绿盟威胁情报中心（NTI）

2017
网络安全观察

NSFOCUS

绿盟科技官方微信

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。在国内外设有 40 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在检测防御类、安全评估类、安全平台类、远程安全运维服务、安全 SaaS 服务等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及安全运营等专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

2017 网络安全观察

NSFOCUS 2017 Cyber Security Insights Report

NSFOCUS

目录

绿盟威胁情报中心（NSFOCUS Threat Intelligence, NTI）

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技为落实智慧安全 2.0 战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

执行摘要

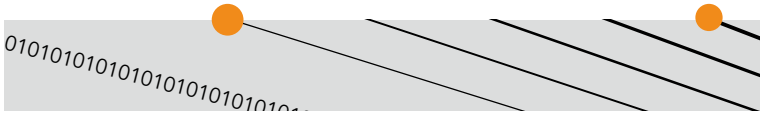
孙子曰“知己知彼，百战不殆”，话又说“知易行难”。知己已是不易，各种开源软件涌入信息系统，各种 API 调来调去供应链越来越长，各种微服务“一言不合”就上线。这种动态环境下，知己——清楚地了解洞悉自身网络中的资产、价值和安全属性、逻辑分布和依赖关系等无疑很挑战。 但知彼是更难的挑战。“彼”的识别就是个大问题。什么目标和动机？定向的，还是非定向的；什么技术水平？高级的，还是一般的；当前什么趋向，什么漏洞和利用在流行？数百万的安全告警背后分别是什么威胁？

赵粮 博士

从名义和定义上看，威胁情报是一个很好的“知彼”渠道。一般来说，市场上可以获得的数十数百种威胁情报，包括免费开源的、商业的，在实际安全运营活动中，有时候显得太多，数以千万的各种威胁信息，需要占用大量资源才能加以分析利用；有时候又显得太少，当重大或特定安全事件发生时，又发现诸多威胁情报“面面相觑”，都不能提供有价值强关联的可行动信息。几年的实践下来，业界意识到威胁情报只有在消费分析闭环里的不断”提炼 " 中才能展现价值，自身也才能越变越精准。 在这个闭环中，消费到分析的阶段最为关键。威胁情报的消费过程本身也构成了新的“情报”，新的情报再次加入新的“消费”环节，于是威胁情报的用户和提供商一起构成了一种事实上的网络防护生态， 这种“生态”能带给成员最为鲜活的威胁动态和动力，实现一种可持续的、可运营的知“彼”手段。

如果说 2016 年发生在 Dyn 攻击事件是物联网威胁的“叫醒”铃声的话，那么到了 2017 年，物联网设备已经是网络攻击的常客。绿盟威胁情报中心数据显示，物联网设备 IP 已占有总恶意 IP 的 12%，物联网设备中恶意 IP 所占物联网总 IP 数量的比例达到 4.8%， 是普通 IP 空间相应恶意 IP 占比的 3 倍。不难预计，物联网设备带来的安全威胁将继续不断升高，对物联网威胁的相应防护能力将会成为安全防护体系的标配。

2017 年，在我们持续监控的超过 390 万个攻击源中，大约 20% 的恶意 IP 曾对多个目标进行过攻击，0.39% 的攻击源对 90% 的攻击



事件负责。对这些“惯犯”的针对性跟踪、分析、画像、对抗等可以有效地提高安全防护的效率和效果，相应地，“惯犯”覆盖也将成为最为核心的威胁情报能力之一。

对这些“惯犯”的针对性跟踪、分析、画像、对抗等可以有效地提高安全防护的效率和效果，相应地，“惯犯”覆盖也将成为**最为核心的威胁情报能力之一**。

如年中安全观察所报告的，我们发现恶意 IP 在一个国家总 IP 数量中的占比与该国家的整体经济发展水平有非常明显的线性关联关系，也就是说，经济程度发展较低的地区，互联网安全治理水平也相对落后，安全防护提升跟不上电脑的普及速度，从而计算机被感染成为被控主机、攻击其它系统的概率更高，例如，越南恶意 IP 占比高达 17%， 印度高达 11%……这些基础威胁统计信息可以作为 UEBA/ 安全行为分析的重要输入，建立更智能的安全检测体系。同时，我们应该看到，追逐利润的安全威胁越来越体现出全球化运作的特点，这也要求威胁情报也具备全球化运作的监视、分析和响应能力。

2017 年，我们监测到的拒绝服务攻击的总流量达 64 万 TB，相比 2016 年增长 79.4%。全年 DDoS 平均攻击峰值为 14.1Gbps，比 2016 年增长 39.1%。单次 DDoS 攻击规模最大的一次发生在 2017 年 5 月份，峰值达 1.4Tbps，而 2016 年的攻击峰值是 730Gbps。

反射放大型攻击依然占据了拒绝服务攻击类型的主流位置，值得注意的是，反射攻击武器库里又有新的致命武器。几天前，著名代码托管站点 GitHub 遭受高达 1.3Tbps 的拒绝服务攻击。这次攻击了利用 Memcached 的反射拒绝服务攻击漏洞。绿盟威胁情报中心 NTI 数据显示，全球有 10 万多的 Memcached 服务器在互联网上开放，考虑到这些服务器的大带宽、高在线时长，Memcached 有可能成为新的反射 DDoS 攻击大杀器。

点滴分享，帮助您洞察威胁……

1. 攻击地区分布

1.1 攻击源地区分布情况

从攻击源绝对数量上来看，中国、美国、印度、中东部分地区仍然是攻击源 IP 主要分布的地区。

图 1 攻击源地区分布

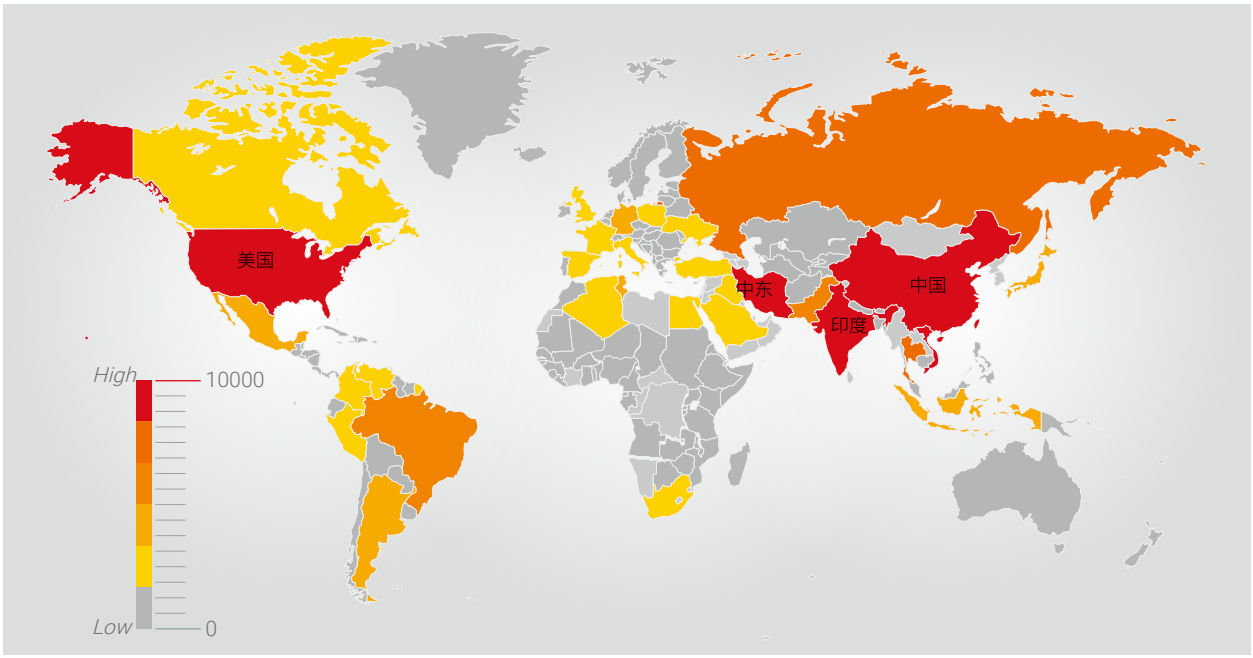
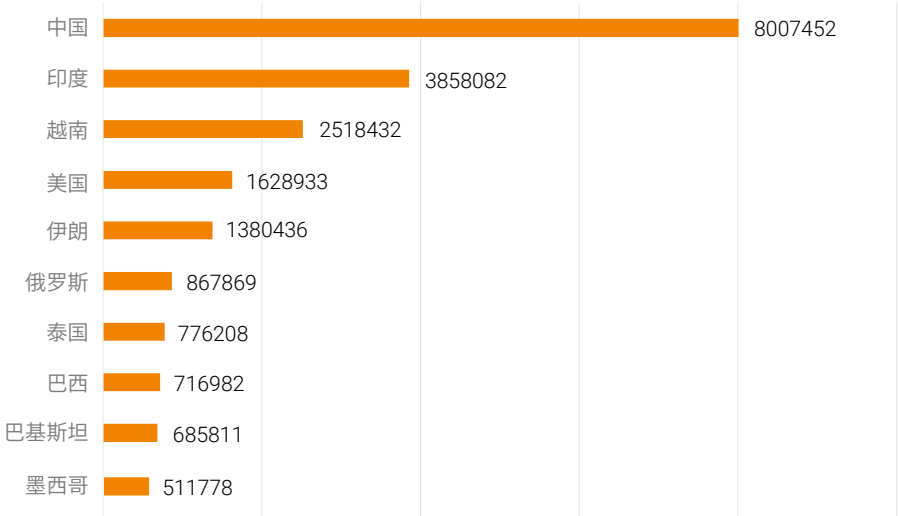
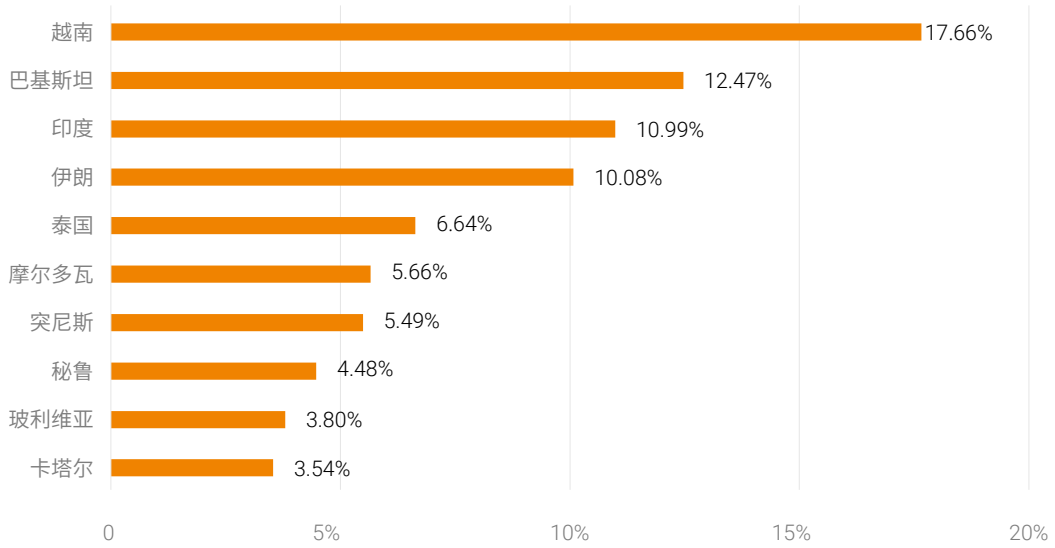


图 2 攻击源数量 Top10 国家（地区）



另外，我们通过 ASN 编号归属，按照 ASN 管理机构所在地区，对恶意 IP 占比情况进行了统计：我们发现经济程度发展较低的地区，治理情况也相对滞后，这些地区或国家发起过攻击的 IP 占比较高，最高的地区越南占比高达 17%。值得注意的是，这些地区的 IP 虽然发动攻击频率是最高的，但并不意味着存在更多的黑客组织，因为黑客利用的网络资源其实是不分地域的，能够利用互联网中所有脆弱性高的设备作为攻击工具，这些地区是因为治理上的疏漏，成为黑客活动的重点地区位置。

图 3 恶意 IP 占比 Top10 国家（地区）



另外，从单个 ASN 来看，攻击源数量最多的 ASN 如下：

表 1 恶意 IP 数量排名 Top10 的 ASN

ASN	国家地区	机构归属	攻击源 IP 数量
AS4134	中国	CHINANET-BACKBONE	2688819
AS9808	中国	China Mobile Communications Corporation	1658532
AS9829	印度	National Internet Backbone	1495907
AS45899	越南	VNPT Corp	1478966
AS4837	中国	CHINA UNICOM China169 Backbone	1302938
AS24560	印度	Bharti Airtel Ltd., Telemedia Services	733811
AS45595	巴基斯坦	Pakistan Telecom Company Limited	633042
AS7552	越南	Vietel Corporation	591468
AS56046	中国	China Mobile Communications Corporation	586240
AS12880	伊朗	Information Technology Company (ITC)	437364

我们建议企业结合自身业务特点，对访问企业网络的 IP 按照 ASN、地区归属进行合理的过滤与限制，尤其针对高危地区和 ASN 号段，这样的控制能够大幅降低不必要的攻击风险。

1.2 受害者地区分布情况

从国家分布来看，受灾最严重的国家包括美国、中国、英国、德国、日本，攻击数量与地区发达程度是正向相关的，因为一个地区的发达程度与信息化程度以及信息资产价值是直接关联的。对于中国、美国、欧洲地区，这些地区存在大量联网的高价值信息资产，是网络攻击中重点针对的地区。

