天枢实验室
NSFOCUSTIANSHULAB
绿盟科技天枢实验室推荐

NSFOCUS

2018 网络安全观察

绿盟威胁情报中心(NTI)

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。

目录

1

执行摘要

执行摘要

从 1987 年 9 月 14 日，中国向世界发出第一封电子邮件到如今，中国的互联网发展已过去整整 31 个年头。从消费互联、产业互联到万物互联，互联网正在加速改变我们的交流方式和交易方式，一次次重塑了国家的经济形态和延展了人民的生活边界。与此同时，截止到 2018 年 6 月，中国网民规模达到 8.02 亿人，互联网普及率为 57.7%[1]。互联网已事实上成为国家经济和人民生活中的必需品，网络安全的重要性也就更为凸显。

随着网络安全的重要性凸显，互联网安全事件受到的关注度也在逐步增加，其中漏洞类、恶意软件类、DDoS、信息泄露以及物联网是最受关注的五类安全事件。从我们的观测数据可以看出，上半年的高峰出现在 3 月份，该月安全事件的主角是 DDoS，重点事件是 GitHub 遭受了峰值 1.35 Tbps 的流量冲击，以及五天之后，在针对美国的一家服务提供商的 DDoS 攻击中，峰值再次刷新纪录，达到 1.7 Tbps。在 2018 年下半年，各类安全事件呈上升趋势，主角则换成了信息泄露和恶意软件。Facebook 和 AcFun 等网站的用户数据外泄，新勒索软件样本发现，已知勒索软件解密工具公布以及样本中出新算法等等，均与老百姓的生活息息相关。网络的互通互联，让更多的人能够切身感受到网络安全的重要性。

安全厂商的脚步也在加快。2018 年 RSA 的口号是”Now Matters”，到 2019 年的”Better”， 联动防御和破除孤岛已成业界共识，厚积薄发，化被动为主动，关注落地实效和响应时效的提升。“知己知彼，百战不殆”，2019 年 RSA 的创新沙盒冠军 Axonius 正是因为提供了更为有效和细致的“知己”能力而拔得头筹，提升给定范围内的资产可见性，持续地评估、消除资产的脆弱性。而“知彼”能力中最重要的威胁情报，已逐渐成为安全厂商的核心后台能力，通过嵌入各个安全产品和运营体系，来完成数据能力和防护能力的交付。

2018 年，在我们监测到的所有恶意 IP 中，有 15% 的恶意 IP 使用了多种攻击方法，且随着时间迁移，攻击源会随着攻击链的深入或趋利目标改变攻击类型，例如发起 Web 攻击的攻击源，有 50% 的可能性在之后尝试进行更复杂的漏洞利用操作；参与 DDoS 攻击的受控源 IP，有相当一部分产生过挖矿行为。

攻击源和攻击目标主要集中在中、美两国。从国内来看，主要集中在江苏、浙江、北京、广东等省份，可以看出，攻击源和攻击目标的分布和所在地的经济发展与计算机行业发展正相关。此外，我们继续针对历史上被监测到多次恶意行为的攻击源进行分析，即所谓“惯犯”。在《2018 上半年网络安全观察》

1 http://www.cac.gov.cn/2018-08/20/c_1123296882.htm

执行摘要

报告中我们指出，攻击源中 25% 的“惯犯”承担了 40% 的攻击事件 [1]。2018 年全年所监控到的攻击源已由上半年的 2700 万增加至 4300 万左右，“惯犯”占比为 17%，“惯犯”告警数量占比为 35%，整体告警占比与上半年相比均有所降低，但“惯犯”的活跃程度在增加，一定程度的说明了攻击资源的重复利用。同时，39% 的“惯犯”都曾被僵尸网络所控制，也暴露了这部分公共网络资源安全状况长期得不到改善的严峻性。

在漏洞公布及漏洞利用方面，NVD 官网发布的 2018 年 CVE 漏洞数目为 1.58 万 ，其中高危漏洞 4096 个。其中设备类漏洞明显增加，针对设备漏洞的攻击也在逐年增加。“永恒之蓝”漏洞被众多恶意软件使用，逐渐成为被利用率最高的漏洞之一。

在 Web 攻击方面，在针对 Web 服务器的攻击中，85% 以上的攻击仍然是一些常规的攻击手段，但对 Web 服务软件的漏洞利用逐年增长。在 Web 漏洞中，反序列化漏洞由于其简单，可远程利用的特点格外受到黑客的青睐。漏洞从披露到出现有效攻击的时间间隔已经缩短到小时级别，给传统的防护和升级策略提出了更高的挑战。

DDoS 攻击规模持续普遍增大，DDoS 即服务增长迅速。DDoS 反射型攻击放缓，综合多种攻击手段值的关注。挖矿病毒方兴未艾，虽因加密货币价格缩水而略受影响，但整体活跃度在恶意软件排名中仅次于后门程序。蠕虫种类繁多，部分病毒已活跃多年。大部分蠕虫病毒最早发现时间距今都有 5 年以上，2018 年全年监测到的最为活跃的蠕虫病毒种类共计 39 个，其中从发现至今超过 5 年的病毒占比 60% 以上。木马活跃度略有下降，暗云系列仍层出不穷。2015 年至今，暗云木马已感染数以百万的计算机，并经过了几次的更新迭代，各变种层出不穷，查而未绝。从蜜罐捕获和僵尸网络跟踪的角度看，Mirai 和 Gafgyt 两大家族的物联网恶意样本数量最多。异常物联网设备主要被利用进行 DDoS 攻击。Coinhive 在 2018 年 10 月控制的物联网设备仍有 2.6 万台，绝大部分仍是 MikroTik 的路由器，巴西为重灾区，物联网设备难升级修复是物联网安全的巨大挑战。

1 http://blog.nsfocus.net/network-security-observation-report-2018/

2

重要观点

2. 重要观点

观点1 漏洞从披露到出现有效攻击的时间间隔缩短到小时级别，给传统的防护和升级策略提出了更高的挑战。

观点2 DDoS攻击规模持续普遍增大，DDoS即服务增长迅速。攻击治理初见成效，反射型攻击减少。

观点3 在物联网等新型风险激增的同时，传统威胁仍然不可忽视。在2018 年的活跃恶意软件中，后门程序的活跃程度最高，其次是挖矿和蠕虫。其中活跃超过5年的蠕虫病毒占比60% 以上。

观点4 设备类漏洞呈逐年增加态势，针对设备漏洞的攻击主要集中在路由器及摄像头等主流网络设备和物联网设备。网络/物联网设备数量众多、分布广泛，以及物联网的快速发展，加剧了设备漏洞的威胁，亟需广谱监测和升级/防护方案。

观点5 超过半数的异常物联网设备被利用进行DDoS 攻击，大量物联网设备并未得到妥善维护。

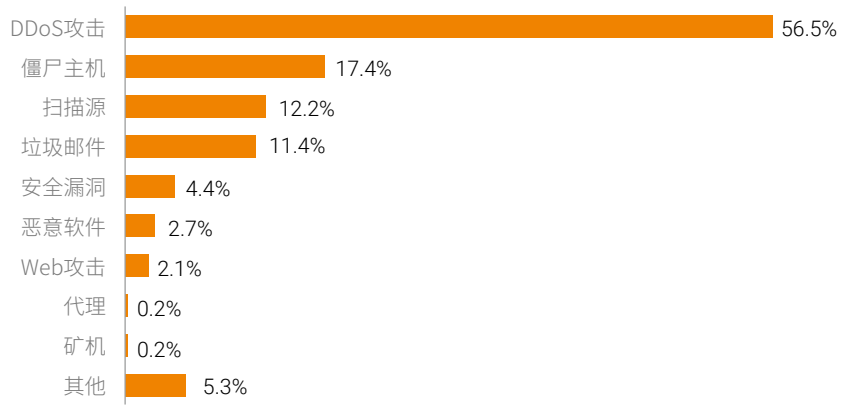
3

态势总览

3.1 攻击类型分布

从攻击类型来看[1]，参与 DDoS 攻击的 IP 是最多的，占所有恶意 IP 的一半以上。其次是僵尸主机，扫描源，垃圾邮件。

图 3.1 攻击类型分布



在所有的恶意 IP 中，有 15% 的恶意 IP 使用了多种攻击方法。对参与多种攻击的 IP 进行跟踪，发现不同类型的攻击源之间有一些特定的转换模式，例如：

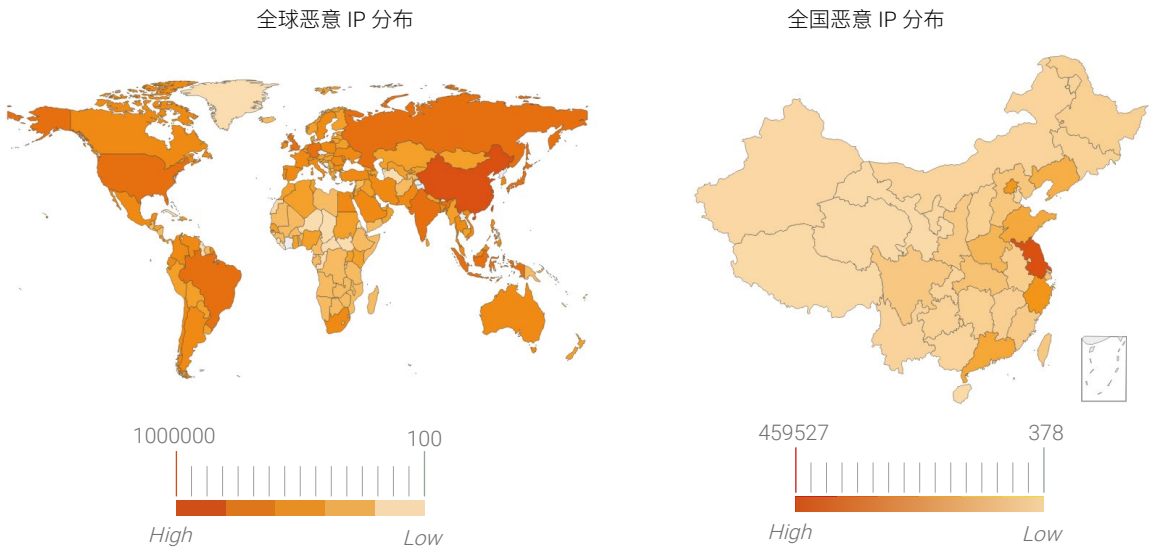
- 一个参与垃圾邮件攻击的 IP 有超过 90% 的概率会在互联网进行恶意扫描。恶意扫描和垃圾邮件都需要较多的主机资源，因为同一批资源可能同时在两种攻击中被使用。
- Botnet 客户端主机与多种类型的攻击存在关联，最常见的行为就是进行恶意扫描，此外也包括垃圾邮件、网络钓鱼等恶意行为。
- 发起 Web 攻击的攻击源，有 50% 的可能性在之后尝试进行更复杂的漏洞利用操作。由于 Web 攻击复杂度低，通过 Web 漏洞拿到较低的权限或其它敏感信息，再利用搜集到的情报，有针对性的进一步使用漏洞进行渗透和利用。
- 参与 DDoS 攻击的受控源 IP，有相当一部分产生过挖矿行为。攻击者是趋利的，会充分的利用手头的资源，在没有 DDoS 攻击的时候，利用受控主机挖矿为自己谋求利益。

1 由于存在一个 IP 参与多种类型的攻击，故百分比之和是大于 100% 的。

3.2 地域分布

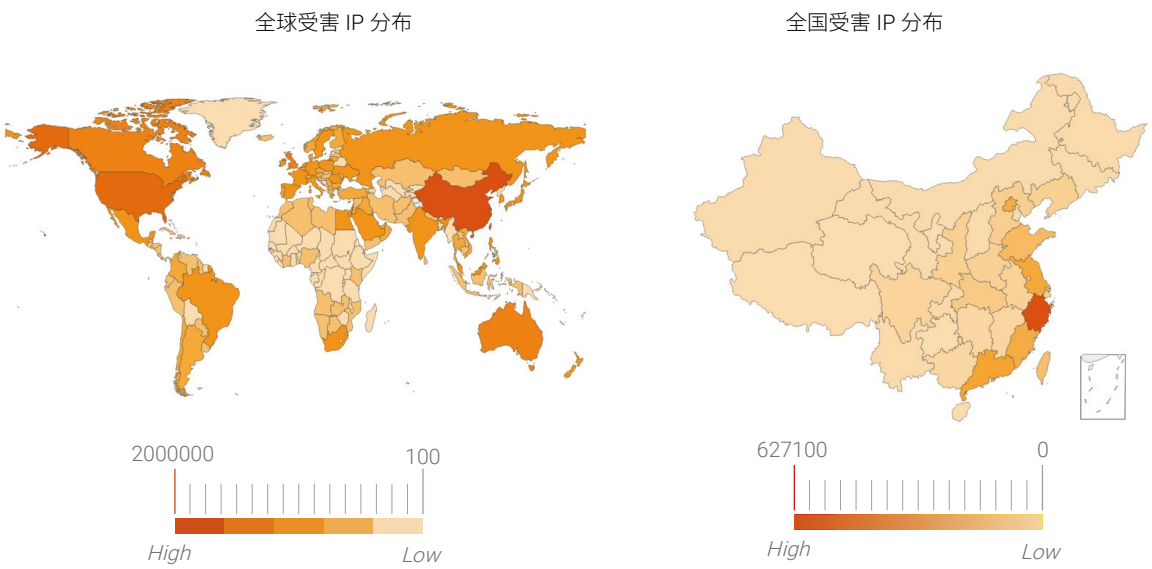
按攻击源 IP 的分布来看，在全球范围内，主要集中在中国、美国、俄罗斯、英国、印度等计算机行业比较发达的国家，从全国来看，主要集中在江苏、浙江、北京、广东、 辽宁等地区。

