2017 中国网站

安全形势分析报告

360 威胁情报中心

2018 年 1 月 23 日

主 要 观 点

网站漏洞问题依旧严峻，教育和政府行业最值得关注

本次报告从漏洞自动检测和人工挖掘角度对国内教育、政府等十余类典型行业的网站进行了安全性对比研究。

从漏洞数量来看。云监测平台扫描检测的网站中，教育培训、政府机构和事业单位是存在漏洞最多的三个行业。在补天平台中，政府机构及事业单位、教育培训和互联网是人工收录漏洞数最多的三个行业。

从漏洞修复情况来看。通信运营商、金融和教育培训类网站是漏洞修复率最高的三个行业。96.9%的通信运营商网站漏洞都进行了修复，90.6%的金融行业的网站漏洞进行了修复，83.3%的教育培训网站进行了修复。

僵尸网络继续瞄准物联网

在 2016 年 mirai 僵尸网络攻击造成美国东海岸大面积断网事件之后，2017 年以来，又有三个著名的僵尸网络出现 http81、IoT_reaper 和 Satori。其中，http81 和 IoT_reaper 都是针对 IoT 设备的僵尸网络。仅 http81 在国内感染的摄像头设备就超过 5 万台，而 Satori 则以 12 小时 26 万台的速度感染某品牌家用路由器，成为史上传播速度最快的僵尸网络。

挖矿木马成为网站最大现实威胁

2017 挖矿木马疯狂的敛财暗流。挖矿木马是 2017 年非常流行的一种针对网络服务器进行攻击的木马程序，此类木马程序通过自动化的批量攻击感染存在漏洞的网络服务器，并控制服务器的系统资源，用于计算和挖掘特定的虚拟货币。由于挖矿木马长期占用 CPU 率达 100%，因此，服务器感染挖矿木马后，最明显的现象是服务器响应非常缓慢，出现各种运行异常。如果挖矿木马攻击的是整个云服务平台，则平台上所有网站和服务系统都会受到严重影响。

另外，2018 年 1 月 8 日，我们第一次见到 Satori.Coin.Robber 僵尸网络利用“肉鸡”扫描正在挖矿的设备，并通过篡改其挖矿设备的算力和代币，致使其挖掘的虚拟货币流向自己的口袋。

反人工检测技术大范围流行

2017 年网络黑产大范围使用反人工检测技术，对网站进行黑词黑链篡改，攻击者在向网页中植入黑词黑链的同时，还会在页面中加入一段识别程序，该程序可以识别出访问请求是来在搜索引擎爬虫还是来自个人用户，如果访问请求来自搜索引擎爬虫，则进入带有黑词黑链等非法信息的页面；如果访问来自个人用户，则显示未经窜改的原始页面，对于未采用防篡改保护技术及缺乏相关经验的技术人员，这种攻击很难被发现，从而使带有非法信息的页面可以在网站中潜伏更长的时间。

WebLogic 反序列化漏洞攻击可能在 2018 年大爆发

2017 年 12 月末，国外安全研究者 K.Orange 在 Twitter 上爆出有黑产团体利用 Weblogic 反序列化漏洞（CVE-2017-3248）对全球服务器发起大规模攻击，大量企业服务器已失陷且

被安装上了 watch-smartd 挖矿程序；但此类攻击在国内还很少见到。不过，2018 年 1 月 11 日，360 安服团队在应急响应过程中，发现某门户网站遭到了 Weblogic 最新反序列漏洞攻击。

由于国内外对此漏洞的重视程度明显不足，有可能导致基于该漏洞的网络攻击在 2018 年大规模爆发。

弱密码问题依然是网站安全最大隐患　依然普遍存在

360 安服团队参与处理的网站安全应急响应事件中，60%以上都与弱密码有关。包括 2017 年大规模流行的挖矿木马，其成功攻击的主要原因也是由于网站管理员使用弱密码。本报告也总结了大量相关攻击实例，可供读者参考。

