2019上半年
云安全
趋势报告

FREEBUF

腾讯安全

声明

本报告为 FreeBuf 与腾讯安全联合研究成果。报告中所涉及的数据来自网上公开数据，或采取合法技术手段、深度调查、抽样调查等方式获取。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。此外，报告中所涉及的人名均为化名。

本文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。

关于FreeBuf研究院

FreeBuf.COM是斗象科技旗下、国内领先的互联网安全新媒体，每日发布专业的安全资讯、技术剖析，分享国内外安全资源与行业洞见，是深受安全从业者与爱好者关注的信息安全网站与社区。FreeBuf研究院则集结了行业内经验丰富的安全专家和分析师，常年对信息安全技术、行业动态保持追踪，呈现有深度的安全行业现状和趋势分析。

关于腾讯安全

腾讯安全作为互联网安全领先品牌，致力于成为产业数字化升级进程中的安全战略官，依托20年多业务安全运营及黑灰产对抗经验，凭借行业顶尖安全专家、最完备安全大数据及AI技术积累，为企业从“情报-攻防-管理-规划”四维构建安全战略，并提供紧贴业务需要的安全最佳实践，守护政府及企业的数据、系统、业务安全，为产业数字化升级保驾护航。

关于报告

《2019上半年云安全趋势报告》基于**互联网**、**产业互联网**及相关领域在上云过程当中面临的**安全态势**、**风险趋势**、**应对力量**以及**监管状态**等进行了梳理，以期为行业提供阶段性的总结和建议，助力云上各方有策略的建立安全能力，更好应对安全风险。

CLOUD SECURITY

出品方

FreeBuf研究院：

谢忱、鲍弘捷、施东奇、许皓翔、金方成城

腾讯安全：

刘志高、王婷、谢灿、宋兵、喻峰、张祖优、李智鹏、

谭光西、郭佳楠、江慧敏、郭佳楠、周耀辉、王冠楠

美术设计：

姚媛

CONTENTS

目录

FOUR

重点威胁及攻击趋势分析
Key threats and attack trend analysis

FIVE

安全建议
Security advice

CHAPTER ONE

CHAPTER ONE

引言

引言

FREEBUF | 腾讯安全

第一章 引言

《2019年国务院政府工作报告》提出，新旧动能接续转换包括传统产业升级和新兴产业的规模化，将成为中国未来发展的重点目标之一。依托产业互联网构建新型的、产业级的数字形态，打通各产业间、内外部的连接，以新兴产业的技术提高传统产业效率、以传统产业的市场带动新兴产业规模，达到 1+1>2 的效果，从而能够支持动能转换更好更快地实现。

产业互联网以数据作为基础，综合运用互联网、移动互联网、物联网、大数据、云计算、人工智能等下一代信息技术，来促进传统产业转型升级，同时带动新兴产业发展。利用信息技术，传统产业的物理产品将嵌入越来越多的数字功能。这促进了硬件产品向软件化、服务化的方向发展，使得用户和企业都可以持续保持连接和交互，按使用购买服务的方式将广泛普及。

随着云计算等企业级技术应用的发展普及，产业互联网实际已经在各行各业展开实践。广度上不仅覆盖服务业、工业和农业，还从商业扩展到公益和政府，整个社会走向全面互联网；深度上，从营销服务、生产研发到运营管理，互联网渗透到组织内部的各个环节。数据信息由此实现从消费端到供给端的高效流通，数字产业与传统产业相互协同带动，助推中国经济迈向高质量发展阶段。

在新旧动能接续转换的过程中，传统产业的数字化升级和新兴产业的数字化能力建设，使当前的安全趋势发生了变化。《2019年上半年云安全趋势报告》基于互联网、产业互联网及相关领域在上云过程当中面临的安全态势、风险趋势、应对力量以及监管状态等进行了梳理，以期为行业提供阶段性的总结和建议，助力云上各方有策略的建立安全能力，更好应对安全风险。

CHAPTER TWO

CHAPTER TWO

2019上半年云安全概况

2019上半年云安全概况

FREEBUF | 腾讯安全

第二章 2019 上半年云安全概况

2.1 现状与趋势

2019年上半年，数字化转型的浪潮席卷全球，越来越多的企业开始应用云计算技术。云计算丰富的扩展性、便捷性逐步成为促进企业积极上云的驱动因素。在选择是否上云的过程中，安全是企业首要关注的问题，一方面，企业重视对自身数据在云端的安全性，另一方面，企业也担心自身业务的稳定性是否能够在云上得到保证。

2.1.1 云安全对企业的战略意义凸显

2019 年 3 月，Gartner 发布了 2019 年七大新兴安全和风险管理趋势。Gartner 指出，安全和风险管理对于企业的业务能力和成果具有战略意义，企业的安全投资正在从威胁防御向威胁检测转变。此外，随着云计算在各行各业的不断渗透，网络安全的人才缺口不断扩大，专业安全供应商的价值愈发受到重视，而云计算平台投资的主要方向也在向云安全能力方向迁移。

目前，国内的各大云平台厂商均推出或更新了自身的安全运营系产品，如态势感知、安全运营中心等，加强用户侧风险管理和运营。

2.1.2 AI等预测技术成为安全防护的重点

2019 年上半年的另一个明显变化就是云情报、机器学习等人工智能预测技术成为安全防护的重点。传统的安全架构中，较多依赖特征匹配的模式。在这种模式中，防护设备需要先将某个漏洞或攻击事件写入特征库，然后才能防御或检测该类攻击，而且安全特征库数量非常有限，在云环境中存在一定滞后性和局限性，防护方永远落后于攻击方，对 0day 等未知威胁无能为力。如今，网络安全界的潮流是转后手为先手，让安全变得更主动、更前置，主要的技术手段包括云安全情报和机器学习预测技术。

2.1.3 相关法律法规明确安全发展方向

密集出台的法律法规和标准，明确了几个安全发展方向，一是网络安全等级保护作为国家网络安全保障的基本制度、基本策略、基本方法，监管对象有了很大扩展，等级保护建设和测评成为安全合规的必经之路。二是保护作为“国家基础性战略资源”的数据，对重要数据和个人信息的数据安全和控制权等提出更高要求。加之等保2.0及密码法（征求意见稿）等法案的发布，进一步确保了核心数据资产保护及加密策略的有效应用。三是安全可信，可信计算已成为保卫我国网络安全战略的核心技术，从通信网络、区域边界、计算环境构建健康、安全、可信的网络体系。最后是国产密码技术，加密算法是安全的基础，国产密码技术将在关键基础行业加强推广力度。

2.2 危机预警情况

2019 年上半年，腾讯云官网累计发布高危预警 38 次，其中对云上用户影响面较广且危害极高的漏洞覆盖 Windows、Linux、Unix 等多个版本系统，同时也覆盖到了 Kubernetes、Docker、runC 等云相关容器及运行环境以及包含 Tomcat、ThinkPHP 等常用应用。

2.3 危害案例

2019 年 5 月 14 日，微软发布了高危安全漏洞 CVE-2019-0708 紧急通告，披露了其操作系统远程桌面服务（Remote Desktop Services）存在严重安全漏洞，攻击者在没有任何授权的情况下，可以直接远程攻击操作系统开放的3389服务，在受害主机上执行恶意攻击行为，包括安装后门，查看、篡改隐私数据，创建拥有完全用户权限的新账户，影响范围从Windows XP到Windows 2008 R2。腾讯安全云鼎实验室情报团队监测到来自暗网的RDP漏洞探测流量，正在为下一步的攻击收集相关情报。

2019年6月，腾讯云安全中心情报平台监测到 Linux TCP "SACK PANIC" 远程拒绝服务漏洞，攻击者可利用该漏洞构造并发送特定的SACK序列请求到目标服务器，导致服务器崩溃或拒绝服务。近十年的Linux内核版本包括Unix均在影响范围之内，由于本次的漏洞涉及内核处理TCP协议问题，影响面巨大。

除此之外，2019年上半年还出现了不少“明星漏洞”：

TOP TEN OF MAXIMUM IMPACT VULNERABILITY

2019上半年影响范围最大漏洞TOP 10

排名	上榜漏洞
01	Linux TCP "SACK PANIC" 远程拒绝服务漏洞（CVE-2019-11477,CVE-2019-11478,CVE-2019-11479）

上榜理由：

影响范围广：近10年的Linux内核均在受影响范围，涉及Redhat、CentOS、Debian、Ubuntu、FreeBSD等发行系统，涉及全球数百万主机。

02

Windows RDP 服务远程代码执行漏洞预警（CVE-2019-0708）

上榜理由：

危害大，影响面较广：企业操作系统方面虽然只影响Server 2003和Server 2008/2008R2操作系统，但漏洞可被远程直接控制，且漏洞一旦被利用，具备类似Wannacry的感染力，故排名第二。

03

Intel 处理器微体系架构数据采样 （MDS）漏洞风险预警

上榜理由：

影响面广，硬件漏洞：虽然属于信息泄露漏洞，危害较低，但由于是硬件类漏洞，总会引起行业高度关注，因为本身利用难度较高也开始逐步被大众遗忘。

04

Intel SPOILER 信息泄露漏洞

上榜理由：

影响面广，硬件漏洞：借 Spectre（“幽灵”）漏洞之势，再次进入大众视野，同上面的MDS漏洞，几乎所有现代英特尔处理器都存在该漏洞，但由于利用难度、修复复杂度等原因，最终也没有掀起大的波澜。

05

容器运行环境runC逃逸漏洞（CVE-2019-5736）

上榜理由：

容器界影响极广的漏洞：runc是一款广泛用于生成及运行容器的CLI工具，Kubernetes、Docker、containerd或者其他基于runC的容器技术在运行时层均存在漏洞，该漏洞允许恶意攻击者对主机系统进行root访问，被称为多年以来容器领域曝出的最为严重的问题。

06

Oracle WebLogic 组件远程代码执行漏洞预警（CVE-2019-2725，CVE-2019-2729）

上榜理由：

频繁而危险：可以说这五个字形容再贴切不过，属于比较危险（可导致远程代码执行）的漏洞，同时也是频繁出现的漏洞，历史上Weblogic的RCE不在少数，每次也是缝缝补补的。

07

Docker cp命令容器权限逃逸安全漏洞（CVE-2018-15664、CVE-2019-11246、CVE-2019-1002101）

上榜理由：

值得关注的容器漏洞：容器安全在2019年上半年开始被各行各业重点关注，尤其是这次的权限逃逸，让大家对容器安全开始更加重视，此次的漏洞影响虽然集中在本地，但容器的使用不当（如运行不信任的容易，在节点执行 docker cp），却也会放大该漏洞的危害。

08

ThinkPHP 多个版本远程代码执行漏洞（5.0、5.1、5.2等多个版本）

上榜理由：

频发RCE的CMS漏洞：由于ThinPHP在国内的广泛使用，导致ThinkPHP的每次漏洞爆发，都会引起较大关注，2019年伊始爆发的2次多个版本的RCE漏洞影响让很多人记忆犹新。

09

知名邮件代理程序 Exim 远程代码执行漏洞（CVE-2019-10149）

上榜理由：

看似危害很大实际国人体味不深的漏洞：该漏洞各大外媒报道受影响量达数百万主机，而国内讨论声寥寥，可说是“雷声大，雨点小的漏洞。

10

Ubuntu Snap本地提权漏洞（CVE-2019-7304

上榜理由：

小有威力的本地提权漏洞：大家理解的本地提权可能影响有限，但由于默认安装到了Ubuntu18.04，且漏洞PoC很快公布，在一小段时间里却也引起了大家较大关注。

CHAPTER THREE

CHAPTER THREE

云安全黑灰产新变化

云安全黑灰产新变化

FREEBUF | 腾讯安全

第三章 云安全黑灰产新变化

随着云计算越来越便捷高效，大量企业逐渐把业务迁移到云上。但基于同样的原因，恶意程序也在向云上转移。当黑灰产利用云资源发起各种恶意行为时，往往导致云厂商为其“背锅”。因此，如何加强情报和分析能力，及时识别云上的恶意用户和恶意主机，将是云安全领域一项长期的较量。

3.1 黑灰产借力云 AI 化

近几年，由于深度学习技术的突破性发展， AI 逐步开始替代许多劳动密集型工作，而这些技术，黑灰产也在积极跟进。通过分析发现，黑灰产通过租用云端 GPU 训练恶意模型也在逐渐增多，例如通过 DeepFake 生成换脸色情视频、训练验证码自动识别引擎、更加拟人化的自动化攻击技术等。可以预见，未来一到两年安全领域从业者将不得不面临如何和 AI 斗智斗勇的问题。

3.2 漏洞曝光和利用周期变短

互联网存在大量已知漏洞，但被黑客利用的仅仅是其中一小部分。腾讯安全监测显示，由于黑客基础设施的完善，针对新漏洞的探测和利用尝试周期正在逐渐变短。过去针对新漏洞的大规模扫描需要过几天才会出现，而现在往往在新漏洞被发现的第一时间，就会爆发大量的扫描行为。由于这个时间的缩短，导致企业的开发和安全运维人员几乎无法在合理的短时间内完成打补丁操作来应对安全威胁。

3.3 黑产犯罪国际化趋势明显

东南亚菲律宾、越南、柬埔寨等地逐渐成为赌博、诈骗类犯罪的温床，例如今年非常火爆的“东南亚杀猪盘”诈骗类型，以情感欺诈为切入口，再利用云上的博彩、交易平台等形式，诱骗对方充值。甚至出现一个网站只针对一个被骗对象的情形，一旦对方被骗，直接网站销毁。对云服务商来说，如何监管并减少用户在线运营非法业务，也是一场持久战。

3.4 针对性勒索增多

自从2017年“永恒之蓝”漏洞曝光，勒索软件经历了2年的黄金时期，许多企业的云上服务都遭遇了勒索。从2019年来看，除了广撒网式的勒索之外，针对性勒索逐渐增多。黑客通过人工主动渗透确认高价值服务器后，加密数据并勒索高额赎金。针对性勒索大大降低了黑客程序曝光的概率，未来可能占比更大。

CHAPTER FOUR

CHAPTER FOUR

重点威胁及攻击趋势分析

重点威胁及攻击趋势分析

FREEBUF | 腾讯安全

第四章 重点威胁及攻击趋势分析

4.1 云主机类

随着云计算、大数据等技术高速发展，企业业务不断上云，以数据为载体的数字资产已逐渐成为企业核心资产。同时，黑客将通过多种恶意攻击手段，有针对性的对云主机进行攻击，一旦入侵成功并窃取核心资产，将给企业带来巨大损失。因此，面对日益严峻的网络安全形势，企业需要建立强大的安全防御体系，不断增强对恶意攻击的对抗能力。

4.1.1 云主机安全意识概况

随着云计算的发展，云的应用越来越广泛。对于企业来说，云主机则是一项非常重要的主机设备。

云主机是基于云计算发展的产物，因此，除了会受到传统的主机安全威胁以外，潜藏在云中的风险也时刻威胁着云主机的安全。云主机安全至关重要，但这也并不代表其本身的安全性不值得信赖。