图 3.2 攻击源 IP 地域分布



按攻击目标 IP 的分布来看，在全球范围内，主要集中在中美两国，从全国来看，主要集中在浙江、广东、江苏、福建、北京等地区。经济活动越活跃，受到攻击的可能性就越大，这体现出攻击者逐利、逐名的攻击诉求。

图 3.3 攻击目标 IP 分布

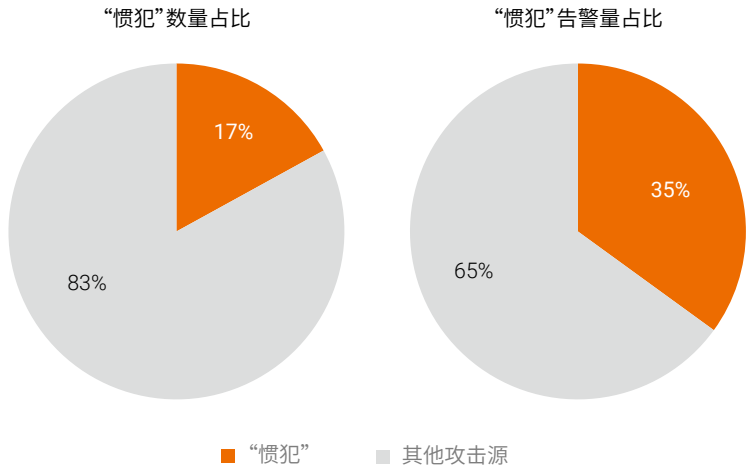


3.3 惯犯观察

所谓“惯犯”，即历史上被监测到多次恶意行为的攻击源。在《2018 上半年网络安全观察》报告中我们指出，攻击源中 25% 的“惯犯”承担了 40% 的攻击事件[1]，“惯犯”的数量及威胁程度均不容小觑。2018 年全年所监控到的攻击源已由上半年的 2700 万增加至 4300 万左右，“惯犯”占比为 17%，“惯犯”告警数量占比为 35%，与上半年相比均有所降低。但 17% 的“惯犯”承担了 35% 的告警，威胁程度同上半年相比更加严重。

1 http://blog.nsfocus.net/network-security-observation-report-2018/

图 3.4 “惯犯”数量及告警分布图



“惯犯”的地域分布情况同上半年数据基本一致，从全球的数据来看，中国、美国是“惯犯”高度活跃的地区，俄罗斯、印度紧随其后。与此同时，中国、美国也是受害最为严重的国家，俄罗斯、澳大利亚、巴西以及欧洲部分国家也是“惯犯”攻击的目标。从国内地域分布情况来看，“惯犯”主要集中在山东、江苏、浙江、广东等沿海地区，其次是河北、河南等内陆地区的一些人口大省。其攻击目标也主要集中在北京和这些沿海经济发达省市。

图 3.5 “惯犯”全球分布

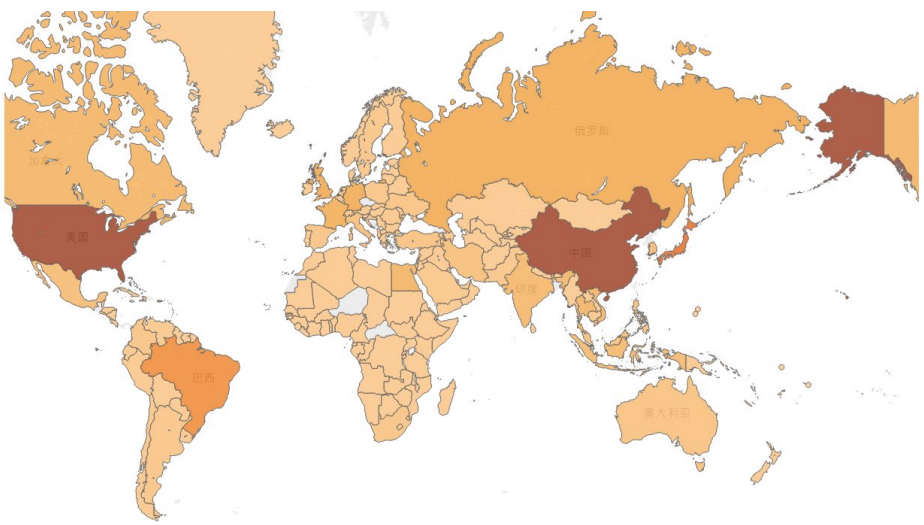


图 3.6 “惯犯”攻击目标全球分布

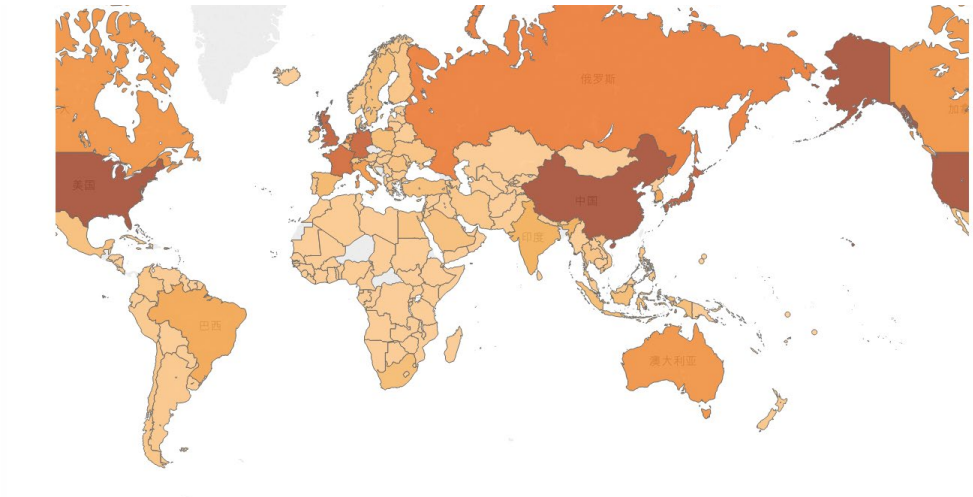


图 3.7 “惯犯”国内分布

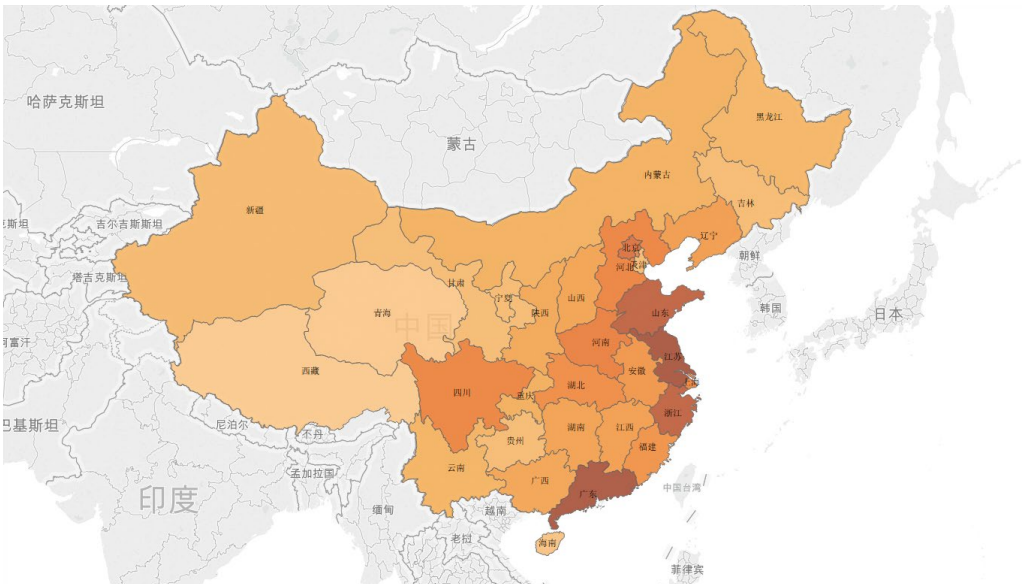
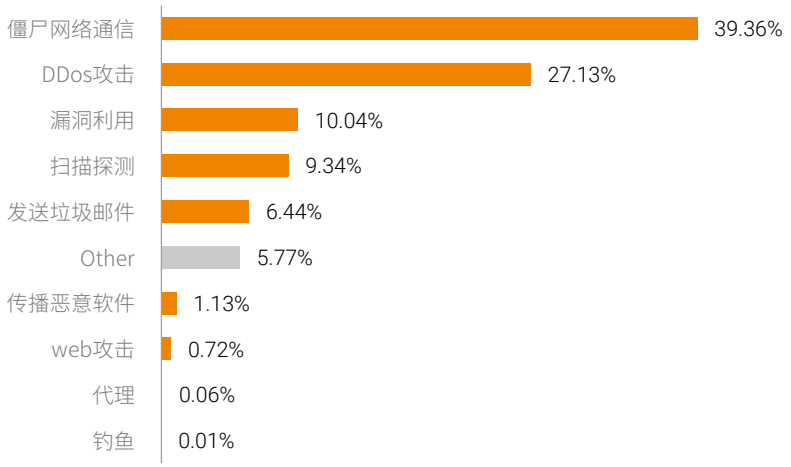


图 3.8 “惯犯”攻击目标国内分布

从图 3.9 中“惯犯”异常行为类型分布可知，39.36% 的“惯犯”曾被僵尸网络所控制；27.13% 的“惯犯”参与过 DDoS 攻击，仅这两种异常行为就占据整体的比例的 66.49%。其次是漏洞利用和扫描探测，我们认为，网络中有相当一批的僵尸主机在持续且频繁的进行着漏洞扫描与利用行为。

图 3.9“惯犯”异常行为类型分布

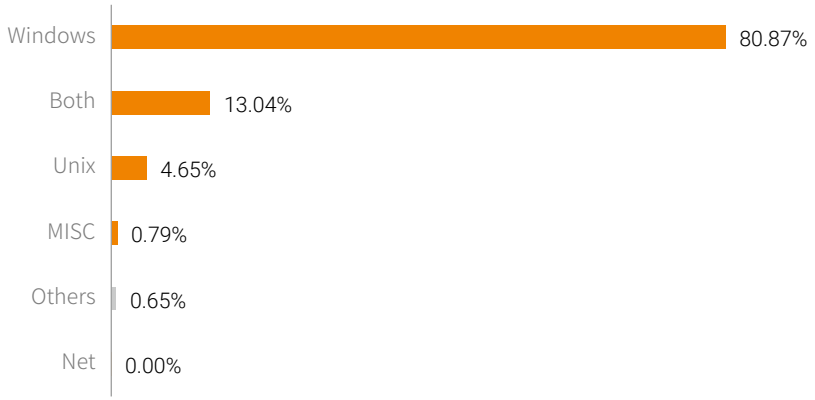


基于对这些“惯犯”的长期跟踪，我们从其攻击特点的攻击系统、攻击服务、攻击方法、攻击类型四个方面进行画像：

攻击系统

“惯犯”在一次攻击事件中仅针对 Windows 发起的攻击占比为 80.87%，其次为同时针对 Windows 和 Unix 两种操作系统发起攻击，占比为 13.04%。由此可见，Windows 与其他操作系统相比饱受惯犯青睐，承担了绝大多数的攻击。原因在于 Windows 系统个人电脑多，整体基数大，且可利用的安全漏洞多，容易入侵。

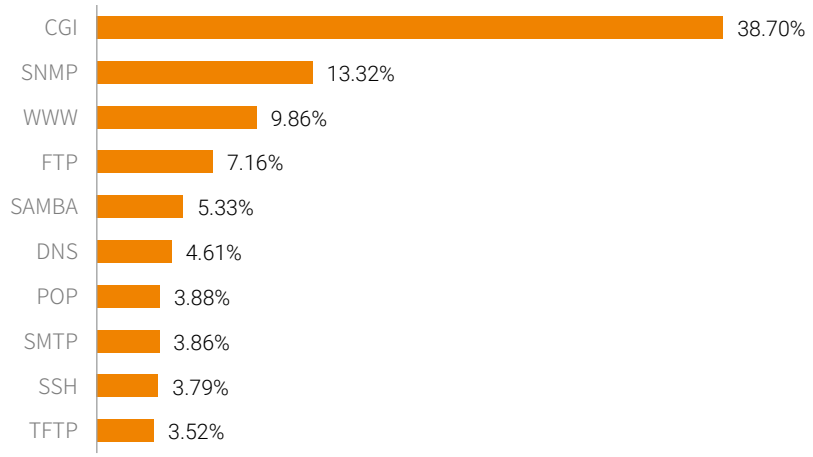
图 3.10“惯犯”画像之攻击系统



攻击服务

所有的攻击类型中仅 CGI 和 SNMP 两项占整体比例的一半以上。CGI 是网页表单和程序之间通信的一种协议，本身并不负责通信，而是将输入数据转化成一种固定格式输出，方便任何符合 CGI 协议的程序调用。SNMP 是简单网络管理协议，实现对网络设备的规范化管理，共有三个版本，其中 2c 版本黑客利用最多。

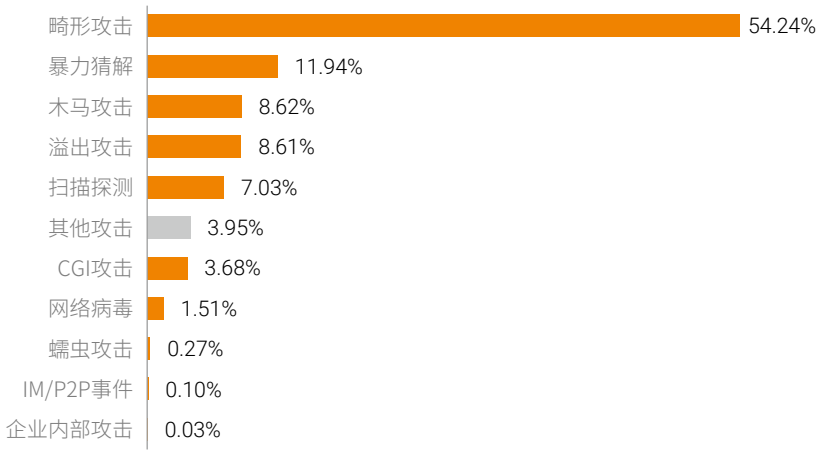
图 3.11 “惯犯”画像之攻击服务（前十）



攻击方法

畸形攻击占所有攻击比例的 54.24%，畸形攻击作为网络攻击的一种，主要通过向目标系统发送有缺陷的报文，使得目标系统在处理这样的报文时耗时很大甚至出错、崩溃，给目标机器构成威胁、带来很大的损失。除畸形攻击外，暴力猜解、木马攻击、溢出攻击、扫描探测也是“惯犯”常用的攻击手法。