摘　要

网站漏洞检测分析

- 2017 年 1-10 月，360 网站安全检测平台共扫描检测网站 104.7 万个，其中，扫出存在漏洞的网站 69.1 万个（全年去重），共扫描出 1674.1 万次漏洞。扫出存在高危漏洞的网站 34.5 万个，占扫描网站总数的 32.9%，共扫描出 247.0 万次高危漏洞。
- 从域名类型统计来看，全球通用域名中.com 域名最多，占比为 64.2%；其次是.cn（23.0%）、.net（5.9%）；作为本土化域名，.gov 占比为 3.6%，.edu 占比为 1.6%。
- 从网站检测出漏洞的危险等级来看，2017 年高危漏洞数量占比为 11.5%，中危漏洞占比为 5.0%，低危漏洞占比为 83.5%。
- 360 网站安全检测平台全年共扫描发现网站高危漏洞 247.0 万次，较 2016 年 480.8 万次降低了 48.7%，平均每天扫出高危漏洞约 8097 次。
- 根据 360 网站安全检测平台扫描出高危漏洞的情况，跨站脚本攻击漏洞的扫出次数和漏洞网站数都是最多的，稳居排行榜榜首。其次是 SQL 注入漏洞、SQL 注入漏洞（盲注）、PHP 错误信息泄露等漏洞类型。下表给出了 2017 年 1-10 月份高危漏洞 TOP10。
- 应用程序错误信息（287.7 万次）、发现敏感名称的目录漏洞（184.1 万次）和异常页面导致服务器路径泄露（122.7 万次）这三类安全漏洞是占比最高的网站安全漏洞，三者之和超过其他所有漏洞检出次数的总和。
- 2017 年全年，360 云监测平台共对 7.94 万个网站进行扫描检测，扫出存在漏洞的网站 6.35 万个，占比为 80.0%，共扫描检测出 2428.8 万次网站漏洞。其中，扫描出高危漏洞网站 2.24 万个，共扫描出 121.3 万次高危漏洞。
- 从 2017 年云监测扫描检测的网站中，人工挑选出十个行业进行分析。教育培训类网站是检测出网站漏洞最多的行业，总计为 555.3 万次网站漏洞，其次是政府部门的网站，共检测出 455.9 万次网站漏洞，事业单位的网站，共检测出 92.0 万次网站漏洞。
- 进一步对不同行业网站扫出的高危漏洞进行分析，我们发现，政府部门网站扫描出高危漏洞次数最多，为 31.76 万次，其次为教育培训类网站，共扫描检测出高危漏洞 16.89 万次。

网站漏洞攻击分析

- 2017 年 1-10 月，360 网站卫士共为 187.5 万个网站拦截各类网站漏洞攻击 26.4 亿次，较 2016 年 17.1 亿次，增长 54.4%，平均每天拦截漏洞攻击 868.9 万次。
- 截止到 2017 年 10 月，全年遭到漏洞攻击的网站共计 79.8 万个（全年去重），占 360 网站卫士覆盖总量（187.5 万）的 42.5%。平均每月约有 8.0 万个网站遭遇各类漏洞攻击，同比下降 44.2%。
- 360 网站卫士拦截漏洞攻击次数最多的 10 个漏洞类型，这十个类型共遭到攻击 22.0 亿次，占到漏洞攻击拦截总量的 83.4%。

- 59.7%的网站漏洞攻击类型都为“SQL 注入”，稳坐第一。其次为“Webshell”和“通用漏洞”，占比分别为 8.2%和 3.6%。
- 从遭到漏洞攻击网站服务器 IP 的地域分布来看，83.4%受害者 IP 来自境内地区 IP，境外的受害者仅为 16.6%。从境内受害者的 IP 地域分布来看，23.1%来自北京，居于首位；其次分别为浙江（15.8%）、广东（11.7%）等。
- 从发起漏洞攻击 IP 的地域分布来看，45.3%的攻击者 IP 来自境内地区，来自境外的攻击占比为 54.7%。从境内攻击者的 IP 地域分布来看，21.5%来自北京，居于首位；其次分别为江苏（16.5%）、河南（12.3%）等。
- 漏洞攻击在一周之内的分布统计。星期四是一周中漏洞攻击最为集中的一天，占总攻击量的 15.3%，周日仅居其次，为 15.2%，而周五的攻击量则相对最少，仅占总攻击量的 14.5%。就平均性而言，周一周二周六较安全，而周四、周日最危险。

