NSFOCUS

2018 上半年 网络安全观察

绿盟威胁情报中心（NTI）

© 2018 绿盟科技

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。

2018 上半年网络安全观察

绿盟威胁情报中心（NTI）

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

2018 年上半年，在我们持续监控到的超 2700 万攻击源 IP 中，有 25% 在历史上曾被监测到多次攻击行为，我们称之为“惯犯”。

近年来，安全事件逐渐成为媒体的宠儿，尤其是个人信息泄露、银行资金窃取和 IoT 设备的攻击利用事件，牵动着众人的眼球。在公众关注度方面，从近两年的百度指数就能看出，“个人信息泄露”和“黑客”等关键词的整体日均值都在历史中高位波动，网络安全和信息安全已经不仅仅是一个技术问题，而是关乎普罗大众的民生问题。

与此同时，安全厂商的视角也在慢慢变化。从 RSA 近年的主题上看，2016 年的“Connect to Protect”，2017 的“Power of OpportUNITY”到 2018 年的“Now Matters”，同时，关键词也从往年的威胁情报、人工智能到今年的应急响应和威胁狩猎，可以看出，安全厂商们不再满足于概念性的奔走呼号，联动防御和破除孤岛已成共识，在多年的技术积累上厚积薄发，真真正正化被动为主动，切切实实关注落地实效和响应时效。

漏洞发现，攻击利用和应急响应，是攻防双方角力的主战场。兵者诡变，从去年的臭名昭著的 Wannacry 事件到后来的 WannaMine 和 Smominru，永恒之蓝漏洞相继被用在勒索软件和挖矿僵尸网络中，攻击的目标和攻击的手段在变，唯一不变的是攻击者对利益的诉求。兵贵神速，安全的战役，难就难在防御者如何才能在攻防条件不对等的情况下，快速地跟进形势，扩充自己的武器库和提前布局。孙子曰“知彼良知，胜乃不殆；知天知地，胜乃不穷”。威胁情报的核心正是一个“知”字，从数据到信息到知识，这几年来的落地实践逐渐让安全厂商能够从海量的攻击数据、基础数据和外部情报中，去伪存真，抽丝剥茧，对攻击者个体能够形成多个剖面的详尽刻画，同时对攻击者群体能够快速提取共性及关联，构建出网络空间的深层感知体系。

据绿盟威胁情报中心观测，近 20% 的攻击源发起过多种类型的攻击，其攻击类型的转换时序满足攻击链逐步深入的特性，例如百分之五十的 Web 攻击者会在随后尝试更为复杂的漏洞利用攻击。僵尸主机也有相当部分具备蠕虫的特性，在被感染后相继进行扫描和漏洞利用操作，快速补充僵尸军团的新生力量。同时，不同类型的攻击资源存在复用的情况，例如发起恶意扫描的攻击源，其中的

44% 在之后成为垃圾邮件源。一方面可以看出，攻击者较为关注自身的攻击成本，尽可能榨干获取的肉鸡价值。另一方面也可以看出，时间成本和规模效应也是攻击者关心的重点。

从攻击流量来看，挖矿病毒、蠕虫和木马等类型的恶意软件的活跃数量在 2 月下旬到 3 月上旬期间均有一定程度的回落或在低位徘徊，当时正逢新春佳节，一定程度上说明监测范围内的大部分攻击者应为华人。另一方面，比特币价格的持续萎缩似乎并没有影响攻击者对加密货币的投机偏好，挖矿类恶意程序在春节过后持续升温，其活跃状况暗合加密货币的涨跌趋势。在各类挖矿病毒中，针对门罗币的 WannaMine 尤为活跃，在挖矿活动中占比超过 70%。Palo Alto Networks 研究 [1] 也表明门罗币是恶意程序最为青睐的币种，5% 的门罗币经由恶意程序开采出来。

2018 年上半年，在我们持续监控到的超 2700 万攻击源 IP 中，有 25% 在历史上曾被监测到多次攻击行为，我们称之为“惯犯”。惯犯产生的可能原因有二，其一为攻击资源的复用，其二是暴露在公网上大量 IP 基础设施的安全状况长期得不到改善，被不同的攻击者利用。惯犯承担了 40% 的攻击事件，其中僵尸网络活动和 DDoS 攻击是惯犯们的主流攻击方式。

今年上半年披露的漏洞主要集中在中危漏洞，高危和漏洞比例与去年同期相比均有所下降。值得关注的是，其中获取和利用难度低、危害程度大的漏洞主要集中在数个移动设备或者网关类设备制造商的相关产品中。设备类和网关类产品通常覆盖面广，一旦被攻击者利用，影响面会快速扩大。

网络空间可以说是全世界的软件开发者构建起来的，软件开发流程越来越依赖世界各地的开发者通力合作，在这期间形成了各种包管理器、版本管理工具和代码分享与托管平台等软件开发基础设施。据观测，Pastebin 和 GitHub 等代码分享与托管平台日渐成为恶意软件的温床，许多恶意可执行文件经 base64 编码后上传，同时此类平台往往全站使用 HTTPS，使得该类行为在流量层面更加难以检测。同时，我们也监测到此类平台造成大量的信息泄露，例如开发者的代码段，电子邮件用户名密码，数据库结构等。

1 https://researchcenter.paloaltonetworks.com/2018/06/unit42-rise-cryptocurrency-miners/

1. 威胁观察

1.1 19.3% 攻击源参与多种类型攻击

按照攻击源 IP 的地区分布来看，北京、江苏、浙江、山东、广东等几个省份恶意 IP 最为集中，在全球范围内，中美两国仍然是攻击源最为集中的地区。攻击受害者的分布略有不同，从中国看，受害者集中于东南沿海地区，而在全球范围内，除中美两个网络大国，东南亚、欧洲地区也出现了较多的受害者。经济活动越频繁，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 1.1 攻击源及攻击目标国内分布

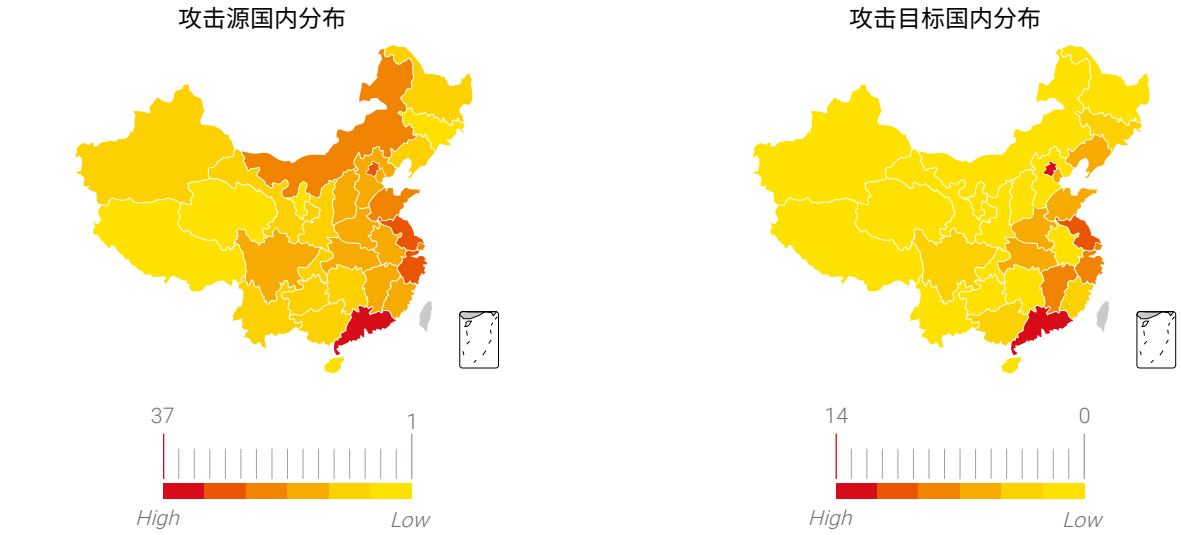
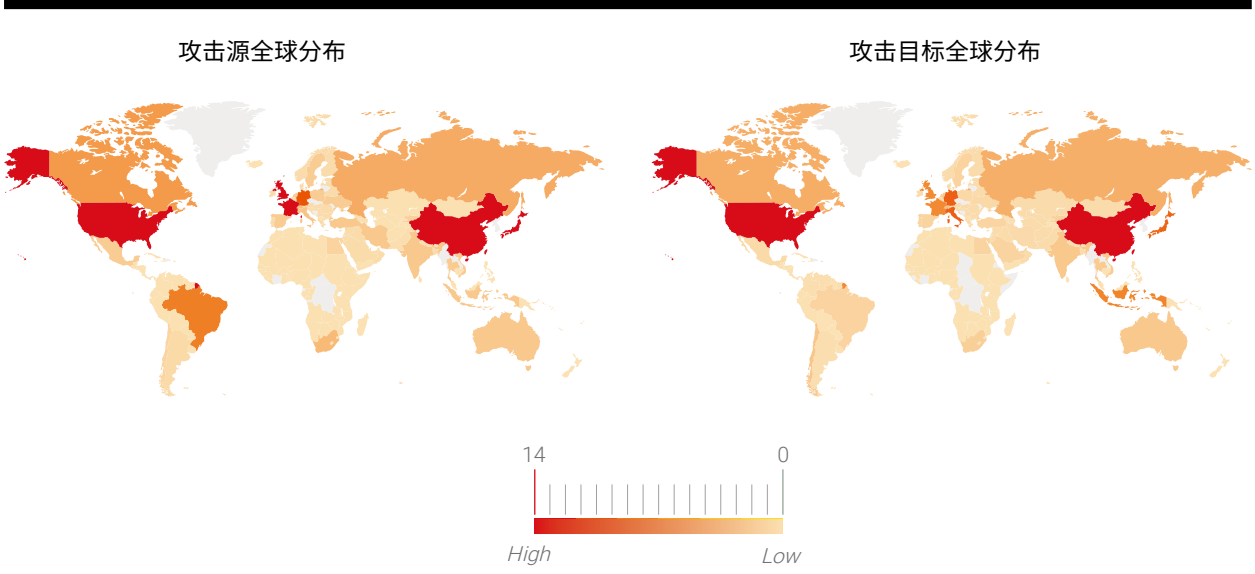
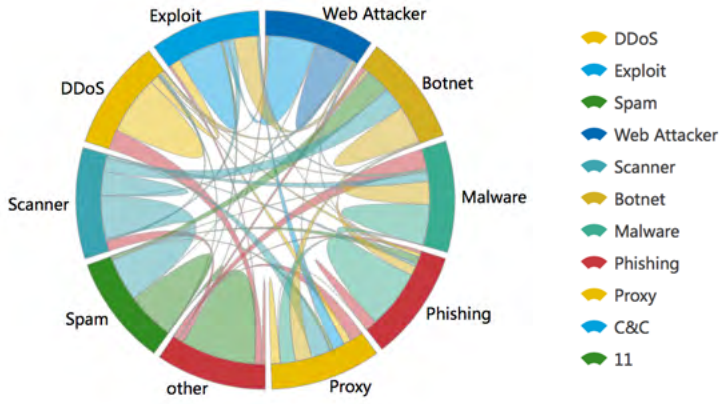