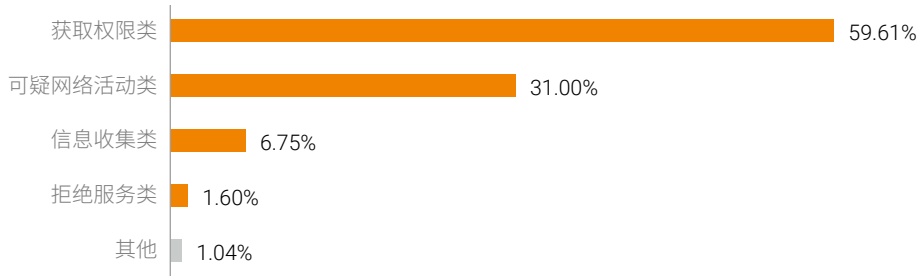
图 3.12“惯犯”画像之攻击方法



攻击类型

信息收集主要包括收集目标的操作系统类型及版本，目标所提供的服务，各服务器程序的类型与版本以及相关的社会信息；获取权限一般发生在黑客信息收集活动之后，利用收集到的信息，找到相关的漏洞，选择相应的攻击方式并实施攻击行为；在获取权限后，黑客可以实现诸如挖矿病毒恶意文件下载等各类破坏行为。

图 3.13“惯犯”画像之攻击类型



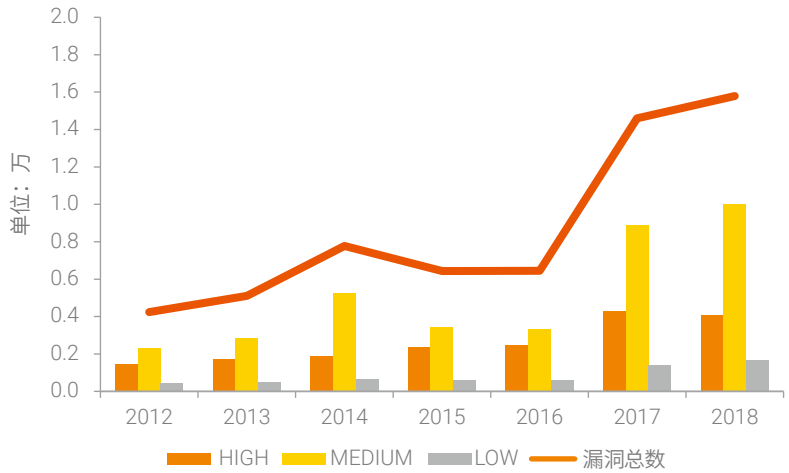
4

漏洞观察

4.1 总体态势

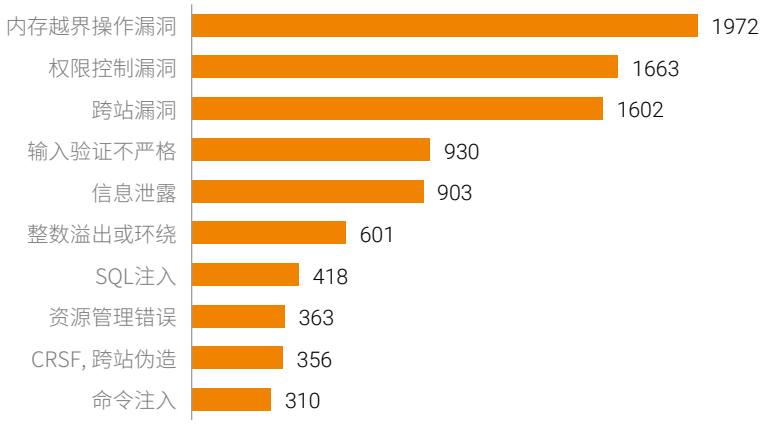
截止 2018 年 12 月 31 日，NVD 官网分布的 2018 年 CVE 漏洞数目为 1.58 万，其中高危漏洞 4096 个。和 2017 年相比，漏洞总数增长了 8.2%，而高危漏洞减少了 4.8%。漏洞披露数量放缓，可能在于漏洞报告较以前更加分散化，大量漏洞未得到官方收入。

图 4.1 CVE 漏洞变化趋势



我们按照 CWE 给出的标准，对漏洞类型进行分类，2018 年的漏洞类型的分布情况如图 4.2 所示。

图 4.2 2018 年 CVE 漏洞分类



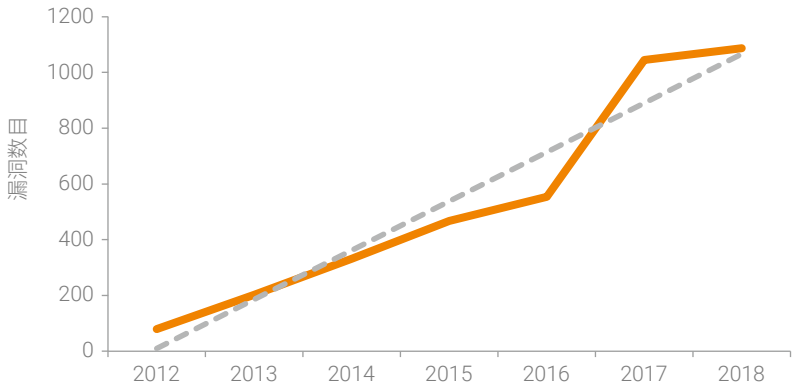
从漏洞类型上看排名前 5 的漏洞类型分别为：

- **CWE-119/125 内存越界操作漏洞** 通过漏洞，黑客可以获取任意代码执行权限，有时可以造成系统崩溃。 这类漏洞主要集中在设备固件、操作系统、浏览器、office 及 PDF 等软件，这些软件对性能要求苛刻，绝大部分都是基于 C/C++ 开发的。这类漏洞数量是最多的，有 1760 个，其中高危漏洞接近 40%。
- **CWE-264/284 权限控制漏洞** 这类漏洞与具体业务密切相关，包括越权访问、权限提升等常见的操作，在服务器操作系统、数据库类应用、内容管理系统方面比较常见。这类漏洞有 1500 个，绝大多数漏洞属于中危漏洞。
- **CWE-79 跨站漏洞** 这类漏洞单个漏洞威胁似乎较小，但是它们数量非常多，在各类建站系统中尤其常见，几乎防不胜防，它们如果配合其他漏洞使用，通过组合式的攻击手法可以完成复杂的攻击，进而获得系统权限。
- **CWE-20 输入验证不严格** 黑客通过畸形的输入，导致程序出现异常的行为，最终实现控制、窃取、使设备瘫痪等多种攻击目的。
- **CWE-200 信息泄露** 攻击者触发漏洞能够导致敏感信息泄露。此外在一些设备的固件中，该类漏能够导致权限控制失效，导致设备失陷，例如 D-Link 设备固件 CVE-2018-10106 漏洞。

4.2 设备类漏洞明显增加

近几年来，设备类的漏洞快速增长。原因在于制造商对安全的忽视，而设备系统难以更新及使用者对安全的不够重视也是一个不可忽略的因素。

图 4.3 设备类漏洞变化趋势



由于设备类资源数量大，防御少，获取难度普遍较低，相关的漏洞利用难度也普遍较小，一旦利用成功能够获取到设备系统较高的权限，因此这类漏洞受到攻击者的关注，需要安全厂商及相关从业人员格外重视并探索防御的技术与方案。

在 2018 年披露的 CVE 漏洞中，设备类漏洞有 986 个，其中高危漏洞 482 个，占全部高危漏洞的 12%。初步统计，这些漏洞涉及 145 个厂商的 1503 款产品，包括处理器，路由器，摄像头，智能设备等多种类型。

在 2018 年 1 月，Google 的安全团队发布了 CPU 芯片的两组漏洞，分别是 Meltdown（熔断，CVE-2017-5754）与 Spectre（幽灵，CVE-2017-5753/ CVE-2017-5715），成为最近几年来严重的安全问题。在随后的一年中，又有 14 个类似 Meltdown 的漏洞和 13 个类似 Spectre 的漏洞被披露 [1]。

Meltdown 破坏了位于用户和操作系统之间的基本隔离，此攻击允许程序访问内存，因此其他程序以及操作系统的敏感信息会被窃取。这个漏洞“熔化”了由硬件来实现的安全边界。允许低权限用户级别的应用程序“越界”访问系统级的内存，从而造成数据泄露。

Spectre 是一个存在于分支预测实现中的硬件漏洞，含有预测执行功能的现代微处理器均受其影响，允许恶意进程访问其他程序在映射内存中的内容，是一类潜在漏洞的总和。它们都利用了一种现代微处理器为降低内存延迟、加快执行速度的常用方法“预测执行”的副作用。具体而言，Spectre 着重于分

1 https://www.kaspersky.com/blog/35c3-spectre-meltdown-2019/25268/

支预测，这是预测执行的一部分。Spectre 不依赖单个处理器上内存管理及系统保护的特定功能，而是一个更为通用的漏洞。

由于涉及硬件，该漏洞无法通过芯片的微码（microcode）更新进行修复，需要通过内核级别的修复来解决，据研究表明，修复该漏洞会牺牲 5%-30% 的性能。

路由器设备的漏洞，同样也形势严峻。美国消费者协会发布了关于路由器安全的报告《Securing IoT Devices: How Safe Is Your Wi-Fi Router》[1]，文中指出有 83% 的 WiFi 路由器存在已经披露的安全漏洞，这些未及时更新的路由器设备会成为网络攻击的入口，给消费者带来经济和隐私方面的损失。

在 2018 年 3 月，Cisco 发布的一个远程代码执行漏洞 CVE-2018-0171，4 月 6 日，一个名为 "JHT" 的黑客组织利用这这个漏洞攻击了包括俄罗斯和伊朗在内的多个国家网络基础设施。

2018 年 4 月 30 日，vpnMentor 公布了 GPON 路由器的两个高危漏洞，绕过验证漏洞 (CVE-2018-10561) 和命令注入漏洞 (CVE-2018-10562)。结合这两个漏洞，只需要发送一次请求就可以在 GPON 路由器上执行任意命令。在该漏洞披露后的十天内，该漏洞就已经被多个僵尸网络家族整合、利用，并在公网上以蠕虫的方式传播。

1 https://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities. pdf

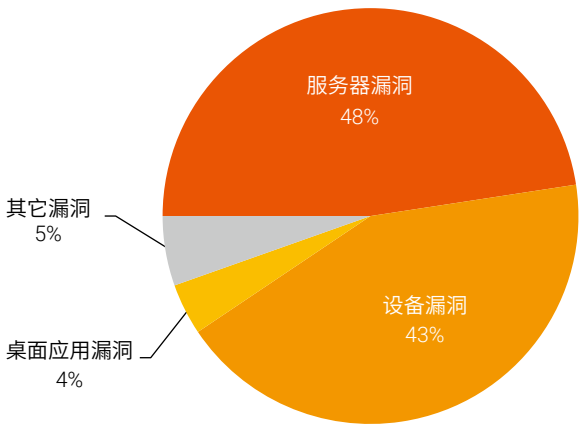
5

恶意流量观察

5.1 漏洞利用

我们按照漏洞所在的主机环境或业务场景，将漏洞粗略的划分为服务器漏洞、桌面应用漏洞和设备漏洞。其中服务器漏洞主要为服务器上的系统服务与程序，用于支撑或提供网络管理与实际业务，常见的服务包括邮件、HTTP、网站脚本语言解析等；桌面应用主要提供文档、多媒体、主机管理等功能，常见的包括各类客户端（例如浏览器、邮件客户端）、杀软、Office 办公软件、Flash 播放器、PDF 阅读器等，这类软件漏洞常常被利用，常见的是通过恶意邮件、恶意网页的方式传播，通过诱使用户执行来感染目标主机；设备漏洞属于比较特殊和新晋的漏洞类型，包括各类移动终端、物联网设备等，他们共同构成一种新的威胁类型。

图 5.1 漏洞利用各类型占比



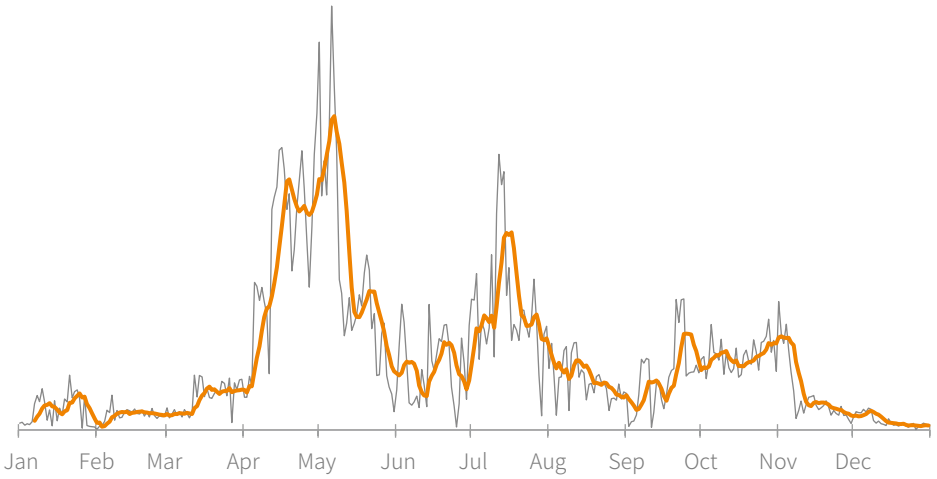
5.1.1 设备类漏洞从未缓解

从图 5.1 中可以看到，针对设备漏洞的攻击占全部利用漏洞攻击的 43%，这和近两年智能路由器等联网设备大规模增长密切相关。正如绿盟科技在《2017 年物联网报告》[1] 中提到的那样，很多智能设备在设计之初，安全问题并没有被严肃对待，于是随着设备的推广，市场上出现大量常年不更新不维护的高危设备。即使厂商已经发现甚至很早前已经推出解决方法或升级补丁的设备，但是仍有大量设备的脆弱性状况至今仍未有改善，这和设备升级维护机制设计不合理有很大的关系，毕竟设备和传统 PC 不同，