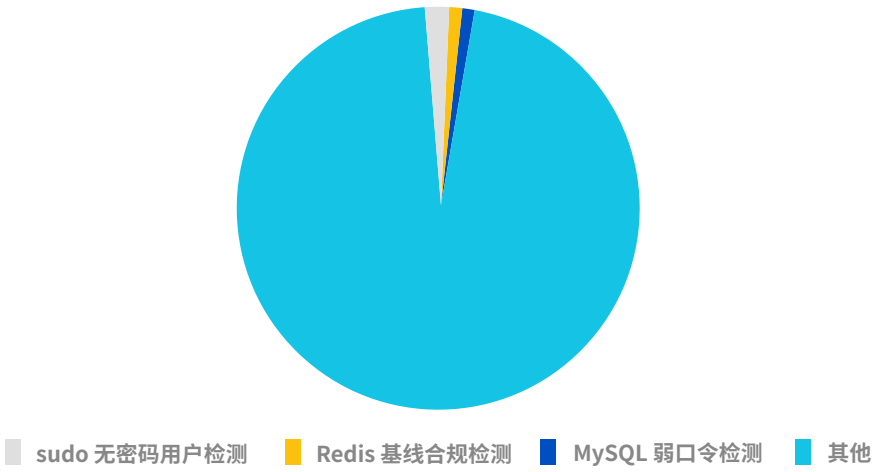
系统本身的脆弱性以及网络世界中充斥的大量木马、后门、恶意程序等问题，使得云主机时刻遭受着来自内外的双方安全压力，这也是对于其本身防护能力的重大考验。

1）弱密码及未授权访问情况

一直以来，弱密码就是系统安全的最大内部威胁，每次都年度弱密码排行中，诸如“123456”、“password”这样的密码组合也都未曾缺席。屡禁不止的情况下，这些脆弱的主机就犹如案板上的鱼肉一般，任人宰割。

在本次统计中，弱密码及未授权访问主要存在于以下几个方面：sudo无密码用户检测、Redis未授权访问、MySQL弱口令等。

截止到2019上半年，以上三种漏洞影响机器占到云服务器总数比例：



近年来，由于部分安全厂商已经开始从购买服务起就向用户传递加强密码的设置，所以弱密码在云上影响机器的比例是非常小的。

4.1.2 云主机漏洞概况

漏洞入侵是攻击者最喜欢使用也是出现频次最高的一项攻击手段。不同威胁级别的漏洞所造成的危害也有所不同。使用正确的漏洞利用代码，只需很短的时间即可获得服务器比较高的权限，甚至是完全的控制权。

如今，很多安全厂商对服务器漏洞的关注度明显提升，并着手自主研发漏洞检测引擎。无论是系统漏洞、应用漏洞都能够进行及时、准确的检测，并提示用户尽早修复漏洞。

1）漏洞总数及类型

VULNERABILITY & BASELINE RISK RATIO

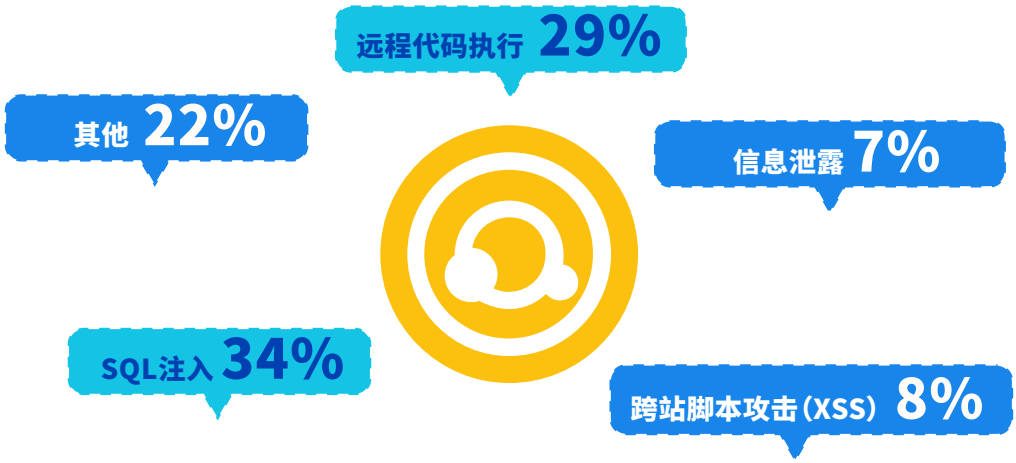
漏洞&基线风险占比

在对2019年上半年的漏洞检测脚本中，平均每月检测漏洞&安全基线数量14.8万个，以漏洞对服务器哪部分影响进行分类，其中安全基线占比59%，系统组件漏洞占比22%，Web应用漏洞占比19%。

VULNERABILITY TYPE RATIO

2019上半年漏洞类型占比

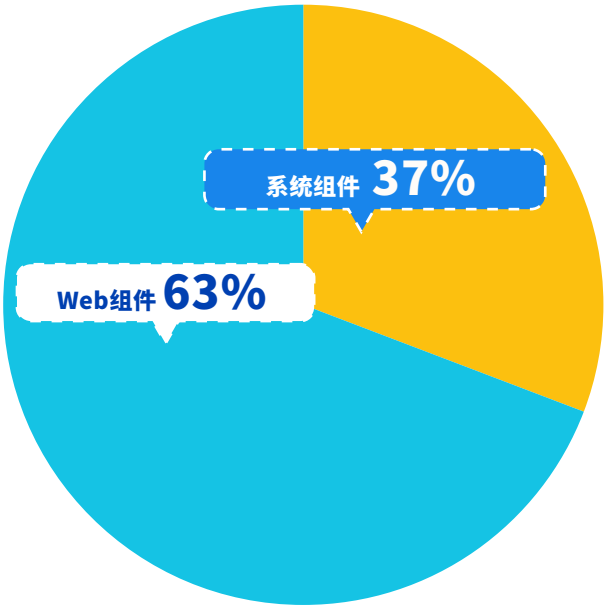
而根据漏洞类型区分，最常见的为SQL注入、远程代码执行、XSS以及信息泄露等，其中SQL注入漏洞占比高达34%，其次为远程代码执行漏洞占29%。



COMPONENT TYPE RATIO

2019上半年组件类型比例

识别组件分为两类，一类是系统组件，一类是web组件。比例如下：

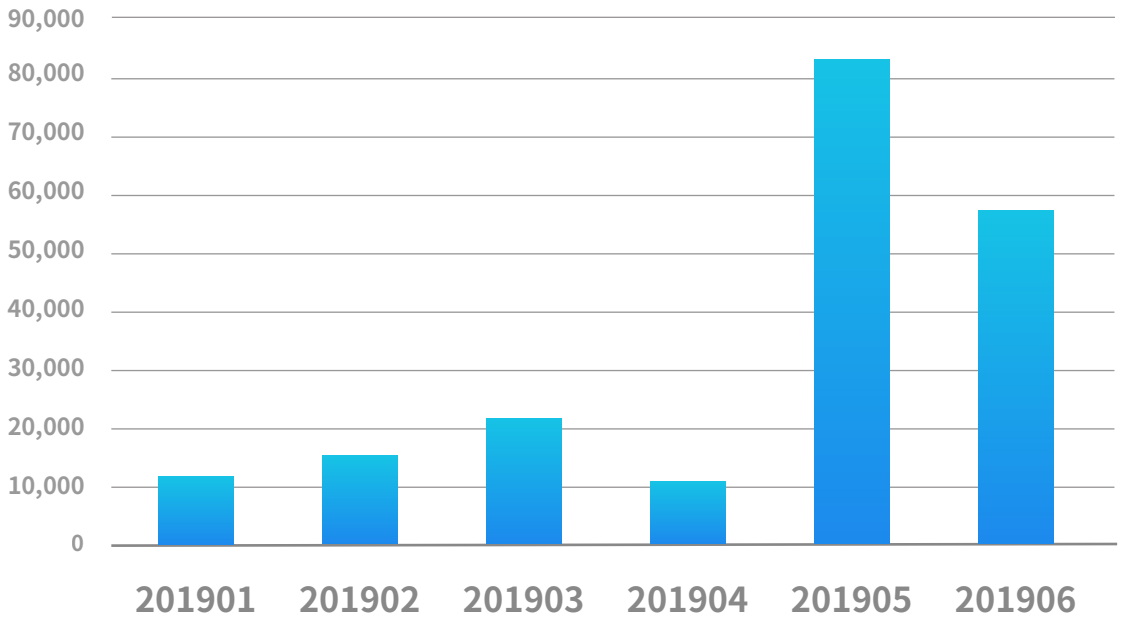


2）漏洞对用户的影响

一般来说，主机/服务器的漏洞，往往都会造成一定程度的损失。随着当下网络攻击的针对性愈加明显，漏洞带来的威胁甚至可致上亿用户的数据资料丢失。对于安全工作者/安全厂商来说，漏洞监测与防护就成了日常工作中的重中之重。

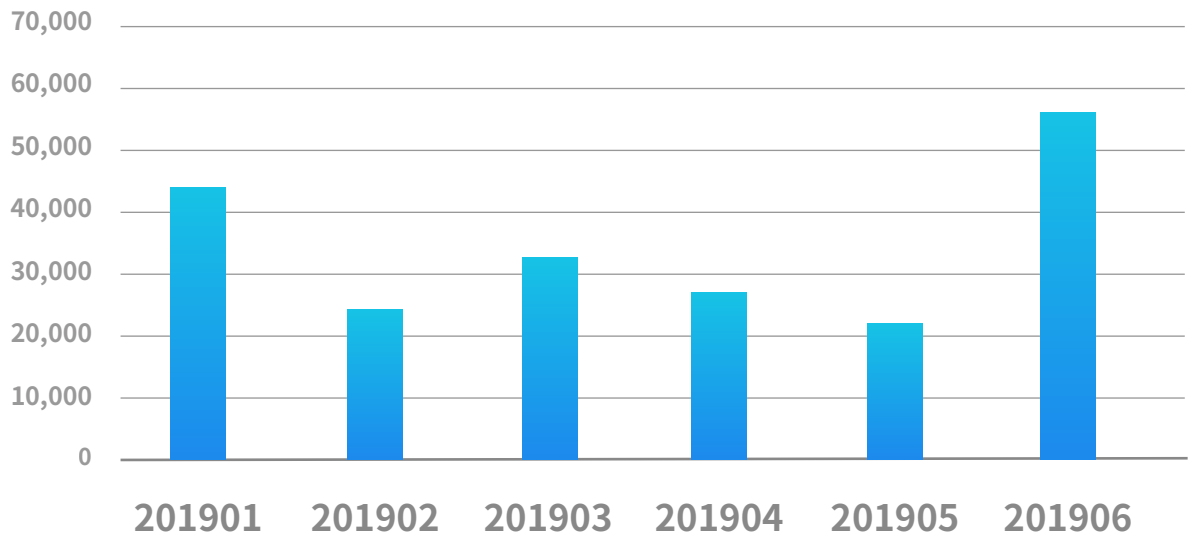
漏洞数量

2019上半年，系统组件漏洞数月度统计如下：



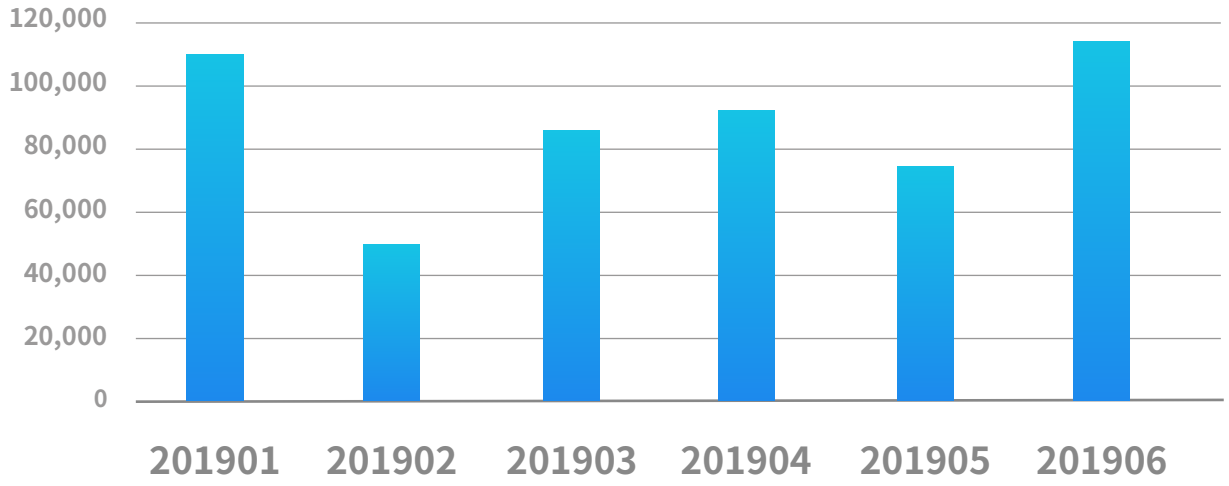
系统组件漏洞在2019年5月有一个小爆发，原因是5月披露的Windows远程桌面服务代码执行漏洞（CVE-2019-0708），几乎所有的Windows服务器都受到影响。之后随着漏洞的修复，漏洞数有所下降，但在系统组件漏洞中仍然拥有较大占比。

2019上半年，Web应用漏洞数月度统计如下：



Web应用漏洞变化趋势较为平缓，其中，6月份的增长主要是Web目录信息泄露漏洞影响。

2019上半年，安全基线漏洞数月度统计如下：



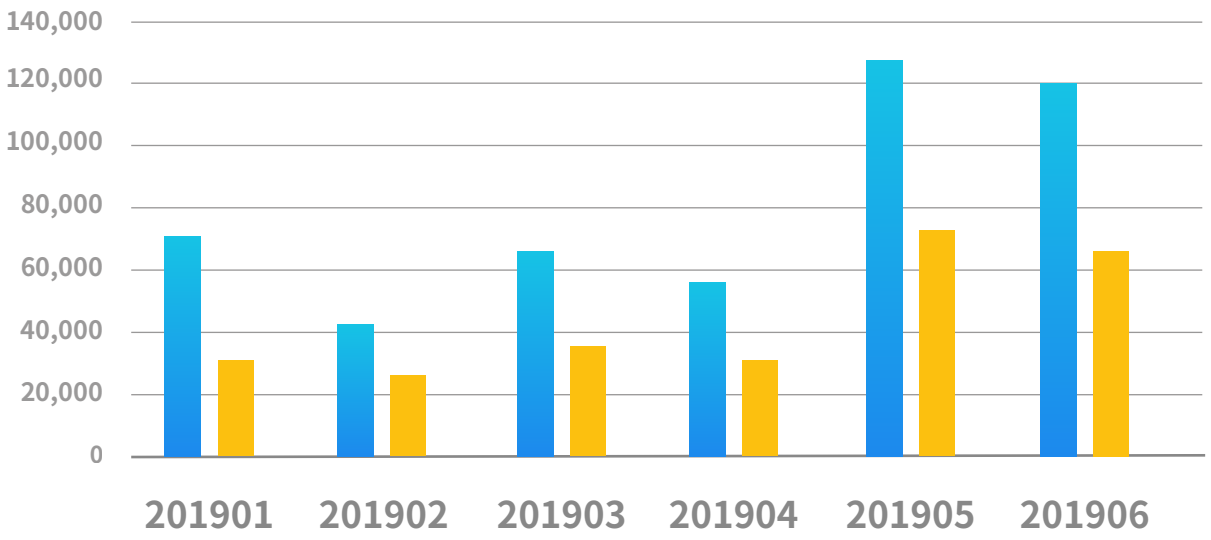
可以看出，安全基线漏洞变化趋势与Web应用漏洞变化趋势类似。

漏洞影响：

2019上半年，漏洞影响机器及用户数的月度统计如下：

VULNERABILITY IMPACT STATISTICS

2019上半年漏洞影响统计



由上图可以看出，5月份 Windows 远程桌面服务代码执行漏洞（CVE-2019-0708）影响确实比较大，使得漏洞影响机器数及用户增长了几乎一倍。

3）2019年高影响漏洞情况介绍：

CVE-2019-2725

Oracle WebLogic wls9-async组件存在反序列化远程命令执行漏洞

披露时间 2019-04-17

漏洞类型 远程代码执行

漏洞描述

部分版本WebLogic中默认包含的wls9_async_response包，为WebLogic Server提供异步通讯服务。由于该WAR包在反序列化处理输入信息时存在缺陷，攻击者可以发送精心构造的恶意HTTP 请求，获得目标服务器的权限，在未授权的情况下远程执行命令。