图 4 受害者地区分布

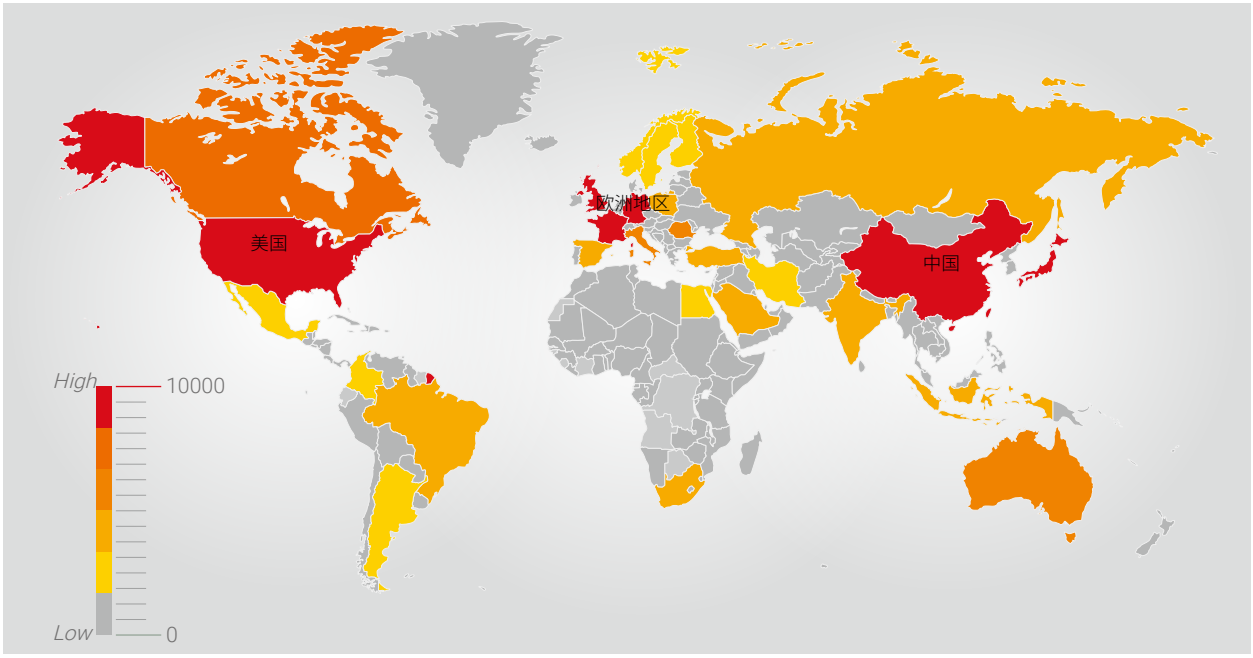
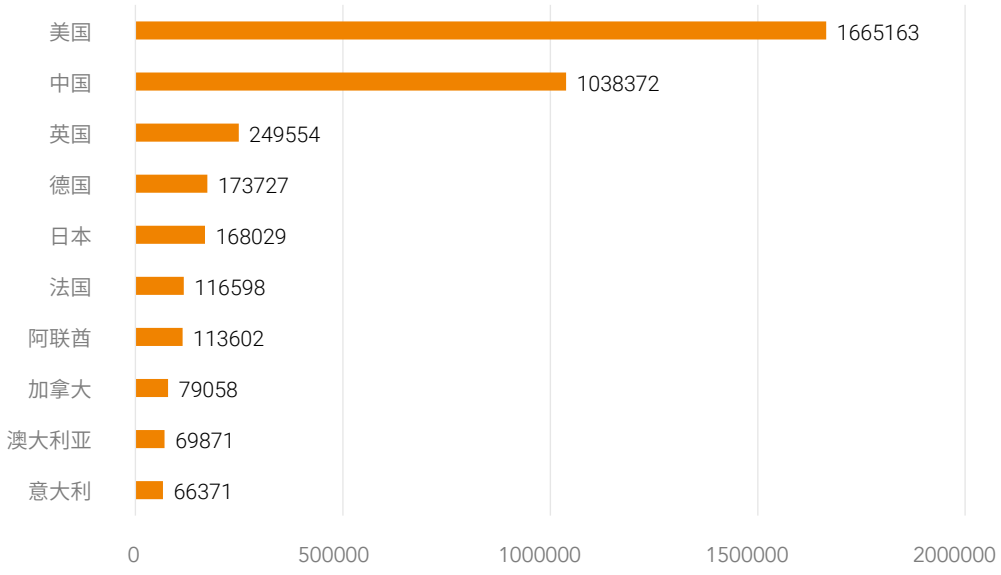


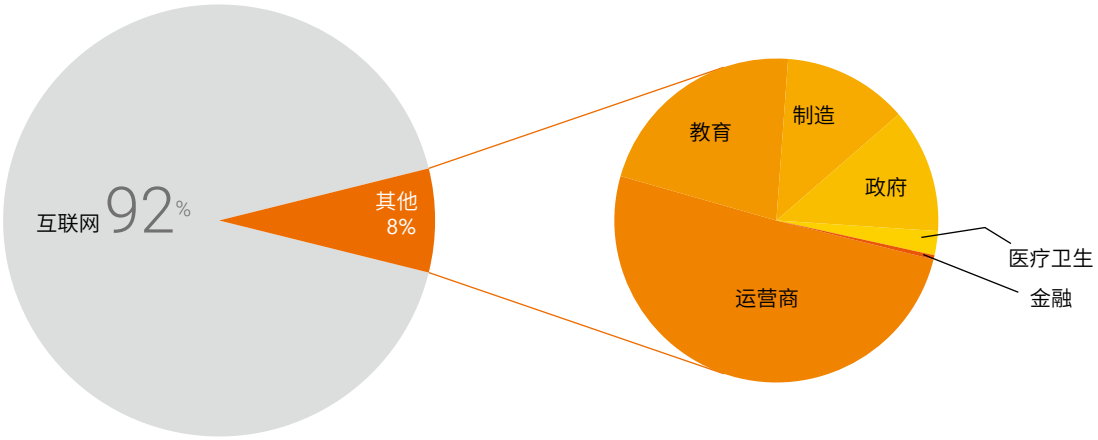
图 5 受害者 IP 数量 Top10 国家（地区）



2. 攻击行业分析

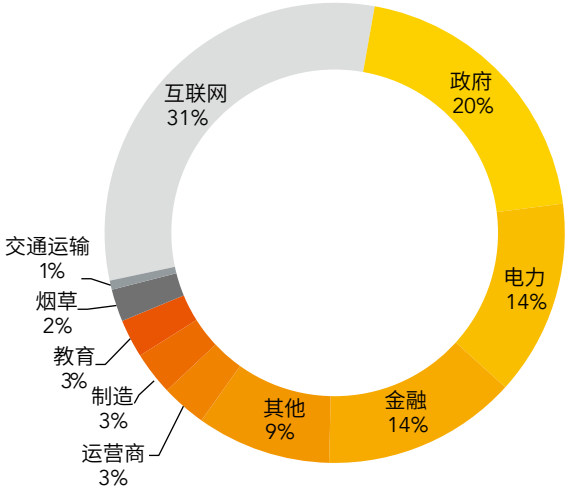
由于各个行业的业务特性都不相同，黑客攻击在不同行业中呈现的侧重点是不一样的。在互联网企业中，业务环境复杂，大量的业务需要提供 Web 界面为客户提供服务，其背后还需要架设复杂的 IT 架构提供相应的技术支撑，使得 Web 类、系统类的攻击在互联网行业中都非常突出，对防护方案的要求也会更加苛刻。从业务流量上看互联网 Web 服务的流量占比是最高的，但是，单从行业自身业务特征看，运营商、教育、制造、政府行业都应该重点关注 Web 类的攻击，进行重点防护。

图 6 Web 类攻击的行业分布



在系统类的攻击中，首当其冲的仍然是互联网行业，其次电力、金融等行业占比非常突出，这类系统自身具有各自的敏感性，历来都是黑客重点关注的对象。金融等行业是勒索、僵木蠕病毒的高发区，恶意代码通常都是利用系统自身的脆弱性（例如错误的配置、弱密码、系统漏洞等）进行大范围传播，而黑客的目的主要是为了制造社会影响和获取经济利益。

图 7 系统类攻击的行业分布



与 Web 类攻击不太一样的是，系统类的攻击会更有针对性，效率更高。在这些行业中可以看到 APT 组织的攻击、加密勒索、社工攻击等复杂的攻击形态，造成客户信息泄露、直接的金钱丢失等等。例如今年绿盟威胁情报中心（NTI）监测发现的 APT-C1 组织，通过一系列的渗透操作直接盗取了客户的数字资产，直接经济损失高达 150 万美元。

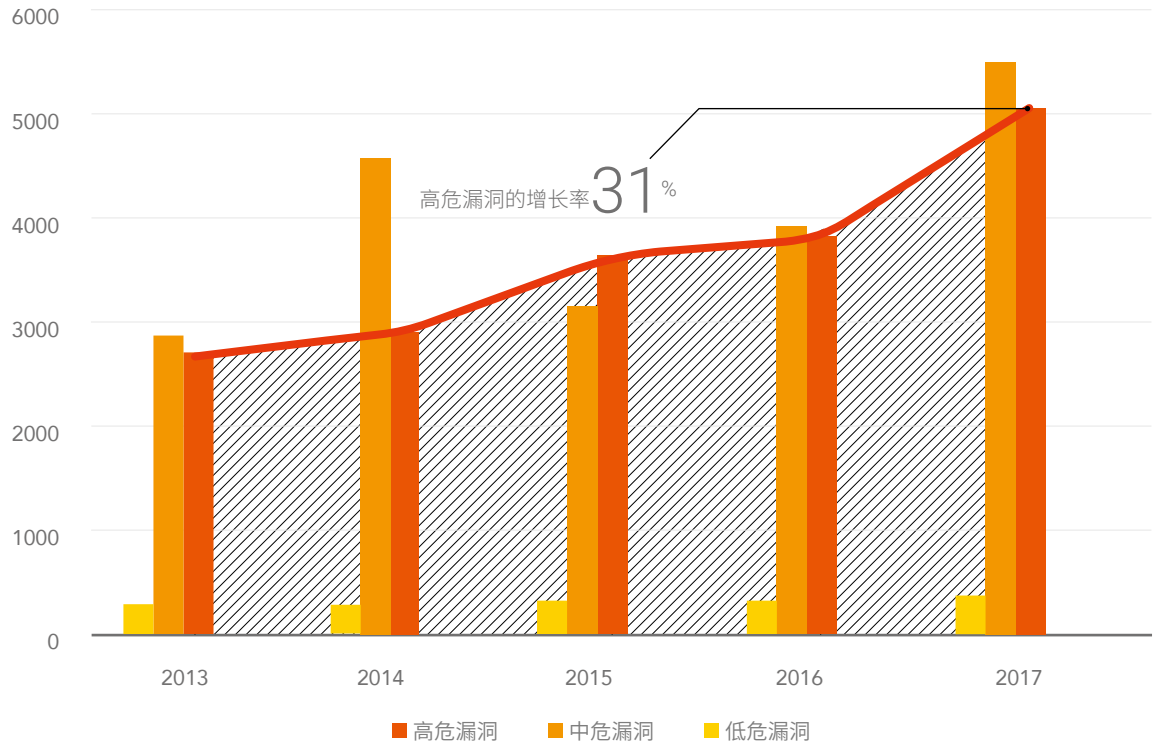
3. 安全态势变化

3.1 漏洞态势

3.1.1 总体态势

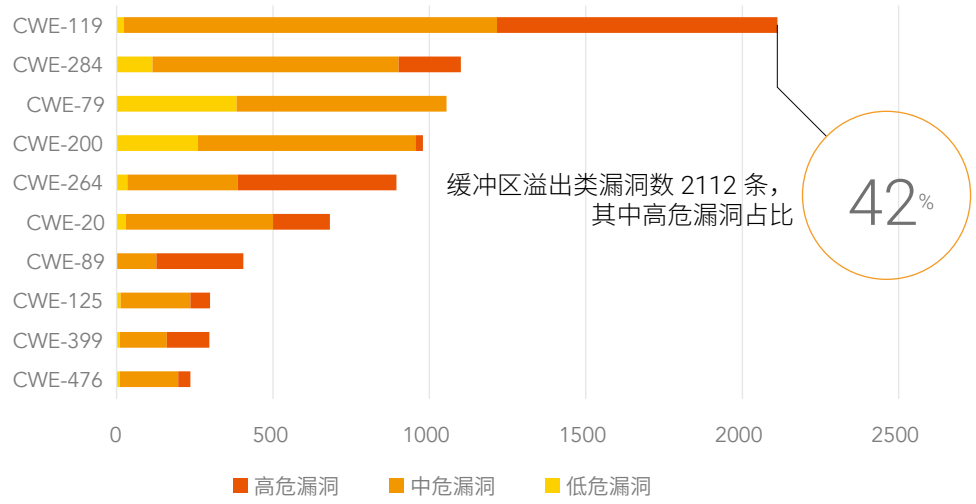
2017 年漏洞总数延续了快速增长的趋势。相较去年，漏洞总数增长了 28%，其中高危漏洞的增长率尤为突出，达到 5 年新高 31%。

图 7 2013-2017 漏洞数量



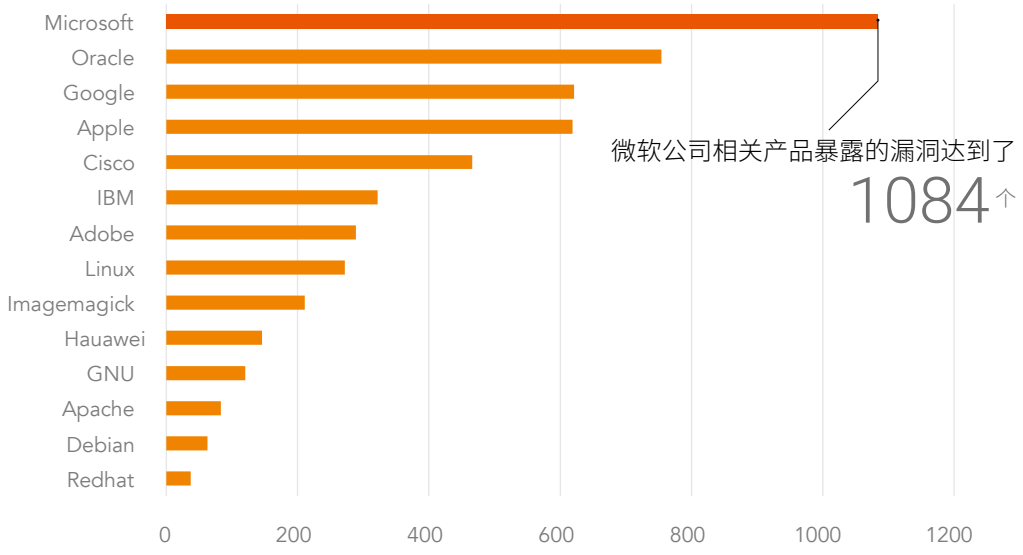
2017 年漏洞按照数量统计，漏洞类型 Top10 分别为：缓冲区溢出（CWE-119）、访问控制不当（CWE-284）、XSS（CWE-79）、信息泄露（CWE-200）、权限访问控制（CWE-264）、输入验证错误（CWE-20）、SQL 注入（CWE-89）、越界访问类（CWE-125）、资源管理错误（CWE-399）、空指针取消引用（CWE-476）。其中缓冲区溢出类漏洞数量最多，达到了 2112 条，其中高危漏洞占比 42%。