图 1.2 攻击源及攻击目标全球分布



从攻击源具体攻击行为看，约占 19.3% 的恶意 IP 进行过多类型攻击行为。

图 1.3 恶意 IP 类型转化示意图



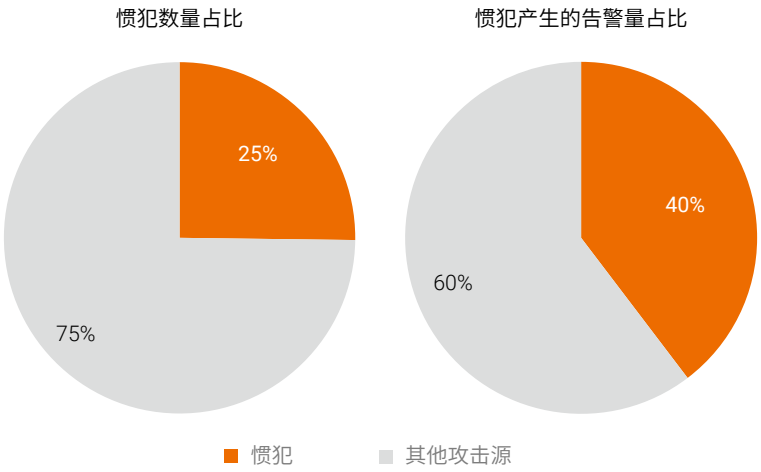
通过对这批攻击源的观察，我们看到攻击源攻击行为随时间演变的一些规律，例如：

- DDoS 攻击源相对比较固定，61% 的 DDoS 攻击源在较长的一段时间内持续地用作 DDoS 攻击资源。这和 DDoS 攻击的技术特征有关，例如常见的 DDoS 攻击资源包括反射器、受控主机或者设备，这类资源相对来说 IP 或者 IP 范围会比较固定。另外我们注意到，约 9% 的 DDoS 攻击源会在之后进行漏洞利用攻击；
- 进行漏洞利用的主机资源，有 24% 的可能性在之后被进一步标记为僵尸主机，我们认为，网络中有相当一批僵尸主机持续而频繁地进行着漏洞扫描与利用行为；
- 发起恶意扫描的攻击源，有 44% 的可能性在之后成为垃圾邮件源。恶意扫描和垃圾邮件攻击都需要较多的主机资源或者 IP 资源，因此同一批资源很有可能同时在两种攻击中被使用；
- 发起 Web 攻击的攻击源，有 50% 可能性在之后尝试过进行更加复杂的漏洞利用操作。大部分的攻击者并不具备精深的安全知识和技术，他们能够做的就是使用现成的工具、脚本大范围地搜捕漏洞主机。这些攻击中，Web 攻击复杂度相对较小，很多时候也是针对服务器进行攻击前最先尝试的步骤，通过 Web 漏洞拿到较低的权限或者其他敏感信息，利用前期搜集到的情报，黑客可以有针对性地进一步使用漏洞进行渗透和利用；
- 被用作代理的主机资源中，其中的 20% 随后成为恶意扫描攻击源。这样的主机资源，其中有一部分很可能是黑客最常使用的，甚至是黑客自己拥有的一批资源，一方面黑客使用它们进行流量代理来隐藏真实身份，另一方面也利用它们进行简单的攻击探测。

1.2 “惯犯”观察

18 年上半年在我们监控到的超 2700 万个攻击源中，惯犯数量不容小觑。所谓惯犯，即历史上被监测到多次恶意行为的攻击源，说明攻击所用资源的重复利用是普遍存在的。而这些攻击源中 25% 的惯犯承担了 40% 的攻击事件，威胁程度较大，应当引起足够重视。

图 1.4 惯犯数量及告警量分布图



中国、美国和俄罗斯的惯犯是最活跃的，攻击目标除中、美国两国外，加拿大、欧洲多国也有很大影响，但中、美两国仍属于受害重灾区。由国内分布情况来看，惯犯主要分布在我国沿海城市以及人口省，攻击目标集中在经济发达区域。

图 1.5 惯犯及攻击目标全球分布

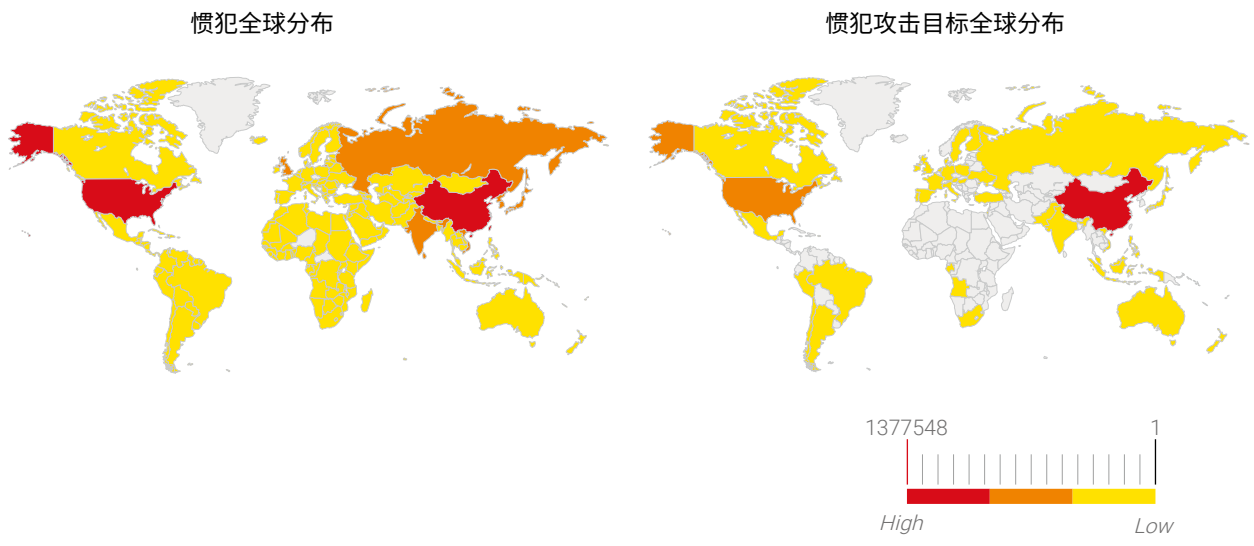


图 1.6 攻击者国内分布

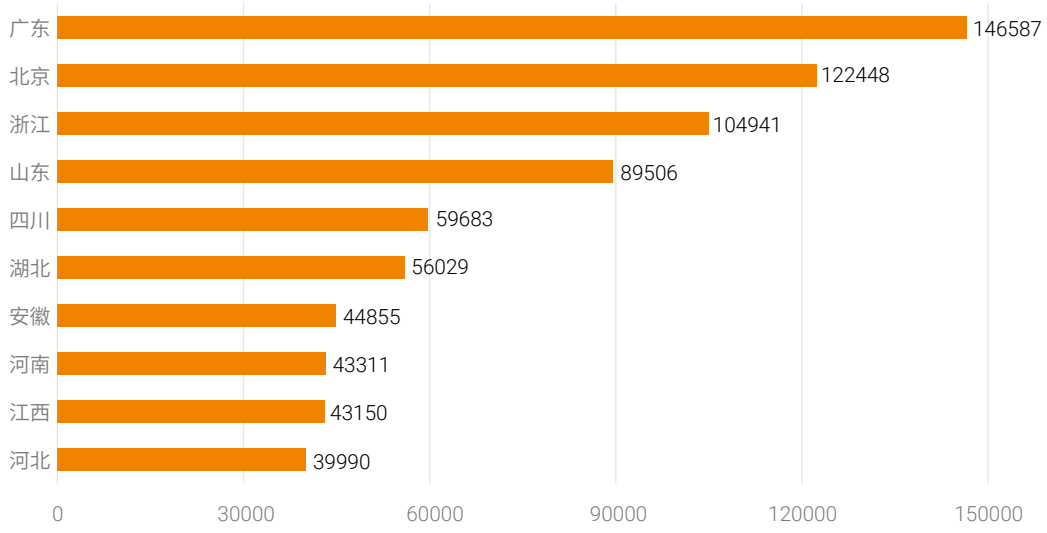


图 1.7 攻击目标国内分布

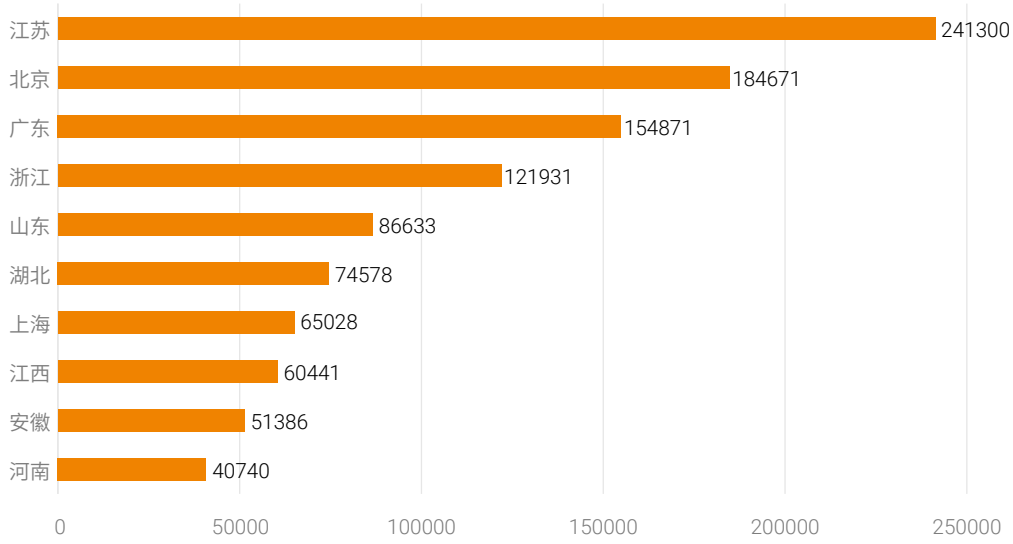
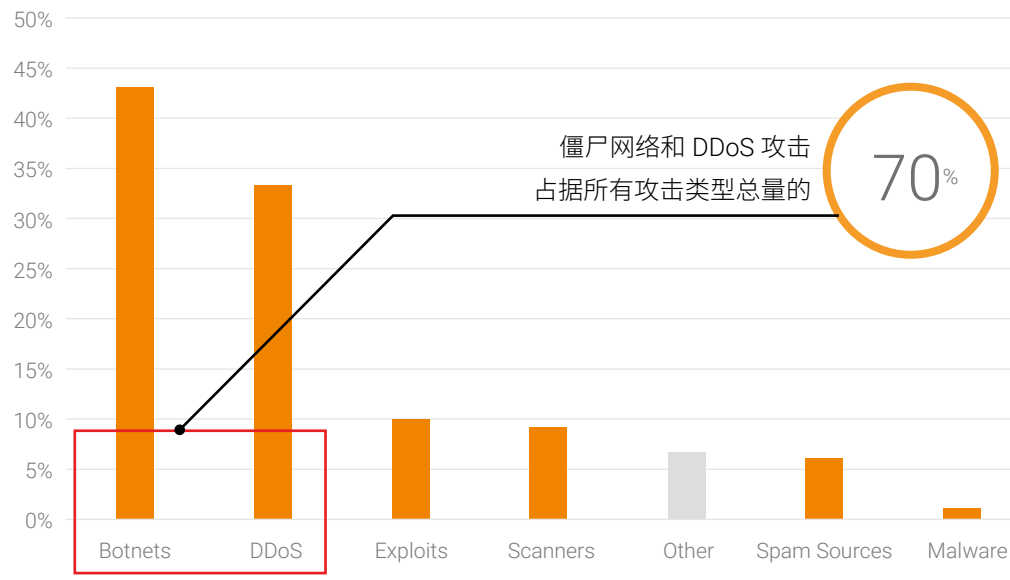