修复方案

官方已于4月26日公布紧急补丁包，下载地址如下：
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html?from=timeline

2019年高影响漏洞情况介绍：

2019年上半年，可以说是主机威胁集中爆发的时段，不论是Windows还是Linux均受到影响。

2019年上半年重要漏洞举例：

CVE-2019-0708

Windows 远程桌面服务代码执行漏洞

披露时间 2019-05-15

漏洞类型 远程代码执行

漏洞描述

微软近日更新修复了远程桌面服务上存在的一个严重远程代码执行漏洞（CVE-2019-0708），该漏洞无需用户交互即可被远程利用，具有一定的蠕虫传播性质，被利用可导致批量主机受影响。

修复方案

官方已发布安全更新修复该漏洞，你可以通过如下链接进行下载：
Windows 7 及Server 2008/Server 2008 R2 用户: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
Windows XP 及Server 2003 用户: https://support.microsoft-.com/zh-cn/help/4500705/customer-guidance-for-cve-2019-0708dance-for-cve-2019-0708dance-for-cve-2019-0708

CVE-2019-11477

Linux 内核中TCP SACK机制远程Dos预警分析

披露时间 2019-06-18

漏洞类型 拒绝服务

漏洞描述

RedHat官网发布报告，安全研究人员在Linux内核处理TCP SACK数据包模块中发现三个漏洞，其中CVE-2019-11477漏洞可能被远程攻击者用于拒绝服务攻击，影响程度严重。

修复方案

更新补丁
https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001/PATCH_net_1_4.patch

4.1.3 云主机暴力破解概况

顾名思义，暴力破解就是攻击者通过使用自己的密码字典对攻击目标的账户进行枚举并尝试登录。理论上来说，只要字典足够庞大，暴力破解就能成功。随着互联网世界中的数据量不断增加，数据泄露的事件也越来越频繁，攻击者的“字典”得到了持续扩充。因此，暴力破解这类攻击方式一直以来深受黑客们的青睐。

1）攻击概况

从2019上半年暴力破解攻击的监测情况来看，1月到6月间，爆破攻击的来源IP在不断增加，同时对爆破攻击事件的防御次数也呈现缓慢上涨的形势。平均每月对暴力破解攻击的IP检测高达100万个，同时每月还要抵御超过5.3亿次攻击。尤其是在今年2月份，最少的攻击来源却有最多的防御次数。也就是说，整个2019年上半年，暴力破解攻击事件有愈演愈烈的趋势。

2）攻击来源及目标

	地域	攻击IP TOP10	攻击次数
01	瑞典斯德哥尔摩	193.***.***.96	60255196次
02	中国河南郑州	111.*.***.239	47034740次
03	中国江苏南京	36.***.*.246	40950970次
04	乌克兰文尼察	193.***.***.12	32300986次
05	瑞典斯德哥尔摩	185.***.***.25	22621568次
06	中国福建福州	112.**.**.228	17366268次
07	瑞典斯德哥尔摩	193.***.***.97	13274824次
08	乌克兰文尼察	193.***.***.158	12521799次
09	中国江苏南京	111.**.**.186	12305453次
10	法国巴黎	212.**.***.101	11737387次

经过对攻击IP的来源分析我们可以发现，境外的攻击大多来自欧洲，其中以瑞典、乌克兰等地区居多，这与世界范围内黑客活跃程度有一定的关联。在国内，郑州、南京、福州等多个地区上榜。值得关注的是，排名靠前的多个攻击源都不是来自互联网最发达的一线城市。

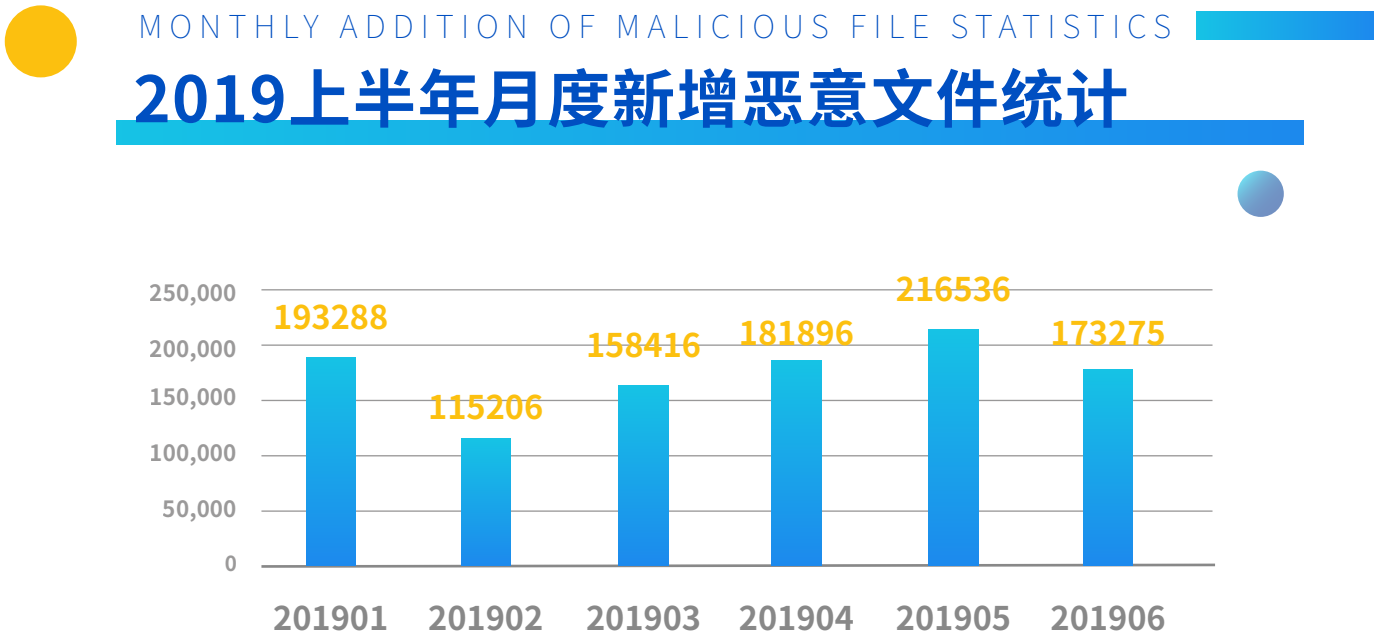
4.1.4 恶意文件入侵

恶意文件（即恶意软件）的由来已久，种类繁多且使用范围庞大。历史上不乏WannaCry、VPNFilter等“重量级”选手。恶意文件入侵以低成本、高效率而闻名，常见有勒索软件、木马病毒、挖矿软件等形式，并伴随以网络钓鱼的方式出现。目标小可至单一用户，大可至整个国家，至今仍然没有完善的解决方案。

1）恶意文件总览

2019年上半年，通过抽样百万云主机，监控新增文件172,375,762个，其中恶意文件1,038,617个，占新增文件的0.6%。

对于新增恶意文件分月度统计，新增恶意文件数月均约17.3万个，如下图所示：

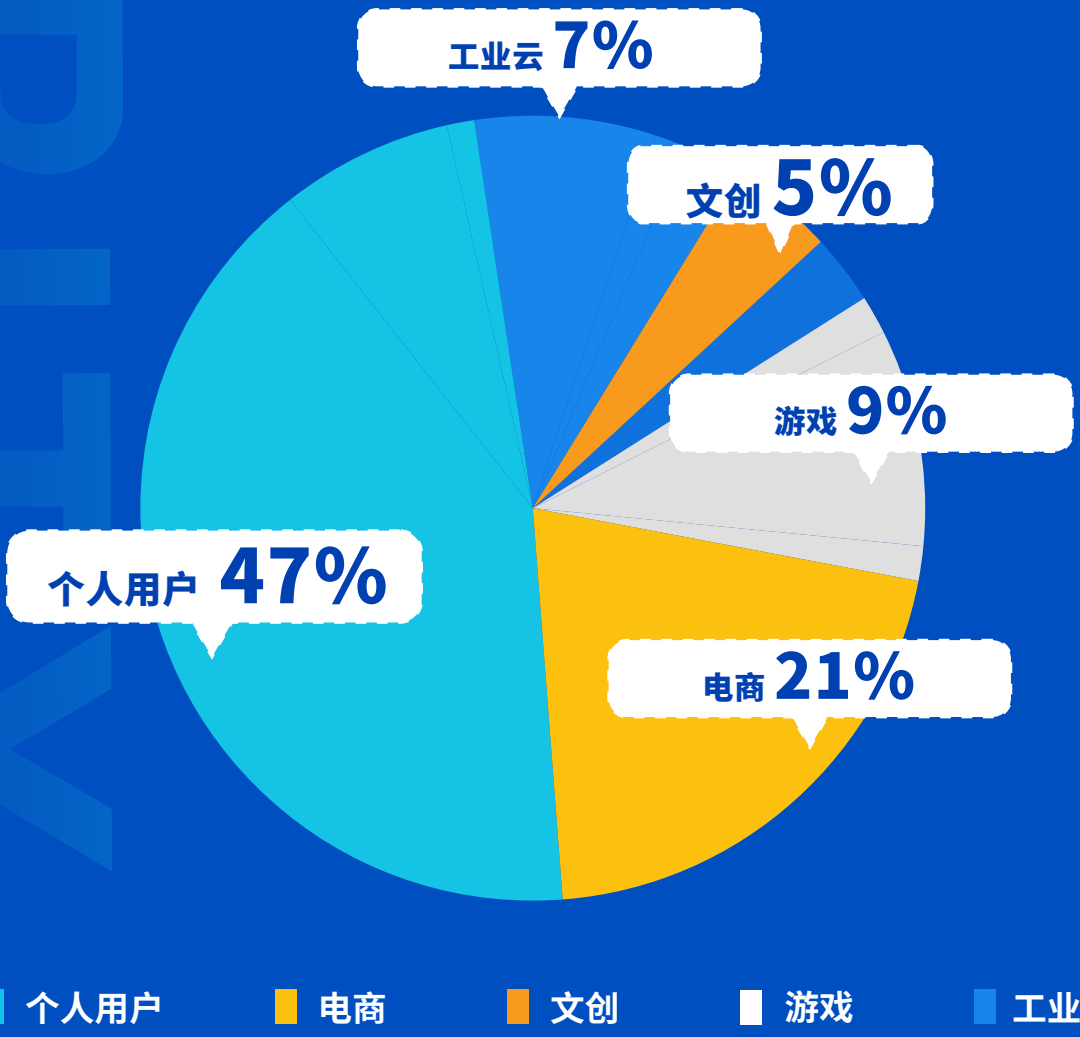


用户行业分布

恶意文件攻击的用户行业分布，个人用户占比最大，其次是电商行业、游戏行业、工业云。个人用户相对企业用户在处理安全风险时，响应速度相对较慢，安全意识还需要加强。总体来看，在有安装云镜主机安全产品的主机上，恶意文件攻击目前处于一个压制状态。

TROJAN HORSE INFECTION INDUSTRY PROPOTION

木马感染行业占比



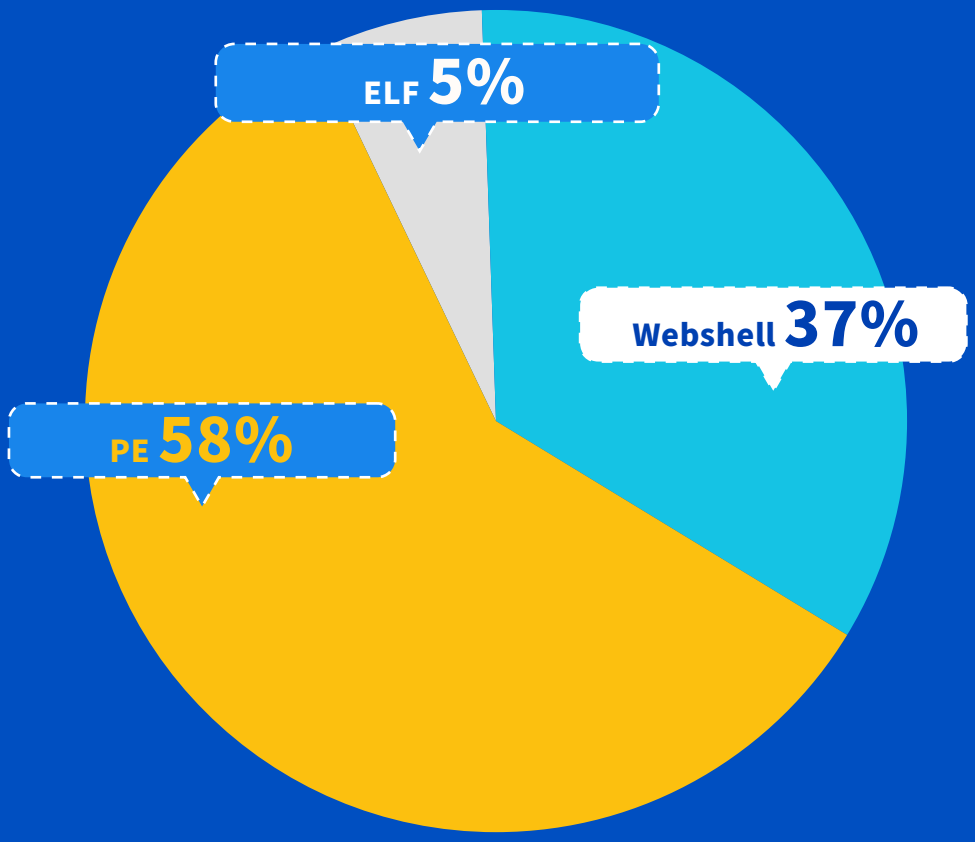
恶意文件攻击的用户行业分布：个人用户占比最大，其次是电商行业、游戏行业、工业云。

恶意文件类型分布

恶意文件主要分为三大类，分别是恶意脚本文件Webshell，基于Windows操作系统的二进制执行程序（PE），基于Linux操作系统的二进制执行程序（ELF）。三类恶意文件的占比PE最多，占到58%，Webshell第二，占37%，ELF仅占5%。如下图所示：

INCREASED PERCENTAGE of MALICIOUS FILE TYPES

2019上半年新增恶意文件类型占比



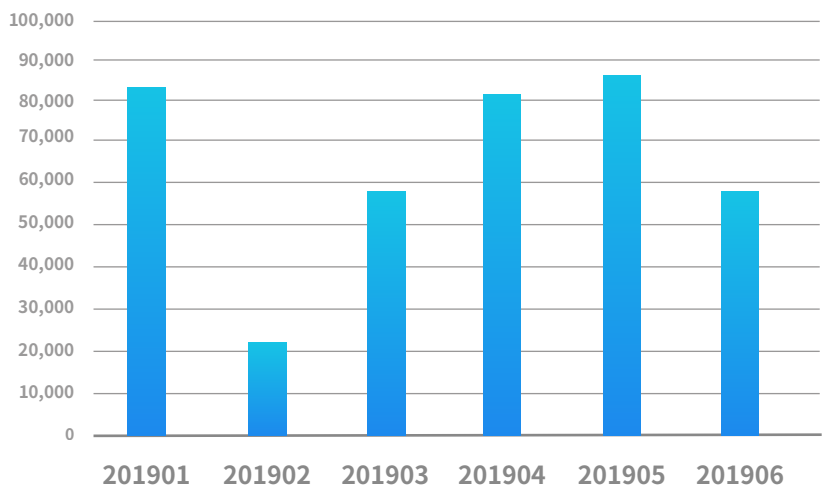
通过上图可以发现，云上新增Windows的恶意文件仍然是最多的，部分全网比较流行的恶意文件在云上也比较流行，其中包括Windows平台上感染型病毒，其主要来源用户安装的第三方程序。而Webshell恶意文件占比也非常高，对于服务器攻击，Webshell恶意文化仍然是最为流行的手段。黑客主要通过各种注入方式（如日志注入）上传Webshell恶意文件。云上Linux的恶意文件虽然占比不高，但仍然需要高度关注。