图 8 2017 年漏洞数量 Top10 的漏洞类型



我们将漏洞数量，根据不同厂商进行排名，几个大厂商的漏洞数是最多的，微软公司相关产品暴露的漏洞达到了 1084 个。

图 9 2017 漏洞数量较多的厂商

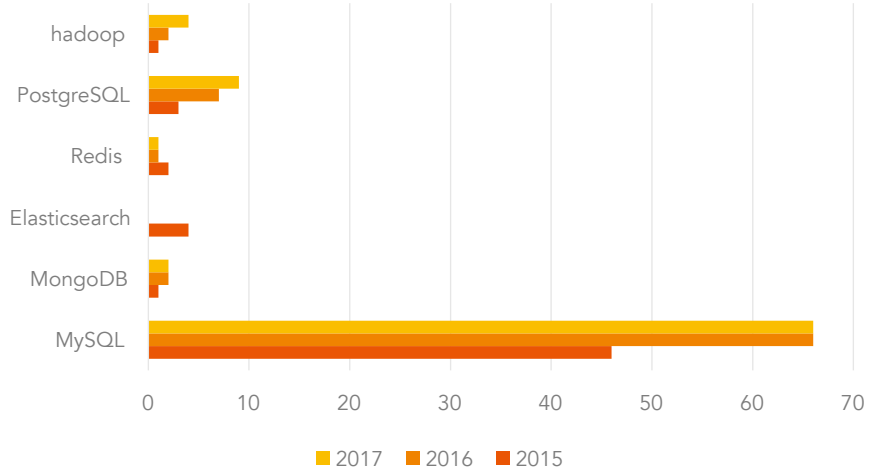


3.1.2 热点漏洞

3.1.2.1 数据库漏洞引发关注

在《2017 年上半年网络安全观察》中我们提到，2017 年 1 月至 2 月其间发生了多起知名的数据库勒索事件。很多数据库的读取接口直接暴露在互联网上，并且没有设置完整的访问控制策略，通过弱密码甚至空密码就可以直接获取数据库的控制权限。数据库勒索主要是指攻击者通过各种方式获取数据库控制权，加密或破坏数据，以此要挟受害者支付赎金。数据库安全成为 2017 年的安全热点，我们统计了三年来涉及攻击的数据库漏洞数量。

图 10 对数据库勒索中涉及到的数据库漏洞数量的统计



其中 MySQL 的漏洞暴露最严重，此外从增速方面来看，PostgreSQL 在过去三年里的漏洞也有较快的增长。相比之下，MongoDB、Elasticsearch、Redis、Hadoop 等数据库则相对安全性，不过仍有一定程度的增长。从数据库漏洞的发展态势上看，数据库的安全问题也越来越受到关注，也许基于漏洞利用的数据库劫持事件将在不远的将来出现。

3.1.2.2 勒索软件利用漏洞进行传播

2017 年勒索软件是不得不关注的安全主题，Wannacry、EternalRocks、Petya、GodenEye(NotPetya)、BadRabbit 这些勒索软件家族在互联网环境中肆意传播造成了很大的影响，也为企业或个人带来重大的数据和经济损失。

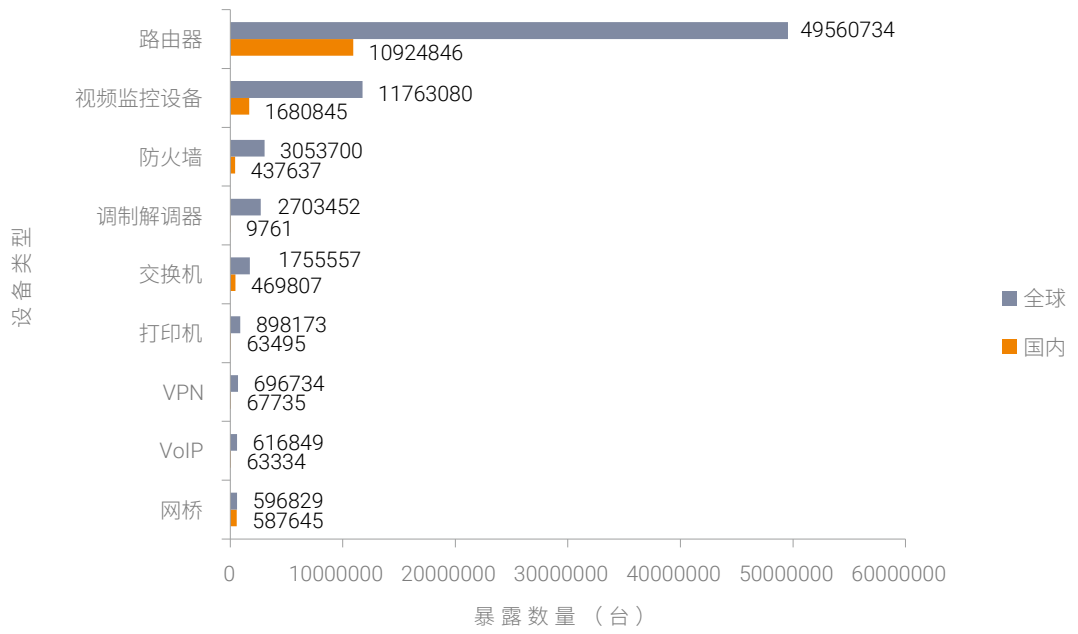
图 11 2017 重大勒索软件爆发事件

这些知名勒索软件的传播手段上有一个共同的特点，它们都是利用 Windows SMB 服务的缺陷 MS17-010（CVE-2017-0143、CVE-2017-0144、CVE-2017-0145、CVE-2017-0146、CVE-2017-0147）进行传播的。

3.1.2.3 物联网设备漏洞情况严重

2017 年 4 月 26 日 Persirai 僵尸网络利用漏洞一举攻陷 12 万台 IP 摄像头设备，引起了很大的关注，以网络摄像头、家用无线路由器为代表的物联网设备安全成为 2017 的安全热点。从全球分布来看，路由器暴露的数量超过了 4900 万台，远远高于其它物联网设备（IoT）暴露数量。视频监控设备的暴露数量超过了 1100 万台，高于防火墙、交换机等传统网络设备的暴露数量，仅次于路由器。打印机的暴露情况令人意外，暴露数量达到了 89 万台之多。

图 12 全球和国内物联网相关设备暴露情况



从设备比例上看，摄像头、路由器、无线接入设备是最数量最多、分布最广的 IoT 设备。这类设备安全防护非常薄弱，常常出现严重的漏洞。我们针对这类设备的漏洞曝光情况进行了统计，发现近三年来，路由器、无线接入设备、视频监控设备的相关漏洞，呈逐年快速上升态势。由于物联网设备更新和防护机制存在很多弱点，我们有理由相信，这些漏洞会存在相当长的时间。例如在后文中我们也提到，今年 Gafgyt 利用 Netcore 中一个 2014 年曝光的后门，进行了大规模的传播，并且活动非常地频繁。

图 13 近三年常见路由器、无线接入设备漏洞数量

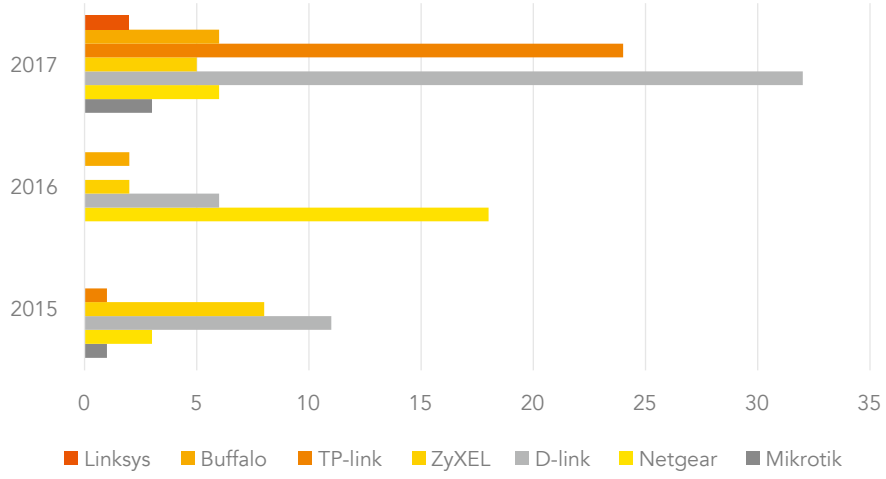
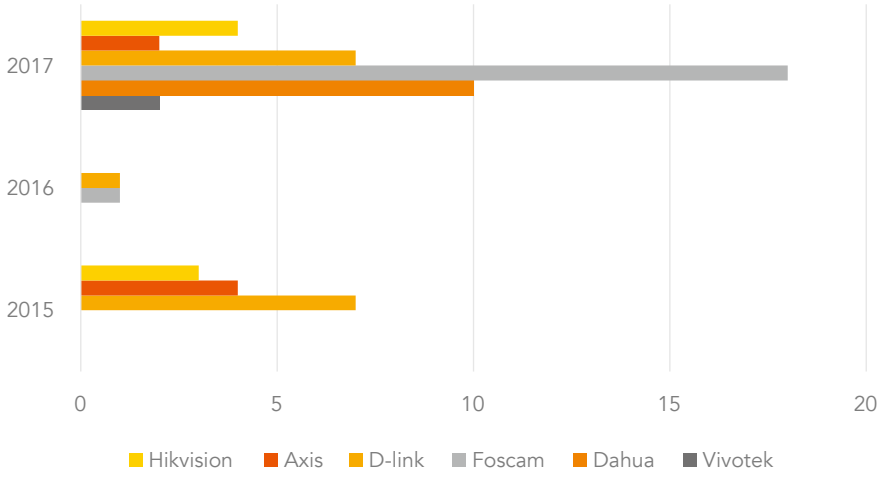


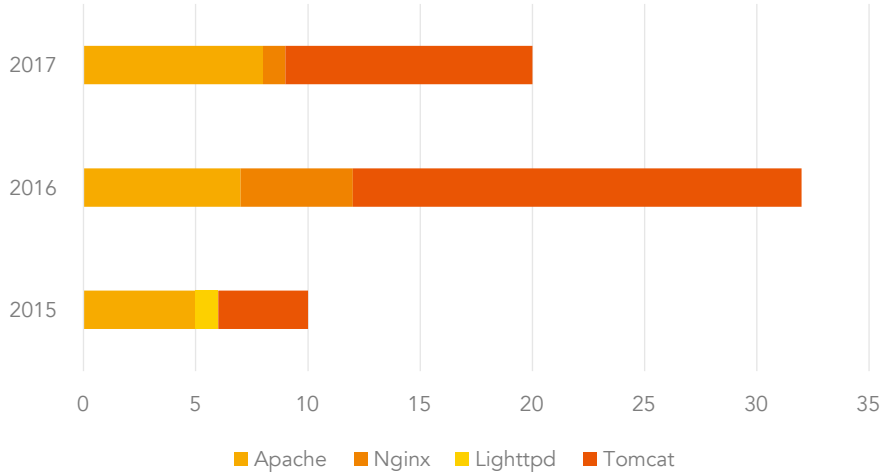
图 14 近三年主流摄像头厂商漏洞数量



3.1.2.4 反序列化漏洞频频出现

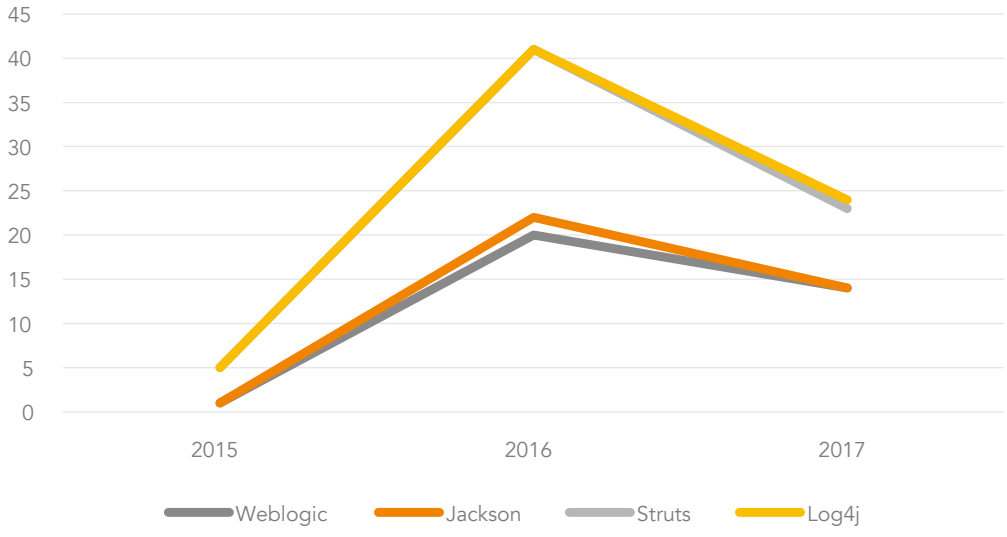
在传统的 Web 服务产品方面，2017 年漏洞总数较 2016 年有下降，主要是 Tomcat 和 Nginx 的漏洞数量较前一年减少了不少。Apache 的漏洞近 3 年轻微上涨，但数量上基本平稳。

图 15 近 3 年主流 Web 服务器漏洞数量



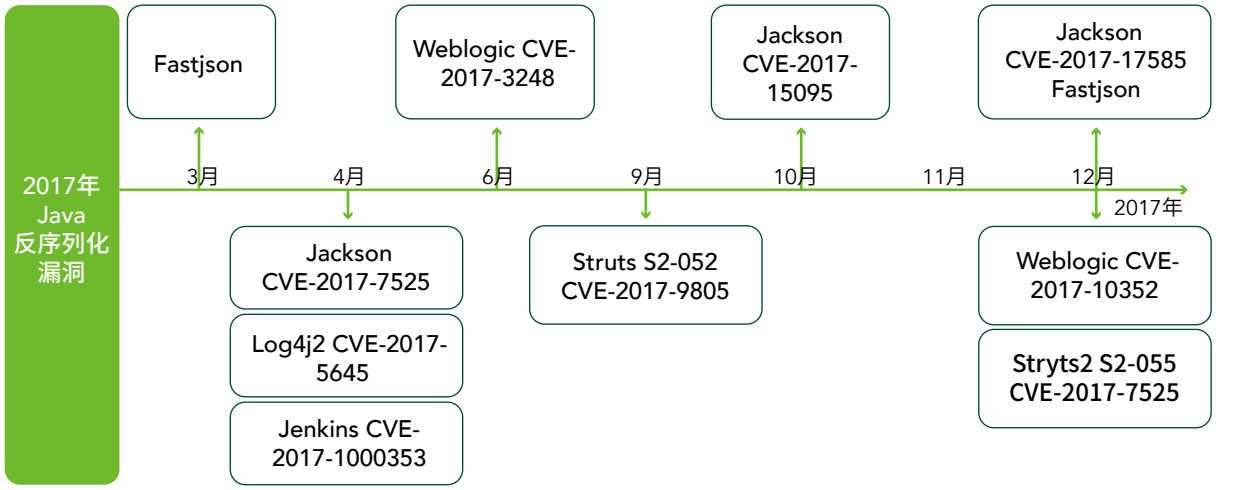
但我们留意到，针对Web服务的攻击中，反序列化漏洞是攻击中是增长最为迅猛的漏洞类型，从漏洞数量来看，2016 年开始就开始大幅度上升，一直到 2017 年，序列化漏洞俨然成为 Web 攻击中的热点。2017 年 OWASP 发布了新的十大 Web 漏洞威胁，其中不安全的反序列化成为排名第八的漏洞类型 ，在我们的视野中，涉及反序列化最主要的 Web 程序包括 Weblogic、Jackson、Struts、Log4j 等。