图 1.8 惯犯的主要攻击类型分布



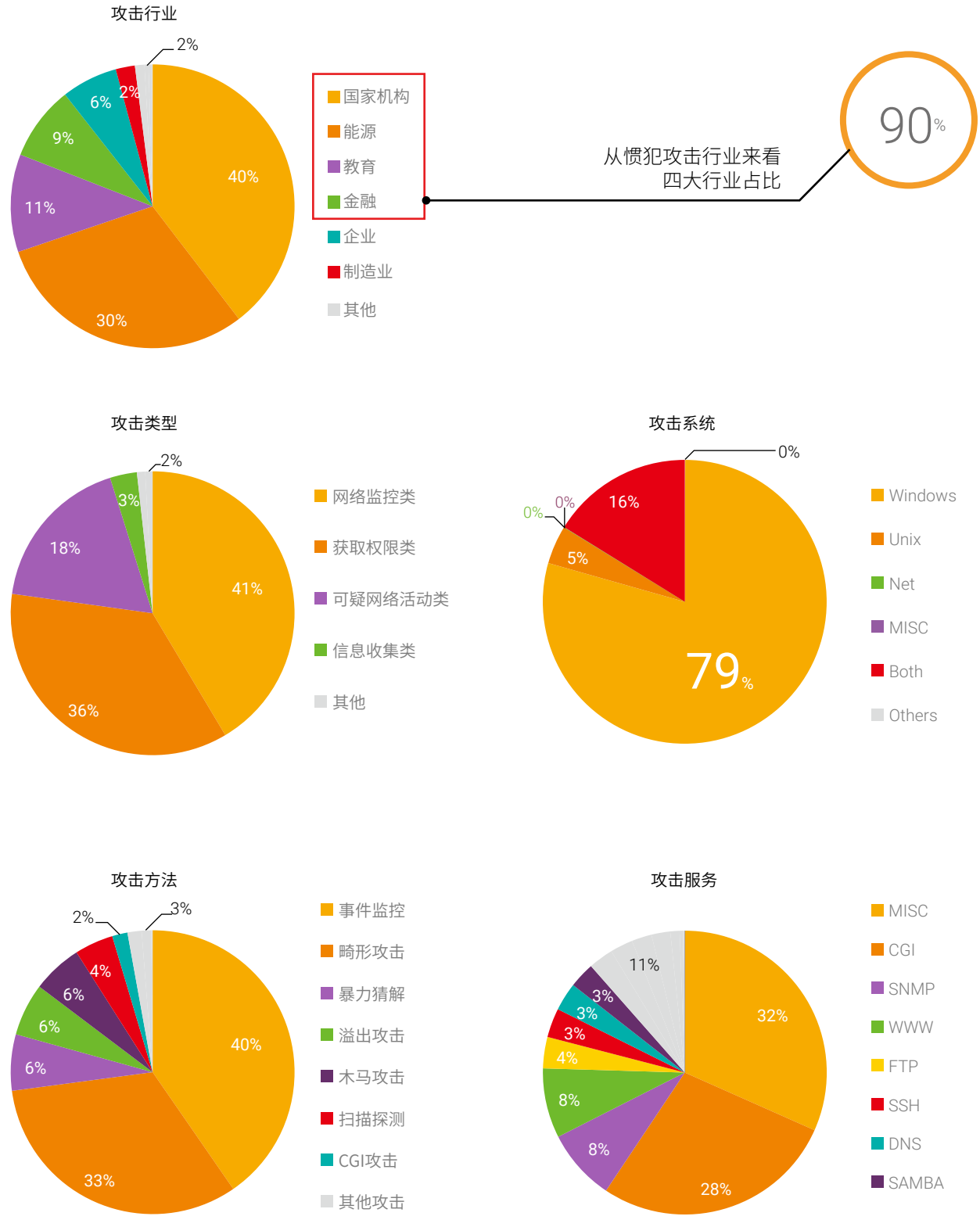
上图是惯犯产生的主要攻击类型，占所有攻击类型总量的 90% 以上。可以看出僵尸网络和 DDoS 攻击是惯犯们参与最多的攻击，占据了所有攻击类型总量的 70% 左右。

可以看出僵尸网络和 DDoS 攻击是惯犯们参与最多的攻击，占据了所有攻击类型总量的 70% 左右，仍然是两种最为流行的攻击方式。2017 年勒索软件席卷全球，而 DDoS 也未曾停止，攻击频率仍然呈现逐年增长的趋势。

针对这些惯犯，我们从其攻击特性的五个方面进行画像：

- 根据各行业自身的业务，以及对其特性和运营者弱点的不断了解，攻击者可以选择合适的攻击目标和方式，其目的、侧重点也会有所不同。从惯犯攻击行业来看，国家机构、能源、教育和金融四大行业占比 90%。上述四种行业体量较大，分布较广，数据更为敏感，往往会成为攻击者的重点对象；
- 网络攻击的发起都会有一个入口点，可能是对漏洞、开放服务扫描，可能是通过社工技术、可利用的公开数据、钓鱼邮件等获取更多信息，确定目标。网络监控、获取权限以及可疑活动类占比 95%，可以看出黑客在前期侦查和入侵的阶段做了很多工作；
- 相对其他操作系统来说，Windows 明显更受黑客青睐，79% 的攻击对象为 Windows 系统。除了及时修复处理系统本身的安全问题外，也要加强管理员安全、规范化的操作；
- 攻击方法中前五种占比 91%，其中事件监控和畸形攻击占比 73%。所谓畸形攻击是通过向目标系统发送有缺陷的报文，有些机器解析这些报文时耗时很大，甚至出错，更甚至崩溃，大量的这种报文将对目标机器构成很大威胁。此外，暴力猜解采用枚举方法逐一尝试，虽然简单粗暴，看起来效率不高，但是对于弱口令问题往往很容易构建字典，猜解成功，因此也是常用方法之一。

图 1.9 “惯犯”画像


攻击行业
2%
2%
6%
9%
40%
11%
30%
国家机构
能源
教育
金融
企业
制造业
其他
从惯犯攻击行业来看
四大行业占比
90%
攻击类型
2%
3%
18%
41%
36%
网络监控类
获取权限类
可疑网络活动类
信息收集类
其他
攻击系统
0%
0%
0%
16%
5%
79%
Windows
Unix
Net
MISC
Both
Others
攻击方法
2%
3%
4%
6%
6%
6%
40%
33%
事件监控
畸形攻击
暴力猜解
溢出攻击
木马攻击
扫描探测
CGI攻击
其他攻击
攻击服务
11%
3%
3%
3%
4%
8%
8%
32%
28%
MISC
CGI
SNMP
WWW
FTP
SSH
DNS
SAMBA

1.3 安全威胁事件频发

今年 6 月初，A 站千万级别的用户信息受到泄露，站点用户普遍受到影响，该事件受到广泛关注，真实的网络空间再一次用刻骨的事实为企业信息安全管理敲响警钟。在互联网环境中，攻防对抗一直在进行，除了传统利用技术手段进行攻击外，还有勾结内部人员进行逐步渗透，但很多时候由于管理措施和分析手段的缺失，一直到事件彻底曝光之前，大多数管理者都处于一无所知的黑暗中。因此建立不同级别、不同粒度的管理体系尤为重要，针对一些敏感的资源，有时可以通过关键行为特征指标进行画像，探寻一些潜在的风险。

绿盟威胁情报中心 (NTI) 对知名黑客组织和事件（包括 APT 事件）都有常年的跟踪，其中的一些关键信息，是非常高价值的判断指标。例如，在对事件中关键指标（IOC）进行监测的过程中，我们发现一些流量有可能预示着防护范围内存在风险。

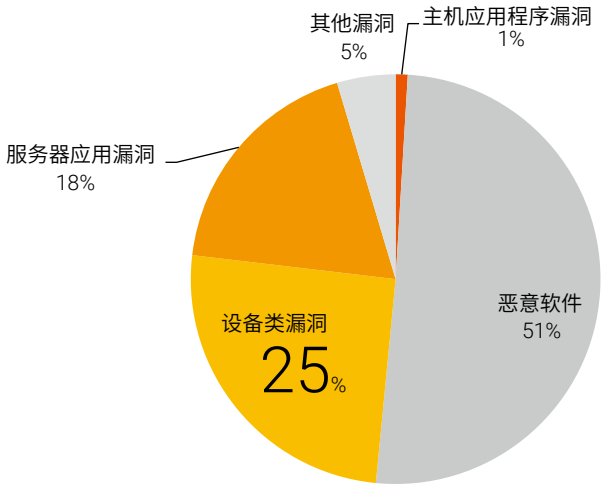
我们梳理了流量监测中，活动最频繁的一些 IOC 指标，在下面列举出对应的事件或组织，希望引起从业者的关注，并加强自己网络内的相关治理。

- **Hadoop Yarn 未授权访问攻击** 在 2017 年 5 月，绿盟威胁情报中心（NTI） 监测到，有大量的 Hadoop Yarn 被攻击。黑客通过未授权的方式直接调用 Hadoop Yarn 集群的 Rest API 接口，下达运算任务。这种攻击最终被大量用于数字货币挖矿。我们利用事件关键指标对事件中出现的一批攻击者进行了持续监测，截止今年 6 月，相关活动仍然频繁；
- **针对 WebLogic 主机挖矿恶意程序** 在 2017 年 12 月，绿盟威胁情报中心（NTI）检测到一系列针对 WebLogic 反序列化漏洞（CVE-2017-3248）的自动化攻击，感染后，主机中被植入挖矿程序，会大量消耗主机资源。通过基本画像，我们对关键指标进行了监测，在 2018 年上半年，相关的恶意利用与传播行为仍然非常频繁；
- **Operation Cobalt Kitty** 这是安全公司 Cybereason 报道的一系列攻击活动，这些活动集中在亚洲地区，目标在于攻陷商业公司获取其核心资料。这一系列攻击具有相似的手法和技术特征，Cybereason 在 2017 年 5 月将其命名为 Cobalt Kitty，公布了相关的分析结果。在我们的检测中 2018 年上半年在部分网络中仍然存在 IOC 的活动迹象，可能与该组织存在关联。

1.4 恶意软件活动猖獗，挖矿病毒成为新秀

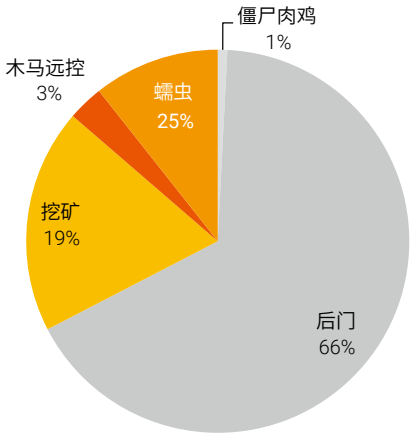
从总体情况上看，攻击流量中，针对各类漏洞的利用依然高度活跃，其中针对服务器应用漏洞的攻击占比达到 25%，而主机类应用程序漏洞的攻击流量占比为 3%。但值得注意的是，我们今年检测到异常活跃的恶意软件活动，在对其恶意网络行为的监测中，我们捕捉到包括挖矿、蠕虫、木马、僵尸网络、后门程序在内的多种类型的恶意活动迹象。

图 1.10 恶意活动类型分布图



从恶意软件的分布上看，活动频繁程度从高到低依次是后门、挖矿程序、蠕虫、木马远控、僵尸肉鸡。挖矿类程序是今年异军突起的恶意品类。近年，比特币、门罗币等多个币种在市场上的交易持续活跃，对加密货币的追逐在各个行业都有所体现，在安全行业内，我们观察到以 WannaMine 为首的各种恶意挖矿程序开始大规模传播。

图 1.11 恶意软件类型分布图

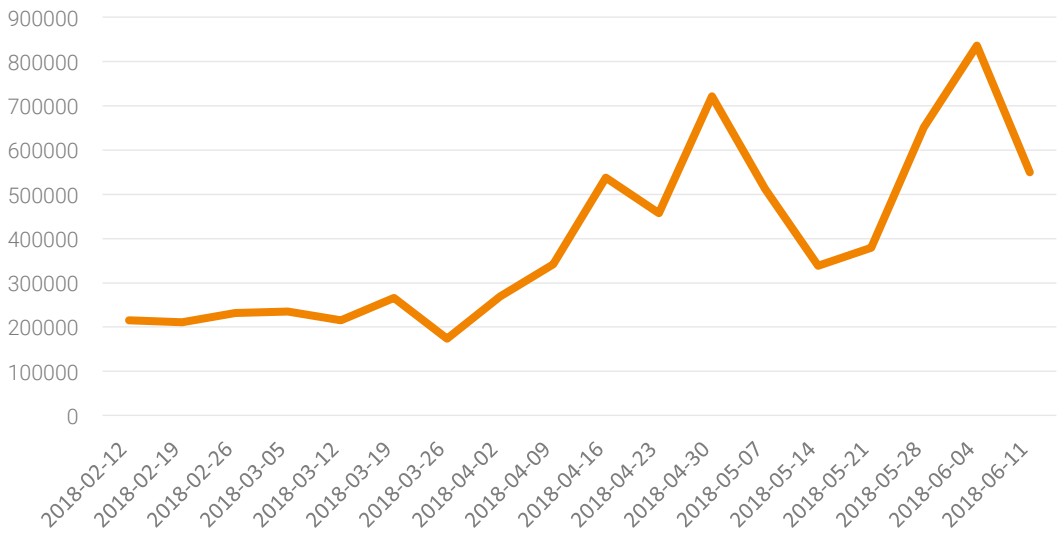


此外，在 2018 年上半年，一些家族、恶意程序的传播非常活跃，我们认为需要引起管理人员的注意，并进行及时的排查。一般来说，病毒的分类没有统一的标准，而病毒也并非规格化生产的产品，都是按照厂商自身的需求和习惯裁剪拼接而成的，因此名为木马的病毒，很可能也具有蠕虫的特征，名为后门程序的也具有木马的特征等等。我们大致地按照直观的共识，根据代码最核心的特征或者功能进行简单划分，例如蠕虫以大规模自传播能力为核心特征、木马的核心功能为信息窃取与其他复杂的远程控制、僵尸（肉鸡）程序的特征在于构建僵尸网络并发挥使用集群进行黑客行为（例如 DDoS 和挖矿）、后门程序和木马比较像但是前者更偏重于为后面的攻击提供持久化的入口。