人工挖掘漏洞分析

- 2017 年全年，补天平台 SRC 共收录各类网站安全漏洞报告 22706 个，共涉及 14416 个网站。其中，3 月份收录的网站漏洞数量最多，为 3338 个。
- 在补天平台被报告漏洞涉及的政企机构中，平均约有 29.6%的网站已注册加入补天平台。
- 从补天平台收录网站漏洞的性质来看，通用型漏洞比例很低，仅为 4.1%，95.9%的网站漏洞都为事件型漏洞。
- 从补天平台收录网站漏洞的危害等级来看，高危漏洞占比为 24.2%，中危漏洞占比为 45.8%，低危漏洞占比为 30.0%。
- 从补天平台收录网站漏洞的具体类型来看，SQL 注入漏洞最多，占比为 32.1%，其次是命令执行和信息泄露，占比分别为 27.4%和 10.5%。占比较高的还有弱口令（10.2%）、代码执行（4.3%）。
- 在补天平台收录网站漏洞中，74.4%的网站漏洞已经进行了修复，25.6%的网站漏洞未进行修复。
- 从省级地域分布来看，补天平台收录网站漏洞最多的十个省份占到了总量的 74.5%。其中，IP 地址在北京的网站漏洞最多，占比为 28.8%，其次广东省为 8.9%，浙江省为 6.4%。
- 从城市地域分布来看，补天平台收录网站漏洞最多的十个城市占总量的 66.0%。其中，IP 地址在北京市的网站漏洞最多，高达 43.5%，其次上海市为 6.6%，杭州市为 3.1%。
- 补天平台收录的网站漏洞中，政府机构及事业单位网站的漏洞数量是最多的，占比为 24.9%；其次，教育培训网站漏洞为 20.8%，互联网行业为 17.7%。每个行业的网站漏洞分布情况。
- 被报告漏洞涉及的不同行业网站中，通信运营商行业网站注册率最高为 62.4%，其次，制造业网站注册率为 50.0%，IT 信息技术行业网站注册率为 49.7%。
- 从高危漏洞网站来看，通信运营商和 IT 信息技术的网站高危漏洞占比最多，均为 45.4%，其次是金融网站高危漏洞为 43.1%。

- 96.9%的通信运营商网站漏洞都进行了修复，其次，90.6%的金融行业的网站漏洞进行了修复，83.3%的教育培训网站进行了修复。

网络扫描

- 2017 年全年，360 威胁情报中心在全球范围内共监测发现扫描源 IP 1400 万个，累积监测到扫描事件 3.93 亿次。全球平均每日活跃的扫描源 IP 大约有 13.3 万个，对应的日均扫描事件约 107.6 万起。
- 网络扫描活动的具体技术方法多种多样，但从扫描的具体目的来看，主要可以分为三种类型：常规恶意扫描、针对性突发扫描和安全监控扫描。
- 通过对 2017 年全年网络扫描器扫描的端口分析发现，扫描器扫描的端口主要为具备远程控制能力的端口和存在信息泄露的端口。23 端口和 2323 端口是被扫描次数最多的端口，网络扫描事件中约 61.8%会扫描 23 端口，约 23.9%会扫描 2323 端口。
- 从扫描事件的数量来看，60.9%的网络扫描事件是从中国大陆发起的，5.0%是从巴西发起的，而美国、俄罗斯和印度位列其后，占比分别为 4.0%、3.4%和 2.6%。
- 而从扫描器的数量来看，43.3%的扫描源 IP 位于中国大陆境内；9.0%的扫描源 IP 位于巴西；印度、俄罗斯、阿根廷分列三到五位，比例分别为 5.4%、4.6%和 4.2%。

网站 DDoS 攻击情况

- 2016 年 12 月 5 日至 2017 年 12 月 5 日，360 威胁情报中心监测到 626.2 万个 IP 在过去一年曾遭到过 1064.3 万次攻击。
- 针对 DDoS 攻击的端口中，80 端口是 DDoS 攻击最常用的端口，占比为 47.8%，其次为 4444 端口（17.0%）、3074 端口（8.7%）。
- DDoS 攻击的网站域名中，51.7%为.com 域名，其占据了半壁江山。其次是.net 和.cn 域名，占比分别为 24.5%和 11.0%。
- DDoS 攻击类型中，amp_flood 类型最多，占比为 55.4%，其次为 syn_flood 和 simple_flood，占比分别为 13.7%和 13.5%。
- 从攻击时长来看，超过五成的 DDoS 攻击持续时间小于 10 分钟，而持续时间在 10 分钟至 30 分钟的攻击占比约为 22.5%，30 分钟至 1 小时的攻击占比约为 8.1%，持续时间超过 1 小时的攻击占比不足 10%。
- DDoS 攻击主要由受控的僵尸网络发动。xor 家族是最为活跃的 DDoS 僵尸网络家族，占比为 38.1%；其次，elknot 家族为 29.5%；gafgyt 家族为 14.7%。
- 僵尸网络攻击的端口也很受大家的关注。80 端口仍是大多数僵尸网络攻击的主要目标，占比为 62.8%，其次是 53 端口为 7.5%，3074 端口为 6.7%。
- 在 2017 年的 DDoS 僵尸网络攻击中，syn_flood 攻击次数达到 22.8 万次，其次是 udp_flood 6.5 万次、STD 为 3.3 万次等。

