御精度，并保证实时检测阻断，YUNDUN 安全运营中心持续升级对抗策略，结合访问行为特征分析，并运用 AI 模型对流量进行实时监测与分析，最终达到保障业务安全运营的目标。

3.3 警惕！一种 " 变种 "DDoS 防火墙绕过攻击

研究 2019 年 DDoS 威胁态势发现，得益于运营商以及云安全厂商双方的共同努力，极大地限制了 UDP 反射类攻击以及传统的 SYN Flood、ACK Flood 等攻击的攻击效果。部分黑客将攻击思路转向如何利用 TCP 反射攻击使攻击流量变成真实 IP 攻击，从而穿透传统 DDoS 防火墙直接攻击后端服务器。

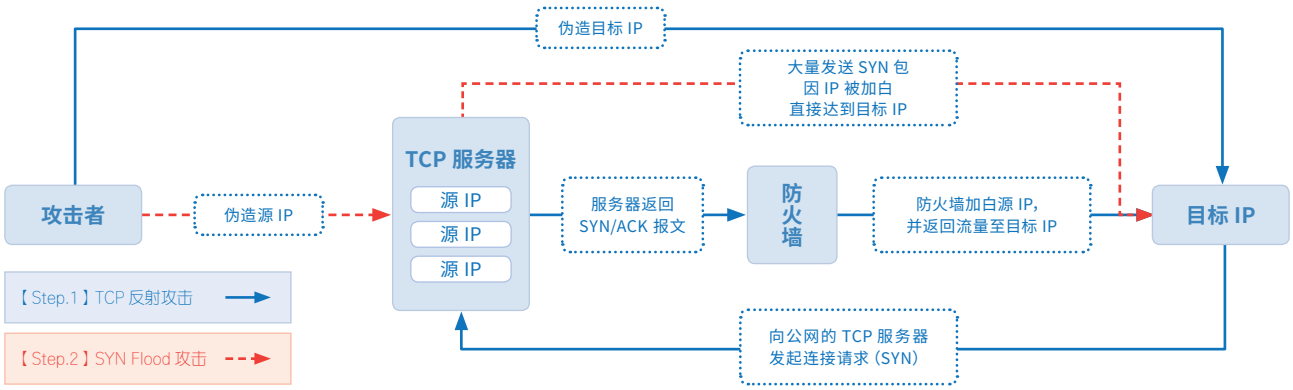
2019 年初，YUNDUN 云安全平台成功防御了一起披着 TCP 反射攻击外皮的 SYN Flood 攻击的典型攻击事件：

第一步：绕过防火墙策略

攻击者发动 TCP 反射攻击，伪造攻击目标源 IP 向公网服务器发起连接请求。由于参与 TCP 反射攻击的公网服务器 IP 均为真实的 IP，具有协议栈行为，可以通过 DDoS 防火墙的源认证，同时被加入防火墙 IP 白名单（白名单内的 IP 发送的数据包将直接被放行）。

第二步：实施真正的攻击

攻击者实施 SYN Flood 攻击，伪装公网服务器 IP（第一步中参与 TCP 反射攻击的公网服务器 IP）发送大量 SYN 数据包，由于攻击使用 IP 已经处于防火墙 IP 白名单内，因此 SYN 数据包穿透 DDoS 防火墙，直接传至后端服务器处，达到 DDoS 攻击效果。

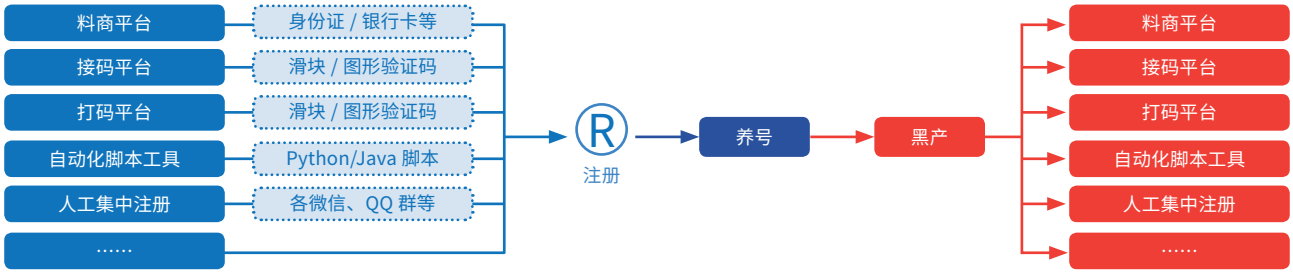


YUNDUN 安全运营中心及时介入调整防火墙策略，最大程度控制了攻击影响面，并优化防火墙检测逻辑，保证后续对此类攻击的防护效果。

此类攻击中，TCP 反射攻击被用作绕过 DDoS 防火墙的手法，最终达到最大化 SYN Flood 攻击效果的目的。黑客的攻击手法已经逐渐转变为更有技术性、更有针对性。