图 16 常见应用的反序列化漏洞数量变化



所谓序列化，就是将数据对象（例如 Json、XML 甚至高级编程语言中实例化的对象）进行编码，通常这样做的目的是为了通讯上的便利，而反序列化就是将编码后的数据进行还原的过程。Java 语言中的序列化机制支持 Java 对象的序列与反序列化，因此黑客通过反序列化机制能够执行许多复杂的命令，危害较大，加上 Java 的运用范围广，Java 反序列化漏洞收到的关注是最多的。2017 年绿盟科技威胁情报中心持续关注 Java 反序列化漏洞的态势，其中有 10 个反序列化漏洞在今年引起业界高度关注。

图 17 2017 年 Web 组件反序列化漏洞



反序列化漏洞之所以层出不穷的一个重要原因，是厂商针对此类漏洞的修复很“敷衍”，通常是简单地在代码中增加被调用类名的黑名单过滤，另外厂商又要保证功能上的灵活多样，最后平衡的结果就是过滤机制被频频绕过，所以，常常看到的是一个漏洞爆出后快速涌现出更多的漏洞来。从这个意义上，我们建议开发厂商认真对待漏洞的修复，认真定位漏洞成因，引入合理的机制杜绝此类漏洞的发生。

3.2 攻击态势

在这个章节中，报告回顾了攻击者、组织、样本家族的角度，并从不同攻击类型的角度对 2017 年攻防态势进行了总结。从攻击者的角度，我们发现 5 个活动相对频繁的攻击组织，从攻击源来看，我们看到有相当比例的 IP 对多个目标进行攻击，而其中的主要肇事者 IP 仅占了不到 0.5%。我们通过对 2017 年攻防数据的统计，分别对不同的攻击类型进行了讨论，从 Web 类攻击、DDoS 攻击、系统类攻击三个角度进行分析，指出其中关键的趋势与特点。把握 2017 年重点的安全态势，能够帮助我们结合自身业务特点进行业务安全的防御部署，建构自身的防御体系。

3.2.1 活跃的攻击者

3.2.1.1 5 个组织攻击活动频繁

针对 200 多个活跃的攻击者、攻击组织及样本家族，我们对其已知的 IoC 指标进行了监控，其中包括 KeyBoy 后门、HiddenCobra、Carbanak 等多个组织及样本家族曾经有过的频繁活动迹象。另外一系列频发的利用 WebLogic 后门植入挖矿病毒的事件，以及一系列的黑帽 SEO 事件也引起了我们的关注。当然，我们也注意到类似 5 月份黑客伪装成知名组织 APT28 进行攻击的报道，由于这些知名组织的攻击设施已被公开，不排除被其

他攻击者冒充的可能性。

- **WebLogic 后门挖矿病毒**

2017 年 12 月，绿盟科技应急响应团队曾发布《WebLogic 主机感染挖矿病毒威胁预警通告》，12 月前后，绿盟科技应急响应团队接到来自金融、运营商、互联网等多个行业客户的安全事件反馈，发现多台不同版本 WebLogic 主机均被植入了相同的恶意程序，该程序会消耗大量的主机 CPU 资源。我们对该轮事件进行了持续的关注，并结合过往日志数据对该后门程序的传播进行了跟踪。

- **KeyBoy**

KeyBoy 是一个后门程序，常常利用 office 程序的漏洞进行植入。通常黑客通过一个恶意构造的 word 文档，利用 office 特定版本中的后门（例如 CVE-2012-0158、CVE-2015-1641、MS12-060）在目标主机上运行恶意代码，远程下载并植入 KeyBoy 后门。该后门程序的活动在 2013 年 6 月由 Rapid7 首次报道，2016 年 11 月又有相关媒体报道了 KeyBoy 后门变种程序的活动情况。据相关分析，该漏洞被用于进行有组织、有计划的 APT 攻击，KeyBoy 后门能够窃取并利用浏览器证书，以便隐藏可以进行键盘记录、安装交互式的 shell。我们对该后门进行持续监控，今年 6 月该后门的活动出现一个高峰。

- **黑帽 SEO 事件**

在 2017 年 12 月，绿盟科技应急响应团队曾经报道过多起黑帽 SEO 事件。黑帽 SEO 利用高权值网站的二级域名泛解析进行 SEO 推广，在这起事件中超过 50 个主域名受到影响，并且这些推广域名中存在着共同的 IP 指向。我们对黑帽 SEO 相关的访问量进行了持续的跟踪和统计，并对 2017 全年数据进行了分析，发现 11-12 月该类网络流量出现较高峰值。

- **Hidden Cobra**

该组织从 2009 年开始，持续对多个目标实施攻击，攻击行动中，黑客通过窃取数据、或者直接破坏 IT 系统对目标进行打击。另外该组织在不同研究机构的报告中有多个不同的命名，包括 Lazarus Group、Guardians of Peace。该组织具有较为复杂的攻击能力，可以利用僵尸网络发起 DDoS 攻击，并且具备复杂体系化的攻击工具，包括使用 CVE 高级漏洞实现入侵的能力，能够获取主机的控制权限、进行键盘记录、破坏计算机系统数据等。包括 symantec、fireeye、xforce、alienvault、Novetta 等多个安全厂商都对该组织进行了相关的追踪和分析，披露出该组织使用的多个恶意样本以及开展的多次攻击行动，最著名的一次行动是 2014 年针对 Sony Pictures 公司的一次 APT 攻击，随后 Novetta 对该组织进行了一次名为 OperationBlockbuster 的追踪和深入调查的行动。在今年 USCERT 发布多个关于该组织的预警通告和相关技术细节，包括该组织的 DDoS 设施、木马后门等。

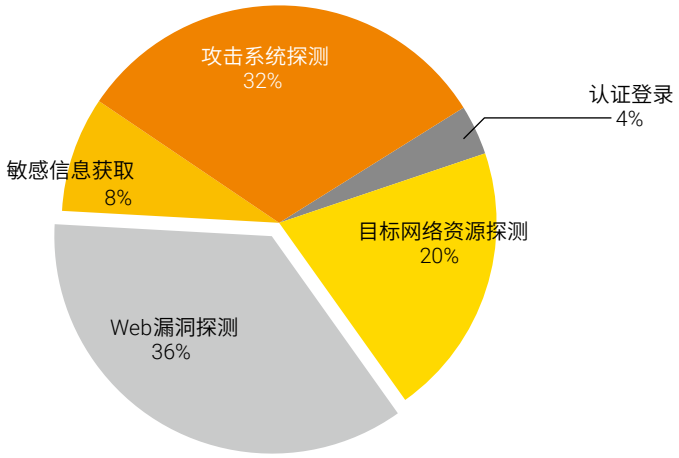
- **Carbanak**

Carbanak 是卡巴斯基实验室 2015 年 2 月公布命名的一个后门程序，主要目标为金融类的组织机构，该后门程序利用 Office 漏洞进行植入，能够窃取目标主机信息的敏感信息，并最终利用机构内的主机实现非法的转账操作，损失累计高达 1 亿美元超过 100 家机构受到影响。

从组织的行为特征看，这类组织在活跃期有大量的扫描探测活动。黑客持续检测目标网络中端口开放的情况以及端口上运行的服务，寻找系统中常见的漏洞，随后针对不同的服务发起不同的攻击测试。这些常见的测试包括，针对 Web 类的 SQL 注入、跨站、路径穿越、常用插件漏洞利用等，而针对系统类的攻击中，会针对敏感的服务进行认证登录、密码爆破等测试，对其他常见服务的高危漏洞也会进行初步的探查。不幸的是，很多情况下，

企业管理员会忽略这样的行为，因为这类探测在日常业务中非常的普遍，但就是这些看起来非常普通的探测，为后续的 APT 攻击提供了非常有价值的资料。 所以，在日常繁杂的日志中利用威胁情报识别这类 IP，进而提炼出与特定组织、样本家族有关的关键告警，是安全运维方面值得投入和认真对待的事情。

图 18 APT 组织对互联网资产漏洞试探行为

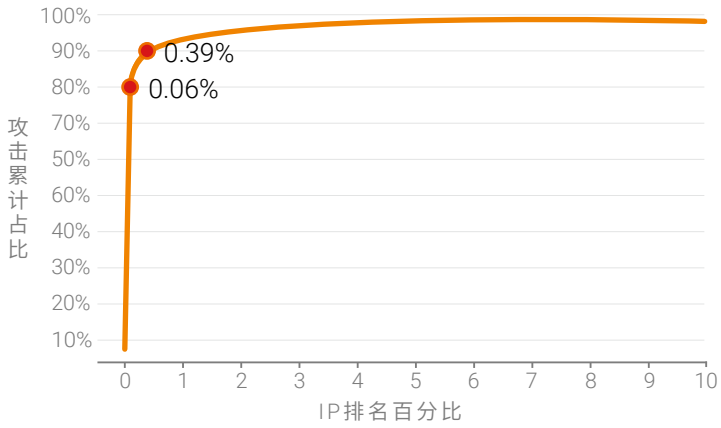


根据绿盟科技的观察，组织机构对自身资产确实缺乏长期系统的运维管理。例如在 2017 年 10 月进行的一次关于金融行业的资产扫描检查中发现，在绿盟科技所接触的客户主机中，至少存在着高达 6% 的主机资产没有进行过合理的配置，有开发、调试后进入闲置状态的主机并未下线，反而长期在线开放着处于默认配置状态，没有进行任何权限控制的网络服务，有的主机则开放了高敏感服务的端口，例如将 SSH、Telnet、RDP、VNC 等远控服务的端口暴露于公网，甚至使用弱密码进行登录，另外一部分主机则把重要的数据资产，包括 Mongo 服务器、Elasticsearch 服务器、Mysql 服务器等未加控制地进行对外开放，这些安全疏漏是非常令人担忧的。这样的安全问题，不在于安全技术水平，而在于管理方法、安全意识的提升。

3.2.1.2 约 20% IP 对多个目标进行过攻击，0.39% 攻击源对 90% 的攻击事件负责

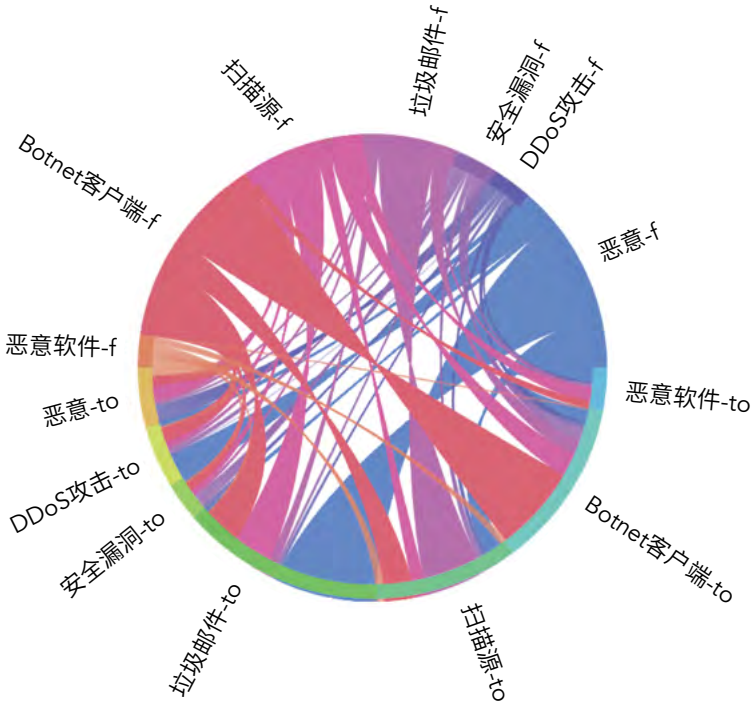
2017 年我们持续监控的攻击源 IP 中，有 390 多万个活跃的攻击源，其中 20511 个参与了多种类型的攻击活动，例如 DDoS 攻击、僵木蠕传播、恶意扫描、网站及其他网络服务的漏洞利用等。数据显示，这批 IP 轮流参与到针对不同目标、不同类型的攻击且活动频繁，是网络环境中的“惯犯”。虽然这些 IP 不一定固定属于某个黑客组织，但是由于 VPS 租用商、主机拥有者对自身资产的监管不严，导致这些设备受到黑客控制的频率相较其他 IP 要高出许多，几乎成为了黑客攻击的“固定资产”。这批 IP 占比不高，但是却在网络中引起了不少的麻烦和混乱，我们注意到这样一个现象：大约 20% 的 IP 对多个目标进行过攻击，0.39% 的攻击源对 90% 的攻击事件负责。

图 19 大量攻击事件集中来源于一批 IP 攻击源



在对这批 IP 的持续关注中，我们还发现，不同类型的攻击源之间存在着一些转换规律，例如一个参与垃圾邮件攻击的 IP 有超过 90% 的概率会在互联网进行恶意扫描，而 Botnet 客户端主机与多种类型的攻击存在关联，最常见的行为就是进行恶意扫描，此外也包括垃圾邮件、网络钓鱼等恶意行为。

图 20 攻击源类型变化规律



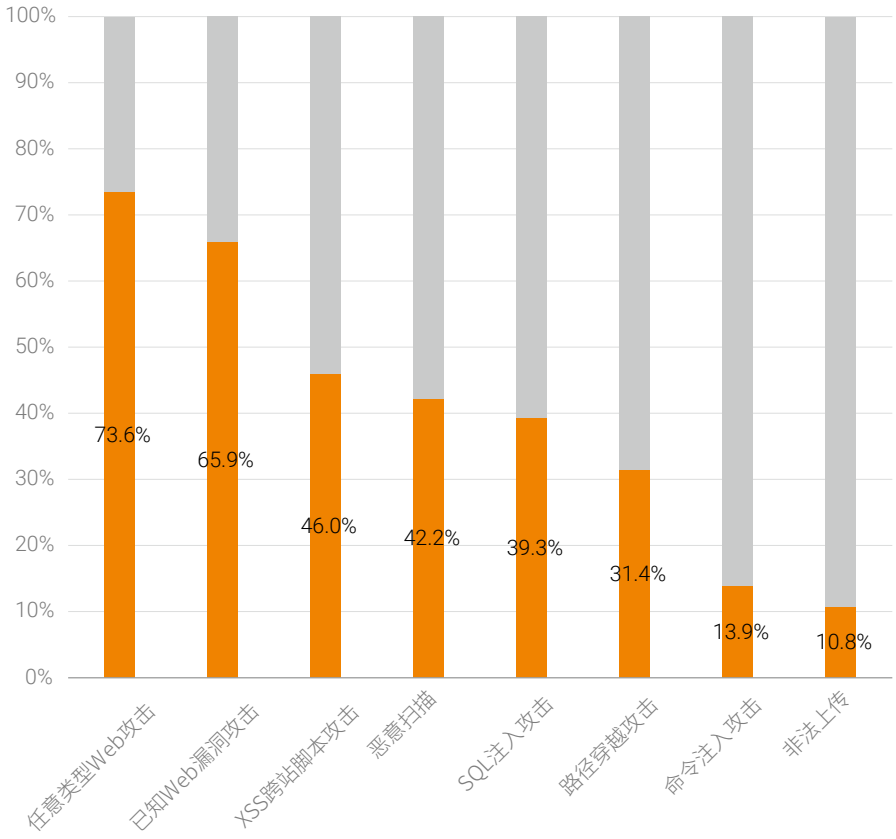
对于这批高危 IP，我们建议可以基于威胁情报直接阻断此类网络行为，以便有效减少日常业务维护中的防御负担。