1 http://www.nsfocus.com.cn/content/details_62_2646.html

没有复杂的内置应用，也无法有效提供丰富的检测防御和自动维护服务，这样一来黑客攻击成功率极高，成本和复杂度极低。

图 5.2 设备漏洞利用抽样统计



在 2018 年，和其他攻击流量对比，设备漏洞攻击的情况从未得到有效缓解，另一方面也说明，设备漏洞状况长期为人所忽略。从监测情况来看，下列设备及漏洞被黑客攻击还是比较严重的：

- Netcore / netis 路由器后门
- D-Link dsl-2750b 任意命令执行漏洞
- 大华监控设备非授权访问漏洞
- TP-Link 无线路由器 http/tftp 后门漏洞
- D-Link 路由器 user-agent 后门漏洞 (CVE-2013-6026)
- ASUS 路由器固件 Asuswrt Lan 后门命令执行漏洞 (CVE-2014-9583)
- 华为 HG532 路由器远程命令执行漏洞 (CVE-2017-17215)
- 施耐德派尔高 Sarix Pro 网络摄像头 import.cgi xml 实体注入漏洞
- 施耐德派尔高 Sarix Pro 摄像头 session.cgi 程序缓冲区溢出漏洞

- Motorola 无线路由器 WR850g 认证绕过漏洞 (CVE-2004-1550)

在 2018 年 2 月，Radware 的信息安全专家 Pascal Geenens 分析了一个 DDoS 攻击组织，该组织利用一个名为 JenX 的恶意带软件感染的物联网设备发动 DDoS 攻击。具体而言，JenX 正是利用 CVE-2017–17215 和 CVE-2014-8361 感染华为 HG532 路由器和运行 Realtek SDK 的设备，和完全分布式僵尸网络 Mirai 不同的是，该僵尸网络由服务器完成漏洞利用和僵尸主机管理的任务。在 7 月，黑客利用 CVE-2017–17215 仅仅在一天内就构建了一个 18000 台僵尸网络主机构成的僵尸网络。可见 JenX 的影响面之大 [1]。

5.1.2 服务器漏洞利用

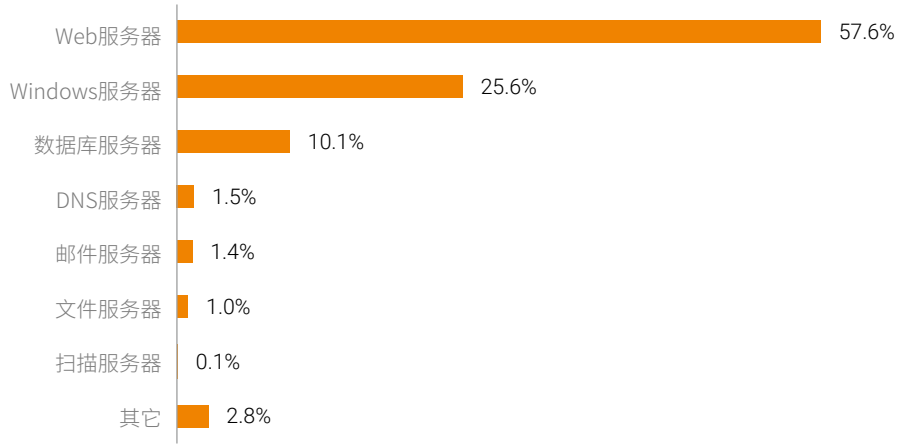
在所有的漏洞利用中，服务器漏洞是被利用最多的。从告警日志量来看，4,5 两个月被攻击的数量是最多的。

图 5.3 服务器类漏洞抽样统计

在针对服务器的漏洞攻击中， Web 服务器受到的攻击最多。大多数网站都存储有价值的信息，如信用卡号，电子邮件地址和密码等。这使他们成为攻击者的目标。另外，污损的网站也可用于传播宗教或政治意识形态等。我们将在 5.2 节对此做详细的分析。

1 http://www.nsfocus.com.cn/upload/contents/2019/03/20190308101905_52741.pdf

图 5.4 服务器类漏洞按应用分类



Windons 服务器的漏洞利用排在第二位，大多数是和 Samba 服务相关的漏洞。在 2018 年被利用比较多的漏洞有：

- windows smb server 信息泄露漏洞扫描 (CVE-2017-0147)
- windows smb 远程代码执行漏洞 (shadow brokers eternalblue)(CVE-2017-0144)
- windows smb 操作解析远程代码执行漏洞 (ms11-020)
- windows smb 远程堆覆盖漏洞 (CVE-2008-4834)
- samba 远程代码执行漏洞 (永恒之红)(sambacry)(CVE-2017-7494)

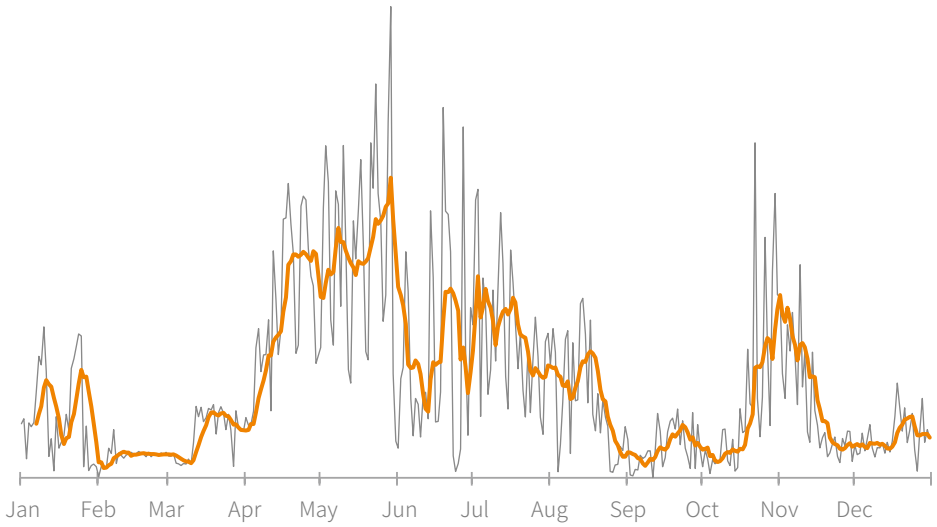
臭名昭著的 WannaCry 蠕虫正是利用了“永恒之蓝”漏洞 (MS-010, 包括 CVE-2017-0144、CVE-2017-0147 等多个 SMB 漏洞编号)，感染了大量的计算机，该蠕虫感染计算机后会向计算机中植入敲诈者病毒，导致电脑大量文件被加密。在 2018 年 8 月，台积电遭受 WannaCry 勒索病毒攻击导致生产线瘫痪，造成 25.96 亿新台币损失。

另外，Petya 勒索、NotPetya 勒索、FancyBear 窃取信息、Retefe 银行木马、WannaMiner 挖掘、ZombieBoy 木马、bulehero 蠕虫病毒等一系列样本都利用了“永恒之蓝”漏洞，另外，APT 组织也将“永恒之蓝”纳入武器库，“永恒之蓝”漏洞逐渐成为被利用率最高的漏洞之一。

5.1.3 应用类漏洞

应用软件类漏洞攻击主要针对个人用户与使用者，当然这些用户中也会包括核心资产的管理人员，黑客利用钓鱼邮件，通过恶意链接、恶意附件的形式投递恶意程序，在用户点击相关资源时，对应程序的漏洞会被触发，最终导致感染和信息泄露。

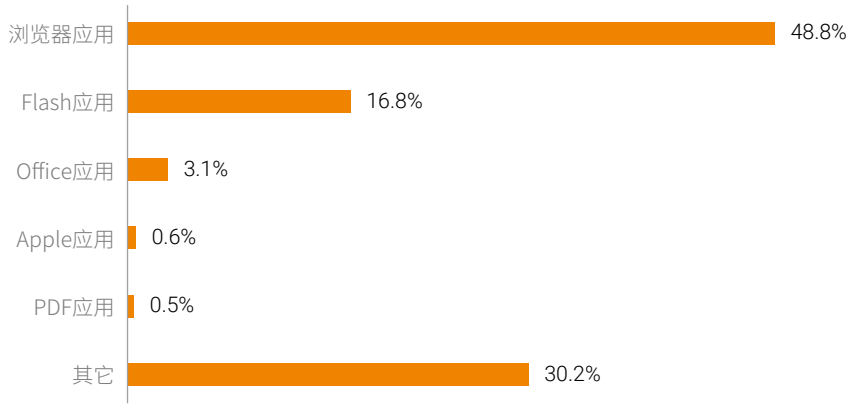
图 5.5 应用软件类漏洞抽样统计



在应用软件类漏洞利用攻击中，浏览器类受到的攻击最多，占到了全部分此类攻击的 56.7%，微软的 Internet Exporer/Edge 是被攻击最多的应用软件。浏览器漏洞利用比较高的漏洞有：

- microsoft edge profiledldelem 类型混淆
- mozilla firefox/thunderbird/seamonkey http 响应分离漏洞
- microsoft internet explorer 远程内存破坏漏洞 (CVE-2016-7287)(ms16-144)
- microsoft ie 对象处理内存破坏漏洞 (ms08-078)
- microsoft edge scripting engine remote 内存破坏漏洞 (CVE-2018-0773)

图 5.6 应用软件类漏洞按应用分类



Flash 虽然被爆的漏洞数目相对少一些，但利用率还是比较高的，在 2018 年，被攻击最多的漏洞 TOP5 如下：

- Adobe Flash player shader 缓冲区溢出漏洞
- Adobe Flash player 远程拒绝服务漏洞
- Adobe Flash player "asnative 301" 函数空指针引用拒绝服务漏洞
- Adobe Flash 0day 漏洞 CVE-2018-4878
- Adobe Flash player localeid determinepreferredlocales 越界访问漏洞 (CVE-2017-3114)

Office 漏洞常被大家忽视，但却备受黑客喜爱，众多专业黑客组织对重要目标的攻击，会选择使用 Office 高危漏洞。APT 缓和 BlackTech 就利用 Office 公式编辑器漏洞 CVE-2018-0802 和 CVE-2017-11882 实施过攻击 [1]。我们监测到的被利用比较高的漏洞有：

- Microsoft Word 文件信息块内存破坏漏洞（MS08-009）
- Microsoft Office 远程代码执行漏洞 (CVE-2017-8570)
- microsoft frontpage post 请求远程缓冲区溢出攻击

1 https://www.freebuf.com/column/159865.html

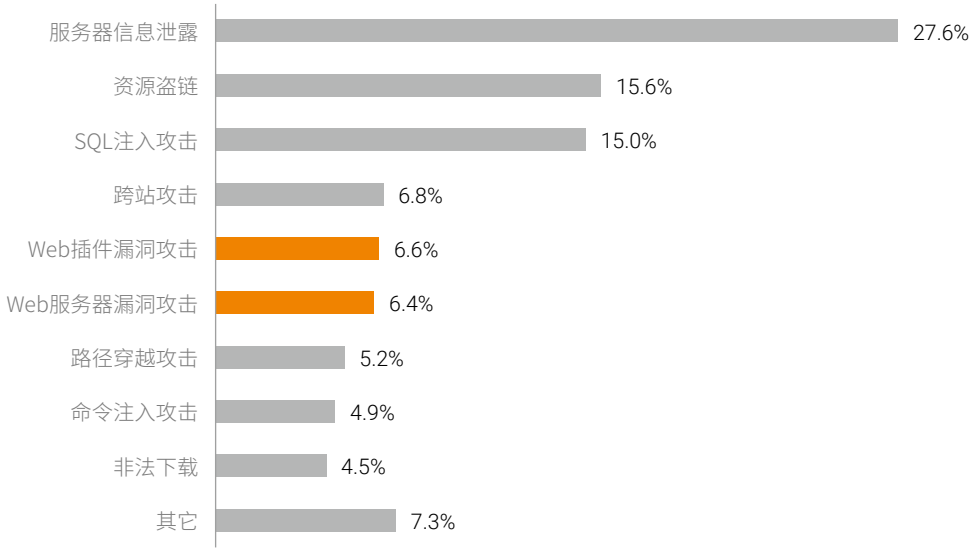
- Microsoft Office Sharepoint Server 管理权限提升漏洞（MS08-077）
- Microsoft Office 远程内存栈溢出漏洞 (CVE-2018-0802)