3.4 解析黑灰产业链源头 – 恶意注册

一直以来，安全防御理念局限在常规的漏洞扫描、防火墙、安全审计、防病毒等方面的防御，然而很多人都忽视了业务安全，很多重大的信息安全事件往往都因为业务安全引起的，例如恶意注册、撞库攻击、薅羊毛等。白山云科技安全专家深入研究黑灰产业链，发现注册，养号，黑产已形成一个完整的产业链，其中恶意注册更是产业链的源头所在。



在白山云科技 ATD 平台服务的客户中，某客户主要面向互联网用户提供新的生活方式平台入口，通过视频、图文等方式分享美好生活，带动线上进行购物，该客户业务平台流量和零门槛优惠券备受黑产青睐。

2019 年某日，该平台上线提供面额 30 元零门槛购物券的促销活动。活动当天注册用户数为 203971，经白山云科技 ATD 平台识别到恶意注册用户数达到 146694，活动真实用户仅为 28.08%。经过跟踪发现，平台活动后一周平均流量仅为活动当天流量 50% 左右，恶意注册用户仅为活动当日带来流量，活动结束后，恶意注册用户再未登陆平台。

此次促销活动，平台未达到活动预期，优惠券 80% 以上进入黑产口袋。

白山云科技 ATD 团队通过解析白山云科技 ATD 平台中针对恶意注册主要手段的观测数据，结合客户平台正常的注册流程，及预置的非法访问请求拦截逻辑，**针对客户痛点的恶意注册问题提供解决方案：**

- 利用白山云科技 ATD 平台可编程对抗功能，对抗 python、Java 等脚本攻击；
- 利用 AI 机器学习等技术，对特定注册路径进行历史访问行为分析，识别微信、QQ 群等真人集中恶意注册行为；
- 利用安全事件编排功能，联动 WAF、防火墙等安全设备，及时拦截恶意注册行为；
- 梳理注册功能逻辑，制定注册页面合法注册基线。

3.5 UEBA 行为分析技术加持，精准检测爬虫攻击

随着互联网、移动互联网以及各个企业在线业务的发展，数据变得越来越重要，对于黑灰产或者竞争对手来讲，获取到别人的数据来促进自身的发展或者用于牟利，就逐步变成了一种产业，爬虫就是其中最重要也是最难以防范，也最为典型的手段。一旦爬虫攻击触及到了用户个人隐私数据或者涉及企业核心的数据，如信贷数据、简历数据、房屋数据、交易数据、评价数据、物流数据等等，就将会对企业的数据安全造成非常恶劣的影响，甚至影响其正常的业务经营。

如今的爬虫攻击逐渐呈现智能化和拟人化，传统的基于规则安全防护手段，很容易被攻击者绕过，防护能力甚微。接入白山云科技 ATD 平台前，某著名在线房屋交易网站的楼盘评论数据，便长期遭受恶意爬虫的攻击威胁；接入后，经白山云科技 ATD 平台识别分析，发现该爬虫有如下特征：

- 不断变化自身浏览器标识用于模拟真实浏览器；
- 控制爬取频率，绕过基于频率的安全防护手段；
- 为规避 ATD 系统，动用同网段的代理池，不断的更换 IP 继续爬取数据；
- 代理池爬虫 IP，存在清晰的角色分工，包括负责激活 session，负责爬取数据，负责混淆行为等，进一步加强识别难度；

基于 UEBA 行为分析的算法模式的白山云科技 ATD 平台，通过对访问行为在多种维度上的数学建模，进而对该用户和同一滑动时间窗口内的群体用户行为进行个群对比算法来识别恶意行为。针对该房屋交易网站遭受的爬虫攻击 IP，观测经 ATD 系统识别绘制的威胁画像可以看出，其与群体行为在 Referer 最大相似占比、平均请求长度等维度上都存在着较大差异，说明其在个群对比分析算法中处于离群点的位置，是恶意的攻击行为。