2）恶意脚本文件（Webshell）

Webshell作为完全控制服务器的“跳板”，是黑客攻击服务器的最主要手段。2019上半年，监控发现新增脚本文件96,170,166个，其中恶意脚本文件386,120个，占新增脚本文件的0.40%，占总恶意文件约37%。

MALICIOUS SCRIPT SAMPLE TREND

2019年上半年恶意脚本样本趋势

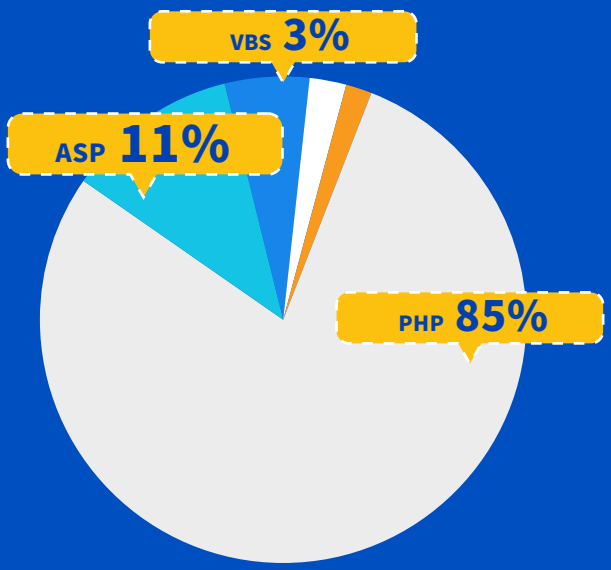


2019上半年恶意脚本文件感染事件月度统计可以看出，上半年3月到5月是攻击高峰时期，进入6月有一个显著的下降。

针对不同类型的服务程序，黑客（组织）开发出不同类型的恶意脚本文件，除了传统的PHP、ASP、JSP之外，还有诸如VBS、JS、PYTHON、SHELL、BATCH、PS1等。

MALICIOUS SCRIPT FILE TYPE RATIO

2019上半年恶意脚本文件类型占比



对云主机攻击最主要的恶意脚本文件类型是PHP，占到所有恶意脚本文件的84.63%。第二位是ASP，占10.69%。VBS的占比达到3.09%，排名第三。

2019上半年感染量排名前20的脚本恶意文件类型列表如下：

Script.PHP.Small.bx	Script.ASP.GetHtml.bya	Script.Asp.Webshell.cc	Script.Php.Ramnitinfected.ba
Script.Php.Downloader.ac	Script.PHP.PackGen.xz	Script.JS.Staser.apz	Script.Php.Small.bbk
Script.VB.Ramint.a	Script.VBS.Ramnitinfected.ba	Script.Php.Downloader.aa	Script.Php.Small.bc
Script.Php.Small.bt	Script.vbs.zuimihu.ba	Script.Vbs.Downloader.c	Script.Php.Small.bx
Script.Php.Small.bbe	Script.Php.Small.bb	Script.asp.small.bp	Script.PHP.GetEcho.ca

可以看到，排名前20的主要是三类恶意脚本文件：一类是一句话木马；一类是常规的Webshell；需要注意的是第三类被感染脚本文件（Ramnit）。被感染脚本会在客户端浏览器上下载生成一个二进制（Windows）恶意文件，此文件会搜索感染机器上其它的脚本文件，插入感染的脚本程序实现无限感染。

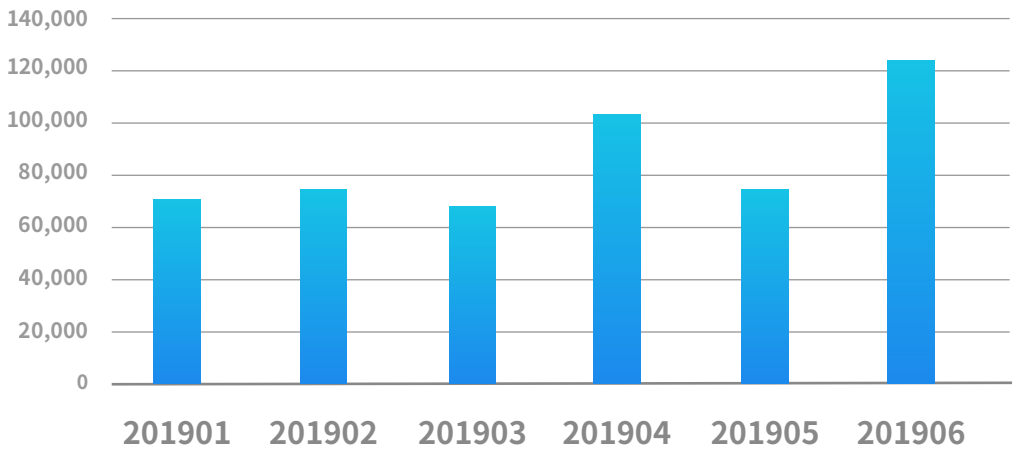
3）恶意二进制文件（木马病毒）

恶意二进制文件是攻击者获取利益的直接手段。2019上半年，云镜监控腾讯云上新增二进制文件76,205,596个，其中恶意二进制文件652,497个，占新增恶意二进制文件的0.86%，占总恶意文件约63%。

目前主流的服务器平台分为Linux及Windows，所以恶意二进制文件的统计分析分为两部分。在Linux平台上运行的二进制文件使用ELF格式，在Windows平台上运行的二进制文件使用PE格式。

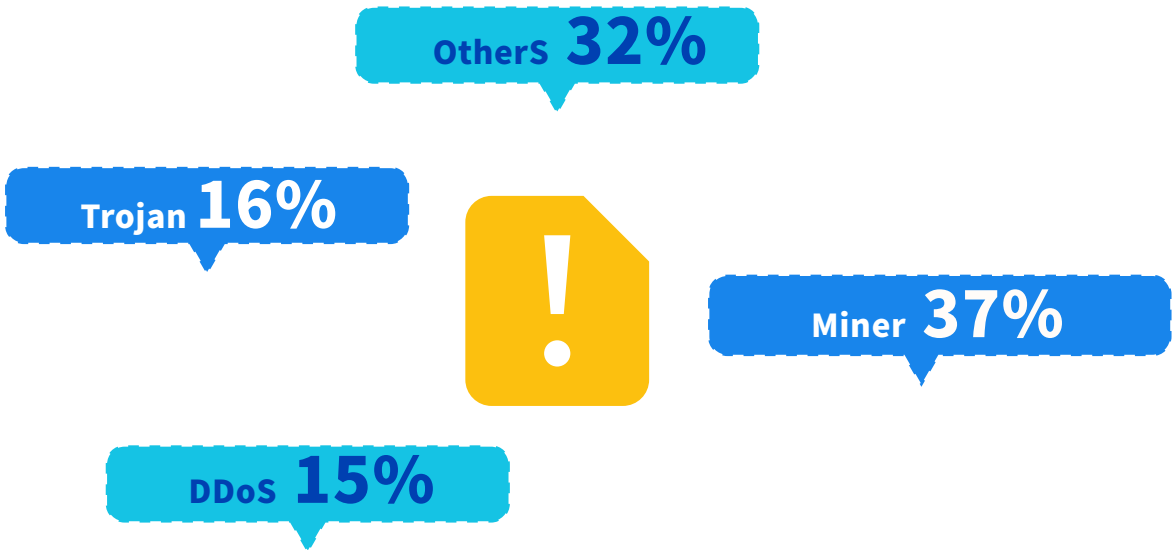
Linux平台

2019上半年，Linux平台上恶意二进制文件（ELF）新增50,137，占新增恶意二进制文件的7.68%，相对来说，Linux平台上恶意二进制文件较少。



PROPOTION OF INFECTED MALICIOUS BINARY FILE TYPES

2019上半年感染恶意二进制文件(ELF)类型比例



从感染所占比例来看，挖矿及DDoS攻击的恶意二进制文件已经占到攻击的50%以上，需要重点关注这两类恶意二进制文件（攻击方式）。

2019上半年，感染量影响机器排名前20恶意二进制文件（ELF）类型排名如下：

Elf.Trojan.Agent.fu	Elf32.Trojan.BillGates.da	Elf.Backdoor.Ssh.a	Elf.Backdoor.Agent.ca
Elf.Trojan.Agent.gr	Elf32.Trojan.Setag.da	Elf32.RiskTool.CoinMiner.n	Elf64.RiskTool.CoinMiner.n
Elf.Rootkit.Processhider.b	Elf.Backdoor.Mayday.g	Elf.virus.Xorddos.pgm	Script.Php.Small.bc
Elf.virus.SSHBrute.ugx	Elf.Rootkit.Processhider.a	Elf32.Trojan.Miner.c	Elf32.Trojan.Mrblack.da
Elf.riskware.Portscan.jhm	Elf32.Trojan.Mrblack.dd	Elf.HackTool.PNScan.a	Elf64.Hacktool.Expscan.c

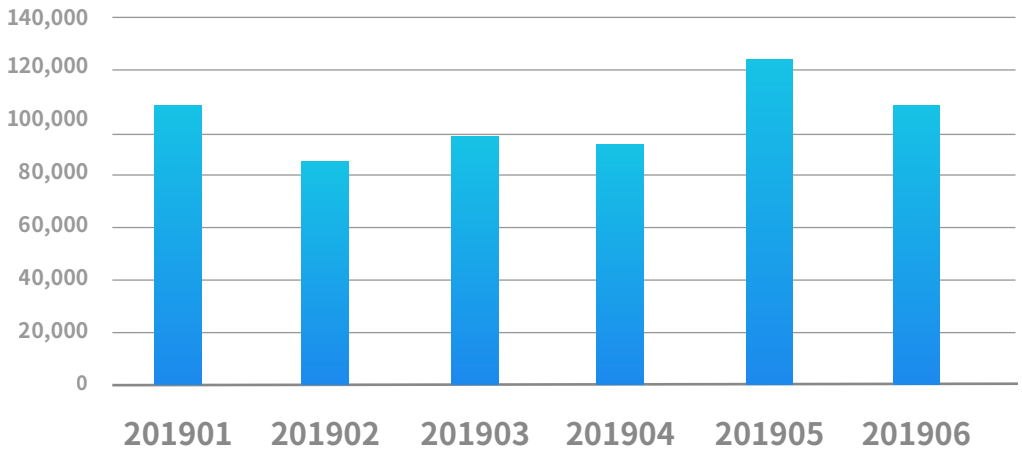
可以看到，对云上linux服务器主要构成威胁的为2大类，一类是传统的木马，另一类的挖矿木马。越来越多的攻击者攻击服务器以占用CPU挖矿获取利益，攻击者比较偏爱门罗币。

Windows平台

2019上半年，Windows 平台上恶意二进制文件（PE）新增602,360个，占新增恶意二进制文件的92.32%。

ADDED MONTHLY STATISTICTS FOR MALICIOUS BINARY FILES

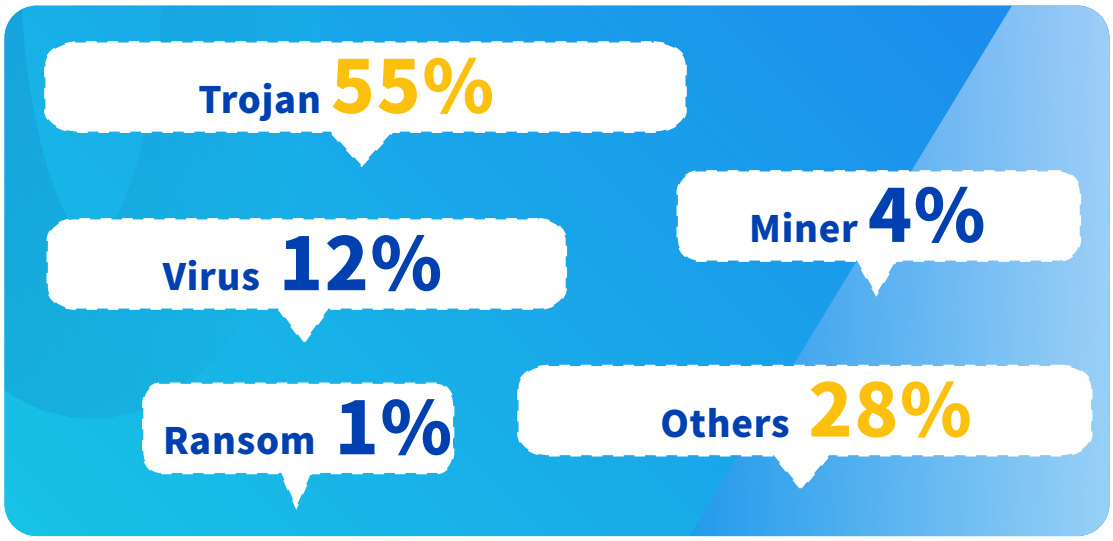
2019上半年新增恶意二进制文件（PE）月度统计



通过上图可以看到，新增恶意二进制文件（PE）维持在10万上下波动。此量级是恶意二进制文件（ELF）约10倍，Windows服务器受到攻击形势严峻。

MALICOUS BINARY FILE TYPE RATIO

2019上半年恶意二进制文件（PE）类型比例



Windows平台传统木马及感染型病毒占到恶意PE的67%，挖矿及勒索类型的恶意PE也越来越流行起来，尤其是勒索类恶意二进制文件，虽然占比很少，但是对用户核心数据破坏和进行勒索，影响非常恶劣。

2019上半年，感染量影响机器排名前20恶意二进制文件（PE）类型排名如下：

Win32.Virus.Ramnit.cb	Win32.trojan.XPACK.xg	Win32.Downloader.Miner.m	Win32.Virus.Ramnit.a
Win32.trojan.Black.xg	Win32.Trojan.Generic.dicv	Win32.Trojan.Generic.osar	Win32.Trojan.Generic.rydz
Win32.Trojan.Generic.zuxj	Win32.Trojan.Generic.upzt	Win32.virus.Sality.at	Win32.Trojan.Generic.ybtr
Win32.Trojan.Generic.eiqy	Win32.trojan.Agent.lyg	Virus.Win32.Ramnit.efg	Win32.Trojan.Generic.nlbp
Win32.Virus.Ramnit.ca	Win32.Trojan.Generic.xzqj	Win32.Trojan.Wanna.mhea	Win32.trojan.Dropper.xg