5.2 Web 攻击

5.2.1 Web 攻击态势

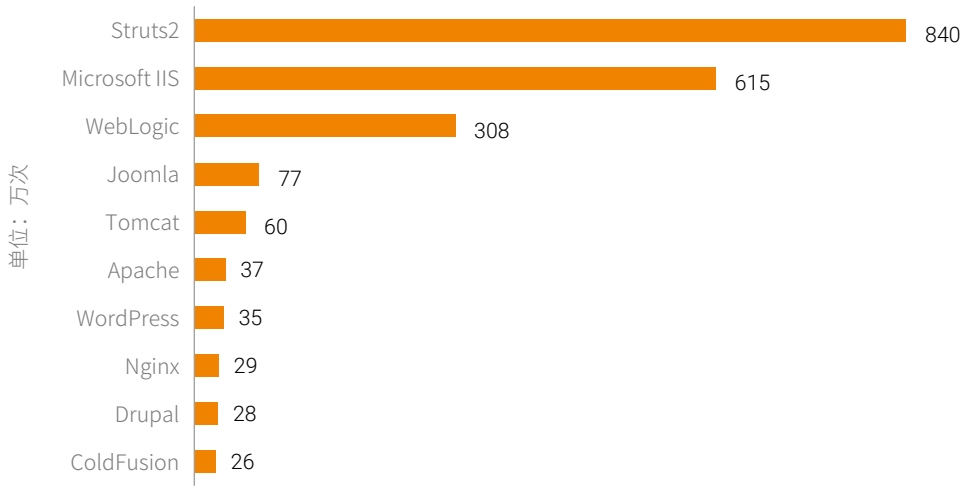
在 2018 年， 针对 Web 服务器的攻击中，89% 的攻击仍然是一些常规的攻击手段，包括服务器信息泄露，资源盗链，SQL 注入，跨站脚本攻击等。传统的攻击手段仍然被大量的使用，需要持续关注。

图 5.7 针对 Web 攻击的攻击类型分布



黑客利用 Web 服务器漏洞或插件漏洞的攻击比例在逐年增加。在 2018 年，利用漏洞进行的 Web 攻击占了占全部 Web 攻击的 11%，和 2017 年相比有所增加。也不容小视。受攻击最多的 Web 框架有 Struts2、Microsoft IIS、WebLogic 等。

图 5.8 针对 Web 漏洞攻击的 TOP10



5.2.2 Web 漏洞利用

Struts2 框架一直是攻击的热点。从 2007 年 7 月到 2019 年 3 月这十多年间，Struts2 被披露的漏洞数目 57 个，其中远程代码执行漏洞，由于威胁性大，利用难度低，被黑客大量使用。在 2018 年，我们监测对针对 Struts2 的攻击中，被利用比较多的漏洞如下：

- **Struts2 远程代码执行漏 (2-45/S2-46)**
  这两个漏洞都是由报错信息包含 OGNL 表达式，并且被带入了 buildErrorMessage 这个方法运行，造成远程代码执行。在 2018 年，一半以上的针对 Struts2 的攻击都是利用的这个漏洞。
- **Struts2 远程代码执行漏（S2-32/S2-33/S2-37）**
  这三个漏洞都是抓住了 DefaultActionInvocation 中会把 ActionProxy 中的 method 属性取出来放入到 ognlUtil.getValue(methodName + “()”, getStack().getContext(), action); 方法中执行 OGNL 表达式。
- **Struts2 远程代码执行漏 (S2-16)**
  DefaultActionMapper 类支持以 action:，redirect: 和 redirectAction: 作为访问前缀，前缀后面可以跟 OGNL 表达式，由于 Struts2 未对其进行过滤，导致任意 Action 可以使用这些前缀执行任

意 OGNL 表达式，从而导致任意命令执行。

- **Struts2 rest 插件反序列化漏洞 (S2-52)**

  当 Struts2 使用 REST 插件使用 XStream 的实例 xstreamhandler 处理反序列化 XML 有效载荷时没有进行任何过滤，可以导致远程执行代码，攻击者可以利用该漏洞构造恶意的 XML 内容获取服务器权限，获取业务数据或服务器权限，存在高安全风险。

由上可见，针对 Struts2 的漏洞利用，除 S-52 外，都是框架执行了用户传进来的 OGNL 表达式，造成远程代码执行，可以造成命令执行，服务器文件操作、危险代码执行等，只不过需要精心构造不同的 OGNL 代码。

而针对 WebLogic 的漏洞利用，主要是以反序列化为主。在 2018 年，有超过 80% 的针对 WebLogic 的攻击使用了以下漏洞：

- **WebLogic ws-wsat 组件反序列化漏洞 (CVE-2017-10271)**

  这个漏洞的本质原因是其引用的 XMLDecoder 库存在远程代码执行问题，可直接导致整个系统被控制。由于该漏洞是走 http 协议，因此备受黑客的青睐。同时这个漏洞也是 2017 年初爆出的 Weblogic 漏洞（CVE-2017-3506）的绕过。

另外，在 2018 年新出现的一些漏洞，我们也监测到了有效的攻击，应该值得我们注意：

- **WebLogic 组件反序列化漏洞（CVE-2018-2628）**

  攻击者可以在未授权的情况下通过 T3 协议对存在漏洞的 WebLogic 组件进行远程攻击，并可获取目标系统所有权限。

- **WebLogic 组件反序列漏洞（CVE-2018-2893）**

  该漏洞通过 JRMP 协议利用 RMI 机制的缺陷达到执行任意反序列化代码的目。攻击者可以在未授权情况下将 payload 封装在 T3 协议中，通过对 T3 协议中的 payload 进行反序列化，从而实现对存在漏洞的 WebLogic 组件进行远程攻击，执行任意代码并可获取目标系统的所有权限。

在 Web 漏洞中，反序列化漏洞由于其简单，可远程利用的特点格外受到黑客的青睐。绿盟科技《2017 年反序列化漏洞年度报告》[1] 中指出，厂商对反序列化漏洞的应对，往往修复、绕过、再修复、再绕过

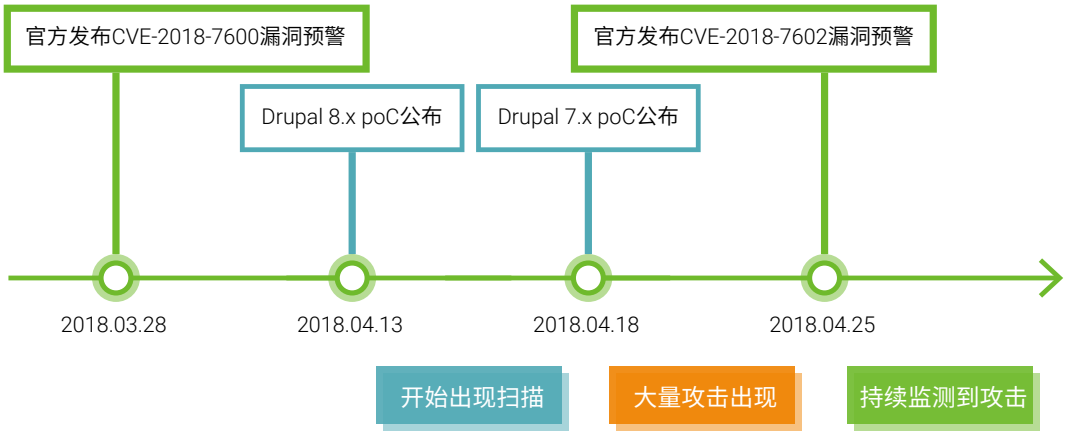
1 http://www.nsfocus.com.cn/content/details_62_2694.html

的恶性循环，因此反序列化漏洞层出不穷。它对于攻击者来说是价值极高的，因为漏洞本身的利用难度比较低，并且一旦利用成功，黑客能够获得较高的权限，是黑客用来传播病毒，挖矿程序等恶意软件的攻击方法之一。

在 2018 年，Drupal 框架的漏洞利用也具有一定的典型性，绿盟威胁情报中心在 5 月针对 Drupal 漏洞被挖矿程序利用的传播感染态势进行了详尽的分析 [1]：

- **Drupal 内核远程代码执行漏洞（CVE-2018-7600）**

  Drupal 官方在 2018 年 3 月 28 日发布 sa-core-2018-002 (CVE-2018-7600) Drupal 内核远程代码执行漏洞预警，之后一个月内又连续发布两个漏洞，其中包含一个 XSS 和另一个高危代码执行漏洞 sa-core-2018-004 (CVE-2018-7602)。虽然漏洞已经披露，相关利用的 PoC 却在两周后才放出，而仅仅在 PoC 披露后几个小时，就发现有利用此漏洞的攻击出现。在随后的时间内互联网上针对 Drupal 程序的攻击迅速增加此后几个月内，互联网上针对 Drupal 程序的攻击都非常频繁。



我们看到从漏洞披露到出现有效攻击的时间间隔已经缩短到小时级别，这给传统的防护和升级策略提出了更高的挑战。

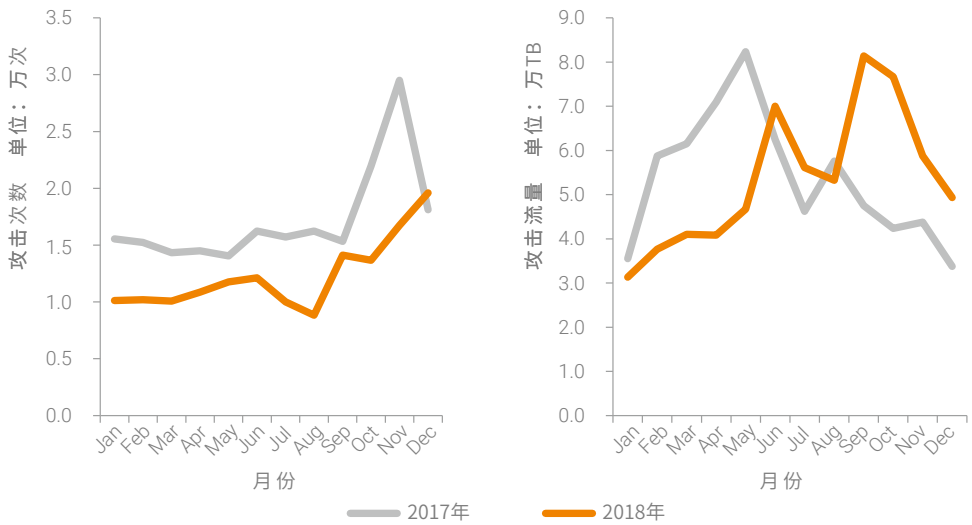
1 http://blog.nsfocus.net/drupal-threat-analysis/

5.3 DDoS 攻击

5.3.1 攻击态势

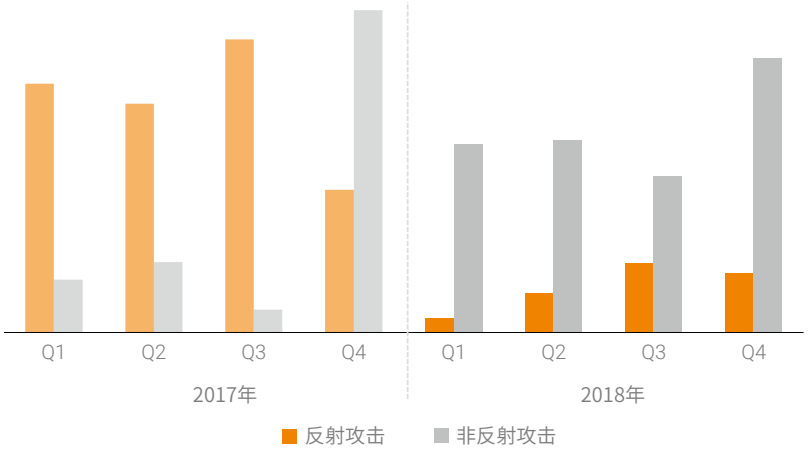
2018 年，我们监控到 DDoS 攻击次数为 14.8 万次，攻击总流量 64.31 万 TB，与 2017 年相比，攻击次数下降了 28.4%，攻击总流量没有明显变化。这主要是因为 DDoS 攻击规模逐年增大，即中大型规模的攻击有所增加。

图 5.9 攻击次数与攻击流量



从全年来看，2018 年 DDoS 攻击次数明显下降，得益于对反射攻击有效的治理。2018 年以来，CNCERT 组织各省分中心，联合各地运营商、 云服务商等对我国境内的攻击资源进行了专项治理，包括使用虚假源地址治理以及对反射攻击源通告等手段。通过治理，有效的减少了反射攻击的成功率，迫使攻击者转向其它攻击手段。从数据来看，2018 年反射攻击减少了 80%，而非反射攻击增加了 73%，反射攻击仅占 DDoS 攻击次数的 3%。

图 5.10 反射攻击次数与其他类型的攻击次数对比图



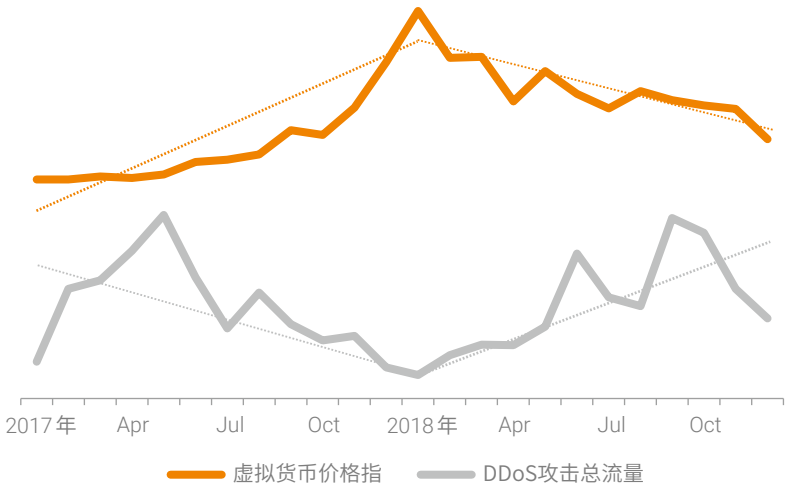
数据来源：电信云堤，ATM

从 2018 年各月攻击次数来看，上半年 DDoS 攻击逐月小幅增长，而下半年有加速增加的趋势。我们认为，DDoS 攻击逐月增加，与虚拟货币的价格回落相关。在《2017 DDoS 与 Web 应用攻击态势报告》[1] 中，我们指出，随着虚拟货币的升值，黑产开始将掌握的“优质” Botnet 资源从犯罪成本较高的 DDoS 攻击活动转而投向犯罪成本相对较低但收益更高的挖矿活动中。在 2018 年，随着虚拟货币的价格回落，挖矿的收益日益减少，攻击者选择 DDoS 攻击的倾向增高，DDoS 攻击逐月增加。