3.2.2 Web 类攻击

3.2.2.1 76% 的网站曾经被攻击

通常来说，企业在互联网上暴露最多的资产就是网站，这导致 Web 攻击成为最常见的攻击之一。观察大量黑客技术论坛及脚本工具，最常见的话题之一就是与 Web 攻击相关的各类讨论。而 SQL 注入、XSS 跨站等攻击手法相对其他针对协议漏洞、程序漏洞、内存溢出的攻击，实施难度和学习成本都比较低。我们观察到 76% 的网站在一年中至少遭遇到一次攻击，当然，如果把视角聚焦到互联网业务领域，其网页是重要的交互渠道，在这种场景下，遭遇攻击几乎是必然的事情。

图 21 遭受 Web 应用攻击的站点占比

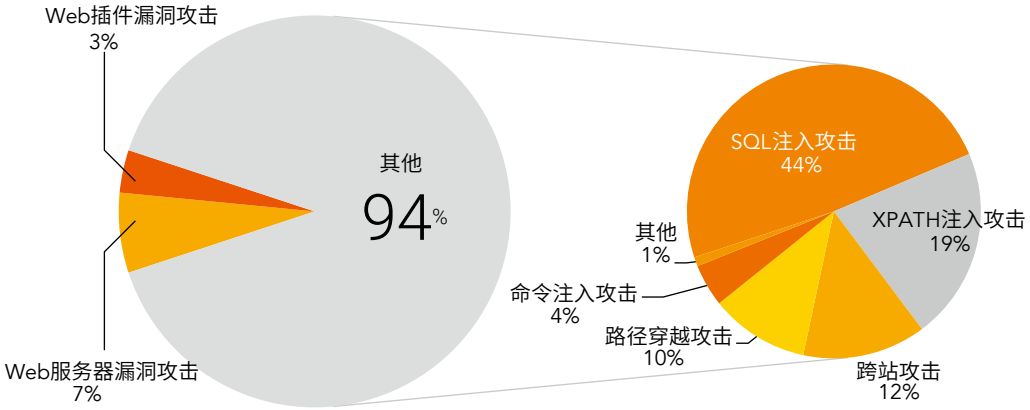


数据来源：中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》

3.2.2.2 传统攻击手段仍然有效

在针对 Web 服务器的攻击中，90% 的攻击仍然是一些最常规的攻击手段，包括 SQL 注入、XPATH 注入、跨站、路径穿越、命令注入等。Web 攻击已经成为一个基本的攻击手段，也是各类攻击中相对容易实施的。虽然近几年来，Web 攻击已经为大众所熟知，但是具体到业务环境中的管理，Web 攻击防御仍然存在很多的问题，所以，黑客也乐意从 Web 应用作为内网突破的入口。从持续不断的攻击行为中，我们看到传统的攻击手段仍然有效的，并且在企业每天面临的攻击中占最多的比例，仍然需要细致的防护。

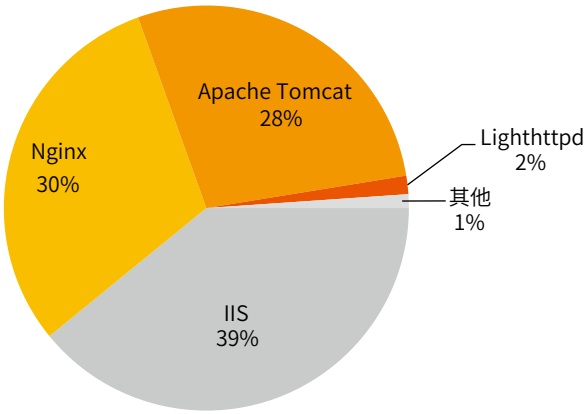
图 22 Web 类攻击类型细分



3.2.2.3 三类 Web 服务器最受关注

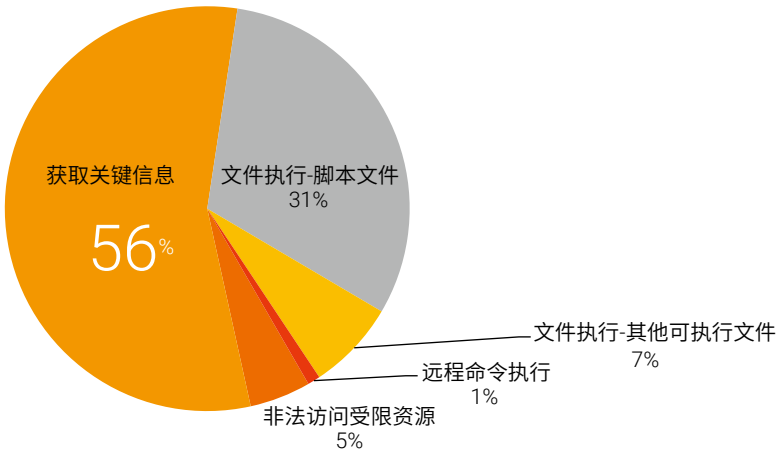
从类型分布上看，受攻击最多的 Web 服务器主要有三类：Apache Tomcat、Nginx、Microsoft IIS。

图 23 受攻击的 Web 服务器类型



从攻击手段上看，大部分的漏洞利用能够导致关键信息的泄露，这包括对目录文件的枚举、文件路径的泄露以及网站脚本文件源码泄露、系统配置文件信息被读取等情况，这部分攻击占全部攻击的 56%。另外一类显著的攻击方式是文件执行类的攻击，这类攻击，通常会利用服务器程序对 URL、文件名解析的缺陷并结合文件上传功能，将上传的文件作为脚本运行，利用 Webshell 实现进一步的入侵操作。此外，还有一部分攻击能够越权访问受限的资源，在受限的目录位置进行文件读取、下载、上传操作，甚至直接执行目录中的可执行文件。

图 24 Web 服务器最常被利用的漏洞类型分布



值得注意的是，与《2017 上半年网络安全观察报告》提到的趋势一致，在对 Web 服务器的攻击中，黑客最常使用的漏洞是一些非常“古老”的漏洞，例如被利用排名前 5 的漏洞 CVE 编号分别为：

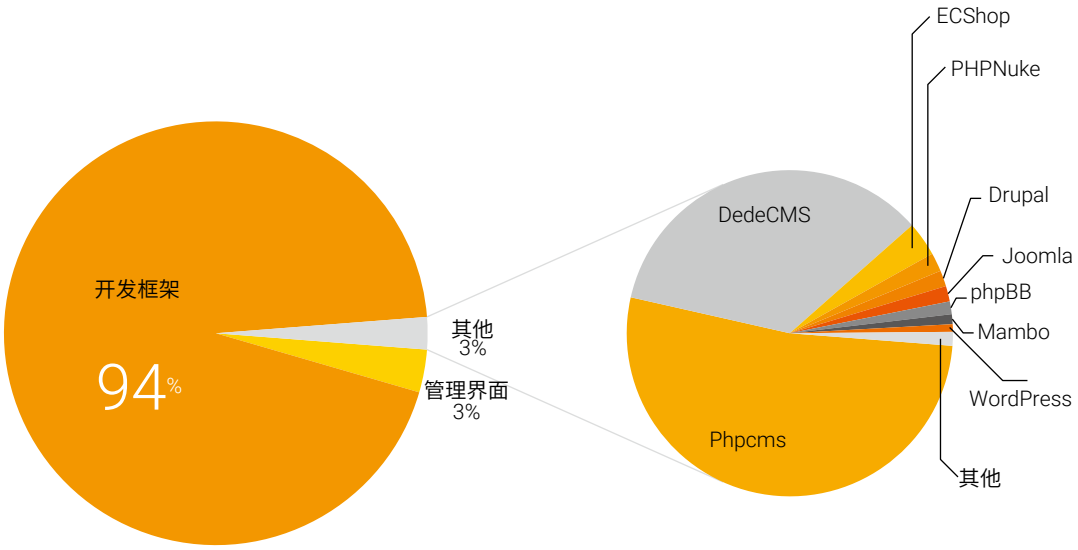
表 2 Web 攻击中利用次数排名前 5 的漏洞

漏洞名称	漏洞描述	产品
CVE-2008-2938	当启用 allowLinking 及 UTF-8 时，Tomcat 在处理请求的编码时存在漏洞，远程攻击者可通过提交包含经编码的目录路径，读取服务器上的任意文件。	Apache Tomcat
CVE-1999-0253	IIS 是通过文件扩展名来决定将一个文件内容直接显示出来还是作为脚本执行的。对于 asp 文件，如果请求中的扩展名是“.asp”那么 IIS 可以正确处理。如果将扩展名后面加一个“.”或者编码为“%2e”，IIS 讲不认为这是一个 ASP 文件而会直接显示出文件内容。但是文件系统会忽略文件名后的“.”，可以正确找到文件。	Microsoft IIS
CVE-2009-4445	可利用此漏洞上传一些可执行文件。	Microsoft IIS
CVE-2009-4444	可利用此漏洞上传一些可执行文件。	Microsoft IIS
CVE-2000-0886	Microsoft IIS 4.0/5.0 在处理 CGI 程序 (.exe, .pl, .php 等等) 时 , 对用户请求的 CGI 程序名没有做完整的安全检查。如果文件名中包含一个特殊字符，可能导致 IIS 错误地打开或者执行文件。	Microsoft IIS

3.2.2.4 Web 框架是攻击中重点针对的对象

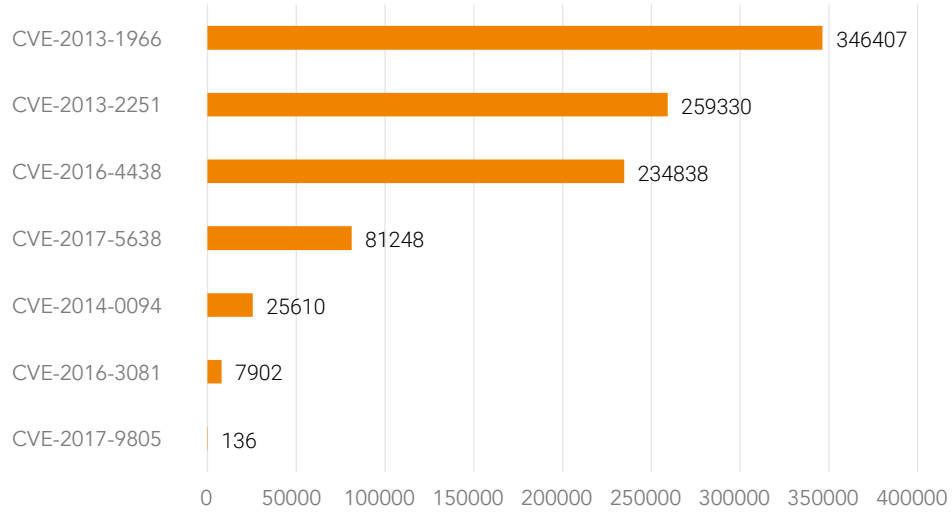
这里 Web 应用所指的范围包括各类建站软件，例如以 PHP、JSP、ASP 语言搭建的各类 CMS，也包括一些特殊的以管理为目的的一些界面，例如著名的 phpMyadmin、各类非关系型数据库的 Web 访问界面等。

图 25 最常被攻击的 Web 应用



Web 框架是指一类用于构建 Web 程序的框架类程序，用来支持动态网站、网络应用程序及网络服务的开发，很多通用型的 Web 业务系统也是基于类似的架构进行开发的，常见的框架包括 Django、ThinkPHP、Apache Struts、Spring 等。在统计中，我们看到对框架类程序的攻击是最频繁的，其中 Struts 漏洞是其中的典型代表，此外 ThinkPHP、Spring 框架也受到较多的攻击。下图是 Struts 框架受攻击次数最多的几个漏洞。

图 26 Struts 漏洞受攻击情况

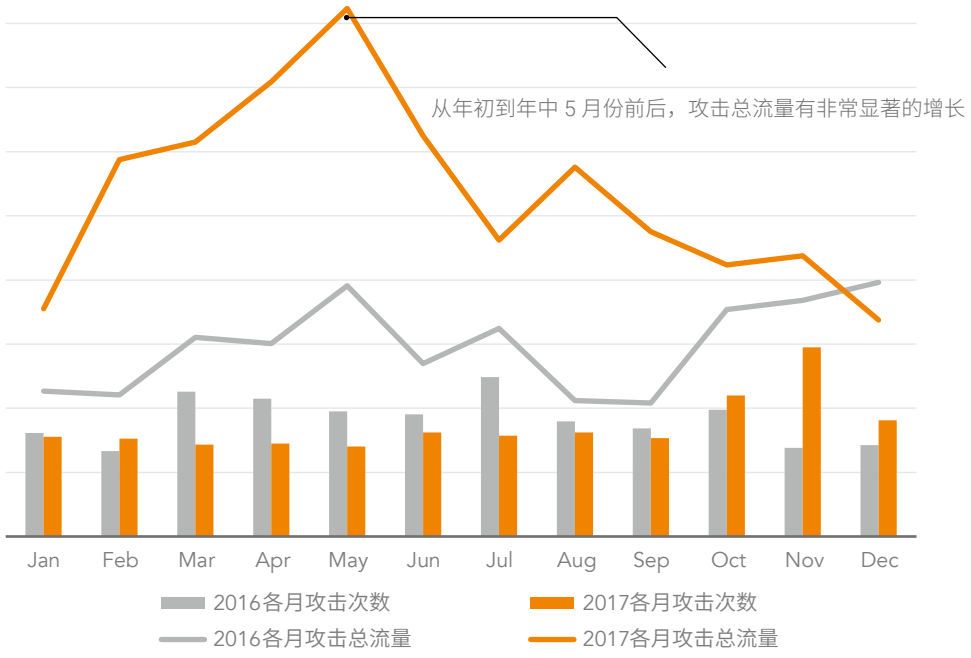


3.2.3 DDoS 攻击

3.2.3.1 攻击仍然频繁，共发生 20.7 万次攻击

2017 年同去年同期相比，攻击发生次数基本保持平稳，共计发生 20.7 万次。但是从攻击总流量上来看有较为明显的波动，从年初到年中 5 月份前后，攻击总流量有非常显著的增长，而 5 月份之后攻击总流量回落至较为平稳的水平。与 2016 年相比，2017 攻击仍然频繁，攻击总流量大幅上升。