通过以上排名，可以看出影响比较大的有四类：

1、感染型病毒：既感染网页也感染PE文件；

2、传统木马：主要用于远控服务器，并具有较强的隐蔽性和对抗性；

3、挖矿木马：主要用于挖矿，资源消耗严重；

4、勒索病毒：将磁盘上的数据进行加密勒索用户。

举例：

Linux watchdogs 感染性隐藏挖矿病毒入侵

危害：

1、占用CPU进行挖矿，导致服务器运行缓慢；

2、被感染服务器会进一步攻击其它服务器；

3、此类木马有一定的对抗性，检测及清理步骤较复杂，清理干净较复杂；

入侵流程：

1、通过Redis未授权访问漏洞入侵机器并修改crontab任务；或者通过遍历known_hosts中的连接历史进行横向扩展；

2、crontab任务执行bash脚本，进行相关清理和下载执行恶意程序watchdogs并横向扩展：

a. 覆写crontab任务；

b. 清理其他挖矿程序；

c. 解锁删除相关系统文件；

d. 下载执行watchdogs；

e. 横向扫描其他机器；

f. 清理相关文件和痕迹。

3、watchdogs执行实现写开机启动、服务项并释放动态链接库实现隐藏，同时释放执行挖矿程序：

a. 获取进程ID写/tmp/.lsdpid；
b. 将/tmp目录下的watchdogs复制到/usr/sbin/目录并加入开机启动项和服务项；
c. 释放libioset.so并写入/etc/ld.so.preload实现进程等隐藏；
d. 访问ident.me获取机器外网IP；
e. 再次覆写crontab任务；
f. 释放挖矿程序ksoftirqds和配置文件config.json并执行；
g. 删除相关生成的文件并检查更新。

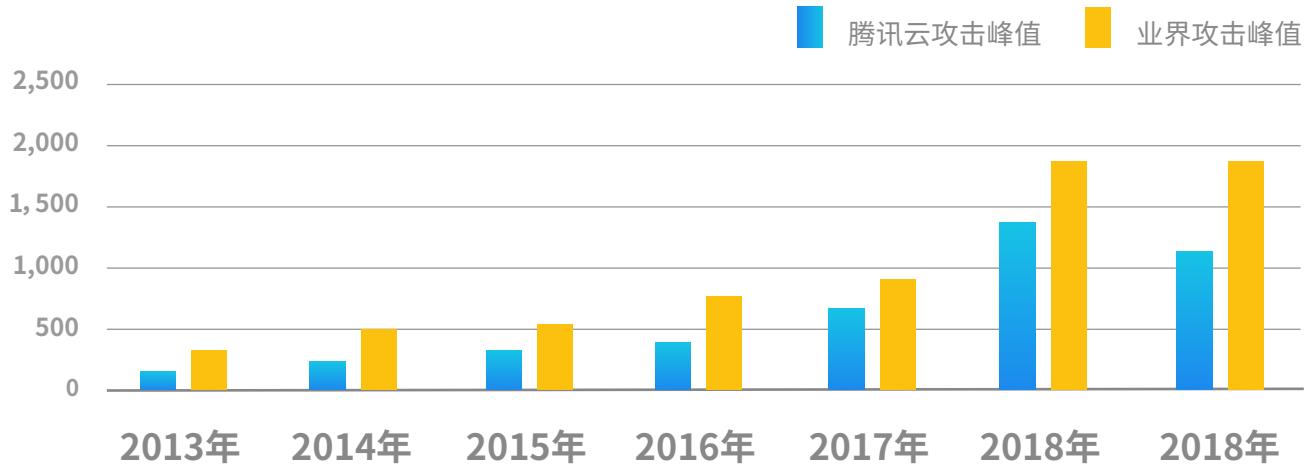
综上，恶意二进制文件对服务器的影响大，破坏性也更强，而且其本身又是服务器被攻破的标志，需要用户高度关注。

4.2 DDoS

4.2.1 DDoS攻击趋势

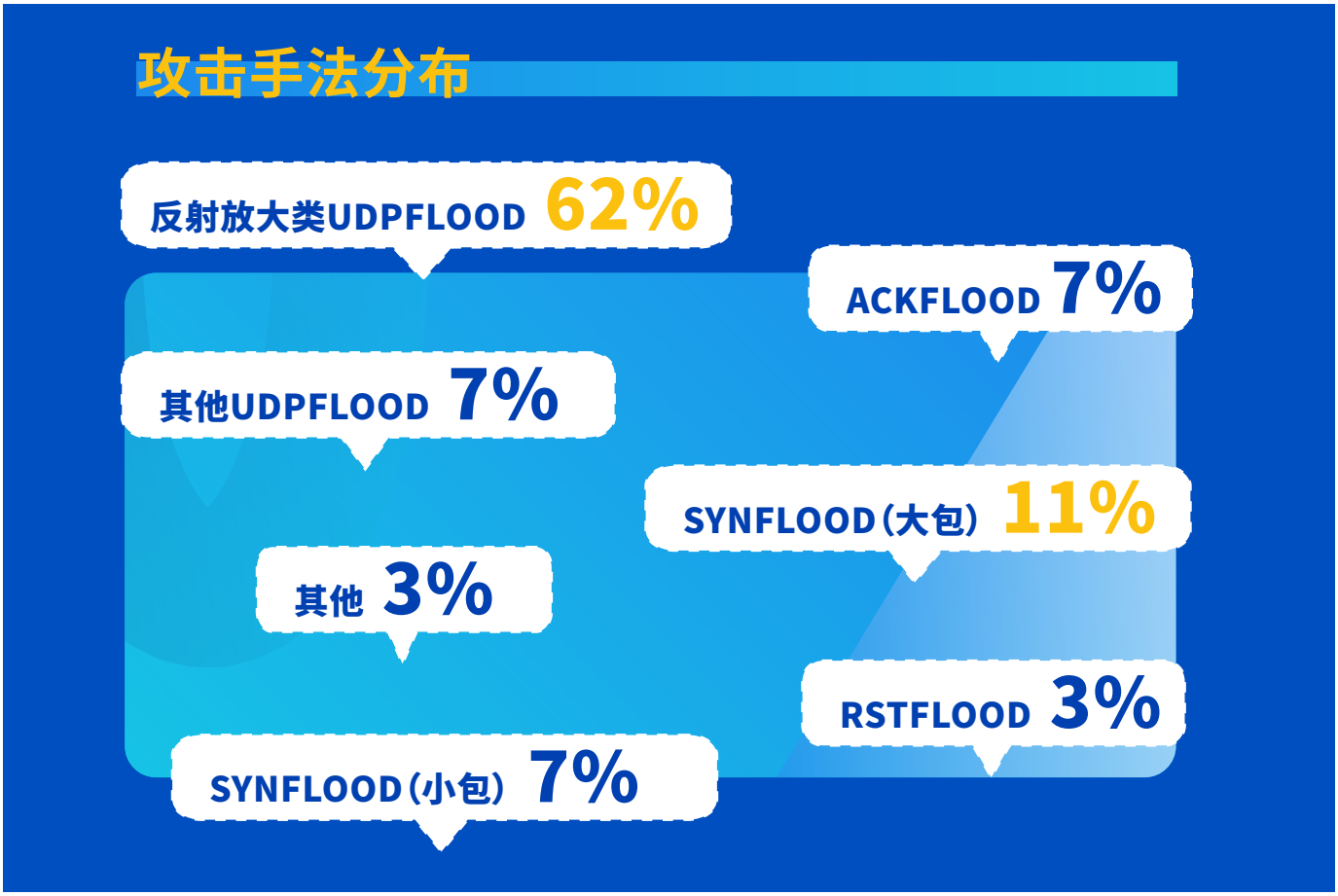
2019年上半年，随着云计算行业的快速增长，云上客户遭受DDoS攻击呈现次数多、强度高、手法新、来源广等特点。相比2018年，2019上半年DDoS攻击次数持续增多，并在2019年6月迎来一波爆发式增长。除此之外，TB级攻击也愈发屡见不鲜。从2013年至今统计结果来看，自去年上半年一起Memcached DDoS攻击，峰值1.7 Tbps创造攻击流量峰值记录以来，近两年的攻击达到了前所未有的强度。

攻击峰值走势

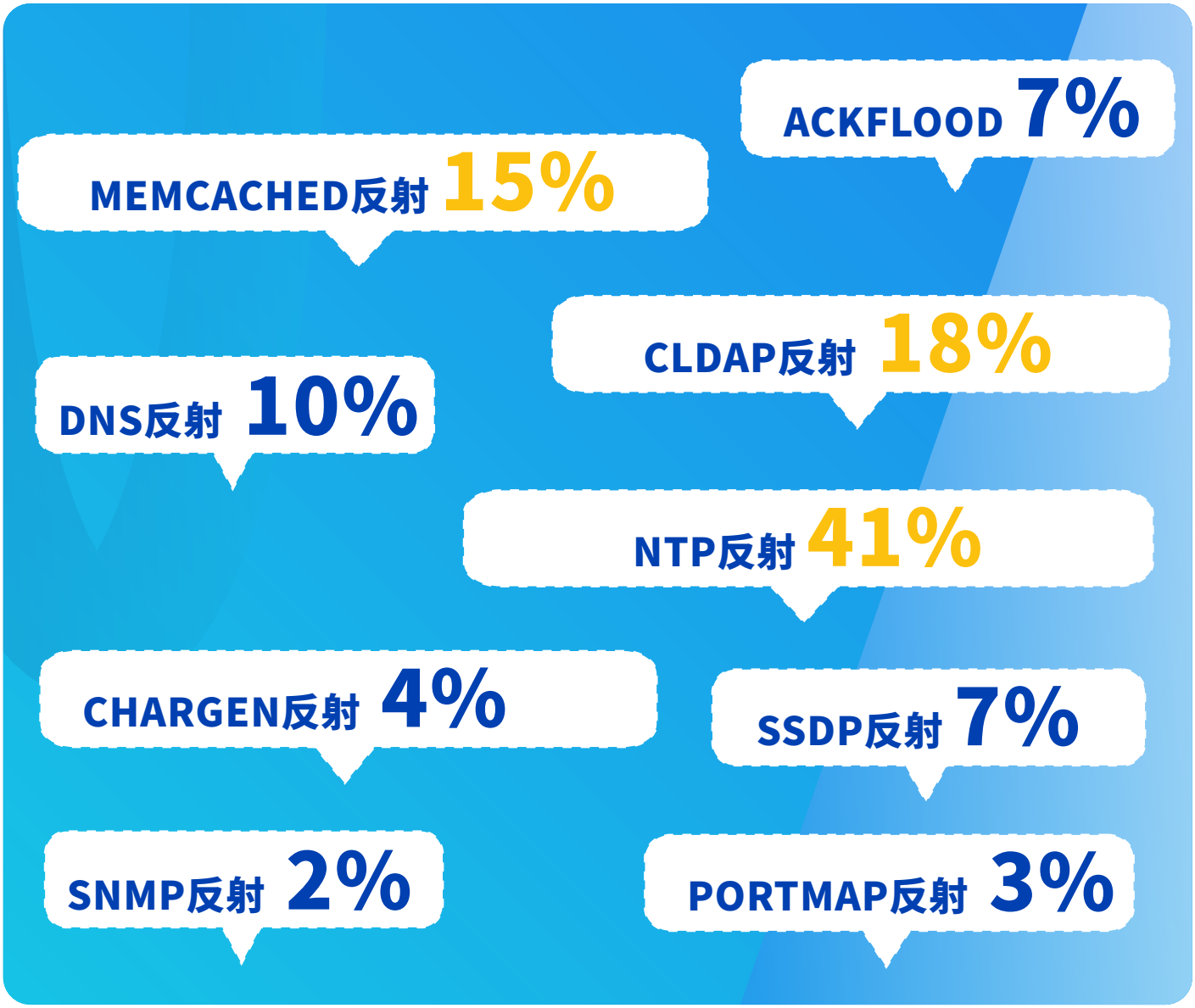


4.2.2 DDoS攻击形势

2019上半年，国内DDoS攻击形势呈现出攻击手法复杂多变，攻击资源来源广泛等特点。从攻击手法来看，HTTPS类攻击崭露头角；TCP反射类攻击成为行业公害，可利用的资源广泛（CDN厂商、云计算厂商大量开放80、443端口）；伪造4层协议攻击浮出水面，攻击手法越来越多样化，防护难度持续攀升。

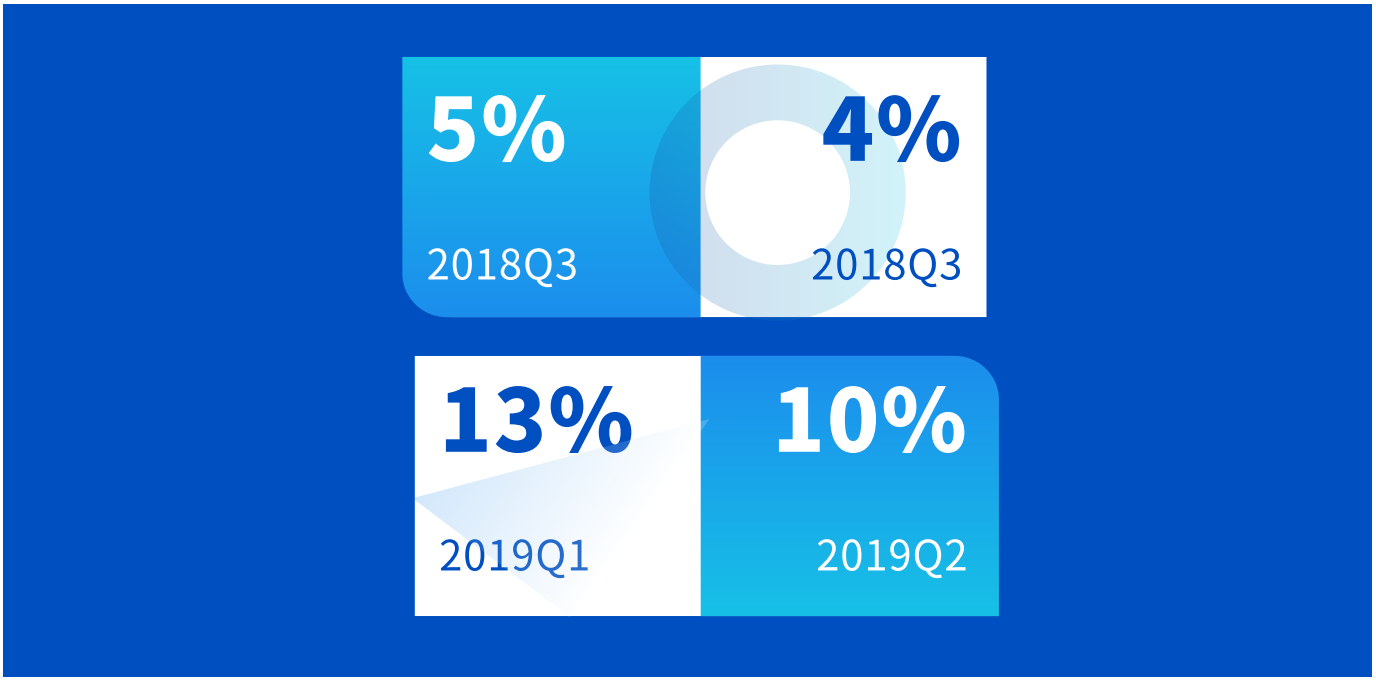


反射放大类攻击手法分布

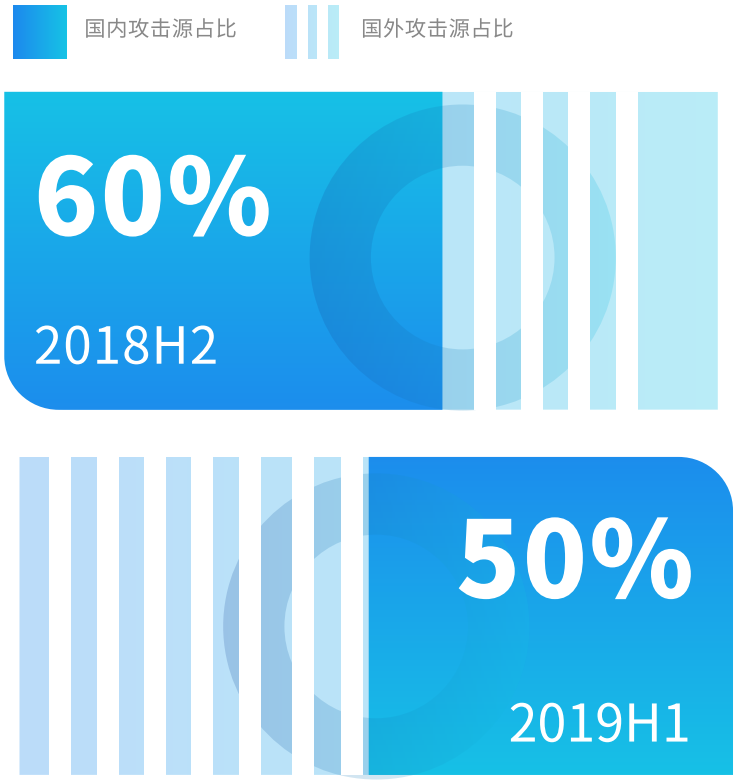


从攻击资源方面来看，更多IoT设备沦为肉鸡，且攻击资源全球化趋势愈发明显。从国内攻击源的分布情况来看，广东、上海、江浙、北京、台湾以及黑龙江等省市及地区占比较高。