将各月份比特币价格与 DDoS 总流量趋势对比，其 Pearson 相关系数为 -0.48，呈一定的负相关性，这更加证实了我们去年的观点。

1 http://blog.nsfocus.net/2017-ddos-Web-report/

图 5.11 比特币价格与 DDoS 攻击总流量趋势对比图



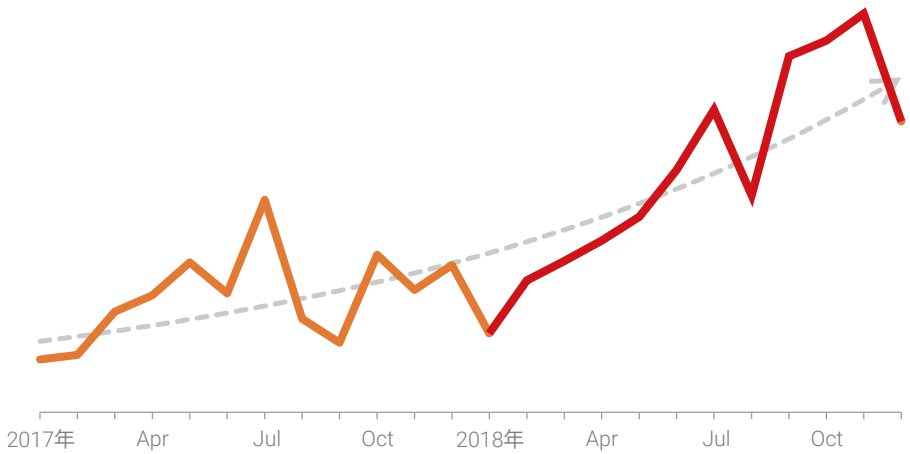
数据来源：电信云堤

近年来，超大规模的攻击事件日益普遍。2018 年 3 月，著名代码托管网站 GitHub 遭受到峰值达到 1.35Tbps 的 DDoS 攻击，而截至目前， DDoS 攻击已经创造了达到 1.7Tbps 峰值带宽的攻击 [1]。

从最近两年各月数据来看，攻击峰值在 100Gbps 以上的大型攻击的次数呈加速上升趋势。大流量攻击事件的增多，说明攻击者掌握的攻击资源规模上升和攻击能力的增强。

1 https://www.wired.com/story/github-ddos-memcached/

图 5.12 峰值大于 100Gbps 的攻击次数变化



数据来源：电信云堤

无论是 DDoS 攻击能力的普遍提高，还是平均峰值创历史新高，都说明 DDoS 攻击态势的严峻性。可以说，黑客普遍拥有了释放特大流量的能力，并且能力仍然处于持续快速提高的进程中，这是防御和治理人员需要应对的挑战。

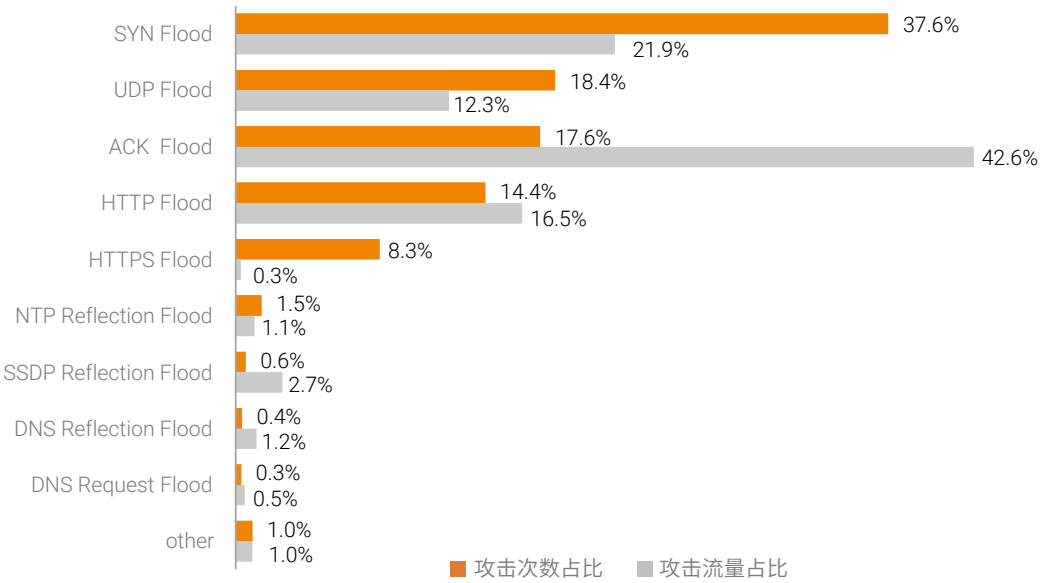
5.3.2 攻击类型分析

2018 年，主要的攻击类型[1] 为 SYN Flood，UDP Flood，ACK Flood，HTTP Flood，HTTPS Flood，这五大类攻击占了总攻击次数的 96%，反射类攻击不足 3%。和 2017 年相比，反射类型的攻击次数大幅度减少了 80%，而非反射类攻击增加了 73%，之所以如此，是相关部门对反射源进行了有效的治理。

从攻击流量来看，ACK Flood 占了全部流量的 42.6%。因为某些行业（如游戏），用户量大，会话数多，长连接，容易受到 ACK 攻击，并且 ACK 报文比较大，从而产生大量的攻击流量。

1 此处对混合攻击进行了拆解

图 5.13 攻击类型的攻击次数分布



SYN Flood 依然是 DDoS 的主要攻击手法。攻击者利用 TCP 协议缺陷，发送大量的 TCP 连接请求，从而使得被攻击方资源耗尽的攻击方法。ACK Flood 很少单独使用，经常与 SYN Flood 一起使用，使主机和防火墙费大量的精力来计算 ACK 报文是否合法以致不堪重负，既消耗了目标的资源，又进行了流量攻击。

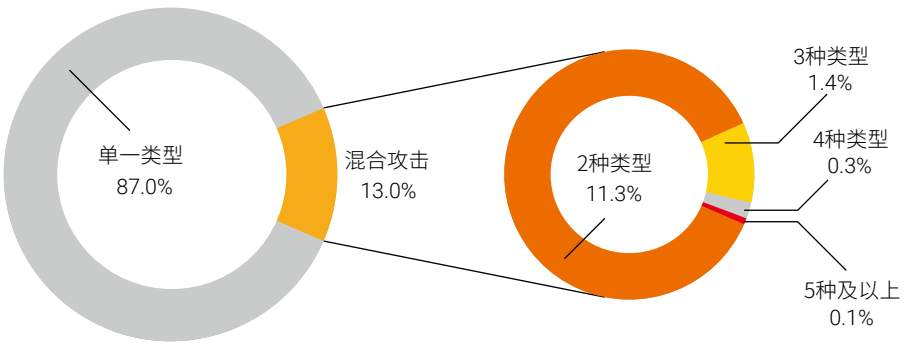
UDP Flood 是长期活跃的流量型 DDoS 攻击。常见的情况是利用大量 UDP 小包冲击 DNS 服务器或 Radius 认证服务器、流媒体视频服务器。UDP Flood 无需建立连接，协议简单，容易打出大流量攻击报文，因此深受攻击者的青睐。

HTTP Flood/HTTPS Flood 是针对 Web 服务在应用层发起的攻击，攻击者通过模拟正常用户对网站执行网页访问行为。这类攻击会引起严重的连锁反应，当客户端不断请求而且附带大量的数据库操作时，不仅直接导致被攻击的 Web 前端响应缓慢，还间接攻击到后端服务器程序，严重的情况下可造成数据库等后端服务卡死，崩溃，甚至对相关的主机，例如日志存储服务器和图片服务器都带来影响。

从 DDoS 攻击事件来看，有 13% 的攻击事件使用了多种攻击手法。攻击者根据目标系统的具体环境灵动组合，发动多种攻击手段，既具备了海量的流量，又利用了协议、系统的缺陷，尽其所能地展开攻

势。对于被攻击目标来说，需要面对不同协议、不同资源的分布式的攻击，分析、响应和处理的成本就会大大增加。

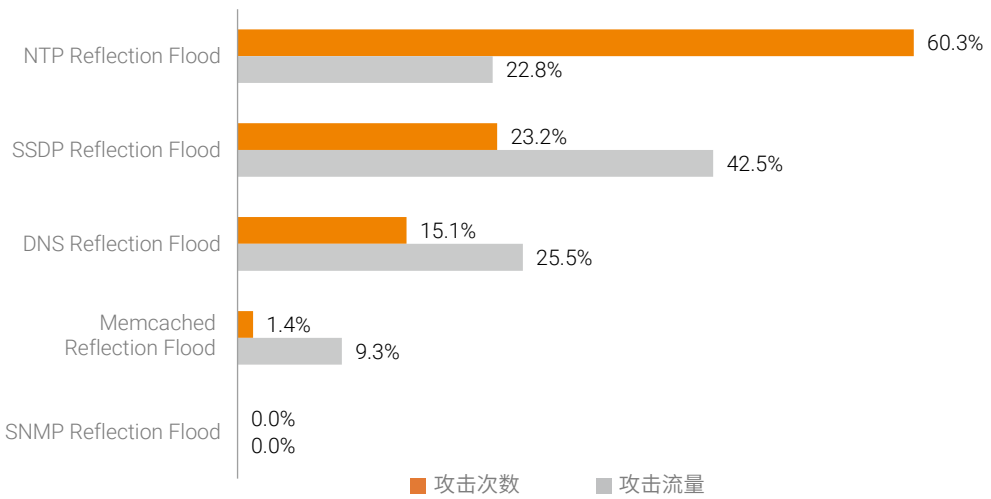
图 5.14 混合攻击分布



2018 年，虽然反射类型的攻击次数大幅减少，仅占全部攻击的 3%，但攻击流量却占了全部流量的 10%，由于反射攻击对流量的放大作用，其危害仍不可忽视。

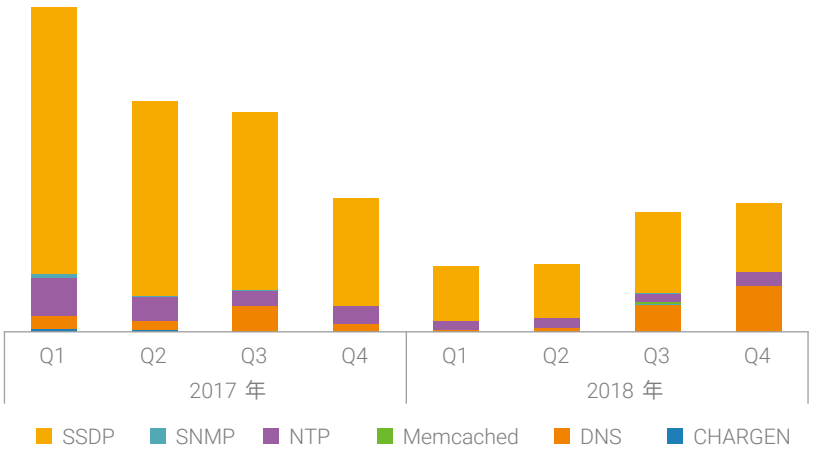
从攻击次数来看，NTP 反射攻击独占鳌头，在全部反射攻击中占比 60%；从产生的流量来看，SSDP 反射攻击占了全部反射攻击流量的 42%。

图 5.15 各类反射攻击次数与流量占比



从活跃反射源数量来看，2018 年下降了 60%，其中 SSDP 反射源有显著的减少，而 DNS 反射源有一定程度的增加。由此可见，相关部门对攻击源的治理，特别是 SSDP 反射源，是卓有成效的。

图 5.16 活跃反射源数量变化

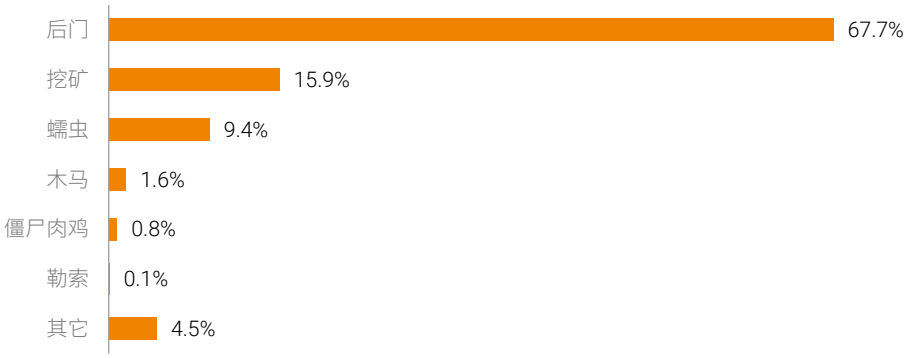


6

恶意软件观察

在 2018 年的活跃恶意软件中，活动程度从高到低依次是后门、挖矿、蠕虫、木马、僵尸肉鸡[1]。后门程序隐蔽性高不易被发现，依旧保持着极高的活跃度。虽然，随着虚拟货币市场的持续缩水，挖矿活动也有所减少，但其活动频繁程度仍仅次于后门程序排名第二。