活跃的挖矿恶意程序

2018 上半年，挖矿类恶意程序的活跃度持续攀升，从 3 月底开始，各类挖矿病毒的活动量出现大幅提升。

图 1.12 挖矿恶意程序的活动监测

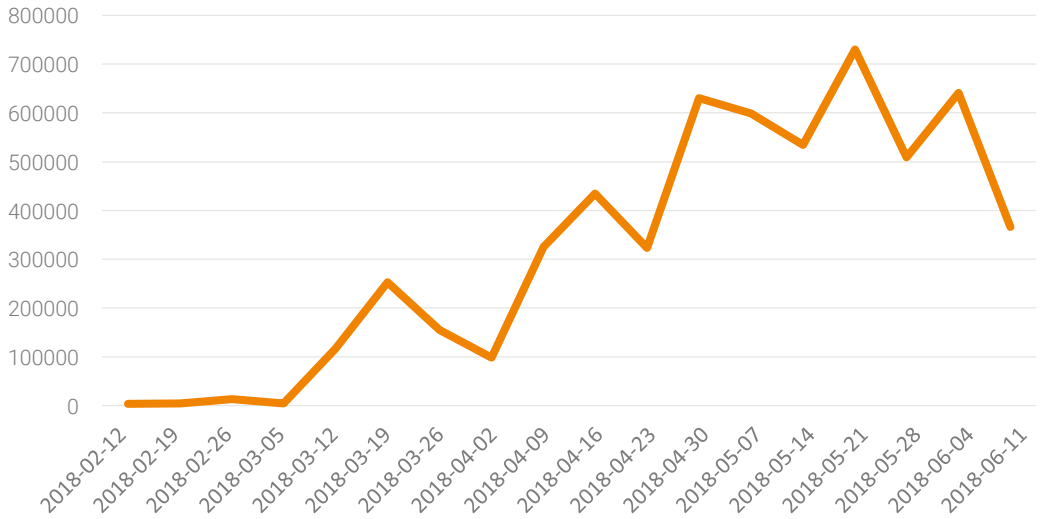


其中，又以 WannaMine 在各类挖矿病毒中显得最为活跃，在所有检测到的挖矿活动中，占比超过了 70%。该病毒最早是由 CrowdStrike 公司在 2018 年年初发现，由于其在传播过程中与红极一时的 WannaCry 一样，利用了“永恒之蓝”漏洞，故此命名。

活跃的蠕虫病毒

从时间维度看，蠕虫活动在 2 月非常少，从 3 月开始持续攀升，虽然有起伏，但是活动量的平均值是持续递增的。

图 1.13 蠕虫活动监测



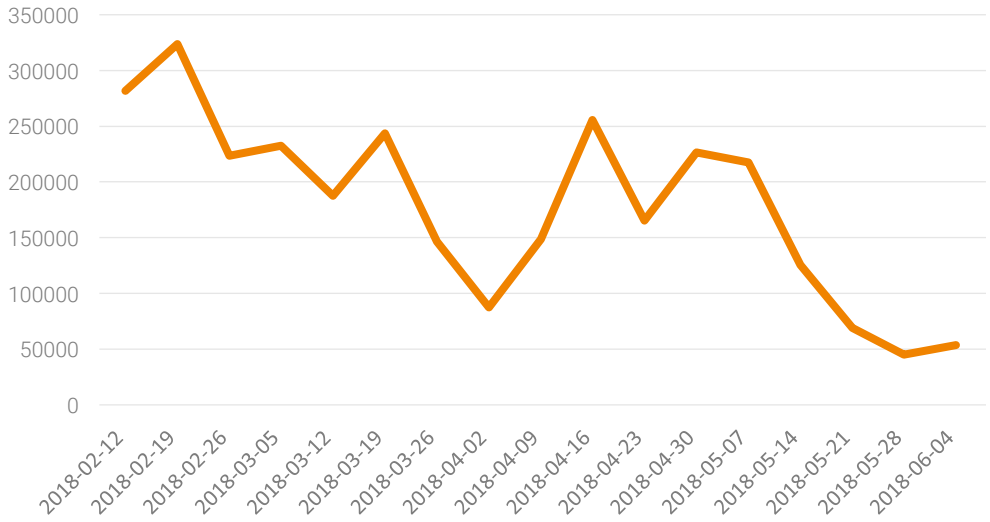
我们监测到最活跃的蠕虫病毒有 28 个之多，大部分蠕虫最早发现的时间距今都有 5 年以上，可见这些蠕虫病毒繁衍、进化的能力，以及在网络中彻底清除的难度。在今年，我们监测活跃度最高的两个蠕虫分别如下：

- **蠕虫 W32.Faedevour** W32.Faedevour 是一种蠕虫病毒，它在受感染的计算机中打开一个后门，窃取信息。在互联网上，公开报道的感染事件很少，但是在我们的统计中，所有蠕虫流量里，W32.Faedevour 家族的传播和扩散是位居高位的；
- **蠕虫 Conficker 攻击** Conficker 病毒，又名 Downup、Downandup、Downadup 和 Kido（刻毒虫）是一种出现于 2008 年 10 月的计算机蠕虫病毒，针对微软的 Windows 操作系统进行攻击。我们对其家族的互动特征进行提取，并且持续监控，我们发现其活动痕迹其实一直未曾彻底消失，2018 上半年仍然持续地出现在互联网中，但我们不能排除该行为是由其他家族的病毒复用 Conflicker 相关通信机制进行传播而导致的。

活跃的木马

今年上半年的监测中，木马的活跃度略有下降，而且与僵尸网络、蠕虫活动的态势相比，今年监测到的木马新品种较少。这可能与近年来，联网主机与设备数量的激增有关系，因为主机获取成本的下降，大量的恶意代码可以用很简单的方式实现快速拓展，因此那种量级较重、功能复杂的木马在数量上不如僵尸程序、挖矿程序推陈出新来得迅猛。

图 1.14 木马活动监测

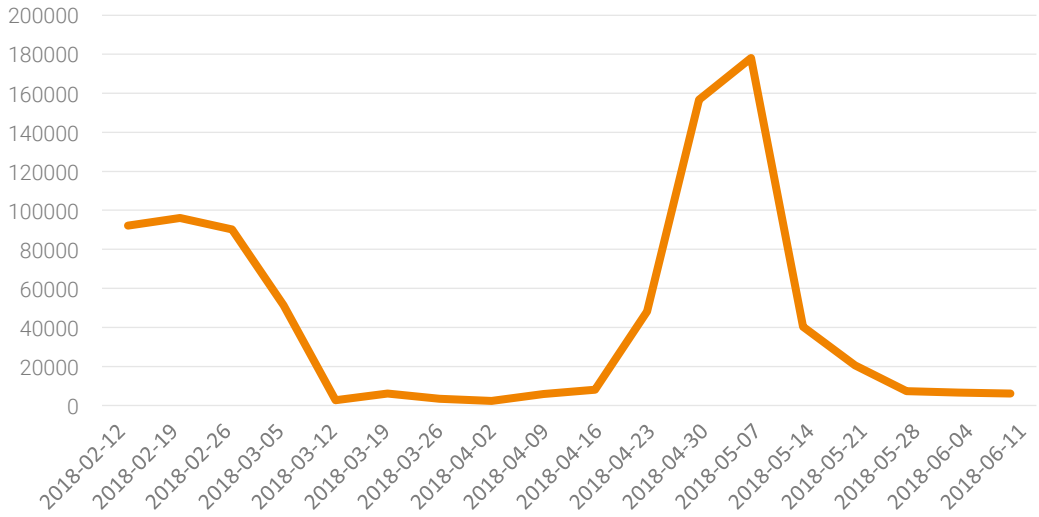


但是活跃的木马家族也超过 30 个之多，无需多言，这类程序的危害是很大的。在今年，最活跃的木马是一个名为“暗云”的木马，而暗云木马在其爆发之初，曾经一度感染过数以百万的计算机，当时暗云木马其使用 BootKit 技术，直接感染磁盘的引导区，感染后即使重装格式化硬盘也无法清除。2018 年上半年暗云木马的活动仍然非常频繁，我们希望从业者可以仔细的排查网络中存在的风险。

活跃的僵尸程序

僵尸网络的活跃度和后门程序的活跃度似有一定关联，僵尸程序在 5 月初与后门程序同时达到了 2018 上半年的活动高峰。

图 1.15 僵尸程序活动监测



与蠕虫、木马类病毒态势不同，活跃的僵尸程序都是比较新的家族或者变种，但是其核心功能和应用并没有发生变化——发动大规模的 DDoS 流量。正如绿盟科技《2017 年 Botnet 趋势报告》[1] 中所指出的，这些程序不断升级换代，它们能够提供的 DDoS 能力更加稳定，流量规模持续提升，并且使得僵尸网络具有了复用性，从 Botnet 感染到出售再到 Botnet as a Service 对外服务形成完整的黑产链条。

上半年监控中，下面几个家族非常活跃：

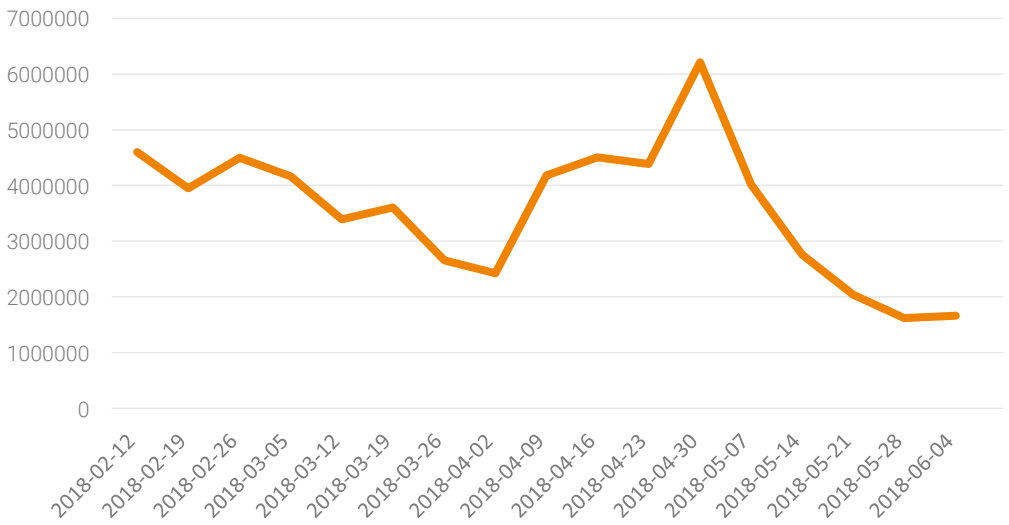
- **BillGates 僵尸网络**　这是一个被广泛使用的僵尸程序，该僵尸程序在 2016 年被发现和命名。僵尸程序用于组建僵尸网络发起大规模 DDoS 攻击；
- **Artemis 僵尸网络**　该僵尸网络在 2015 年前后发现和披露，也被广泛应用于 DDoS 攻击。

1　http://blog.nsfocus.net/2017-botnet-report/

活跃的后门程序

后门程序主要是设备类的后门，路由器又是其中重要的组成部分。今年上半年，后门程序的活动始终保持在高发状态，在 5 月份出现过一次高峰，此后态势回落到平均值附近。

图 1.16 后门程序活动监测



后门程序非常常见，有的甚至仅仅利用了物联网设备的默认登录接口便可获得远程控制入口。在活动最频繁的超过 20 个后门程序中，有 5 个后门是与路由器相关的。后门程序的频繁活动提醒设备和网络管理人员，一定要定期升级并检查设备的配置情况。下面是我们认为值得重点关注的后门应用：