同时通过深入 UA（User Agent）画像，发现在 UA 集合空间特征上，该爬虫攻击 IP 和群体行为存在较大差异：攻击者伪造了百度搜索引擎、Mozilla5 浏览器、iPhone 等多个标识进行爬取，以绕过传统安全手段的检测。但是由于 ATD 识别威胁使用的是基于 UEBA 算法的个群对比算法，所以即使伪造浏览器标识，白山云科技 ATD 平台仍然可以精准监测识别恶意爬虫攻击。

借助白山云科技 ATD 平台，解析复盘了典型的爬取攻击过程：从开始的单个 IP 的爬取行为到后来的使用整个 C 段进行代理池团伙爬取的行为，在整个攻击过程中，攻击者伪造了 HTTP 请求，借用了正常浏览器的 User Agent，同时利用自动化程序控制爬取频率，总体控制频率在 10 次 / 分钟以内。这些代理池的低频爬取行为很容易就绕过绝大部分安全防护手段，使得企业很难避免数字资产流失。

因此，针对恶意爬虫的有效防护，使用传统的基于规则安全防护手段，就很容易被攻击者绕过。但基于 UEBA 行为分析算法的白山云科技 ATD 平台，通过多维度全面分析用户访问行为，智能解析恶意爬取行为与正常用户行为之间的差异点，最终实现精准识别爬虫攻击的防护效果。

04 洞见未来安全技术发展，迎接未知挑战

4.1 AI

随着网络技术的发展，新型攻击形式也日渐增多，新的黑客技术层出不穷，为传统基于规则的防火墙带来了严峻挑战。一方面，在灵活的攻击方式面前，很容易绕过，基于领域知识的规则难以应对新型攻击；另一方面，规则的维护对技术要求高，成本大。另外，随着业务的增长，在海量的日志中进行行为分析和事件关联是一项非常有挑战性的工作。这些因素的驱动下，基于大数据和机器学习的自动化网络安全解决方案，将推动网络安全技术的不断升级。

AI在网络安全应用现状

AI 在网络安全上的很多场景已经得到应用，如恶意流量检测、应用识别、异常行为分析、快速攻击响应等，但真实效果距业界的要求尚有一定差距。主要在于网络安全特定场景的建模较为困难，另外就是训练样本数据的缺乏。尽量有大量的正常访问数据，但入侵样本少，对模型的训练较为困难。且不同的用户业务形态和访问模型不同，难以利用 AI 生成通用的防护策略。此外还面临着算法的工程化、海量数据处理的性能瓶颈，AI 对固有的对结果的可解释性不强、鲁棒性不足等缺点。

AI在网络安全未来方向

当前，AI 在网络安全领域的应用场景多、前景好，但相关核心算法和技术尚未成熟稳定，AI 在网络安全领域的应用尚未普及，就整个网络安全领域而言，AI 的应用目前还处于比较初级的阶段。

随着网络安全数据量的爆发增长、算法的优化改进、计算能力的大幅提升，AI 必将成为下一代网络安全解决方案的核心，AI 在网络安全领域的应用必将呈现跨越式发展。未来的 AI 将更深入结合网络安全业务，在算法的工程化上解决诸多难题，实现千站千面的精细化自动化防护，在行为分析、事件关联等高级场景也将取得更多突破。

从SIEM&AI到SIEM@AI

目前企业的安全运维面临着海量的数据、频繁的报警、艰难的修复，企业真正需要的是将系统运行在一个完全由 AI 驱动的智能平台上（SIEM@AI），无需很多成本甚至完全无需学习成本，即可使用 AI 技术从海量的输入数据流信息中发掘威胁事件，并自动使用 AI 技术对不同业务、不同维度的数据进行智能关联，建立内在联系，并最终自动对威胁事件进行处置处理。在提高识别的准确率和召回率的同时，解放安全工程师的人力并提高其效率，最终实现对于企业外网、业务、内网的三层智能防御。

对于新一代由 AI 驱动的 SIEM 平台来说，比起如何无监督学习进行纵向分析，更有挑战的任务是在表层不相关的海量数据中建立潜在关联，从而实现真正的深度威胁识别。其中最重要的先决条件是通过 SIEM 的采集层收集足够的数据，其次是选择合适的算法对数据进行加工处理，最后是通过 AI 算法对数据进行关联分析。这种关联分析不仅仅对于已知威胁的回溯有帮助，也对未来的安全态势感知有重大意义。