图 6.1 恶意软件类型分布

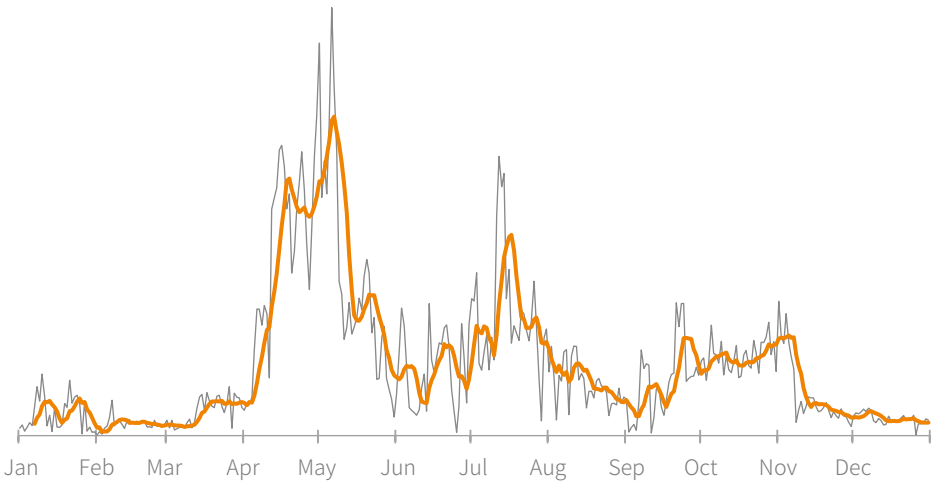


6.1 后门

在信息安全领域，后门是指绕过安全控制而获取程序或系统访问权的方法。后门的最主要目的就是方便以后再次秘密进入或者控制系统。攻击者往往通过一些欺骗手段，诱使用户主动进行一些操作，比如下载或打开装有恶意代码的文件，用户在毫不知情的状况下在算机上创建了一个后门。或者，攻击者在利用其它攻击方式攻陷一台主机后，在该主机上创建后门，这样既可以保证轻而易举的随时入侵又有很好隐蔽性，难以被发现。

1 一般来说，恶意样本的分类没有统一标准，此处是根据代码最核心的特征或功能进行的简单划分，比如：如蠕虫以大规模自传播能力为核心特征、木马的核心功能为信息窃取与其他复杂的远程控制、僵尸（肉鸡）程序的特征在于构建僵尸网络并发挥使用集群进行黑客行为（例如 DDoS 和挖矿）、后门程序和木马比较 像但是前者更偏重于为后面的攻击 供持久化的入口。

图 6.2 后门程序活动抽样统计



后门程序在1月至3月底期间，活动次数较少，起伏不大。4月至10月底都属于活跃期，中间波动较大，4 月、5 月是全年活跃度的高峰时期。11 月开始活动次数逐渐减少，并在一个较低值趋于稳定。

早在 2014 年，国内电子厂商生产的 NetCore 系列路由器等设备被披露存在高权限后门。NetCore 漏洞的存在，使得攻击者可以通过此漏洞获取路由器 Root 权限，可完全控制受影响的产品。目前，很多互联网上还存在有该后门的路由器设备，而这些设备被国外物联网僵尸网络 Gafgyt 家族再次利用。由 18 年全年的数据监测情况可知，该后门利用相关的活动十分活跃。

6.2 挖矿

2017 年加密货币的价格持续飙升，在利益驱使下，传统勒索软件操纵者中很大一部分转向加密货币的挖掘。比特币、门罗币、以太坊等多种加密货币交易一度十分活跃。据不完全统计，目前全球有超过 1600 种加密货币，总市值超过 3400 亿美元。18 年虽然加密货币的价格已大幅缩水，但项目开发并未停滞，市场活动依然活跃，挖矿依旧是攻击者变现的重要手段，短时间内并不会出现颓败现象。

图 6.3 挖矿程序活动抽样统计

2018 年挖矿类恶意程序活跃度震荡起伏，但总体呈现上升趋势。我们监测到上半年从 4 月份开始，挖矿活动渐有起色，五月中旬到达上半年的一个小高峰。相较于上半年的活动情况，下半年活跃度明显波动较大。8 月、9 月进入相对低迷的时期，10 月迅速回温，随后波动经历了一段时间的低谷。这种现象并没有持续很久，12 月突飞猛进一跃达到了全年的峰值。

值得一提的是，在所有挖矿病毒中，WannaMine 最为活跃，传播过程利用了永恒之蓝漏洞。永恒之蓝是美国国家安全局 NSA 旗下的黑客组织 Equation Group 开发的网络攻击工具，利用 Windows 系统的 SMB 漏洞可以获取系统最高权限。

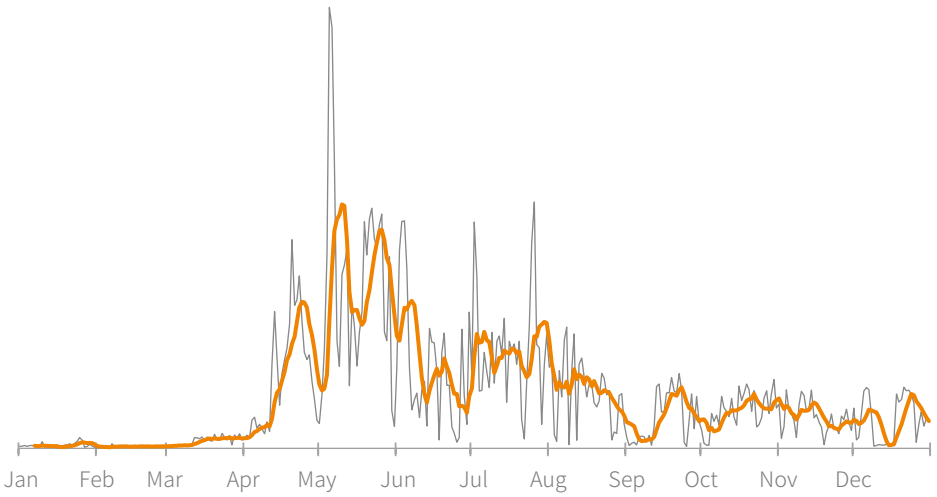
2017 年 WannaCry 席卷全球，五个小时内，包括英国、俄罗斯、整个欧洲以及中国国内多地中招，最终影响国家高达 150 多个，经济损失极其严重。同样是永恒之蓝漏洞，2018 年，WannaMine 家族成为挖矿大军中的主力，上半年在所有检测到的挖矿活动中，占比超过了 70%，传播速度令人咂舌。在攻击武器的选择上，永恒之蓝漏洞攻击被多数挖矿病毒家族所青睐。虽然从 17 年 5 月份曝光至今已超过一年半的时间，但利用永恒之蓝漏洞的攻击仍屡试不爽，这应当引起各行业从业者的重视。

在 18 年的挖矿活动中，我们监测到更多的矿工选择了门罗币而非比特币。门罗币就比特币而言具有更好的匿名性，在交易过程中不会涉及到钱包地址，更加注重交易者的隐私。此外，门罗币降低了挖矿的门槛，任何的 CPU 或 GPU 都可以参与进来，这种对普通用户的开放性也为黑客提供了更多牟利的机会。

6.3 蠕虫

在《2018 上半年网络安全观察》 中我们指出，大部分蠕虫病毒最早发现时间距今都有 5 年以上，可见这些蠕虫病毒繁衍、进化的能力以及在网络中彻底清除的难度。从全年的监测数据来看，这一现象仍然存在。2018 年全年监测到的最为活跃的蠕虫病毒种类共计 39 个，其中从发现至今超过 5 年的病毒占比 60% 以上。

图 6.4 蠕虫活动抽样统计



前 3 个月蠕虫活动较少，4、5 月份活动量急速上升，到达全年的峰值，下半年活跃度稍有起伏，不过总体呈下降趋势，并趋于稳定。结合全年数据来看，活跃度最高的两个蠕虫病毒分别为：

W32.Faedevour 今年上半年中该病毒的表现就尤为突出，综合全年数据来看活跃度仍高居首位，其活动次数远超排名前 5 的其他病毒。它在受感染的计算机中打开一个后门，窃取信息，接受远程攻击者的命令执行截图、下载文件、发送文件给攻击者等一系列操作，该蠕虫试图通网络驱动器和共享文件夹进行传播。

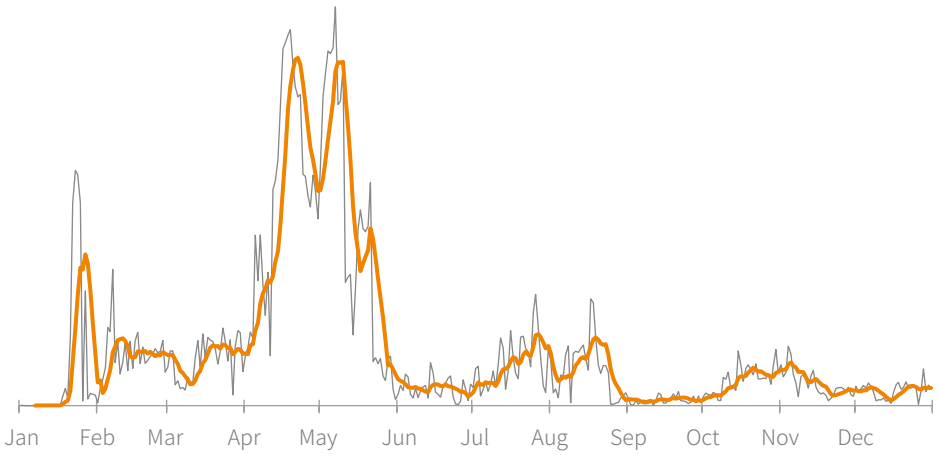
SQL Slammer 该蠕虫病毒利用 SQL Server 弱点采取阻断服务攻击 1434 端口并在内存中感染 SQL Server，通过被感染的 SQL Server 再大量的散播阻断服务攻击与感染，造成 SQL Server 无法正常作业或宕机，使内部网络拥塞。

6.4 木马远控

木马的核心功能为信息窃取与其他复杂的远程控制。与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。而现实中病毒的分类往往没有统一的标准，木马病毒也可以拥有蠕虫特征。在此，我们以木马的核心功能作为简单的划分。

今年是信息泄露尤为严重的一年，从 Facebook 到 A 站再到圆通、华住、万豪等数以亿计的个人信息遭到窃取，与此同时，登录凭证、敏感文件、银行和支付信息等仍是黑客攻击的目标。

图 6.5 木马活动抽样统计



2018 年上半年木马程序相当活跃，4 月初到 5 月底是爆发期，下半年则相对低迷，波动不大。木马活跃度整体虽略有下降但暗云系列仍层出不穷，活动依旧频繁。从 2015 年至今，暗云木马已感染数以百万的计算机，并经过了几次的更新迭代，各变种也层出不穷，查而未绝。其中 Bootkit 木马是迄今为止最复杂的木马之一，其触角已发展到了黑色产业的方方面面。

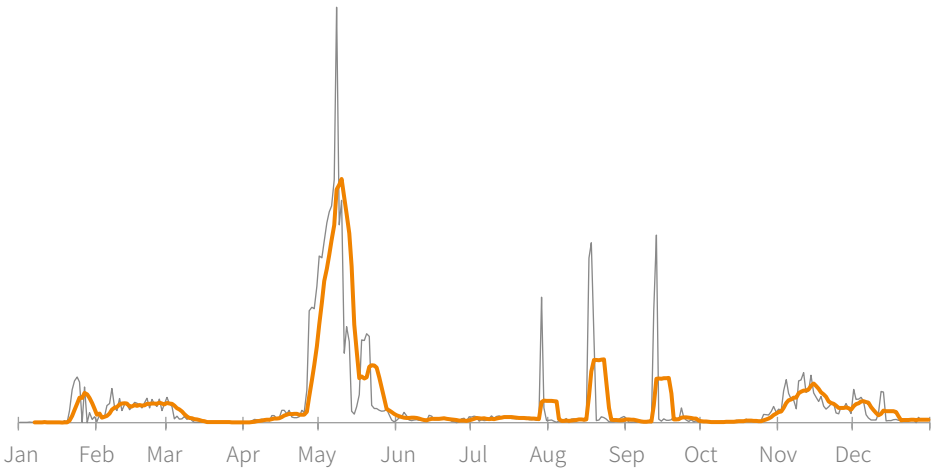
此外，在我们监测到的通信中，XCodeGhost 木马通信仅次于暗云系列。2015 年 XcodeGhos 首次被发现便引起了安全圈的广泛关注。Xcode 作为苹果 APP 开发工具被不法分子利用将恶意代码植入到 Xcode 安装包中并发布到网上。由于部分开发者没有从正规途径下载 Xcode，而是使用含有恶意代码的工具编译 APP，从而影响到大量 APP 用户。控制者可以收集用户设备上的诸多信息，甚至直接控制用户设备进行其他攻击。这提醒我们各开发者和组织也要敲响警钟，注重安全性审核。

6.5 僵尸肉鸡

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 可构成网络攻击的重要媒介，通过控制大量肉鸡发起多种攻击，甚至是结合新的攻击类型发动未知攻击，常见的攻击行为包括 DDoS 攻击，发送垃圾邮件，加密勒索，资源滥用等。

Botnet 目前已有相当成熟的商业运作，在 BaaS”(Botnet as a Service，僵尸网络即服务) 的模式下，平台化日趋成熟，普通用户亦可通过简单的操作来发起大规模的僵尸网络攻击事件，极大的降低了攻击者门槛。

图 6.6 僵尸程序活动抽样统计



对僵尸网络全年的监控可以发现，5 月份是活动的爆发期，其他月份攻击次数相对较低，存在小范围的波动。在《2018 上半年网络安全观察》中我们提到，BillGates 僵尸网络和 Artemis 僵尸网络家族非常活跃。综合 2018 全年数据来看，BillGates 首屈一指，远超其他家族。