- **Netcore / Netis 路由器后门** 在《2017 年网络安全观察》[1] 中我们指出，Gafgyt 僵尸家族的活动异常猖獗，其频繁的活动中最主要的行为是针对 Netcore 路由器早在 2014 年就披露并修复的后门。但是我们看到，其活动依然频繁，与 2017 年年底的活跃程度相当；
- **Doublepulsar 后门** 相较 Netcore 后门而言，Doublepulsar 技术上相对复杂一些，2017 年 Shadow Brokers 公布的 NSA 黑客工具中包含了该后门程序，后来经由广泛传播，在互联网上造成了相当大的危害。2018 年我们监测到 Doublepulsar 后门程序活动十分频繁。

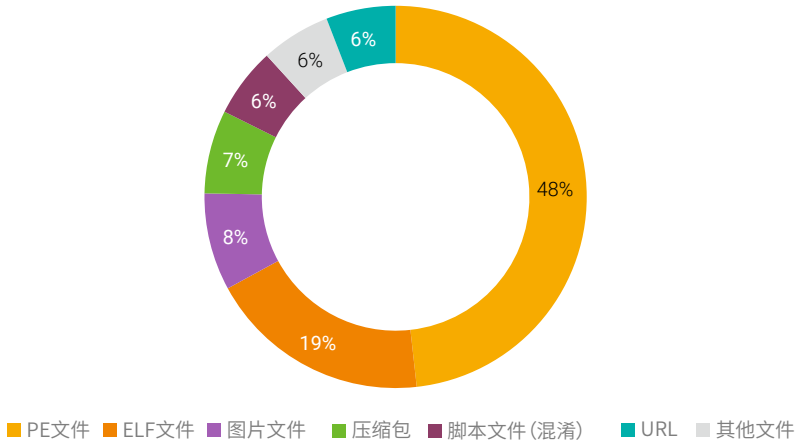
1.5 Pastebin 等代码分享平台滥用情况愈加严重

Pastebin 和 GitHub 是当下流行的代码分享与托管平台，恶意软件常常利用这两个平台传播关键信息。2018 年上半年，我们观测到越来越多的恶意软件利用 Pastebin 和 GitHub 传播。绿盟威胁情报中心 (NTI) 通过对多个代码分享与托管平台的监测，发现各平台的滥用情况愈加严重。

1 http://www.nsfocus.com.cn/content/details_62_2728.html

以 Pastebin 为例，为了能在上面存放文本以外的数据，一部分用户将文件的二进制数据使用 base64 编码后上传。根据我们的监测，我们发现每日新增的 base64 编码文本会承载不同的文件或文本，具体情况如下图。

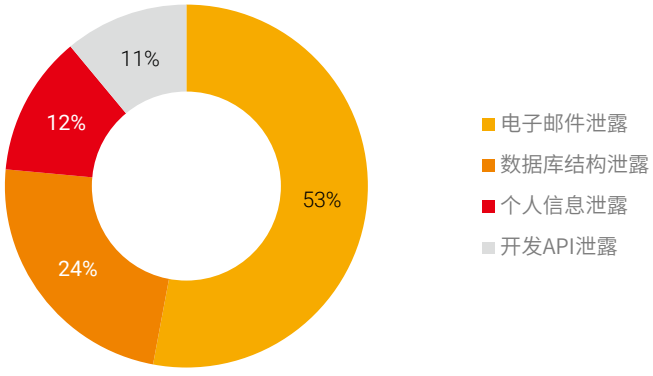
图 1.17 base64 编码数据类型分布



大部分可执行文件经过分析被确认为恶意软件，一些 URL 及 IP 也在我们已知的 C&C 服务器地址中。由于此类代码分享托管平台具有较高的信誉度，通信全程使用 HTTPS 加密，使得各类安全产品只能在终端对威胁进行检测，大大削弱了安全防御体系。为了规避对平台内代码及文本的监测，攻击者也开始采用其他类型的编码方式，或直接在 base64 编码的基础上使用其他加密算法，这也加大了公共平台的治理难度。

除此之外，其他滥用行为也不容忽视。每日有相当数量的电子邮箱地址与密码被上传到 Pastebin，也常有开发者将代码片段上传，其中包含了数据库结构及 API Key。

图 1.18 数据泄露类型分布



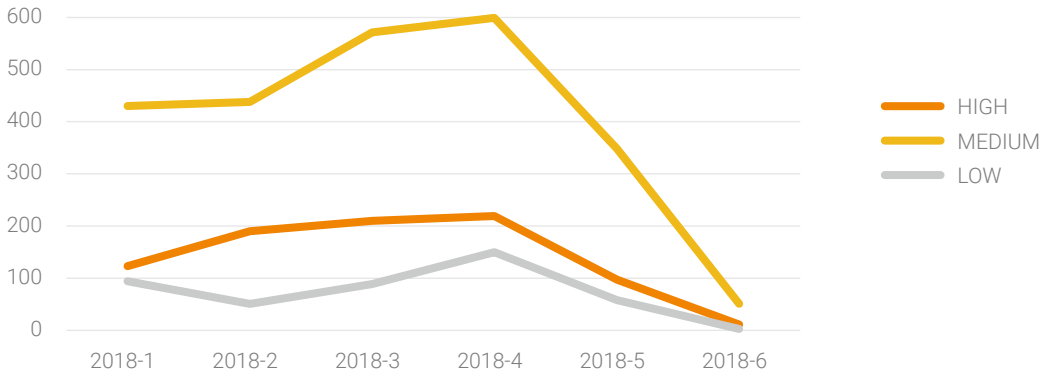
这些软件开发的基础信息与业务安全息息相关。攻击者在渗透前的信息收集阶段也会搜寻代码平台上的有价值信息，此类信息若被利用会给业务的平稳运行带来极大风险。

2. 漏洞观察

2.1 中危漏洞曝光比例高，权限控制需要重点关注

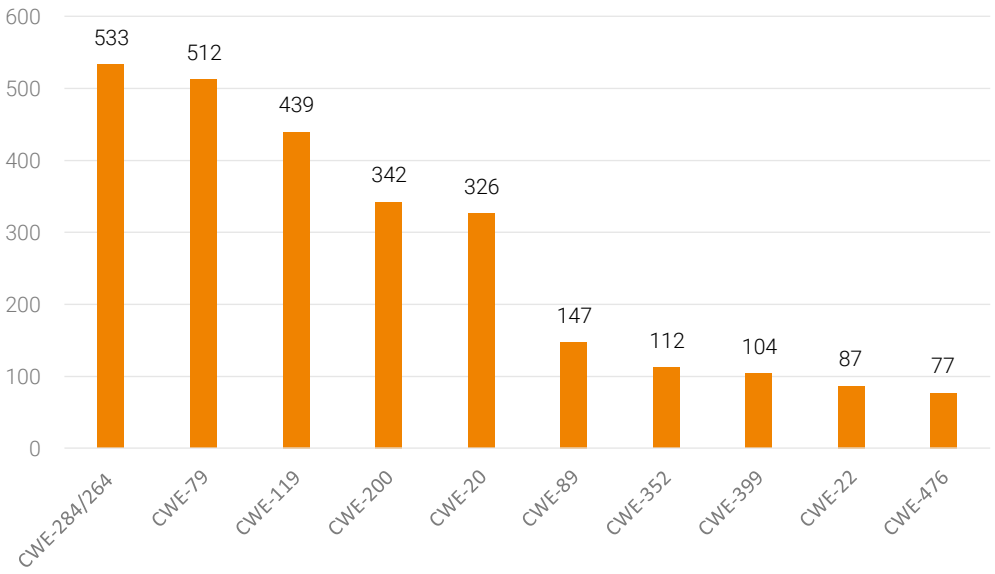
截止 2018-06-19 日，NVD 官网公布的 2018 年 CVE 漏洞数量为 3731 个，其中高危漏洞 850 个，中危漏洞 2437 个，低危漏洞 445 个。与去年同期相比，数量有所减少，其中漏洞数量向中危漏洞集中，高危、低危漏洞比例都有所下降。

图 2.1 漏洞公布数量的月度趋势



中危漏洞相对其他漏洞而言，对系统信息的完整性 (Integrity) 和系统功能的可用性 (Availability) 都有较大的影响，只是利用难度相对较高，因此漏洞评级为中级威胁，但若存在 PoC 或利用工具，中危漏洞依然能够造成非常严重的大规模破坏。

图 2.2 不同漏洞类型的数量分布



从漏洞类型上看排名前 10 的漏洞类型分别为：

- **CWE-284/264—权限控制漏洞** 权限控制类的漏洞曝光频率是最频繁的，大部分属于中危漏洞，这类漏洞与具体的业务密切关联，包括越权访问、权限提升等常见的操作，而其中属于高危漏洞的部分，集中于服务器操作系统、数据库类的应用，以及部分应用较广的开源内容管理系统中；
- **CWE-79—跨站漏洞** 跨站漏洞曝光程度位列第二，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-119—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，在上半年，这类漏洞中高危漏洞有 216 个，中危漏洞有 217 个，在高危漏洞中，排名前三的产品均为浏览器或者 Office 软件，包括 Microsoft Edge、Internet Explorer、Office Word；
- **CWE-200—信息泄露** 黑客触发漏洞能够导致敏感信息暴露。按照产品排名，存在该类漏洞最多的产品为 Windows Server 2016，此外在一些设备的固件中，该类漏洞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；
- **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，今年上半年，相关的高危漏洞为 61 个；
- **CWE-89—SQL 注入** 这是非常传统的攻击类型，通过提交精心构造的输入，绕过系统的防御限制，诱使系统执行 SQL 语句，通常见于网页类应用中，能够对网站数据造成较大危害；
- **CWE-352—CRSF，跨站伪造** 这也是传统的攻击方法，上半年，CVE 编号中存在 112 个跨站伪造漏洞；
- **CWE-399—内存资源管理不当** 这是一个非常大的类别，在内存资源管理不当的情况下，会导致较为严重的后果，例如内存的分配、释放、对象的销毁等等系统级的管理行为；
- **CWE-22—路径遍历漏洞** 攻击者构造特定的输入，可以访问或者部分访问限制目录之外的目录与文件信息；
- **CWE-476—空指针重释放漏洞** 这个漏洞与内存越界、资源管理不当漏洞是类似的，可以引起系统崩溃、代码执行等。

2.2 设备类漏洞态势严峻

从资源获取的难易程度、漏洞的利用难度、利用成功后可能对系统的危害这三方面来看，设备类漏洞是尤为突出的。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，从经济角度，这类漏洞必然受到攻击者的关注，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。从下面的表格我们看到，2018 上半年披露的 CVE 漏洞中，获取和利用难度低、危害程度大的漏洞主要集中在 4 个厂商的相关产品中，这些厂商都是移动设备或者网关类设备的制造商。

表 2.1 2018 上半年设备类漏洞列表

厂商	产品 / 固件	重点高危漏洞
D-Link	DSL-3782、DIR-629、DSL-2640U、DIR-880L	CVE-2018-10746 CVE-2018-10747 CVE-2018-10748 CVE-2018-10749 CVE-2018-10996 CVE-2018-5371 CVE-2018-6530 CVE-2018-8941
Mitel	ST14.2	CVE-2018-5779 CVE-2018-5780 CVE-2018-5781 CVE-2018-5782
Qualcomm	SD 850、SDM 660、SD 845	CVE-2018-3589 CVE-2018-3590 CVE-2018-3591 CVE-2018-3592 CVE-2018-3593 CVE-2018-3594
Cisco	D9800、FTD、RV132W、 Secure Access Control System、IOS XE 等	CVE-2018-0099 CVE-2018-0101 CVE-2018-0125 CVE-2018-0147 CVE-2018-0150 CVE-2018-0151 CVE-2018-0152 CVE-2018-0171 CVE-2018-0238 CVE-2018-0253 CVE-2018-0258

此外还有大量没有分配 CVE 编号或者威胁定级略低的漏洞。上半年我们针对一些重点威胁发布过相关的分析或者威胁通告，包括：

- 施耐德派尔高（Pelco）Sarix Professional 摄像头漏洞
- DrayTek 路由器 0day 漏洞
- VPNFilter 恶意软件传播中所利用的多种设备漏洞