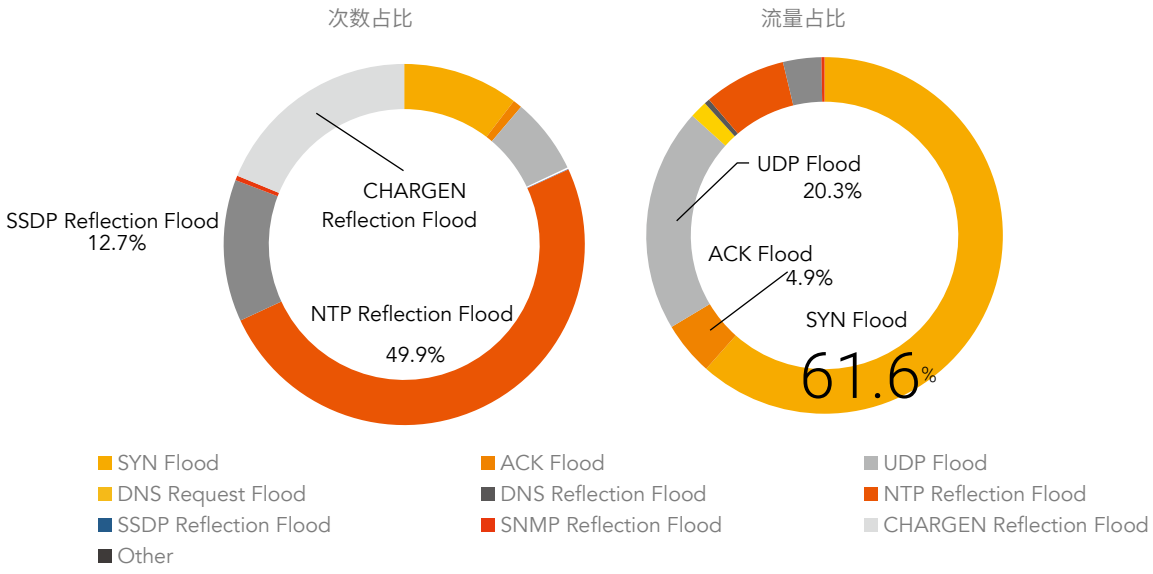
图 27 2017 年 vs.2016 年各月份攻击次数和流量



数据来源：中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》

从类型上看，2017 年攻击次数占比最高的攻击类型仍然为反射型攻击，实施这类攻击，黑客只需要拥有很少的带宽，就能经过放大产生显著的攻击流量。从攻击流量的上看，SYN Flood 今年占比突出，超过 60%。综合今年网络环境分析，我们认为与今年物联网僵尸网络的扩张大有关系，物联网设备基数大、防护弱、长时间在线的特点，天然就是发动 DDoS 攻击的温床。

图 28 DDoS 攻击类型分布

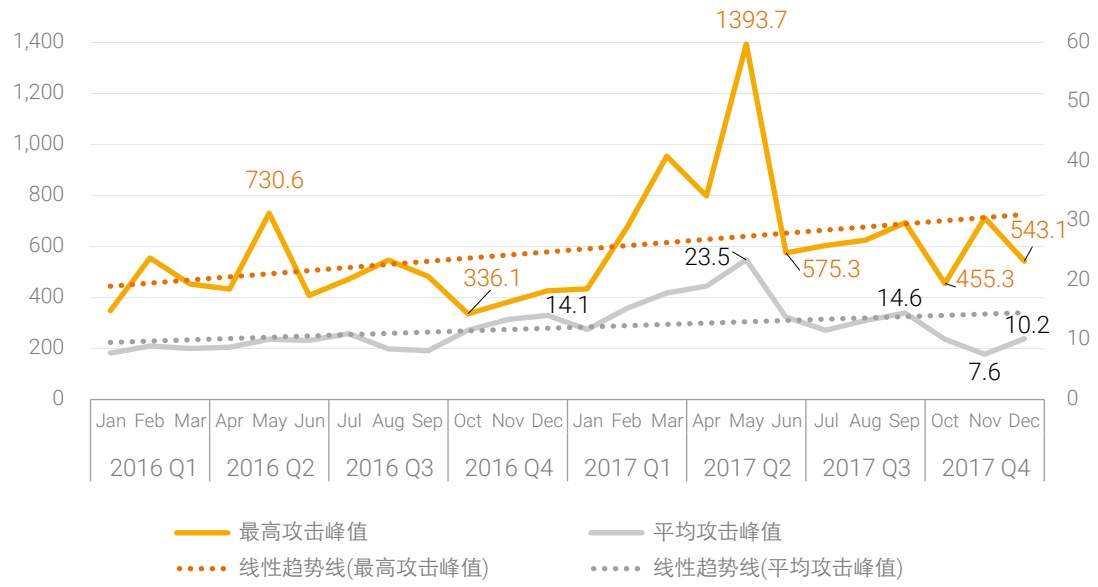


数据来源：中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》

3.2.3.2 攻击峰值再创新高，最高可达 1.4Tbps

流量持续攀升似乎已经不是什么新的态势，从近两年的报告中都可以看到，每个月都会出现超过百 Gbps 的流量，最高的时候流量已经出于 Tbps 的级别，今年在攻击最频繁的 5 月，攻击最高的峰值更是达到了 1.4Tbps 的级别，这种“巨无霸”攻击，一次一次挑战着防御者的能力上线。

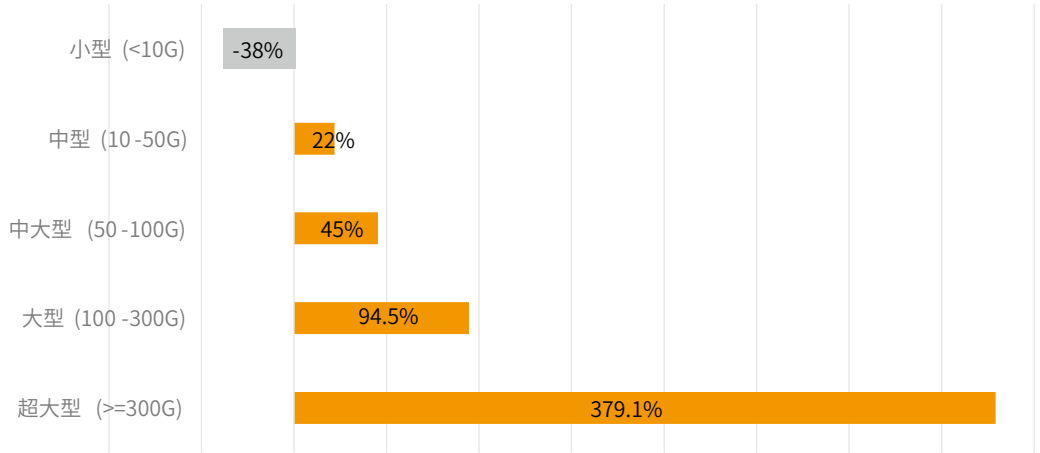
图 29 各月份单次攻击峰值及平均攻击峰值趋势图（单位 :Gbps）



数据来源：中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》

另外，从流量的区间分布来看，大流量攻击明显增多，也是今年一个显著的趋势。

图 30 2017 年 vs.2016 年各攻击峰值区间攻击增长（减少）率

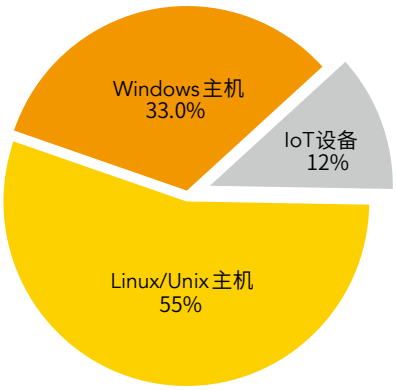


数据来源：中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》

3.2.3.3 来自 IoT 设备的攻击比例达到 12%

在 2017 年的 DDoS 攻击中，攻击源中 IoT 设备的数量已经占据相当的比例，在或大或小规模的 DDoS 攻击中 IoT 设备都有显著的占比，已经成为 DDoS 网络环境中需要重点关注的一个类别。从网络总体态势来看，物联网迅猛发展的过程中必然伴随着安全技术的滞后，可预期 IoT 设备的威胁会进一步提上治理日程，而作为最易实施的攻击类型之一，DDoS 攻击中 IoT 设备的数量会进步增长。

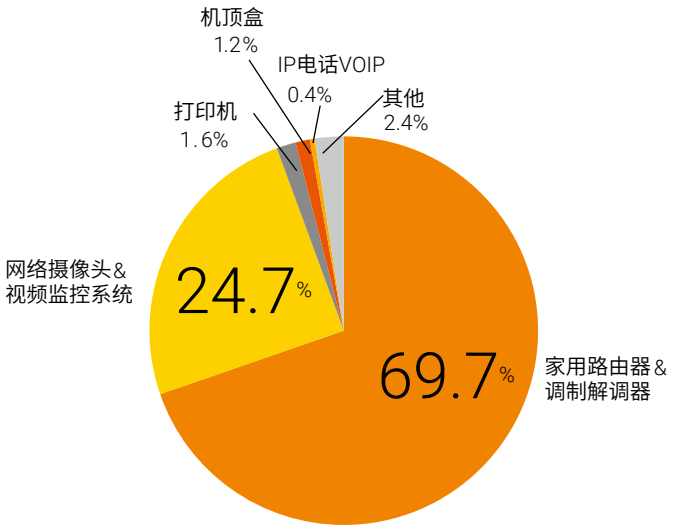
图 31 DDoS 攻击源设备类型分布



数据来源：中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》

在 IoT 设备参与 DDoS 的攻击中，路由器、摄像头是主要的设备类型。这与这两年 IoT 发展的情况基本是一致的，大量的路由器、网络摄像头被引入生产、生活环境，而安全配套措施尚未进一步完善，可以合理预期的是在物联网攻击这个领域会有更多的攻击形式出现。

图 32 DDoS 攻击源 IoT 类设备具体类型分布



数据来源：中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》

由物联网设备引发的 DDoS 攻击行为延展开去，我们还持续追踪并记录了物联网设备引发的其它恶意行为，并为全球物联网设备的总体恶意 IP 做了一个平均基准线，随后惊异的发现，摄像头恶意 IP 比例大幅度跃出，占比为 4.8%，是平均水平的 3 倍多。

3.2.3.4 新型反射型攻击 Memcached 具有强大的攻击能力

2018 年年初一种新型的反射攻击——Memcached 反射放大攻击，引发各方关注。根据相关报道 ，2018 年 2 月 28 日，Memached 反射型攻击曾经达到 1.35Tbps 级别的攻击量级，其攻击能力相当惊人。Memcached 是一个高性能的开源分布式内存对象缓存系统，主要用于提高 Web 应用的扩展性，能够有效解决大数据缓存的很多问题，在全球范围内都有广泛使用。Memcached 基于内存的 key-value 存储小块数据，并使用该数据完成数据库调用、API 调用或页面渲染等。攻击者正是利用 key-value 这项功能构造了反射攻击。从各类反射型攻击的放大倍率来看，Memcached 高居榜首，最高可达 51000 倍：

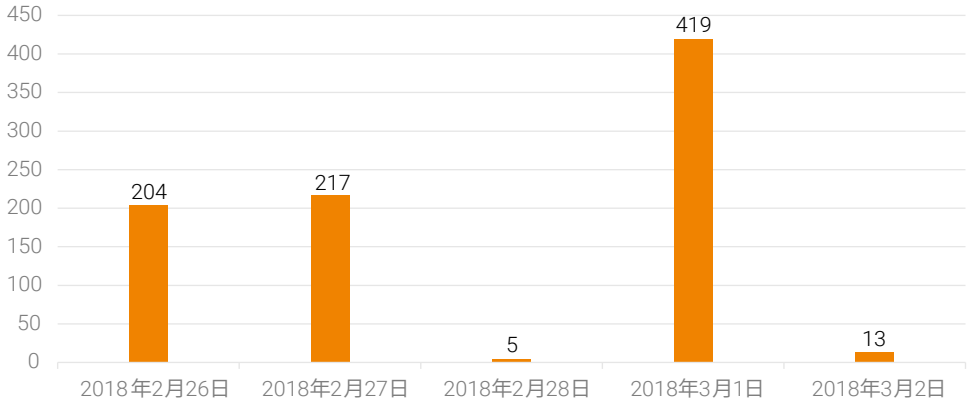
表 3 各类反射攻击放大倍 [1]

反射攻击针对的协议	带宽放大倍数
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP	56 to 70
TFTP	60
Memcache	10,000 to 51,000

1 https://www.us-cert.gov/ncas/alerts/TA14-017A

根据中国电信云堤的数据显示，从周一至周五（2 月 26 日至 3 月 2 日 06:00）短短 5 天内，全球就发生了 79 起利用 Memcached 协议的反射放大攻击。日攻击总流量最高达到 419TBytes。

图 33 Memcached 反射放大攻击日攻击总流量



数据来源：中国电信云堤与绿盟科技联合发布报告《深度剖析 Memcached 超大型 DRDoS 攻击》

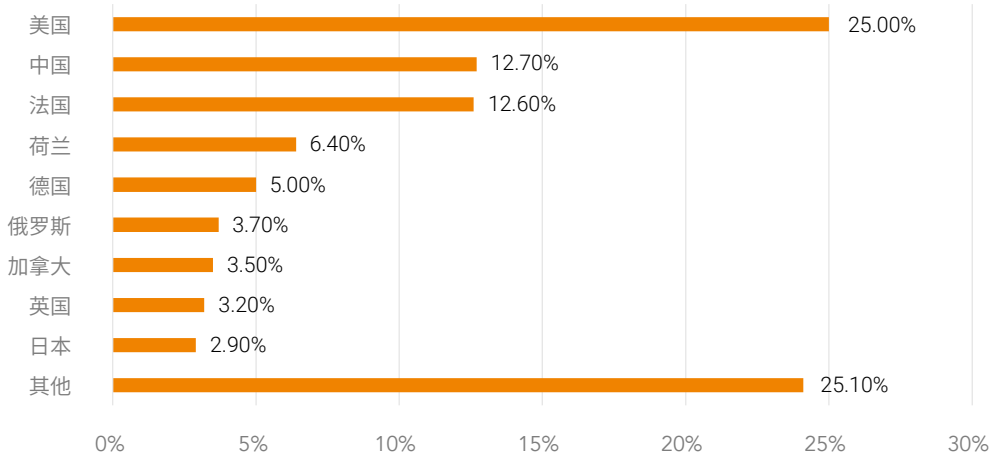
其中，针对我国境内的 Memcached 反射放大攻击就有 68 次，江苏、浙江两省被频繁攻击。针对我国境内的攻击，单次攻击最高攻击峰值达 505Gbps。攻击持续时间最长的一次发生在 3 月 1 日，持续 1.2 小时，总攻击流量达 103.8TBytes。