BillGates 首次披露于 2014 年，是多平台家族，主要运行在类 *nix 平台。在诞生后的 4 年时间内，BillGates 家族不断发展，陆续产生了运行 Windows 平台下的 Webtoos 变种与专门用于感染 arm 等嵌入式设备的 BillGates.lite 系列变种等。由于其提供了 UI 界面使得攻击者使用起来更加便利，因此颇受

黑产组织的欢迎。2018 第一季度，BillGates 家族进入全面活跃期，短时间内进行了大量的攻击并迅速转入静默状态。此次攻击事件持续时间长，攻击范围广泛，具有很高的分析与追溯价值 。

Gafgyt 在 IoT 领域十分活跃，我们于 2017 年开始对这一家族进行了长期的跟踪。在《2018 Botnet 趋势报告》中我们指出，Gafgyt 家族 Botnet 已经实现了由传统的出售攻击流量的获利方式，转变为通过云平台提供僵尸主机租赁服务。在这样的销售模式下，Botnet 的使用门槛被进一步降低，其攻击势必会波及更多的领域。因此，如此类模式成为主流，Botnet 也将整体进入更高的威胁等级。

7

物联网威胁观察

7.1 物联网家族样本分布

我们对 2018 年从威胁捕获系统中捕获的物联网恶意家族的样本数量进行分析，如图 7.1 所示；又对 NTI 和 VirusTotal 的情报系统中的恶意家族的样本数量进行分析，如图 7.2 所示。虽然两张图的数据源不同，但均表明 Gafgyt 家族和 Mirai 家族的样本总和均为前两名，因此物联网恶意家族趋向一致性。主要原因为 Mirai 家族和 Gafgyt 家族的源码已经公布，可以随意进行修改，这些家族变种的修改部分主要集中于 C&C 地址和攻击方式。而这正是“工具党”最显著的特征之一，可见大多数攻击者为工具使用者。

图 7.1 威胁捕获系统的恶意家族样本数量占比

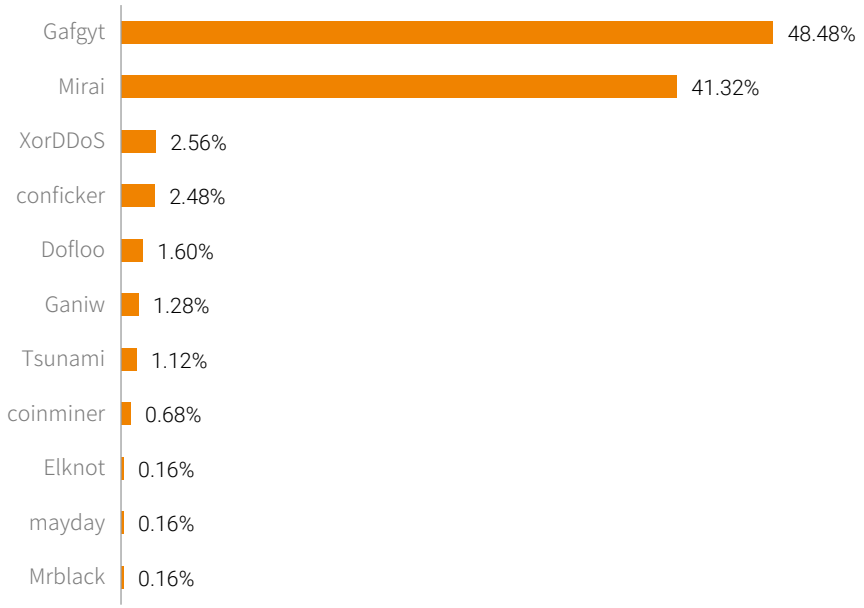
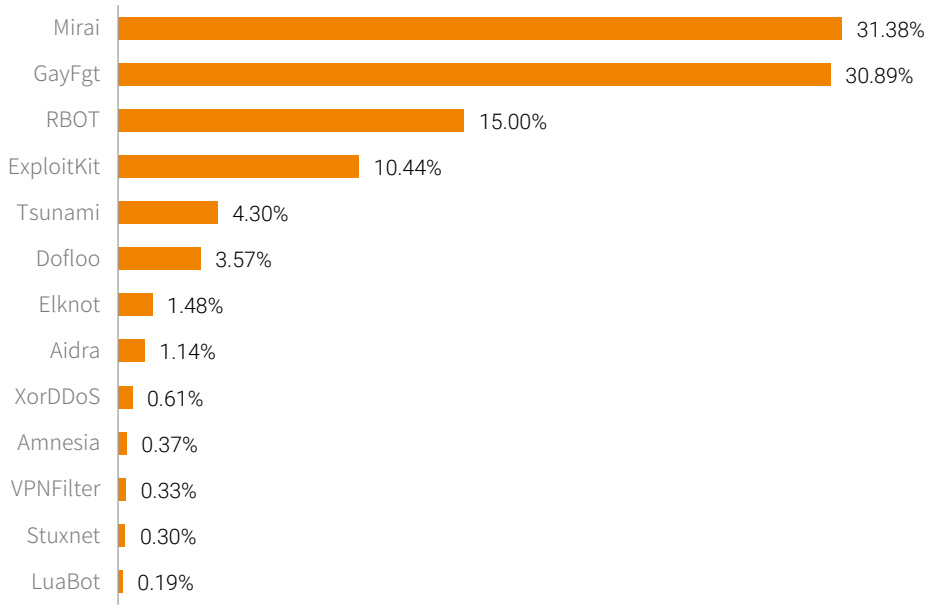


图 7.2 NTI 和 VirusTotal 的恶意家族样本数量占比



通过捕获到的数据分析可知，物联网中的僵尸网络开始服务化，集中化，基本形成托管制度，绝大部分攻击者无需自己构建僵尸网络，通过购买 DDoS 服务即可完成攻击，而服务提供者在不断的改进感染代码，增加漏洞利用方式，以获取更大量的僵尸网络主机，从而提供更大带宽的攻击服务。

7.2 物联网恶意挖矿

对于 2018 年 4 月份发生的 20 万台 MikroTik 路由器遭到恶意攻击沦为挖矿帮凶的事件，本节对其进行持续后续跟踪，对 2018 年 10 月份的恶意挖矿数据进行分析，发现 Coinhive 家族控制的物联网设备数量尚在 2.6 万左右。

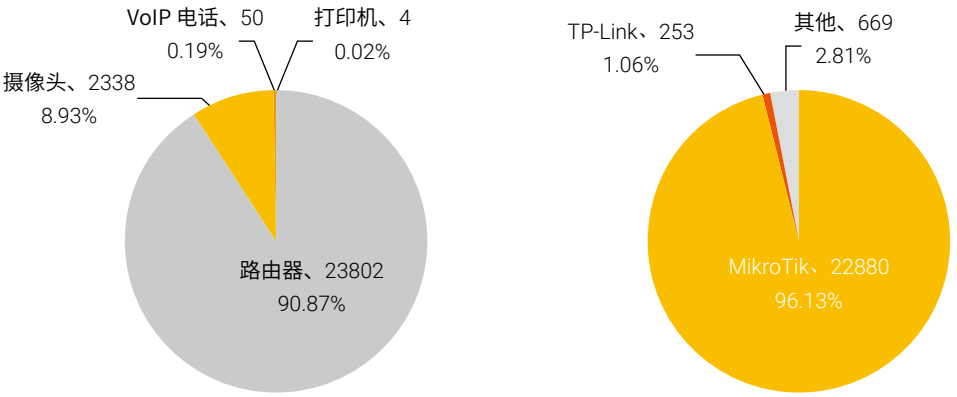
Coinhive 在 2018 年 10 月控制的物联网设备仍有 2.6 万台，绝大部分仍是 MikroTik 的路由器，巴西为重灾区，物联网设备难升级修复是物联网安全的巨大挑战。

表 7.1 2018 年 10 月份 Coinhive 家族控制的物联网设备数量

月份	家族	物联网设备数量
201810	Coinhive	26261

通过表 7.1 可知，在 2018 年 10 月份可监控到的 Coinhive 家族控制的物联网设备数量为 2.6 万，虽较 2018 年 4 月有减少，但危害依然存在。我们接下来将对 Coinhive 家族控制的物联网设备类型以及重要类型的厂商进行分析。

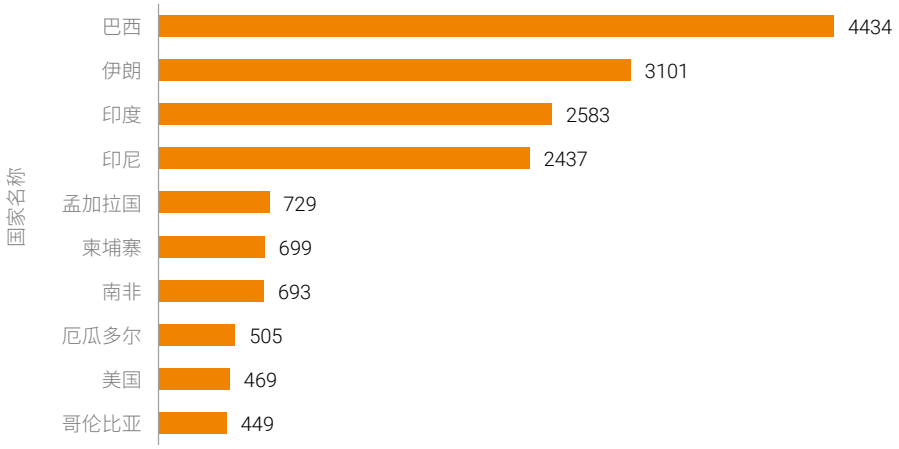
图 7.3 受 Coinhive 控制的物联网设备的类型分布（2018 年 10 月）



（a）受控物联网设备的设备类型分布　　（b）受控物路由器的厂商分布

我们发现 Coinhive 家族控制的物联网设备主要为路由器，占所有类型的 90% 以上，且 MikroTik 的路由器占所有路由器的 96% 以上，如图 7.3（b） 所示。

图 7.4 受 Coinhive 控制的 MikroTik 路由器的国家分布（2018 年 10 月）



与 2018 年 4 月份 Coinhive 控制的 MikroTik 的路由器分布一样，在 2018 年 10 月份巴西仍然是重灾区。

从 2018 年 3 月漏洞爆出，4 月出现大规模恶意挖矿事件，到 10 月依然有大量的设备受控，这说明大量物联网设备没有得到妥善维护，其原因一方面与用户安全意识不强有关，另一方面，普通用户对这些物联网设备知之甚少，物联网厂商也没有提供自动化升级或其他有良好用户体验的升级机制。

7.3 物联网攻击资源分析

结合绿盟科技的物联网威胁情报、DDoS 攻击事件和物联网设备进行关联，进一步分析 DDoS 攻击源 IP 中的物联网设备比例可知，DDoS 攻击源 IP 中有 3.14% 为物联网设备，虽然占比较小，但是由于 DDoS 攻击源 IP 的基数较大，物联网设备所进行的 DDoS 攻击仍然不可小觑。

图 7.5 参与 DDoS 的物联网设备 IP 与全部 DDoS 的 IP 占比

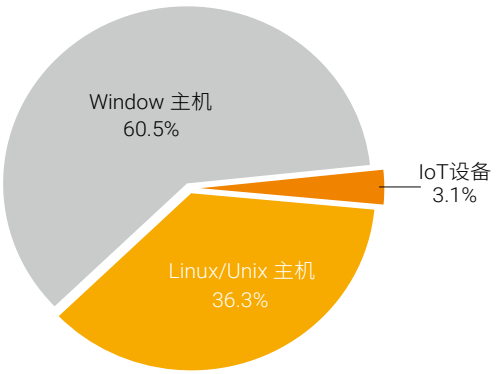
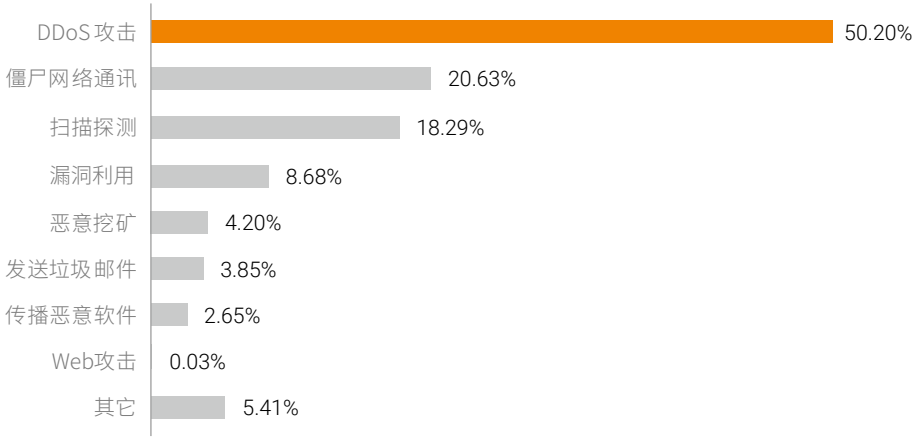


图 7.6 异常物联网设备异常行为占比[1]



我们监测到，全球异常物联网设备的 IP 总量为 408685 个，在全球物联网设备中占比 0.94%。其中参与过 DDoS 的物联网设备所使用过的 IP 数量为 205167，占全部异常物联网设备的 IP 总量的 50.20%。通过图 7.6 异常物联网设备异常行为占比中以看出，在异常物联网设备的异常行为中 DDoS 攻击占比是各个种类中最高的。可以说，异常物联网设备主要被利用进行 DDoS 攻击。

1 由于某些设备具有多种异常行为，故图中累计百分比大于 100%。

绿盟威胁情报中心（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。

绿盟科技天枢实验室：

绿盟科技天枢实验室聚焦安全数据、AI 攻防等方面研究，以期在“数据智能”领域获得突破。

编辑

绿 盟 科 技 鄢君 (平面设计)

THE EXPERT
BEHIND GIANTS
巨人背后的安全专家

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

绿盟科技官方微信