在《2017 物联网安全研究报告》[1] 中我们曾经总结过 2017 年出现过的针对各类新型设备的僵尸蠕虫病毒，我们指出从 2016 年 Mirai 大规模感染事件开始，物联网威胁对于人们来说不再仅仅是一个概念，人们开始关注物联网的威胁和防御。在 2017 年，我们观察到包括 Rowdy、DarkCat、Gafgyt 在内的多种物联网恶意程序，它们针对设备类型从路由器、摄像头到电视机顶盒不断变化，恶意程序在不断地演进。如果注意被攻击的设备类型，这些被感染的设备往往长期在线且使用量大，他们经常使用通用硬件模块及固件，这些特征有利于恶意软件的传播。

2.3 代码管理基础设施治理缺位

早在 1983 年，Ken Thompson 的图灵奖获奖演说《Reflections on Trusting Trust》就展示了如何在编译器中嵌入后门代码，使该编译器生成的程序都受到影响。2015 年的 XcodeGhost 又让这一试验照进了现实。时至今日，软件开发流程越来越依赖世界各地的开发者通力合作，在这期间形成了各种包管理器、版本管理工具和代码分享与托管平台等软件开发基础设施。毫无疑问，基础设施的形成与完善提高了开发者的工作效率，但也带来了一些安全问题。

If an attacker successfully injects any code at all, it's pretty much game over.[2]

知名 JavaScript 包管理工具 npm 安全团队在 5 月发布报告 [3]，确认移除了一个伪装成 Cookie 解析器的包，它可以允许攻击者向服务器注入任意代码并执行。客观地讲，其他包管理工具也有面临此类攻击的风险，但 npm 的一些特点，如非常流行、包依赖关系过于复杂等，使其更容易成为首选目标。

图 2.3 恶意模块的依赖关系

```
mailparser
└── http-fetch-cookies
    └── express-cookies
        └──getcookies
```

2018 年 6 月，代码版本控制工具 Git 被爆出了一个远程代码执行漏洞 (CVE-2018-11235). 由于在 git clone 时没有对 submodule 的文件夹命名做足够的验证，当用户在使用 git clone –recurse-submodules 时 , 攻击者可以通过构造一个恶意的 .gitmodules 文件从而远程执行任意代码。其他基于 Git 的版本控制工具，例如 SourceTree，也会受到影响。

1 http://www.nsfocus.com.cn/content/details_62_2646.html
2 https://developers.google.com/web/fundamentals/security/csp/
3 https://blog.npmjs.org/post/173526807575/reported-malicious-module-getcookies

3. 恶意流量观察

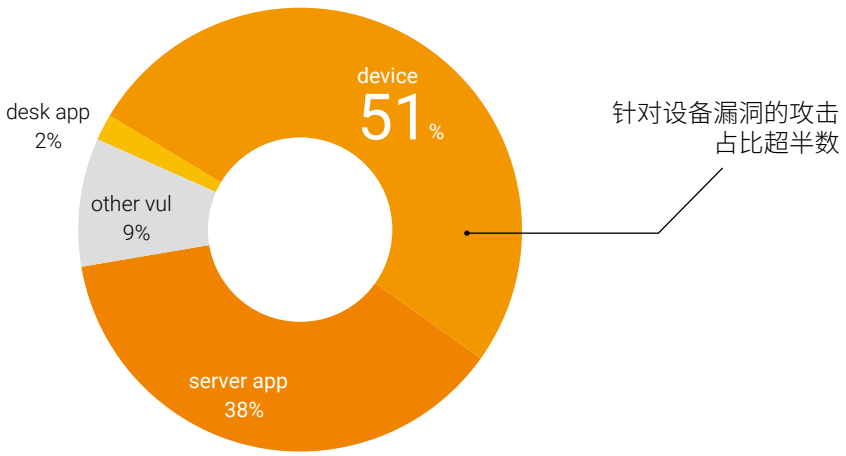
3.1 漏洞利用攻击

关键发现：

- 在所有利用漏洞进行的攻击中，以设备漏洞作为对象的利用占比超过 50%
- 路由器漏洞仍然普遍被治理者忽视
- 从漏洞利用攻击的角度，Windows 服务器、Java 应用服务器、Apache 服务器、邮件服务器、DNS 服务器属于高危服务器类型，这类服务器的漏洞需要重点防御
- 试探性扫描在网络中从未停止，因此，一旦有脆弱设备对外暴露，在极短时间内就有被攻陷的风险
- 桌面类应用漏洞常在钓鱼、垃圾邮件攻击中被使用，个人用户需要提高警惕

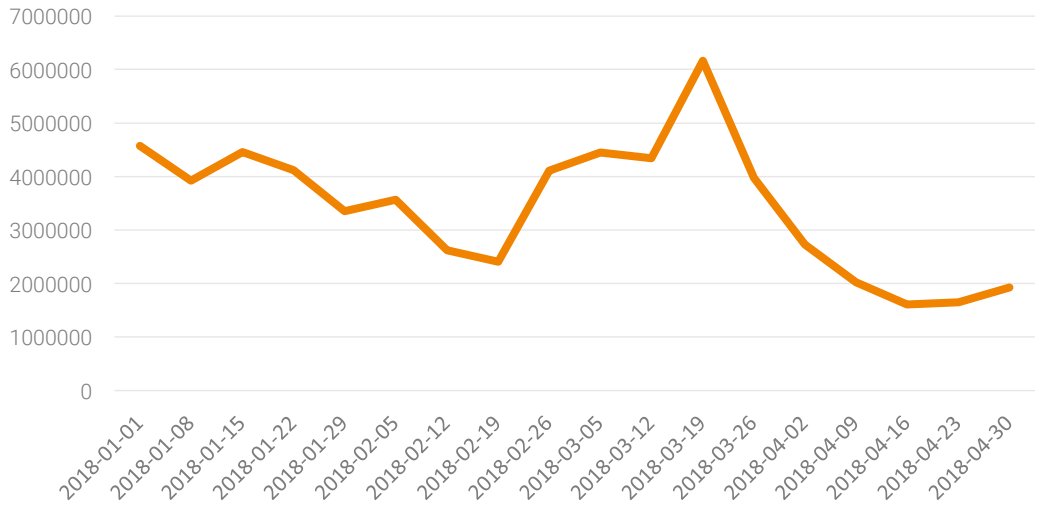
我们按照漏洞所在的主机环境或业务场景，将漏洞粗略的划分为服务器漏洞、桌面应用漏洞和设备漏洞。其中服务器漏洞主要为服务器上的系统服务与程序，用于支撑或提供网络管理与实际业务，常见的服务包括邮件、HTTP、网站脚本语言解析等；桌面应用主要提供文档、多媒体、主机管理等功能，常见的包括各类客户端（例如浏览器、邮件客户端）、杀软、Office 办公软件、Flash 播放器、PDF 阅读器等，这类软件漏洞常常被利用，常见的是通过恶意邮件、恶意网页的方式传播，通过诱使用户执行来感染目标主机；设备漏洞属于比较特殊和新晋的漏洞类型，包括各类移动终端、物联网设备等，他们共同构成一种新的威胁类型。

图 3.1 不同漏洞利用类型的告警量分布



从比例上看，针对设备漏洞的攻击从比例上看已经超过全部攻击事件的 50%，取代往年一直处于主导地位的服务器漏洞的攻击，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。我们观察到，即使厂商很久前就退出解决办法或升级补丁，仍有大量设备的脆弱性状况至今未有改善。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，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 3.1 路由器漏洞攻击利用监测



今年上半年，和其他攻击流量对比，路由器漏洞攻击的情况从未得到有效缓解，另一方面也说明，路由器的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尤为严重。

- Neetcore / Netis 路由器后门漏洞
- TP-Link 无线路由器 HTTP/TFTP 后门漏洞
- ASUS 路由器固件 ASUSWRT LAN 后门命令执行漏洞（CVE-2014-9583）
- D-Link 路由器 User-Agent 后门漏洞（CVE-2013-6026）
- Motorola 无线路由器 WR850G 认证绕过漏洞（CVE-2004-1550）
- Linksys WRT54G 无线路由器 apply.cgi 溢出远程安全漏洞（CVE-2005-2799）
- Cisco IOS 路由器拒绝服务漏洞
- 华为 HG532 路由器远程命令执行漏洞 (CVE-2017-17215)
- HP/H3C 及华为交换机 / 路由器 SNMP 访问敏感信息泄漏漏洞（CVE-2012-3268）

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

在针对服务器漏洞的攻击中，Windows 服务器受攻击最多，紧随其后的是 Oracle 服务。如果把 Weblogic 服务器，与其他 Java 应用服务器一起，我们看到 Java 应用服务器受到攻击的比例高达 27%，此外 Apache 服务器、邮件服务器、DNS 服务器也都是高风险服务器，相关服务频繁受到各类攻击与试探。在所有针对服务器的攻击中，大约 5% 的攻击属于探测性扫描攻击，黑客利用自动化的扫描工具和大量已知漏洞的利用代码进行脆弱性探测，一旦网络中存在相应漏洞，黑客第一时间就能利用和攻陷。因此，作为服务器管理员，应该经常自查和升级相关设备与服务，对于过往的漏洞也不能掉以轻心。服务器类漏洞的利用在 4-6 月较为频繁，期间每天检测到的攻击均在 20 万次左右。

图 3.3 服务器漏洞中不同服务的数量分布图

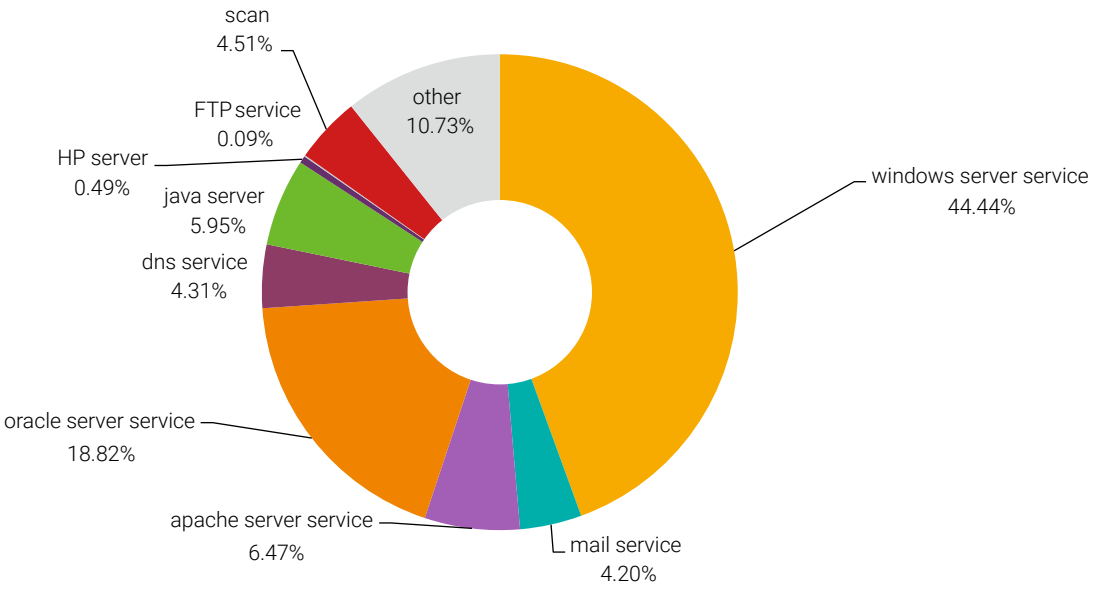
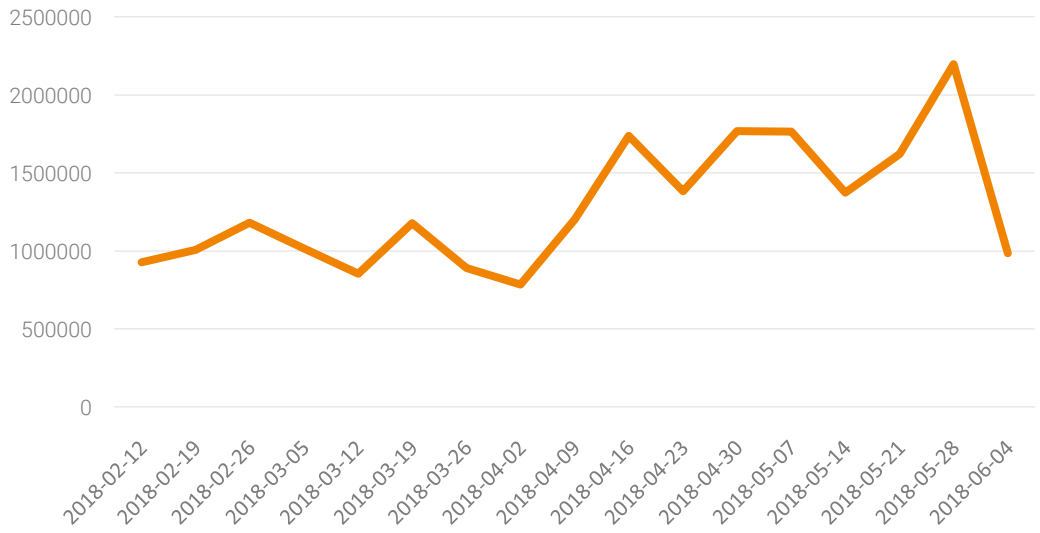
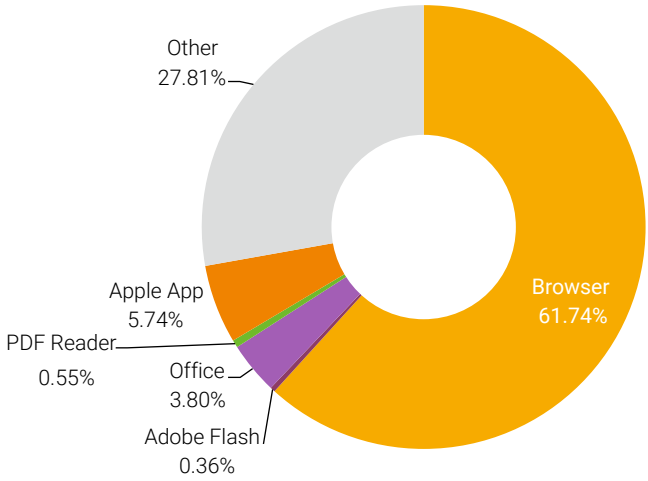