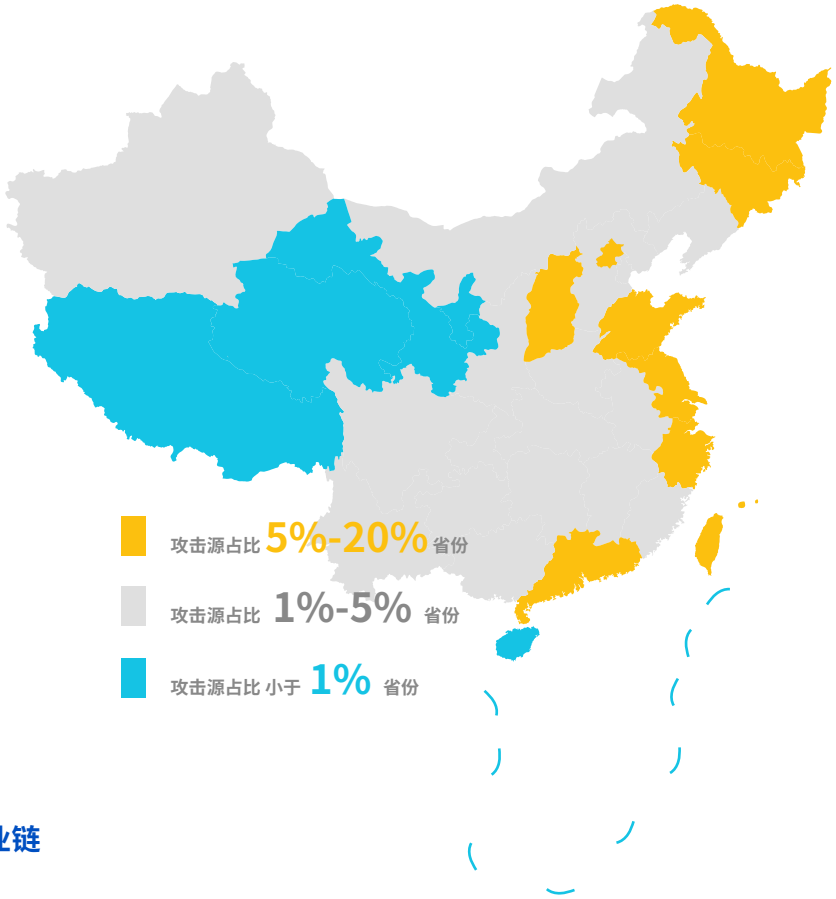
IoT肉鸡占比



国内外攻击源占比



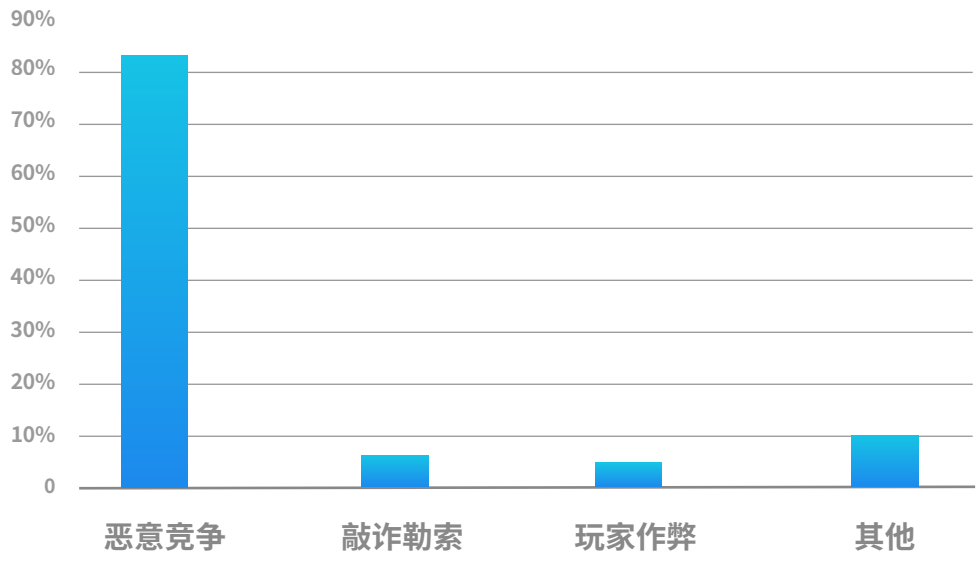
国内攻击源的分布



4.2.3 DDoS攻击产业链

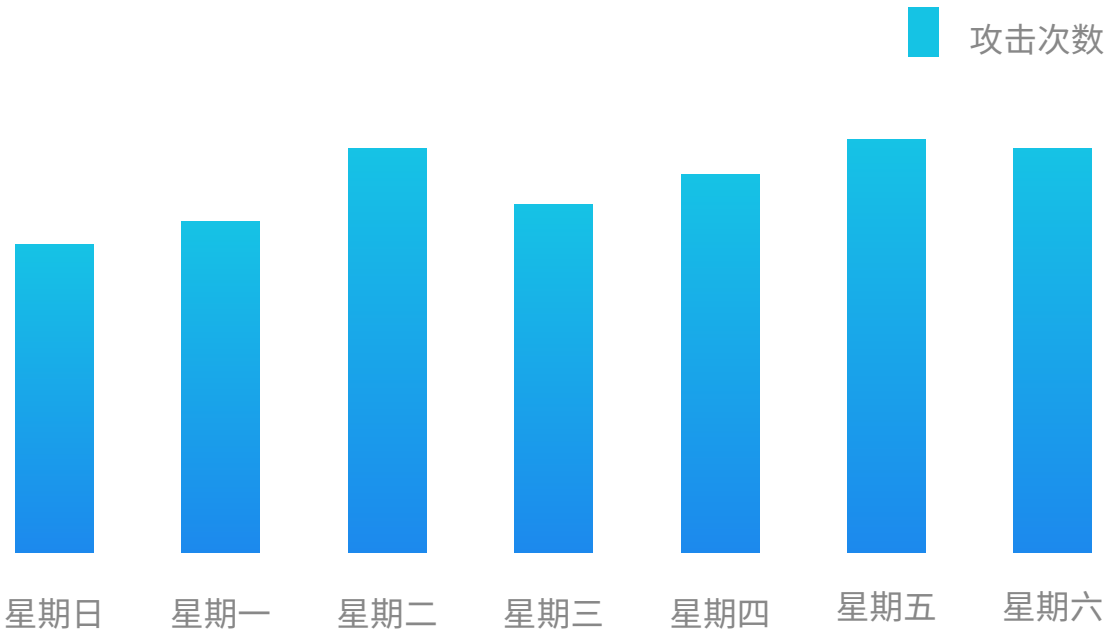
超额利润催生精细化分工，DDoS攻击也不例外。新兴的DDoS服务则完成了多环节自动化发展，页端DDoS攻击平台已成为当下主流。不法分子为发动DDoS攻击往往会搭建攻击站点（每月成本数千元）并出租DDoS攻击服务（每月收入数十万元），而购买攻击服务（每月成本数百元）之后发起勒索（每次赎金数万元），也成为了企业面临的新型威胁。

黑客发动DDoS攻击的动机

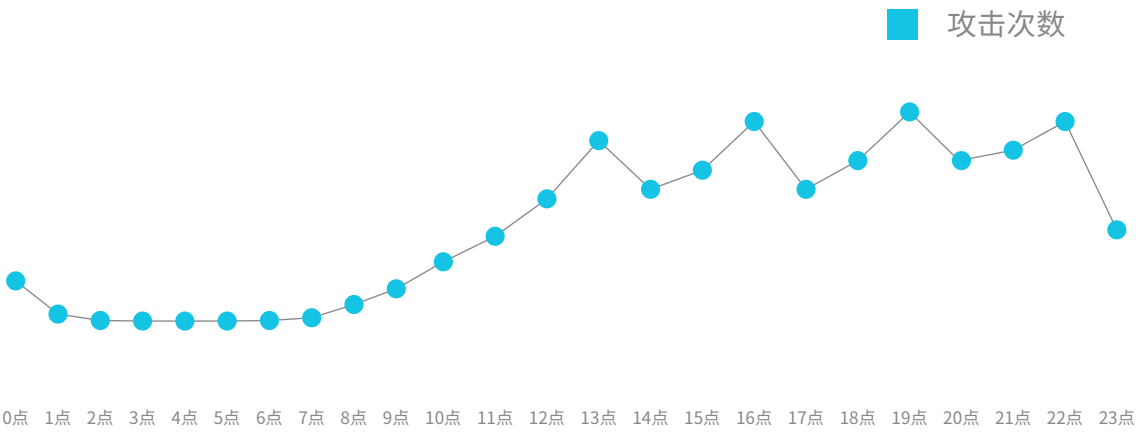


为了赚取超额利润，不法分子几乎做到了全年无休。据腾讯安全的数据统计来看，黑客并没有周末，周二与周五最为活跃。具体到一天24小时，黑客在午后、下午茶、下班时间及睡前最为活跃。

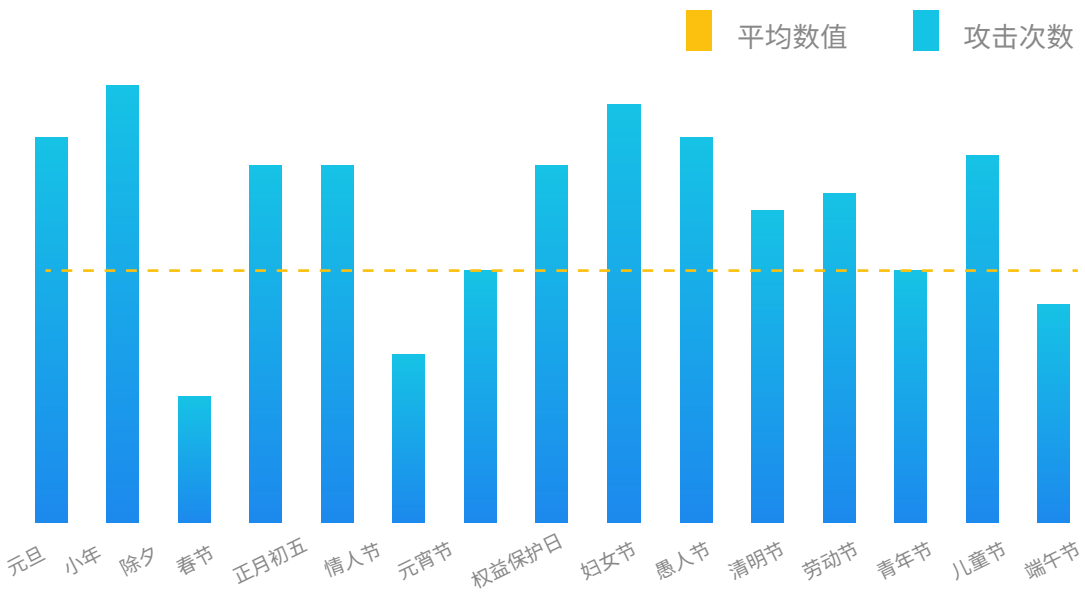
一周7天攻击数据



攻击次数：一天24小时攻击次数



节假日攻击数据



游戏行业因其日流水量最大、变现快，一直站在利益的风口浪尖上，当仁不让地成为DDoS首选的攻击目标，2019上半年游戏行业遭受DDoS攻击全行业占比高达42%，电商、网络服务、企业门户、音视频等紧随其后。而在游戏行业的细分占比中，手游则高达45%，充分体现了“钱在哪儿，攻击者就在哪儿”这一铁律。

DDoS攻击的行业分布

游戏行业细分品类攻击占比

作为出海的主力军，游戏企业不断扩展海外业务。海外DDoS攻击同样很猖獗，企业基本都面临着海外自建DDoS防护成本高、建设周期不可控、溯源难上加难等问题。

4.3 数据安全

数据泄漏是安全界长盛不衰的话题。尤其是个人信息泄漏的影响面极广，可能对个人造成较大伤害，即使是顶尖安全人员也难幸免。2018年，影响最大的个人信息泄漏事件是酒店客户信息泄漏，某酒店集团分别泄漏了3.83亿 和5亿条用户信息。

2019年元旦期间，国外安全研究人员在某服务器上发现2亿中国人的简历泄漏， 接下来的几个月内，共计5亿以上的简历泄漏——而这些还仅仅是被安全人员发现，主动曝光出来的部分。

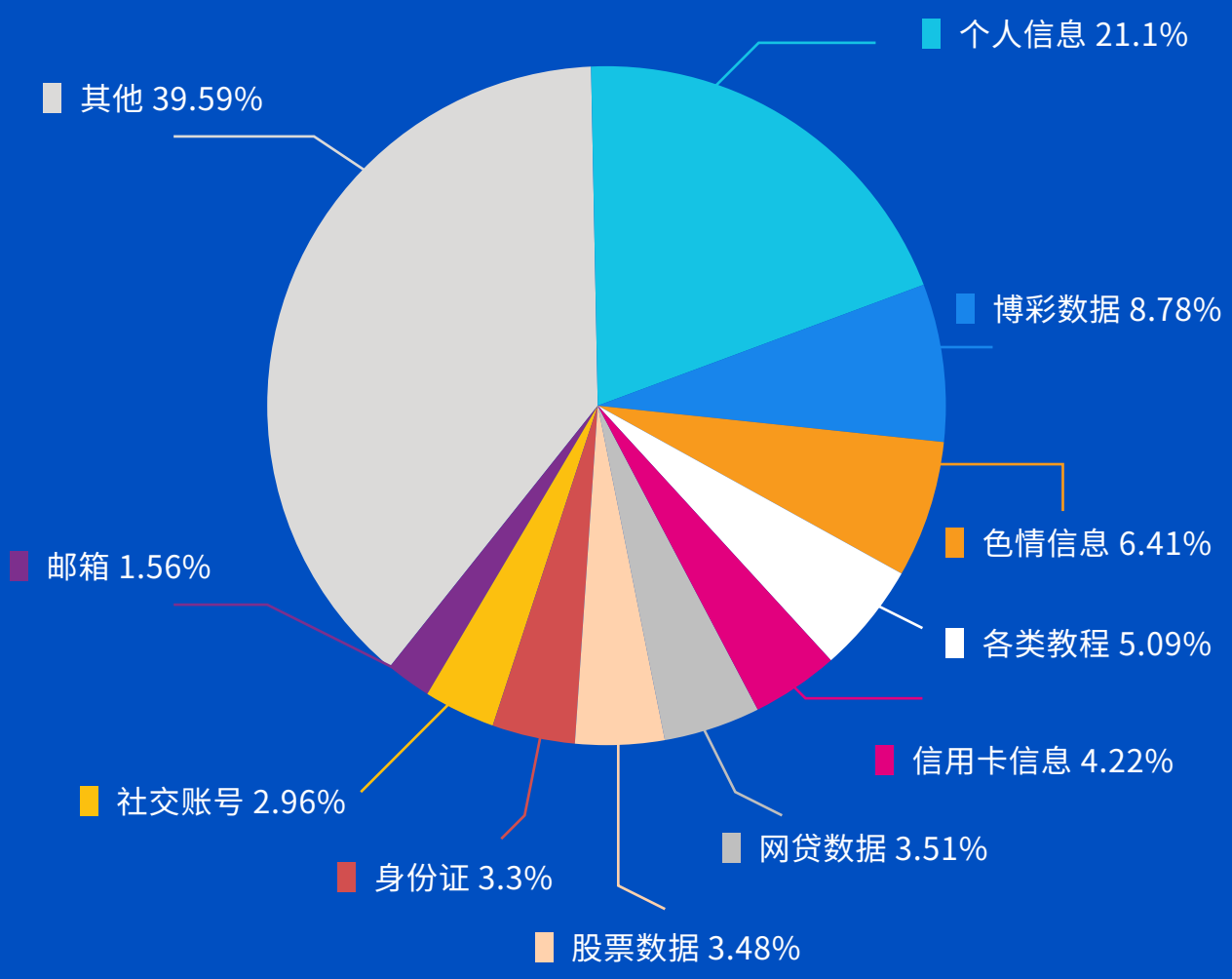
4.3.1 什么数据最受黑灰产偏爱

腾讯安全团队对暗网地下数据交易进行了长期监测，2019上半年的数据显示，暗网中数据关注度占比如下:

DARK NETWORK DATA HEATING RATIO

2019上半年暗网数据热度占比

数据来源:腾讯安全云鼎实验室



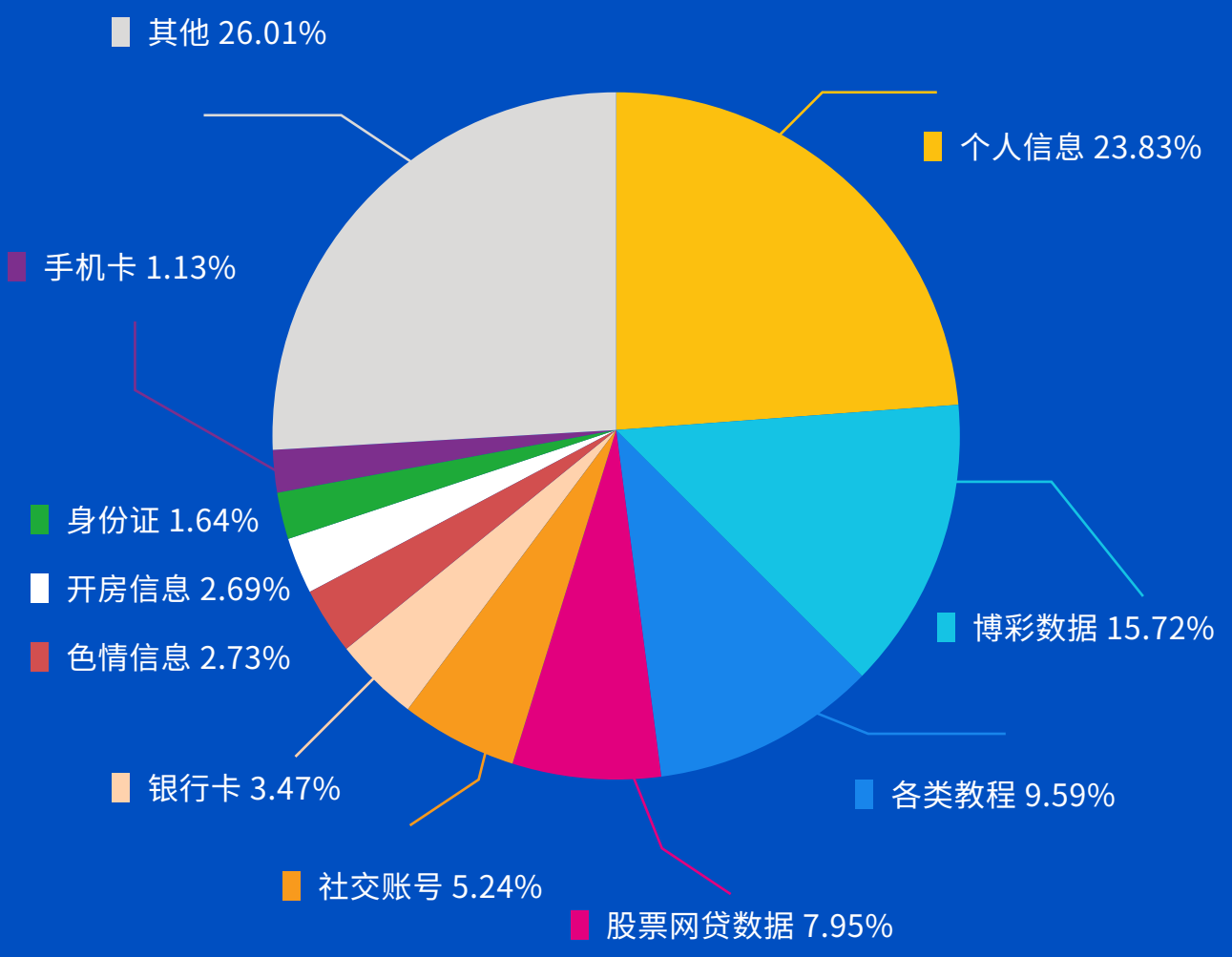
可以看到,个人信息泄漏占据最大比重21%,其次是黄赌类占比15%,再之后是金融数据类(信用卡、网贷、股票)占比11%,以及身份伪造类(身份证、社交账号、邮箱)8%。

另外,我们还监测了实际成交的数据金额占比,稍有些差异,但总体趋同:

DARK NETWORK DATA TRANSACTION AMOUNT

2019上半年暗网数据成交金额占比

数据来源:腾讯安全云鼎实验室



其中博彩和教程类交易金额相较热度的占比有较大增幅,一方面说明博彩类在黑产中盈利能力较高,且其中黑吃黑也较为严重,另一方面说明黑产从业人员还在持续扩张。

4.3.2 常见的数据泄露方式

每年如此多的黑市数据交易，那么数据是怎么泄漏出去的呢？常见的情况通常有以下几类：

1）数据库未授权访问

从今年的简历泄漏事件来看，由于数据库配置问题，不少公司的数据被直接放到公网上可以无密码访问。一方面是技术人员安全意识薄弱，另一方面是存在侥幸心理。在我们之前的研究中发现，每个IP平均每天要遭受数万到数十万次不等的扫描，相当于每天有春运期间一火车站的人在你家窗口偷看里面有什么好东西，如此情况下，数据不泄漏才奇怪了。

2）黑客入侵盗取

高价值公司遭遇定向渗透，数据被盗。

3）内鬼倒卖

相较黑客盗取，企业内鬼倒卖数据远远多过黑客，如某些电商或快递的实时交易数据，各种人肉搜索的调查渠道。

4）平台私自贩卖

部分小厂商，提供服务的同时倒卖用户数据，如有些APP获取额外权限如定位等，用于倒卖盈利；还有一些服务灰产的供应商如短信发送接口，也存在倒卖数据的情况。

5）爬虫爬取

一些公司接口代码不严谨或风控不足，数据被恶意爬取或越权爬取，导致数据泄漏。

6）密码泄漏

一些公司的开发人员由于安全意识薄弱，将代码传到如GitHub等在线服务商处，导致代码中的敏感密码泄漏，造成数据泄漏。类似情况近年频繁发生，如今年某知名视频网站后台源码被上传到GitHub。

4.3.3 数据安全趋势

1）数据泄露背景下，建立以数据为中心的安全架构

大规模的数据泄露事件，尤其是核心关键数据的泄露，将给企业业务带来严重甚至致命性的损失。数据已经成为业务发展的核心和驱动力，企业的安全架构策略也逐步发展为“以数据为中心Data-Centric”的数据安全策略。

2）数据加密，业务安全及和合规遵从驱动

在数据安全策略中，应用密码技术是保障敏感核心数据的机密性、真实性、不可否认性和完整性的有效措施。近年来，全球各国及各行业都发布了关于数据安全及数据加密的法律法规，如中国的等保2.0、密码法（征求意见稿）、香港的CAP 486、欧洲的GDPR、美国的SOX等法案，确保核心数据资产保护及加密策略的有效应用。

3）数据安全及数据加密，云用户关注点

严峻的数据安全态势及加密合规策略推动下，云平台加密基础设施能力成为云用户的核心关注点。

在加密能力支持上，要求云平台能够提供覆盖全数据生命周期，即从数据获取、事务处理及检索、数据分析与服务，数据访问与消费的合规化的加密能力支持；并提供包括密钥管理，敏感数据加密、金融支付、电子政务、电子票据、身份认证、CA、物联网、区块链等不同业务领域的加密应用支持。

在加密策略应用上，当前密码应用中间方案并不完善，用户密码应用仍需大量开发工作。与云平台以及云产品无缝集成的加密组件能力是云用户成功实施加密策略的有力保障，即密码资源、密码运算以及密码应用以组件化、服务化方式输出，随取随用，用户可便捷的将加密组件集成至云上业务系统中，以保障加密措施的有效落地。

此外，密码及加密应用国密化也是今年以来，国内各大行业用户数据保护策略应用重要趋势之一。

4.4 风控安全

在产业快速发展的同时，业务场景复杂化、数据海量化、信息价值不断趋高，为企业带来了更多的新型风险和黑产的觊觎。
据统计，我国黑产从业者规模超百万，年产值高达千亿。而在黑产的分工越来越专业、行动遍布全网、并且由个人方式发展成了“团伙作战”的现状下，如何构建行之有效的风控系统至关重要。
攻击的动力依旧来源于利益，而常见的攻击维度集中在营销风控、内容风控、金融风控几大领域。

4.4.1 营销风控

基于营销目的，企业通常会采取优惠券、现金红包或完成指定任务即发放奖励等激励手段进行拉新，在这个过程中，黑产通过各种手段有规模地薅取企业福利。
基本可以分为3个发展阶段：

1）自动化平台

（1）手机号、账号：由卡商提供手机号，比如常用的物联网卡，用猫池、模拟器、多开软件来养手机号；
（2）验证码验证：通过自动识别字符、图片的技术，如常用的有CNN深度神经网络技术，可以实现百分之九十以上的识别通过率，比较难的验证码则有人工打码平台的支撑；
（3）部分企业自身设置的IP频控策略：任我行、天下游等IP修改软件。

2）群控

购置廉价手机组成手机墙，采用改机工具修改设备信息，如手机型号、串码、IMEI、GPS定位、手机号等，以此不断伪造新设备，甚至直接刷入定制化ROM；同时，采用群控软件操纵手机，模仿真人自动完成点击、APP下载、激活等相应操作。

3）群控+人工

人肉羊毛党、网赚众包。羊头发布任务让人点击、观看广告或完成其他任务来赚钱。众包软件则通过上线任务，吸引用户通过完成操作赚取积分，从而兑换红包。

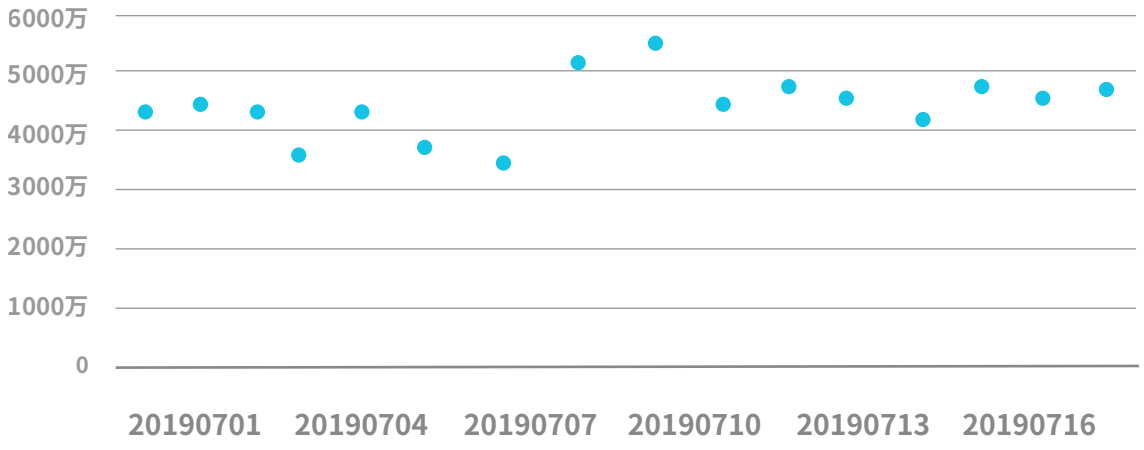
在营销场景的攻击里，618大促是一个典型案例，今年的促销狂欢，某安全企业在“活动防刷”中防护次数就达到16亿次，对抗黑产的薅羊毛行为，保住2.7亿张优惠券。

参考以上攻击手段，不难发现真人羊毛、网赚团伙往往使用大量小号，账号的行为特征和质量都与正常用户偏离。因此，该安全企业基于大数据分析和AI识别模型，通过用户质量检测、设备环境检测以及行为风险检测等两百多个维度，从而准确识别羊毛党、黑产。