图 34 中国各省份地区 Memcached 反射放大攻击次数

数据来源：中国电信云堤与绿盟科技联合发布报告《深度剖析 Memcached 超大型 DRDoS 攻击》

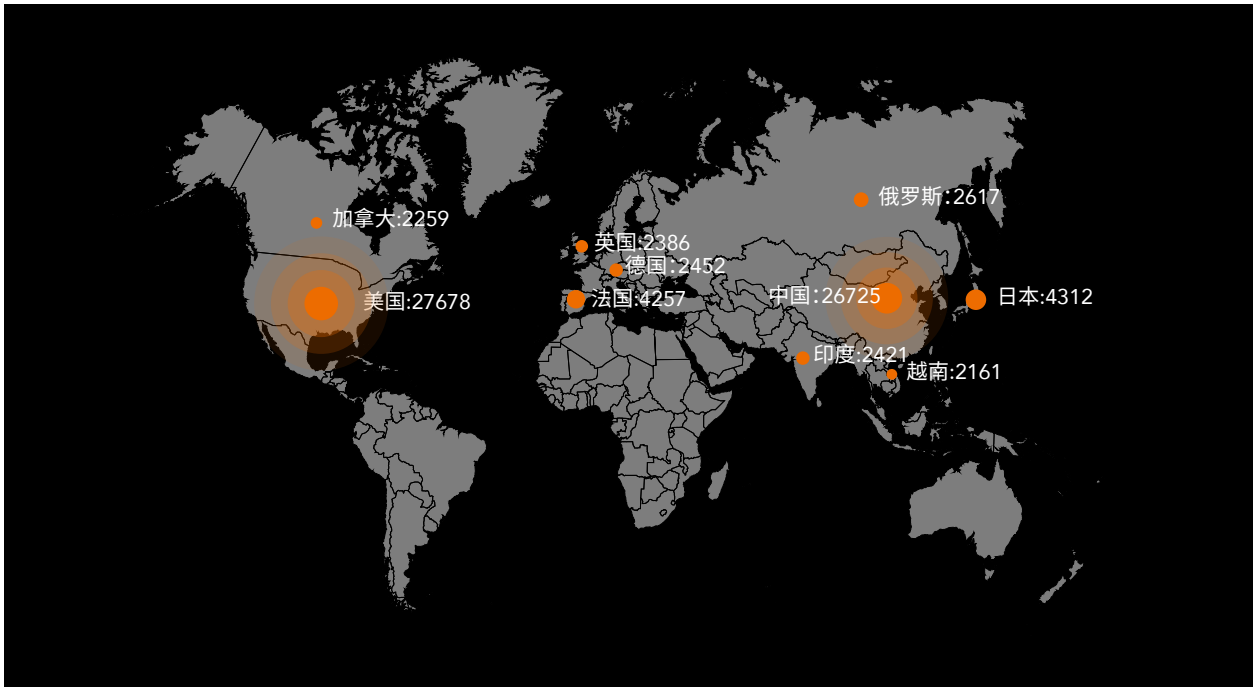
全球总共有 3790 个 Memcached 服务器被利用并参与到这些 Memcached 反射放大攻击。这些被利用反射源遍布于全球 96 个国家或地区，其中，美国境内的反射源就占了全球的 1/4。分布在中国地区的被利用的 Memcached 服务器位列第二位，占比 12.7%。

图 35 Memcached 反射攻击源全球各国家分布占比



数据来源：中国电信云堤与绿盟科技联合发布报告《深度剖析 Memcached 超大型 DRDoS 攻击》

绿盟威胁情报中心（NSFOCUS Network Threat Intelligence，简称 NTI）的统计结果显示，全球范围内存在被利用风险的 Memcached 服务器达 104,506 台。从地理分布来看，美国可被利用的 Memcached 服务器最多，其次是中国。



数据来源：绿盟威胁情报中心

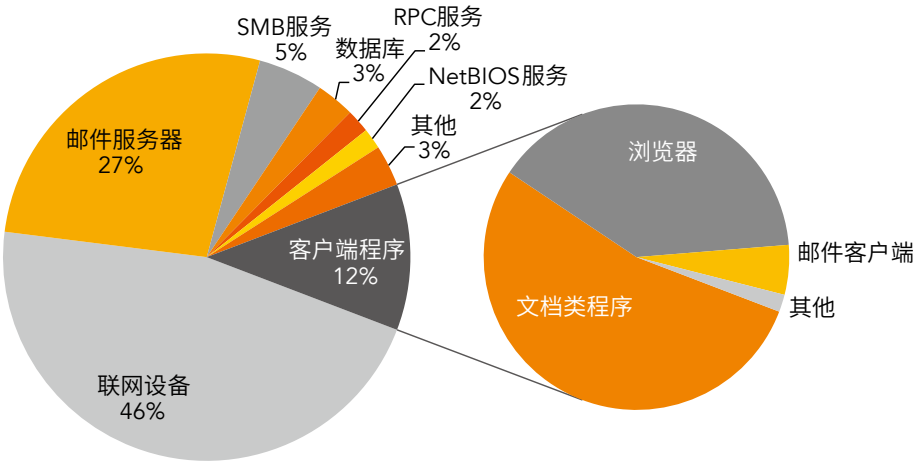
大量的可利用的 Memcached 反射器为构造超级反射放大攻击 DRDoS 提供了有力的先决条件。如果不及时修复治理，预计基于 Memcached 反射攻击的攻击事件会继续增加，后果不敢想象。

从攻击影响范围来看，所有互联网的业务都可能成为 Memcached DRDoS 的攻击对象。一方面带宽或业务遭受超大流量的攻击，导致出口带宽完全被占满，正常业务无法访问；另一方面企业内部的 Memcached 系统可能被不法分子利用成为攻击帮凶。我们呼吁各地区、各行业客户保持高度警惕，谨防 Memcached 反射攻击对服务器造成直接冲击，或利用 Memcached 反射攻击作为障眼法，混合其他攻击造成信息安全危害。关于 Memcached DRDoS 的具体的防护和加固建议请详见[2]《深度剖析 Memcached 超大型 DRDoS 攻击》。

3.2.4 系统类攻击

从常见的网络产品与服务的来看，针对服务端的攻击占比 88%，针对客户端的攻击占比 12%，在所有针对服务端的攻击中，我们看到一个非常明显的趋势，有 46% 的攻击是针对一些联网设备，例如路由器、打印机等。另外针对邮件服务器的攻击占比也达到 27%，这部分攻击中大部分操作是利用邮件服务发送垃圾邮件的操作。在客户端程序侧，我们看到文档类程序、浏览器程序、邮件客户端程序是受攻击最严重的三类程序。文档类程序是指文本图像处理、阅读软件，包括 Microsoft Office、Adobe Reader、流媒体播放器等。浏览器程序包括 Firefox、Microsoft Edge、Microsoft IE 等，都是常受到攻击的应用程序。

图 36 系统类攻击针对的产品与服务



3.2.4.1 “影子经纪人”披露导致众多高危攻击事件

影子经纪人（英语：The Shadow Brokers，缩写：TSB），是 2016 年夏季出现的一个黑客组织，它发布了包括美国国家安全局的黑客工具在内的数个漏洞，其中包括数个零日攻击。这些漏洞针对企业防火墙、杀毒软件和微软软件。影子经纪人称这些漏洞来自与美国国家安全局特定入侵行动办公室有关的方程式 Equation 组织。其中永恒之蓝 EternalBlue 工具所包含的 Windows SMB 服务漏洞被用于 WannaCry、Petya、BadRabbit 勒索软件的传播与攻击，引起了非常大的社会关注。在所有的攻击中，“影子经济人”相关的攻击占比为 3.47%，但是攻击的潜在危害却是最大的。在这些攻击中：

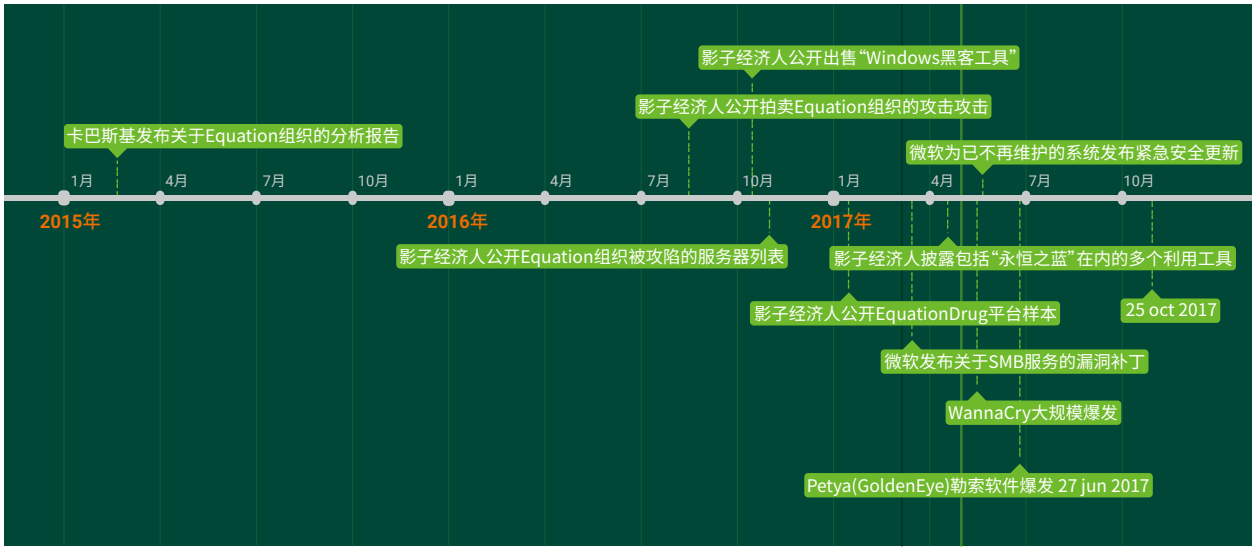
2 http://blog.nsfocus.net/memcached-drdos-analysis/

- 针对 Windows SMB 的攻击占所有攻击的 89.8%。在“影子经济人”披露的各类工具中针对 SMB 的利用和攻击是最多的，包括著名的永恒之蓝 EternalBlue、永恒冠军 EternalChampion、永恒浪漫 EternalRomance 等。

- 后门工具 Darkpulsar 的活动占比 3%。Darkpulsar 是一个简单的后门程序，该后门的功能相对较少，主要功能有执行 shellcode 和加载 DLL。为以后植入复杂的后门做准备。

- 此外，还有一定数量针对 Windows RPC、Windows RDP 服务的攻击。黑客利用工具进行攻击后，都能够取得系统的控制权限植入后门，为进一步入侵做准备。

图 37 影子经济人重大事件



从上图可以看到从 2016 年 8 月，影子经济人逐步地拍卖或者出售从 Equation 组织获取到的黑客工具，一直到 2017 年 4 月，影子经济人在互联网上集中披露了一批利用工具，这批工具中就包括了后来影响恶劣的 EternalBlue，工具中包含的 SMB 服务漏洞被三个家族的勒索软件大肆利用，包括 5 月爆发的最著名的 WannaCry 勒索软件，6 月底爆发的 Petya（又称 GoldenEye）勒索软件和 10 月爆发的坏兔子 BadRabbit 勒索软件。这些勒索软件所利用的漏洞其实早在今年 3 月中旬就已被微软修复并发布了相关补丁，但直至 10 月，勒索软件仍然能够顺利利用这个漏洞进行大规模的传播。

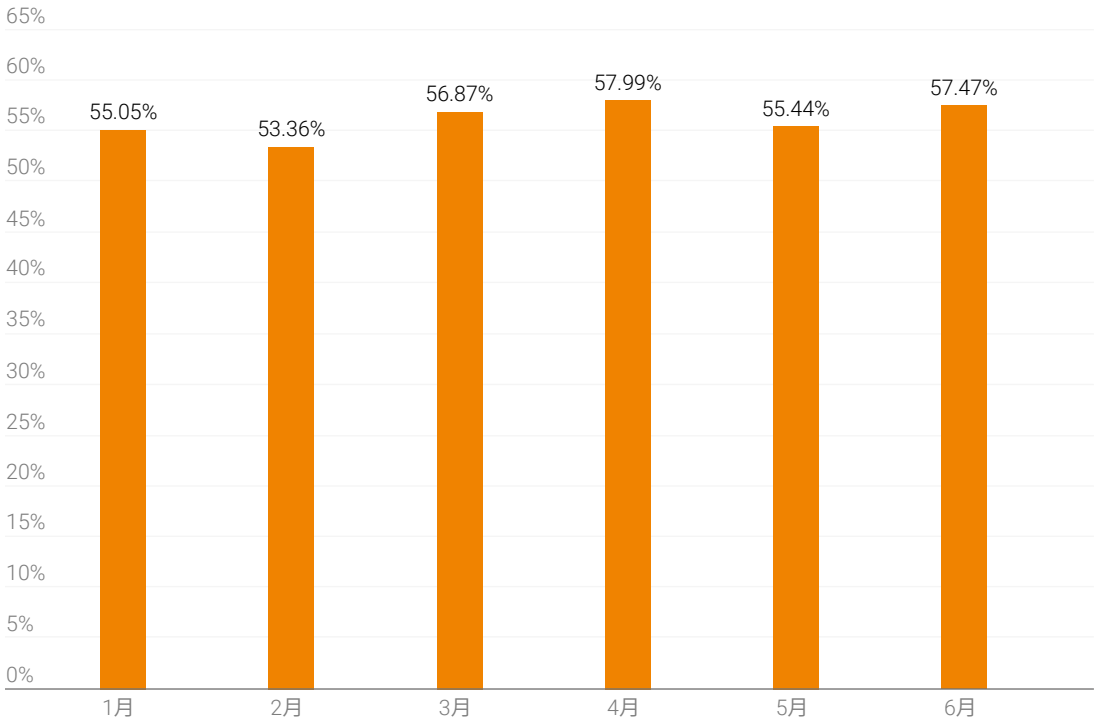
3.2.4.2 邮件成为攻击的重要入口

近年来，多种传播广泛的恶意代码，都将恶意邮件作为重要的传播途径之一。恶意邮件使用社会工程学手段，诱骗用户打开恶意附件中的文件、点击恶意网站链接，进而使用户感染加密勒索软件、木马软件等多种类型的病毒，造成直接的经济损失。据报道，今年经由臭名昭著的垃圾邮件僵尸网络 Necurs 投递的 Jaff、Locky 勒索软件在今年仍然非常活跃 [3]。另外，针对企业的恶意邮件攻击变得常见，并且存在巨大的利益空间，有的直接诱导用户透露关键信息、执行转账操作，就造成严重的经济损失。据统计 [4]，企业电子邮件攻击 BEC 攻击造成的经济损失甚至比勒索软件还要巨大。

3 数据来源于 Proofpoinf：https://www.bleepingcomputer.com/news/security/ransomware-was-the-most-prevalent-malware-payload-delivered-via-email-in-q2-2017/