图 3.4 服务器类漏洞利用的时间趋势图



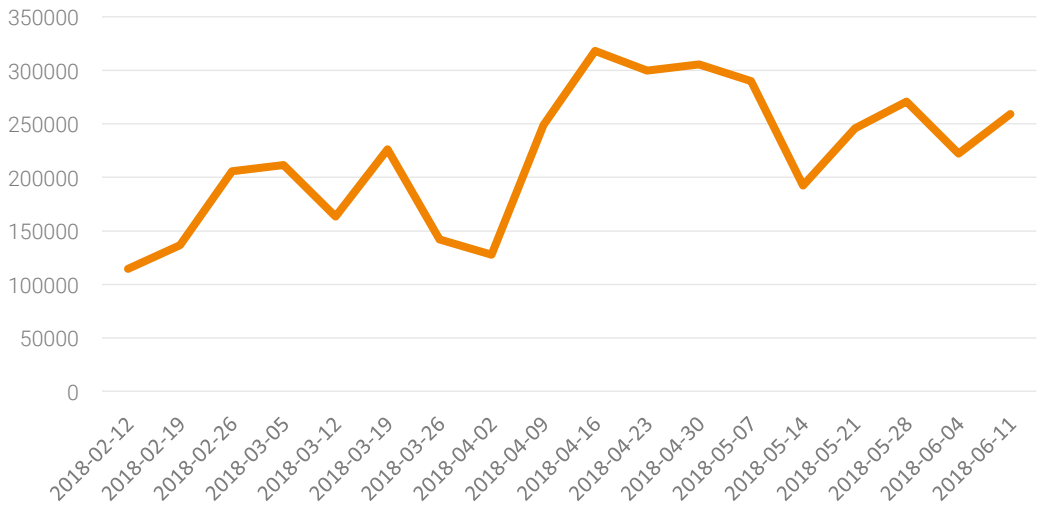
桌面类应用的漏洞攻击主要针对个人用户与使用者，当然这些用户中也会包括核心资产的管理人员，黑客利用钓鱼邮件，通过恶意链接、恶意附件的形式投递恶意程序，在用户点击访问相关资源时，对应程序的漏洞会被触发，最终导致感染和信息泄露。其中利用数量最多的几类应用如图所示，分别为浏览器、苹果主机应用、Office 文档漏洞、PDF 阅读器漏洞、Adobe Flash 漏洞。

图 3.5 针对桌面类漏洞的攻击利用数量分布图



桌面类的漏洞利用趋势与服务器类的漏洞利用趋势相近。桌面类应用在 6 月仍然保持较高的活跃度，并且 4 月之后上升趋势相较服务器漏洞更为明显。桌面类应用漏洞比服务器漏洞平均受到攻击次数较少，高峰时期每天攻击大约为 4 万次左右。

图 3.6 桌面类应用漏洞利用的时间趋势



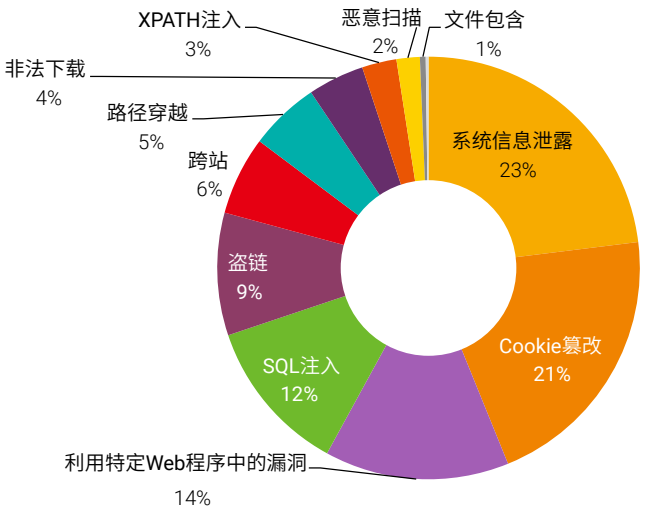
3.2 针对网站的攻击

关键发现：

- 网站安全事件频发，传统攻击仍需重视
- Struts 框架漏洞仍被黑客频繁使用
- 网站漏洞利用周期大幅缩短，网站管理员需要提高升级效率

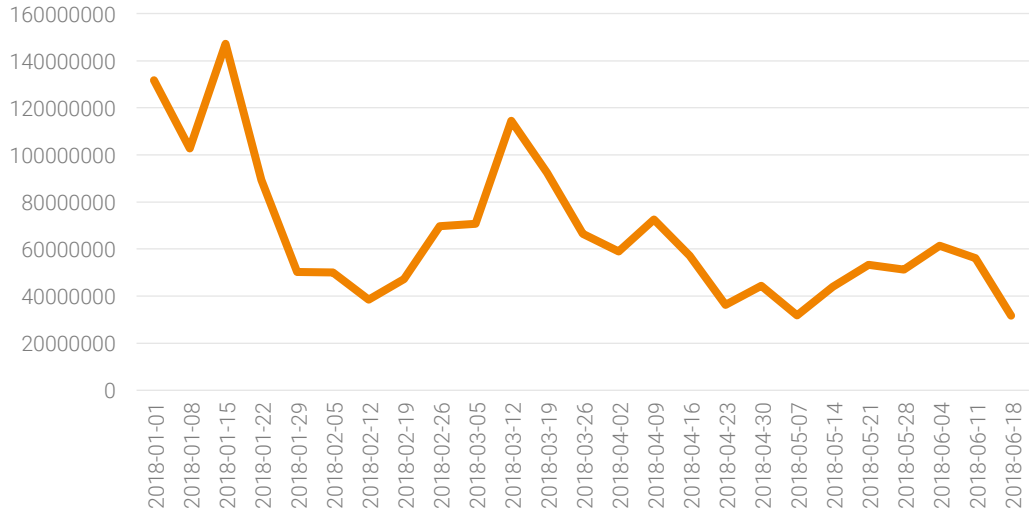
在传统上，用户在防御的过程中，容易关注新的、复杂的、影响范围广的漏洞，往往会忽略传统的攻击手段。但实际上，在每天的业务中，不可避免的面对着各式各样的试探，从简单的扫描，路径遍历，攻击注入到暴力破解。从比例上看不仅仅是高危漏洞、新发漏洞会对资产产生不良影响，对于网站管理而言，传统的攻击手法也会是非常大的困扰，例如对于网站安全，SQL 注入、Cookie 篡改等攻击行为常年居高不下。

图 3.7 针对网站的攻击类型分布图



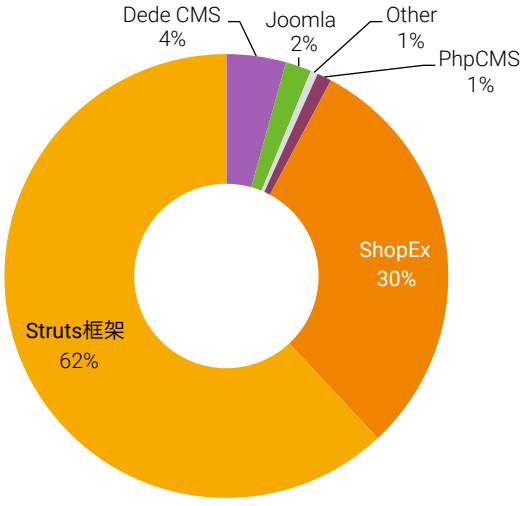
上图中的告警类型许多管理员会习以为常，但值得注意的是，很多攻击正是从这些看似普通的行为逐渐升级的，在网络观察中，我们认为，传统的攻击我们仍然必须认真对待。在 2018 年上半年监测中 1 月攻击次数较高，2 月份有所回落，3 月份有所回升后又回归到之前的平均水平，总体态势平稳。

图 3.12 Web 攻击数量的时间趋势图



在 Web 漏洞中，Struts 和 ShopEx 等几大框架及 CMS 受到的攻击最多，这些框架在国内的网站建站软件选择中相对流行，因此也受到国内黑客的格外关注。

图 3.13 针对不同网站框架攻击利用数量分布



Struts 框架仍然是攻击的热点。Struts 漏洞多属于典型的反序列化漏洞，在绿盟科技《2017 年反序列化漏洞年度报告》[1] 中提到，通过研究厂商对反序列化漏洞的应对，我们看到修复、绕过、再修复、再绕过的恶性循环，这类漏洞在 2017 年进入 OWASP 的 Top10 榜单。Struts 框架漏洞对于攻击者来说是价值极高的漏洞，因为漏洞本身的利用难度比较低，一旦利用成功，黑客能够获得较高的权限。今年上半年 Struts 公布了两个 (S2-055/S2-056) 新漏洞 , 但是利用最集中的漏洞仍然是过去一直受到关注的几个漏洞，包括：

- **CVE-2017-5638** 这是 2017 年年初曝光的一个漏洞，Apache Struts2 的 Jakarta Multipart parser 插件存在远程代码执行漏洞，攻击者可以通过设置 Content-Disposition 的 filename 字段或者设置 Content-Length 超过 2G 这两种方式来触发异常并导致 filename 字段中的 OGNL 表达式得到执行从而达到远程攻击的目的；
- **CVE-2014-0094** Apache Struts2 2.3.16 及之前的版本的 ParametersInterceptor 类中存在安全漏洞。远程攻击者可借助传递到 getClass 方法的‘class’参数利用该漏洞操作类加载器。这已经是多年前的漏洞了，但是在攻击中仍然被经常使用或者尝试，黑客有时仍然能够取得一定的收获；
- **CVE-2017-9805** 2017 年 9 月 5 日，Apache Struts 发布最新的安全公告，Apache Struts 2.5.x 以及之前的部分 2.x 版本的 REST 插件存在远程代码执行的高危漏洞，漏洞编号为 CVE-2017-9805（S2-052）。漏洞的成因是由于使用 XStreamHandler 反序列化 XStream 实例的时候没有任何类型过滤导致远程代码执行。