最近半个月中，天御所接收到的活动防刷请求数每天都超过4000万次，且整体出于持续增长的趋势。其中每天活动防刷请求中，恶意次数占比约为1/3。

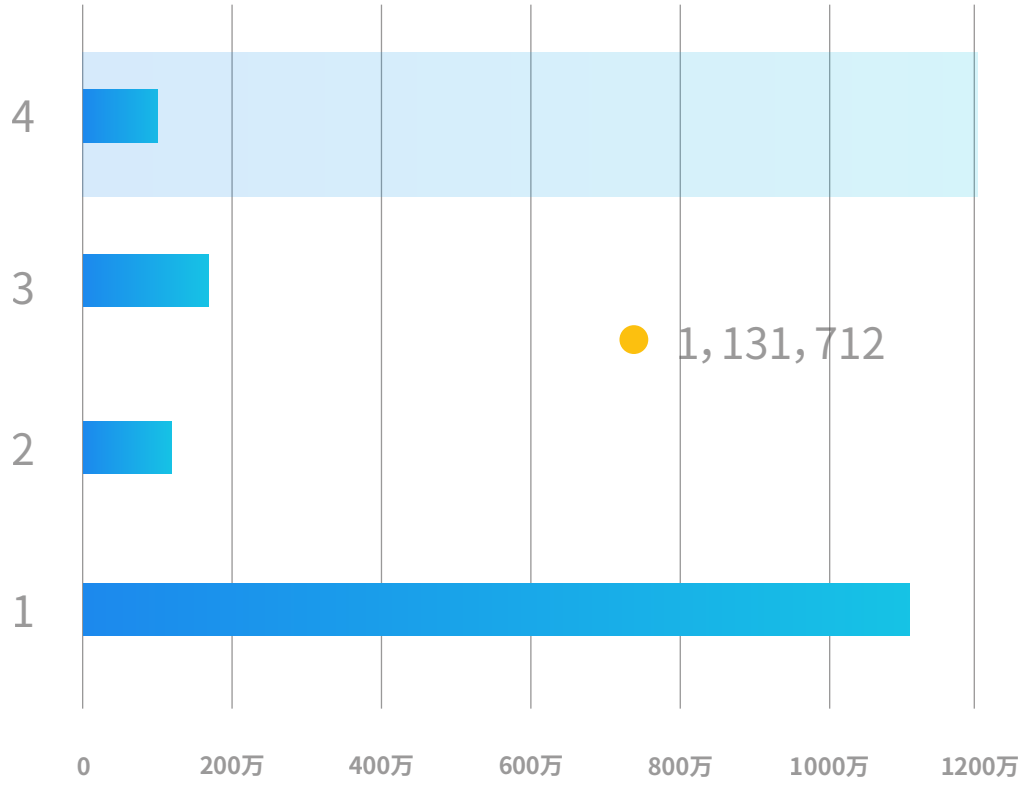
天御活动防刷请求数一览

请求数分布



天御活动防刷昨日业务请求一览

昨日活动防刷请求　总请求:46,003,830　恶意次数:15,198,936　33.04%



4.4.2 内容风控

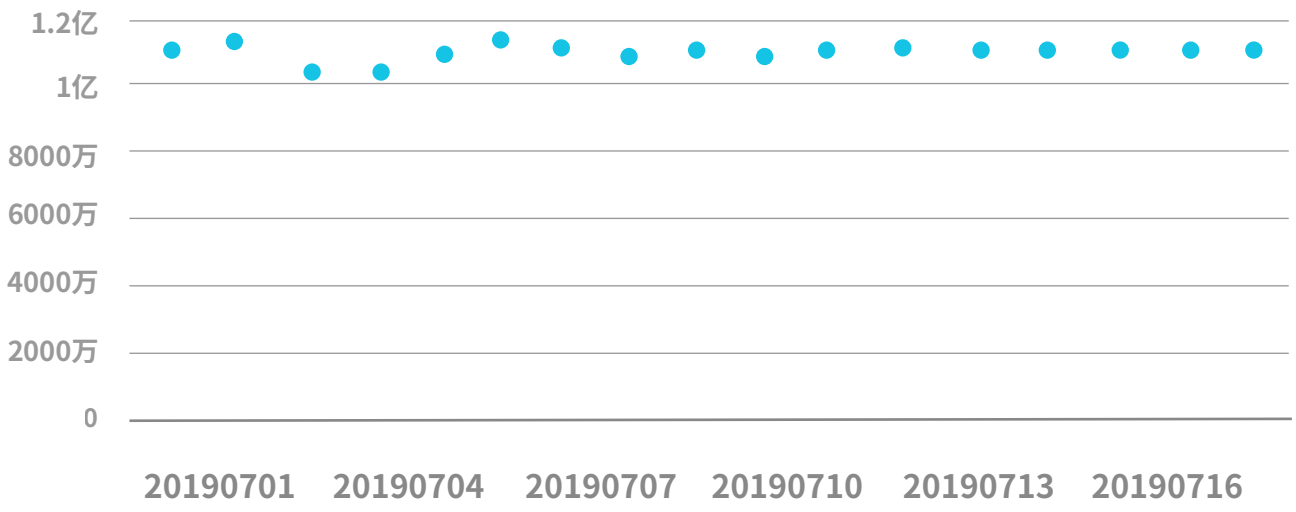
随着网络时代个人发声平台（短视频、直播、即时通讯平台等）不断延展，门槛低，流量高的优势使其同样成为了黑产的娱乐所，用以传播色情、暴力、赌博、垃圾广告等不良信息。

常见的攻击手段：
1、文本变体：使用各种特殊字符暗示销售对象；
2、图片引流：在图片中嵌入文本，结合色情照片引流用户到风险网站；
3、擦边球视频：视频画面无违规，但声音违规（比如各种娇喘声）；

多样、高频的攻击手段，让人工鉴黄难以对抗，而纯靠肤色识别算法进行过滤也早已过时。目前的对抗趋势偏向深度学习进行数据分析，全面覆盖到文本、图片和音频识别。

市场上某产品通过特征提取+智能识别，已经可以实现对涉黄、敏感画面99%的识别准确率。

根据近期监测的数据来看，恶意内容出现的日均频次均过亿，极少出现较大波动，而整体还呈现出微弱上涨的趋势。



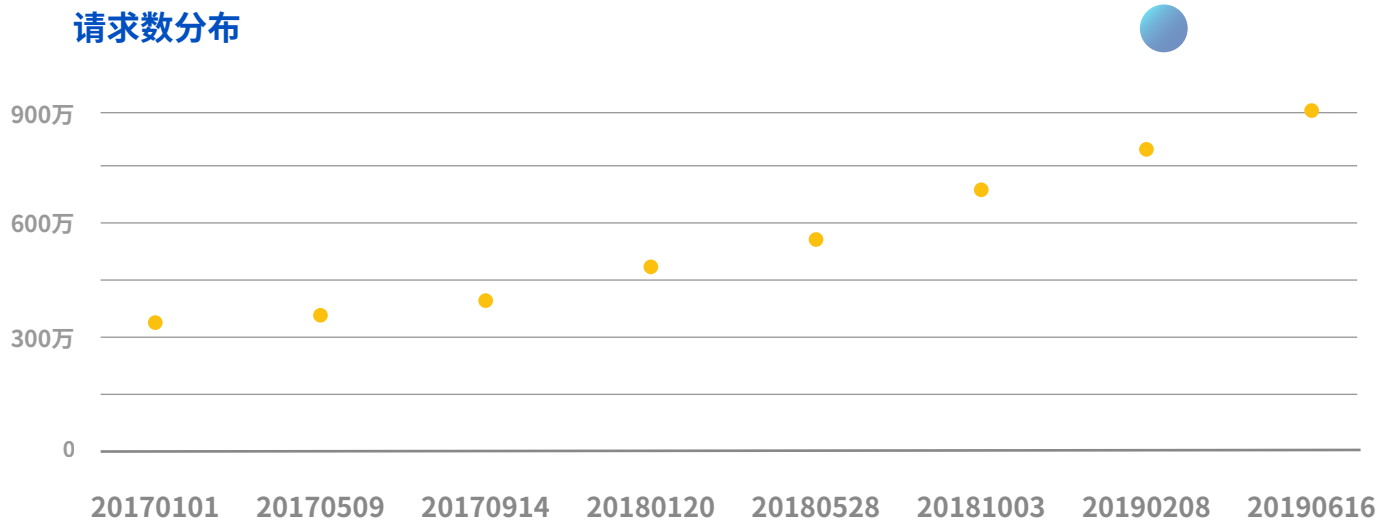
4.4.3 金融风控

互金行业向来是风控重灾区。一方面是支付行业不断向纵深发展，各种新型支付手段和支付工具层出不穷带来的与预授权套现、信用卡大额套现、冲正撤销、持卡人信息泄密、跨境移机、测录等风险事件日趋增多；另一方面是消费信贷不断上升，但整个信贷环节，从贷前、贷中到贷后都面临各种各样的欺诈。

根据天御所监测的数据来看，从2018年下半年开始，金融反欺诈请求数大幅增加。2019年上半年反欺诈请求数均值超过600万，较去年同比增长近一倍。而在所监测到的恶意行为中，最常见的是异常支付行为、信贷中介以及疑似恶意欺诈。

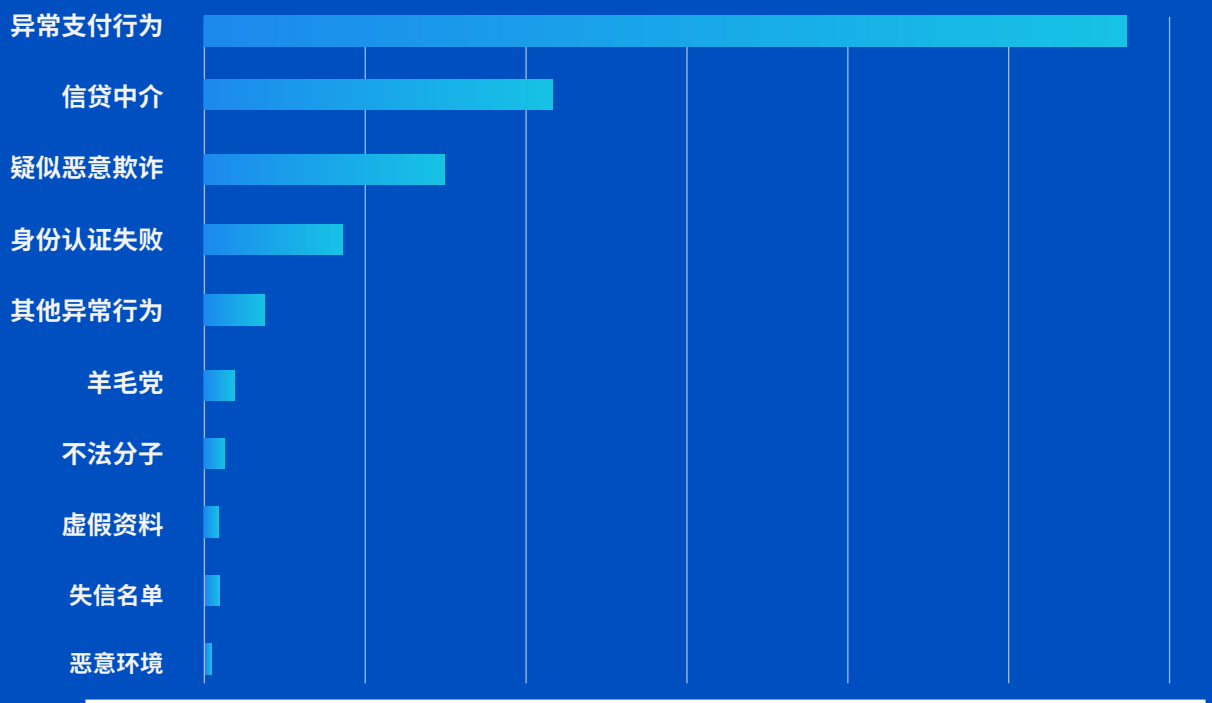
天御反欺诈请求数一览

请求数分布



MALICIOUS ACTS OF FINANCIAL FRAUD

金融欺诈恶意行为TOP 10



针对支付的常见攻击手段包括了身份证伪造生成;活体检测破解;手机号生成;猫池、撞库、伪基站;一键改机软件。

针对信贷环节,攻击链路则包括:

情报收集:在各大平台不断的寻找收集风控规则漏洞

卡商:提供设备、账号、IP、四件套等信息资料;

接码平台:负责快速破解各平台和APP的验证码等

资源工具:提供猫池、模拟器、群控、活体检测破解等工具

面对风控要求更高、环境更复杂的金融业务防护场景,更需要选择分析联网经营数据及上下游业务往来的延续性,从整体供应链的角度做好用户评估,或是参考某款针对小微企业的信贷产品,采用“ABC”(AI+Big Data+Cloud),在流量入口就做好应对。

此外,引入大数据挖掘、反欺诈规则配置、机器学习建模等反欺诈技术能力,也是大势所趋。

CHAPTER FIVE

CHAPTER FIVE

安全建议

安全建议

FREEBUF | 腾讯安全

第五章 安全建议

新技术在促进业务发展的同时，往往也伴随着风险。随着云计算浪潮的进一步扩张，企业的IT架构必将随之变化，网络安全边界也变得越来越模糊。通过前文列举的案例不难发现，直到今天依然有大量的企业用户暴露在危险当中，随时可能中招。报告通过对国内云安全状况的深入分析，总结了部分切实可行的安全建议，期望与大家携手共践云安全防护之路。

5.1 安全运营建议

1、企业可以把更多的精力投入到安全运营上，可借助安全运营中心或事件管理平台所发现的漏洞情报、漏洞告警、入侵事件、安全配置事件进行风险管理和收敛，规避已知事前存量风险；

2、充分利用云上安全组、WAF等功能，做好访问控制和常见威胁的入侵防御，可以规避很多事中的风险利用；

3、做好Windows系统的补丁管理，可以规避很多潜在的Windows蠕虫传播、远程入侵攻击或本地提权行为；

4、做好数据的备份，任何时候，都无法保障关键应用或数据的万无一失，云厂商提供了便捷的快照备份、镜像备份、数据备份功能，这个对于企业尤为重要。

5.2 云主机防护建议

面对黑客入侵的各种攻击方式，主机安全（云镜）建议用户日常需要加强安全意识，提前安装主机安全类产品，做好相应防御措施，有效规避潜在风险。建议如下：

1、设置复杂的密码，一般来说12位以上且字母大小写、数字、特殊字符四种中至少三种，并且尽量包含部分无意义的组合，以此降低被暴力破解的概率。不同服务器设置不同的密码，以防止通过社工的方式猜解密码；

2、关注重要安全公告，及时修复披露的漏洞；对于包含“远程代码执行”、“未授权访问”关键字的漏洞尤其需要关注，此类漏洞相当于将服务器大门敞开给攻击者；同时请一定按照官方修复建议进行修复；

3、至少安装一套安全类软件，通过安全软件可以了解服务器安全情况，及时了解漏洞信息，同时可以查杀恶意文件；

4、加强安全意识，设置密码要达到安全要求，不随意下载运行非官方的程序，尤其是二进制程序，不随意点击来历不明的邮件；对于披露出来的漏洞要加强关注，尤其涉及到个人负责的组件，不能由于“怕麻烦”而放弃或延缓安全修复措施；

5、建立安全评审机制，可定期对服务器进行安全机制评审；如果成本允许，可做安全渗透测试。

5.3 DDoS防护建议

1、在业务主机上要进行IP过滤等设置，以应对同IP发起DDoS的情况。除常规的限次数、限地域外，还要以进行一些固定反射源的过滤，因为有反射源访问业务，一般都是不合理的，这样有助于快速排查问题所在，及时开启防护；

2、隐藏真实的业务IP，进行IP保障，以让攻击者攻击时增加定位难度；

3、针对业务的侧重点不同，要选择有针对性的DDoS防护产品。不用大而全，过度浪费，也不能不设置防御，被攻击时临时抱佛脚；

4、及时进行服务器中的系统及各应用软件的补丁更新，随时关注安全时势动态，针对一些0day或未能及时修复或处理的逻辑漏洞进行人工的临时策略处理。这样可以防止服务器被入侵或被用作反射点，Memcached反射源就是最好的例子。被用作反射源会对外发出大量的数据包，会占用自身海量的带宽，也是一种变相的遭受DDoS攻击的受害者；

4、在业务代码侧与逻辑侧，做好针对DDoS攻击类型的预防，例如针对SYNFlood这种半开连接，可以在业务展前端做一层代理层，来吞吐流量，将TCP成功连接后的再去唤醒业务侧真正的服务处置等。

5.4 数据安全建议

1、开发人员增强安全意识，各种软件环境不使用默认密码或弱密码；

2、规范代码管理和编码安全意识；

3、不把重要数据传送到不规范的服务商；

4、加强安全管理或使用更专业的云安全服务。

5.5 风控安全建议

1、评估是重中之重，务必在风控前做好产业、经营数据、上下游往来业务的全面调查、了解；

2、基于对业务场景的认知和长期积累的对抗经验，需要不断训练风控模型，加强防护；

3、风控人员和运营人员都需增强风险意识；

4、对中小微企业而言，相较于自建风控系统，购买云模式仍是首选；

5、数据决定模型准确率上线：推动风控系统进一步拥抱人工智能；

6、非结构化数据给风控带来新挑战。随着IoT的发展，越来越多的短视频、图片、语音类数据或占数据流主要份额，而这类数据由于结构各不相同、数据非常大但单位价值相对低，如何高效解析和处理这些非结构化数据，避免黑产恶意攻击隐匿其中，成为风控新挑战；

7、新硬件的发展提升风控能力。目前大趋势是计算层面越来越与新硬件的创新紧密结合，而芯片类、存储类等新硬件与软件的配合或将为风控带来更大的力量对抗攻击。

2019上半年

云安全趋势报告

CLOUD SECURITY

出品方

FREEBUF

数据及内容支持

腾讯安全