4.2 IPv6

为解决 IPv4 地址的枯竭问题，以 IPv6 为代表的下一代互联网技术应运而生，由于 IPv6 相对 IPv4 的诸多优势，国家政策层面对 IPv6 的推动，越来越多的用户开始应用 IPv6 网络。虽然 IPv6 的设计对安全性有一定的提升，然而许多在 IPv4 中存在的网络安全问题在 IPv6 中同样存在，IPv6 的一些新特性甚至会带来新的风险，由此一来对于 IPv6 网络的安全需求将激增。

IPv6带来的安全风险

IPv6 虽然解决了网络地址紧缺的问题，但由于海量地址的查询十分复杂，这就为安全检测带来难度。IPv4 防火墙在针对 IPv6 流量的细力度控制上几乎无力，基于协议和端口的报文过滤对于能够灵活变化的通道也几近失效。

从 IPv4 到 IPv6 将使用过渡协议，攻击者可以利用过渡协议的漏洞绕开安全监测进行攻击，因此 IPv4 与 IPv6 的共存会带来一些安全问题。IPv6 规模部署工作呈现加速发展态势，过度期间为保证 IPv4 与 IPv6 的相互通信，会采用相应的过渡机制，然而部分机制自身存在安全缺陷，或将引入新的安全隐患，导致过渡期间安全风险持续叠加。

目前，大多数网络设备仅仅支持 IPv4，不能直接用于 IPv6 网络。少数可以支持 IPv6 的设备安全防护能力较弱，无法应对 IPv6 大规模推广带来的安全问题。对于安全设备和软件而言，由于 IPv6 的新特性，无法继续提供安全保障服务，因此企业业务可能会面临一段时间的安全防护的 " 空窗期 "。

应对方案

安全厂商在支持 IPv6 时，需考虑 IPv6 编址规范、运营商 IPv6 黑洞路由支持以及互联网企业安全产品改造并对接，需要多部门及各厂商共同改造并协同配合。业务迁移至 IPv6 时，涉及网络、业务、应用的调整，需要更全面更系统地梳理应对方案。安全产品 IPv6 升级后与 IPv6 地址相关的策略及逻辑均要重新改造设计，全面测试验证。IPv6 的改造是一项庞大的系统工程，如果用传统方式，需要对服务器、网络以及应用进行全方位的升级，不仅技术挑战大，而且周期长。

上海云盾提供了较完整的 IPv6 解决方案，可帮助企业在短时间内完成业务系统的升级，同时保障业务的连续性。

4.3 5G

5G 是数字世界的基石，是智能化的推动力，是构建起万物智联的纽带，运作模式将会从人与人的连接扩展至物与物的连接。5G 商用紧锣密鼓地展开，将大大促进人工智能、大数据、物联网等新兴技术的不断发展，虽然 5G 发展趋势已经势不可挡，但是其中存在的安全缺陷也是不容忽视的。

物联网安全至关重要

随着 5G 商用化的不断推进，物联网设备也将爆炸式增长，大量的敏感数据通过互联网传输于联网设备之间，安全风险和漏洞有可能危及物联网应用程序中客户数据的安全和隐私。另外，由于物联网设备都是使用简单的处理器和操作系统，无法像传统的 PC 电脑和服务器一样支持复杂的安全防御方案，导致黑客可以轻易对这些物联网设备实现入侵，然后利用这些海量的物联网设备发起超大流量的 DDoS 攻击。

另一方面，5G 为时代带来更高的网络速率和更高密度的网络容量的同时，也预示着更为凶猛的网络攻击流量。

传统边界防护已失效，安全迎来变革

在 5G 万物互联时代，物联网系统越来越复杂，网络拓扑动态变化、内网和外网的边界变得越来越模糊，网络泛化成为一个大趋势，传统的基于网络边界的防护模型将难以为继，5G 网络环境下更容易受到威胁和攻击。

5G 技术引领而来的新时代下，数据将成为网络保护的核心对象，而鉴别 " 谁 " 能通过何种方式访问哪些数据，并实时管控数据的访问行为，也将代替传统的边界防护思想，扎根于新时代下的数据世界安全保护体系中。

关于报告

报告顾问

数世咨询： 李少鹏

作者

白山云科技： 丛磊、王康、符立佳、陈云领
YUNDUN盾眼实验室： 王晓旭、胡金涌、高力

美术设计

白山云科技： 张彪、王思琪

2019 年全球互联网安全态势报告