此外，网站漏洞中，今年还有两个新增漏洞，在互联网中的活动相对频繁：

- **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)，此后几个月内，互联网上针对 Drupal 程序的攻击都非常频繁。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 [2]，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；
- **CVE-2018-1273** Spring Data Commons 在 4 月爆出远程代码执行漏洞（CVE-2018-1273），攻击者可构造包含有恶意代码的 SPEL 表达式实现远程代码攻击，直接获取服务器控制权限。

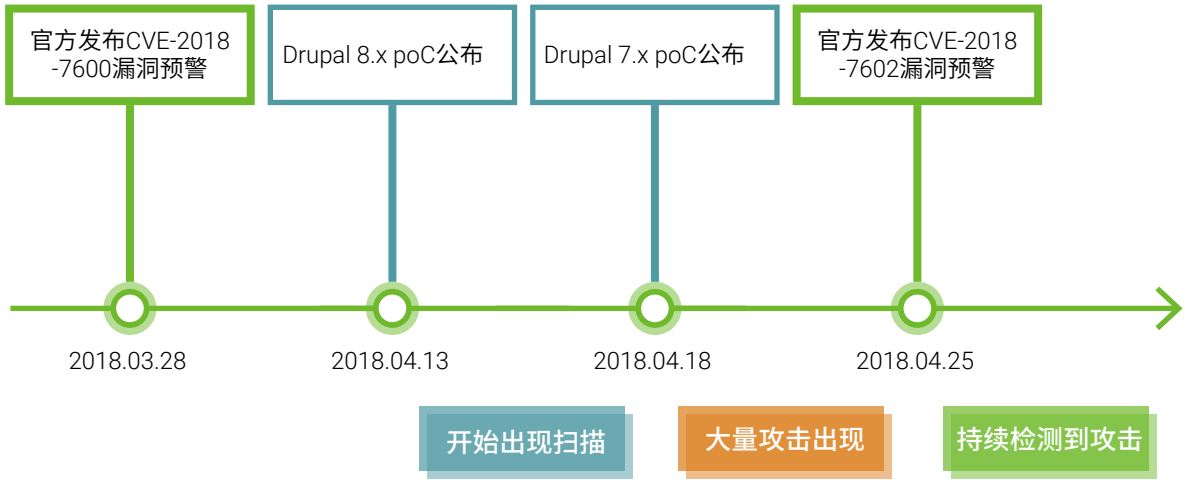
1 http://www.nsfocus.com.cn/content/details_62_2694.html
2 http://blog.nsfocus.net/drupal-threat-analysis/

针对 CVE-2018-7600，我们在 3 月底发布过一份分析报告[1]，梳理了从漏洞公布到实际攻击出现的完整演化过程。从漏洞公布之后，我们在很短的时间内就在互联网中监测到至少三种类型的攻击与利用迅速传播开来（挖矿、远控和 webshell）。之后我们分析了攻击行为最频繁的几个 IP，他们不仅仅针对这个漏洞，也针对了其他一系列的漏洞进行过广泛的尝试（例如 Weblogic 反序列化漏洞，struts2 漏洞等），因此我们认为，这批 IP 并没有特定的攻击对象，其活动目标主要是为了在更大的范围内获取尽可能多的网站权限，他们往往会搜集大量有价值漏洞的利用方法，然后通过搜索引擎、自动化扫描工具等进行大范围地猎捕活动。

我们因此也总结了近期网站攻击所具有的一些非常值得网站管理员重视的显著特征：

- 从漏洞利用细节公布到有效攻击出现，时间窗口非常短暂，留给防御者的时间极其有限。在 CVE-2018-7600 的应急响应事件中，这个时间窗口甚至已经缩短到小时级；
- 黑客普遍追求攻陷主机的数量。黑客在漏洞公布后短时间内，迅速开发相关利用工具，通过自动化的扫描与利用，在互联网上广泛地搜集缺陷主机，存在漏洞的网站普遍都存在着被攻陷的风险。因此管理员需要对网站出现的漏洞有足够的重视，第一时间进行升级和修补。

图 3.14 Drupal 漏洞的生命周期与时间点



1 http://blog.nsfocus.net/cve-2018-7600-analysis/

3.3 DDoS 攻击

关键发现：

- 普通 SYN 攻击、普通 UDP 攻击、NTP 反射、SSDP 反射攻击在上半年占据主导地位
- 黑客释放大规模流量攻击的能力仍然在持续快速提升，丝毫没有缓解迹象
- 2018 年上半年国内网络环境中的 DDoS 流量，在 3 月重大政府活动期间受到明显抑制

在我们的监控中共有 20 余种攻击类型发生，其中在 2018 年上半年中无论攻击次数、攻击流量都占绝对主导地位的攻击类型共有 4 类，分别是 SYN 洪泛攻击、UDP 洪泛攻击、NTP 反射攻击和 SSDP 反射攻击。

图 3.15 DDoS 攻击手段的攻击次数和流量占比

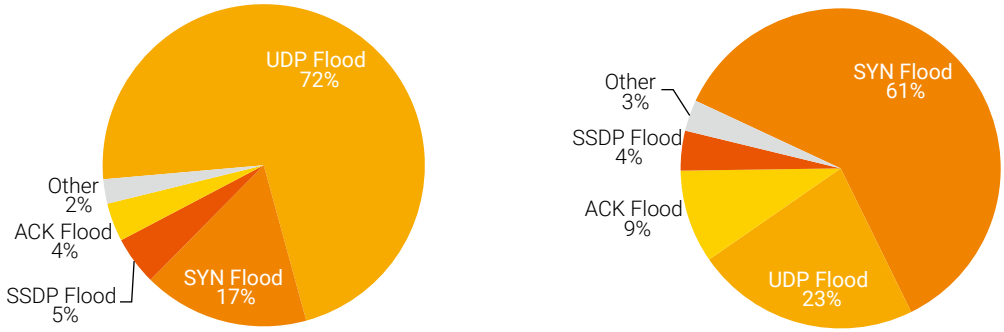
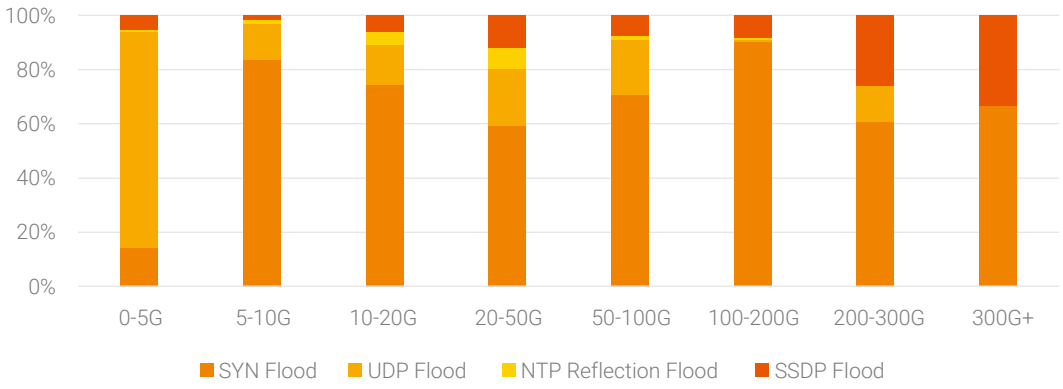
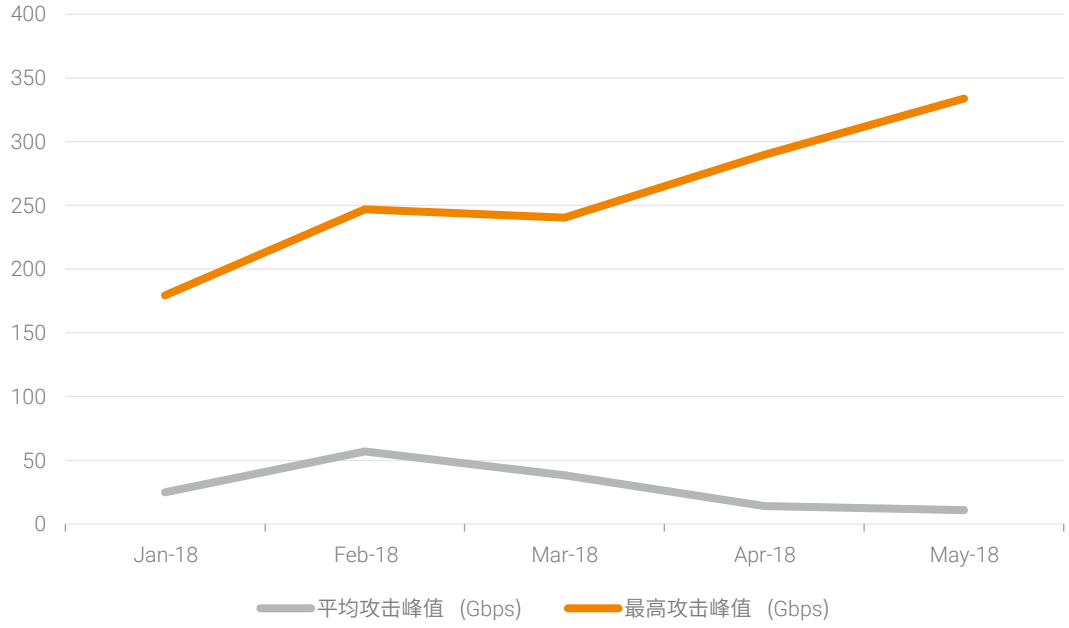


图 3.16 DDoS 各种攻击类型的流量区间分布图



从攻击次数和与从攻击流量和两个角度看，占主导地位的攻击类型是截然不同的，前者显示 UDP 类型的流量占比为主要攻击类型，而后者显示 SYN 类型的流量为主要攻击类型，我们从流量区间看，UDP 攻击主要分布在流量较小的区间内，而 SYN 攻击在大型、中型的攻击流量中较为常见。

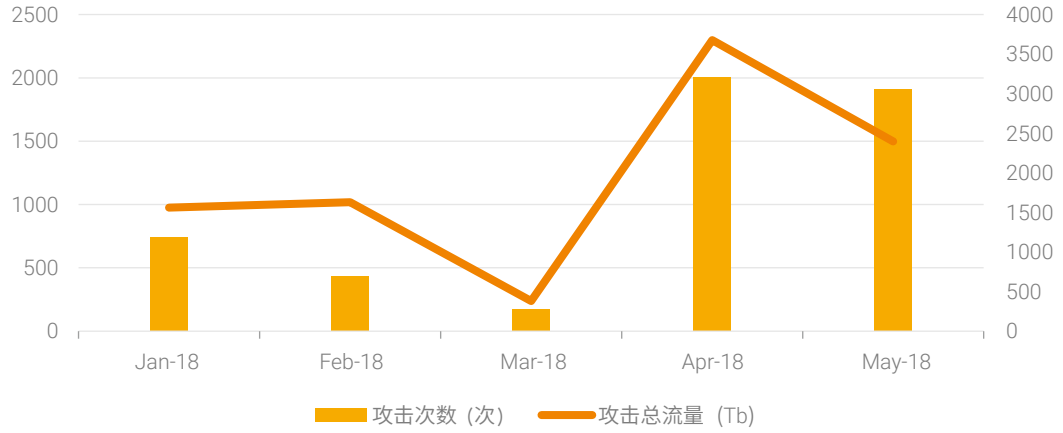
图 3.17 攻击峰值的时间趋势变化



从最高峰值来看，黑客的攻击能力仍然在不断提高，并没有停止甚至缓解的趋势，DDoS 流量继续成为互联网中的“洪水猛兽”。与最高峰值相比而言，平均峰值倒是维持在一个较为稳定的基线附近，为 50Gbps 左右，当然，这个峰值对绝大多数提供互联网服务的企业而言，已经难于招架。

综合以上，我们可以说，黑客普遍拥有了释放特大流量的能力，且能力仍处于持续快速提高的进程中，这是防御、治理人员需要面临的挑战。

图 3.18 DDoS 攻击次数和总流量的月度趋势



从总流量与总次数来看，2018 上半年前期态势较为平稳，3 月回落之后从 4 月开始，流量大幅激增，并且一直保持到五月底。DDoS 作为一种常规攻击手段，从基本原理上讲，并没有其他威胁那样翻新变化，攻防双方并没有根本性的技术革新，通过增加攻击、防御资源的数量，总能取得效果。因此我们总能看到，在政府重点治理时期，网络中的攻击流量呈现出明显的下降趋势。

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