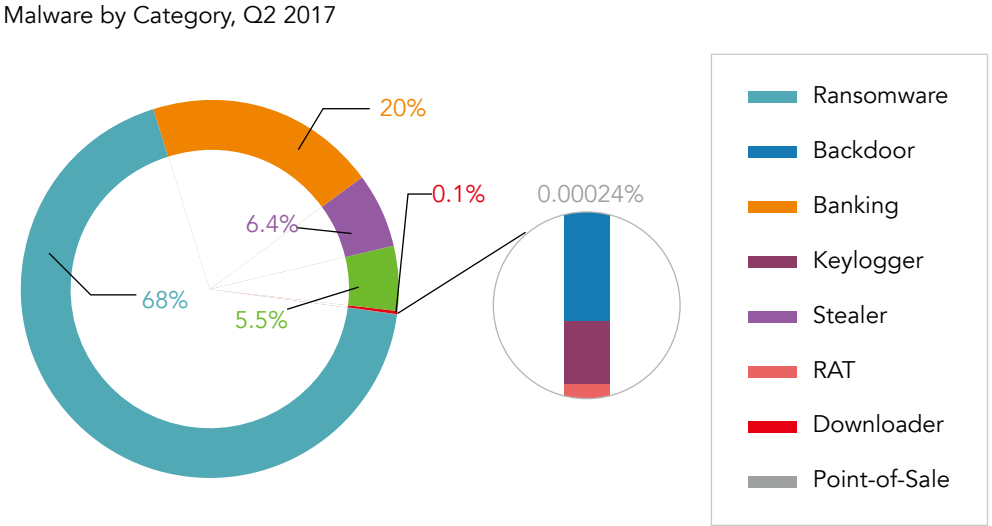
4 数据来源于 NTTSecurity 报告 : https://www.nttsecurity.com/en-us/gtir-2017

图 38 恶意邮件在邮件通信中的占比情况



数据来源：https://securelist.com/spam-and-phishing-in-q2-2017/81537/

图 39 多种类型的恶意软件经由恶意邮件进行传播



数据来源：Proofpoint: https://www.bleepingcomputer.com/news/security/ransomware-was-the-most-prevalent-malware-payload-delivered-via-email-in-q2-2017/

3.2.4.3 Netcore 僵尸网络攻击非常频繁

从攻击的统计中我们看到，针对联网设备的攻击高达 46%，其中绝大部分的攻击是针对路由器设备的。在我们今年的监测中，有一个家族的僵尸程序攻击非常猖獗，其针对的设备是早在 2014 年就被趋势科技通报存在固件后门的 Netcore（中文名为磊科）路由器设备。这款设备强制开启了一个管理接口（用户很难关闭或禁止），并且该管理接口设置的密码是统一的硬编码口令，只要设备可以被访问，就能被黑客控制。在早期的报道中，普遍认为该漏洞可以用作“中间人”攻击，直到近期的攻击监测中我们发现，使得该漏洞被广泛运用的要归功于一个命名为 Gafgyt 的僵尸家族。从 2017 年年初 3 月开始，我们就监控到该僵尸网络的大规模活动，且持续到年底并未有任何减缓的趋势。

图 40 Gafgyt 利用路由器后门进行攻击的事件统计

不论从地理、行业分布来看，网络环境中受该僵尸网络的影响范围是非常广的。正是利用了 Netcore 的后门，Gafgyt 僵尸程序才得以大规模地进行传播。从漏洞公布到现在，历时 3 年，互联网上仍然存在相当多未经修补的设备。

图 41 Gafgyt 僵尸网络攻击针对的行业分布

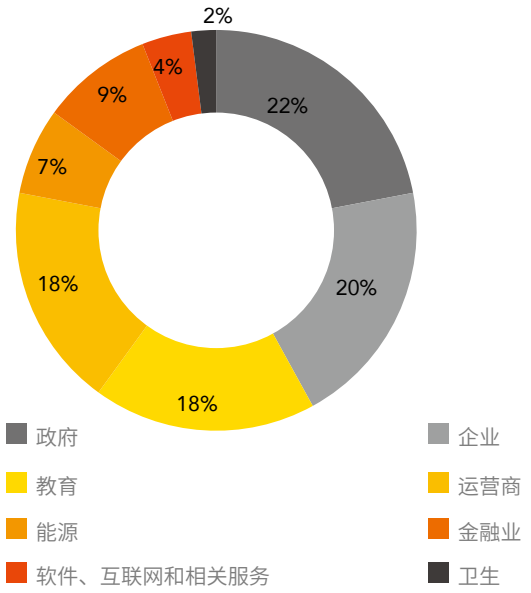
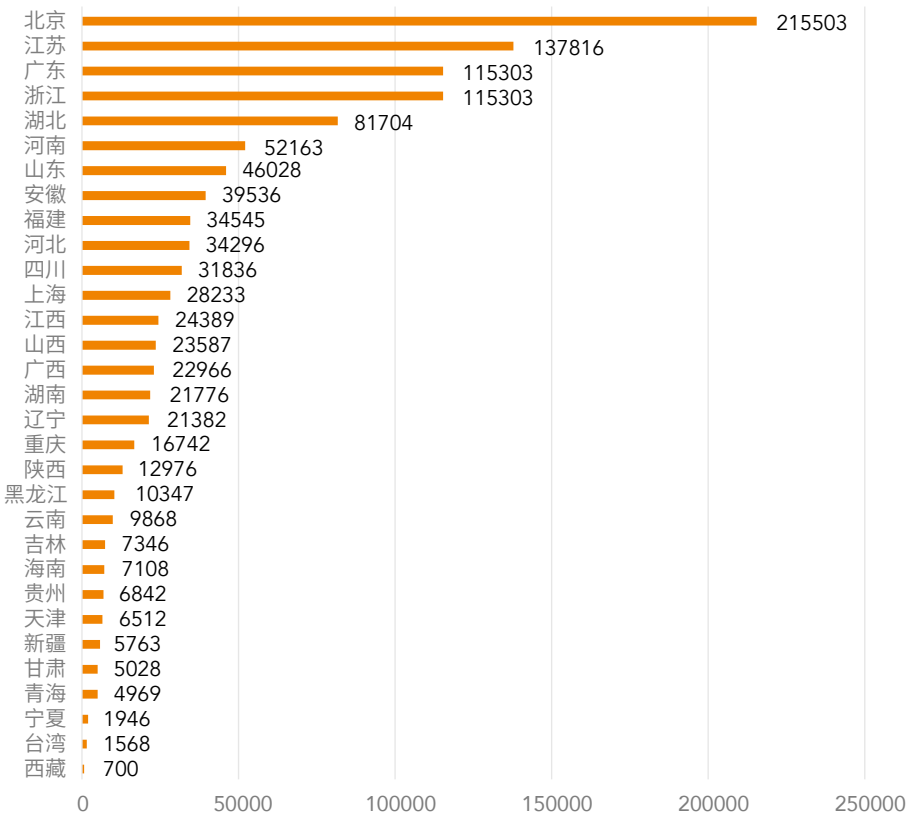


图 42 Gafgyt 僵尸网络攻陷设备省份分布状况



我们建议企业对自身的资产（不限于传统的 IT 资产，也包括各类联网设备，例如打印机、智能路由器等）进行梳理，为设备进行定期的更新升级。这些设备可能是企业内网环境的边界设备，需要加强保护，避免不必要的风险，预防设备成为 Botnet 僵尸网络帮凶。

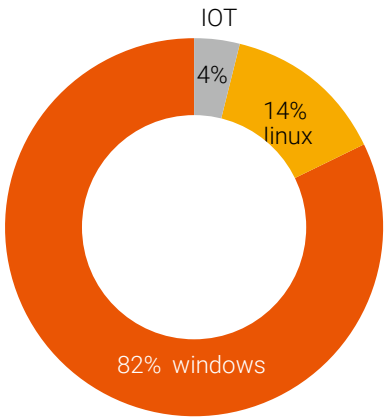
3.3 恶意软件

在 2017 年我们检测到主机被植入勒索软件以及 Bot 软件的事件攻击 310,620 起，涉及到的攻击源来自 34 个国家或地区。在 2017 年各类恶意软件中 Botnet 与勒索软件是最为常见和引人瞩目的。

3.3.1 Botnet 趋势

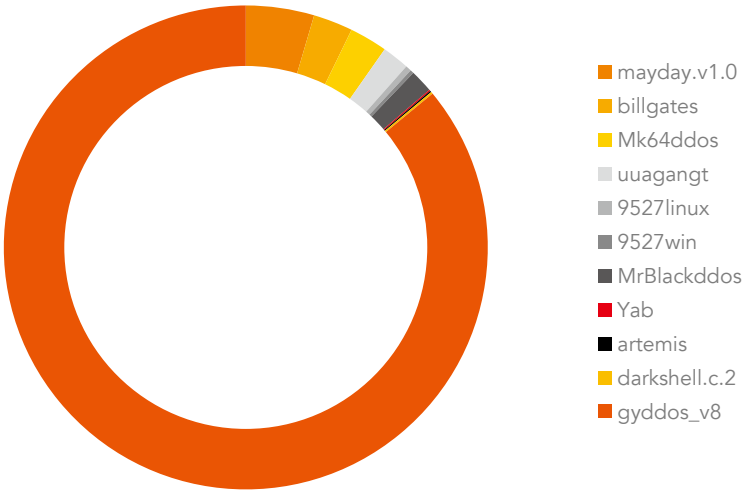
Botnet 一直以来都是互联网环境中不可忽视的危害。作为一种常见的恶意程序，它具有较强的隐蔽性，兼具蠕虫、木马的特征。Botnet 程序能够通过漏洞或者其他脆弱性获取目标主机的控制权，可以窃取目标主机中的信息或者操纵目标进行网络攻击。Botnet 对受控主机乃至整个网络环境都有极大的危害。据绿盟威胁情报中心（NTI）监测的数据显示，2017 年 Botnet 活动仍然十分猖獗，尤其 Q2 季度更是 Botnet 活动的高发期。根据我们监控的 Botnet 的 C&C 攻击指令数据进行统计，Botnet 活动最高峰时期，平均每天共发出 5187 次指令，单个 C&C 每天发出的指令最高达 114 次。2017 年 Botnet 的数量规模不断扩大，CC 主机数量持续增加，进入 8 月后增速明显我们持续跟踪的 Botnet 中，至少存在 4% 的样本攻击目标为物联网设备。虽然 Botnet 形式还是以 Windows 平台的设备为主，但是近年来，随着 IoT 设备、智能设备、移动设备的入网，我们认为针对 IoT 或其他智能、移动设备的恶意样本会越来越多。

图 43 Botnet 运行平台分布



“鬼影”是一个在中国非常活跃的僵尸网络，是基于 Windows 平台发展的一个影响广泛的僵尸网络。在近期 Botnet 活动监测中，我们看到“鬼影”的活动十分频繁，这个家族出现时间早、变种多，具有相当成熟的商业运作。对此，我们认为需要特别关注和治理。

图 44 活跃 Botnet 家族指令数量统计



“鬼影”目前至少存在 10 个不同的版本，每个版本与之前一个版本相比都增加了新的功能，DDoS 攻击技术也不断升级迭代。目前“鬼影”已经成为一个可发动大流量攻击、可大规模传播、支持不同模式商业运作的成熟软件。

3.3.2 勒索软件趋势

2017 年最突出的恶意软件类型就是勒索软件：

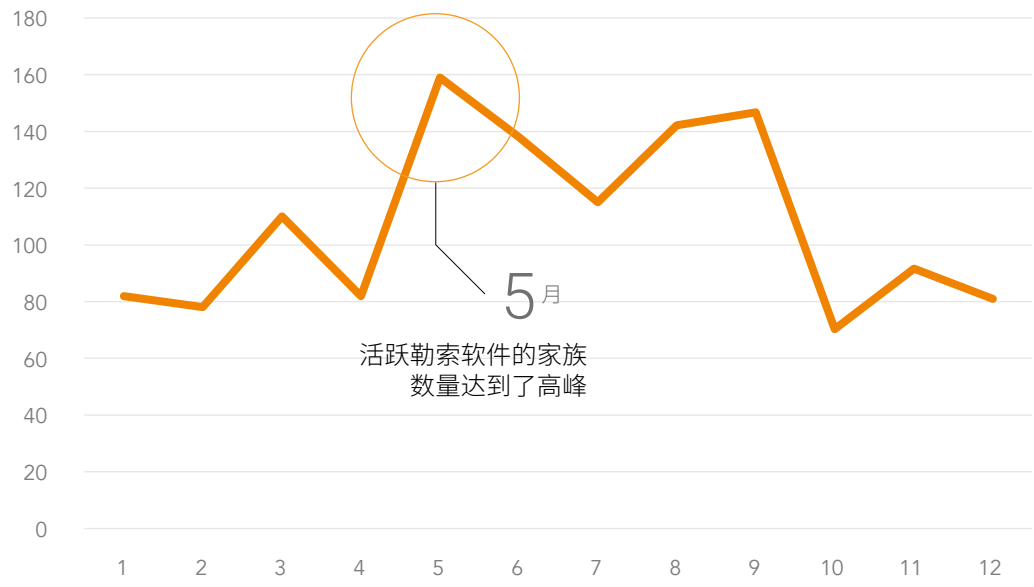
- 2017 年 5 月 12 日，WannaCry 勒索病毒借助 EternalBlue（永恒之蓝）漏洞肆虐全球，影响超过 150 个国家，中毒用户要去在 72 小时内支付价值 300 美金的比特币，并且 3 天后勒索赎金就会翻番，7 天后拒付赎金，计算机文件将被永久加密。

- 2017 年 6 月爆发的 NotPetya 勒索病毒同样采用 EternalBlue（永恒之蓝）漏洞传播，病毒会修改系统的 MBR 引导代码这将使病毒在电脑重启时得到执行，该病毒会在开机时提示用户电脑正在进行磁盘扫描然而实际上病毒正在执行文件加密等操作。当所有加密操作完成后，病毒才弹出勒索软件，要求受害者付价值 300 美金的比特币。在 2017 年 7 月，病毒作者公布了 Petya 系列勒索软件的所有密匙。

- 2017 年 10 月，BadRabbit(坏兔子) 勒索软件爆发，攻击者首先入侵新闻媒体类网站，随后利用这些新闻类网站发起水坑攻击。BadRabbit 要求受害者在 40 小时内支付 0.05 比特币（当时约合 300 美元）。

从活跃勒索软件的家族数量上看，5 月达到了高峰。

图 45 2017 年活跃勒索软件家族数量变化趋势



4. 附录

表 4 CWE 漏洞分类中英文名称对照

漏洞分类 ID	漏洞分类中文	漏洞分类（英文）
CWE-119	缓冲区溢出	Buffer Errors
CWE-284	访问控制不当	Improper Access Control
CWE-79	XSS 漏洞	Cross-Site Scripting (XSS)
CWE-200	信息泄露类漏洞	Information Leak / Disclosure
CWE-264	特权访问控制	Permissions, Privileges, and Access Control
CWE-20	输入验证错误	Input Validation
CWE-89	SQL 注入漏洞	SQL Injection
CWE-125	越界访问类漏洞	Out-of-bounds Read
CWE-399	资源管理错误	Resource Management Errors
CWE-476	空指针取消引用	NULL Pointer Dereference

根据不同厂商进行排名，微软公司漏洞数量在 2017 年里排名也是第一位，达到了 1084 个。

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供
具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com