- DDoS 僵尸网络攻击的国家中，美国是重灾区（7.05 万次）。中国排名第二（5.53 万次），其次为韩国和法国，分别为 3.21 万次和 3.19 万次。

白帽子与安全人才

- 2017 年全年，共有 4199 名白帽子向补天平台提交有效漏洞 2.27 万个，总计获得奖金 489 万元。
- 2017 年获补天平台奖金最多的三位白帽子分别是 lakes、depy 和 jkgh006。从报给补天平台并被收录的漏洞总数来看，挖洞最多的是 carry_your，共贡献 695 个漏洞，大约每天挖洞 2 个。而获得奖金最多的是 lakes，共获得 49.3 万元。
- 2017 上半年，向补天平台提交漏洞的白帽子中，女性白帽子占比仅为 5.8%，男性白帽子占比为 94.2%。
- 根据白帽子的注册信息统计，在 2017 年上半年向补天平台提交漏洞的白帽子中，年龄最小的 14 岁，年龄最大的 67 岁。其中，18 岁-28 岁之间的白帽子数量最多，约占总数的 79.9%。
- 而从年龄段来看，年轻的“90 后”目前仍然是白帽子的绝对主力，占白帽子总量的 75.2%，“80 后”次之，占 10.8%，00 后正在崛起，占比为 9.1%。值得注意的是，相比 2016 年“00 后”白帽子仅占 2.6%，今年约有 9.1%的白帽子是 17 岁及以下的青少年。

关键词： 网站安全、漏洞、补天、白帽子、扫描、DDoS、挖矿

目　　录

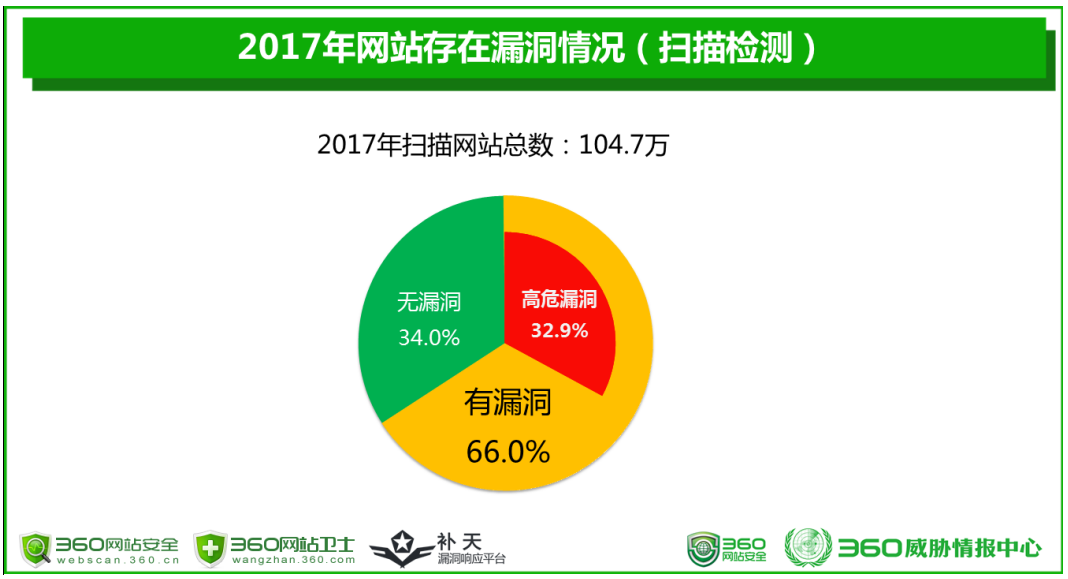
第一章　网站漏洞检测分析

网站漏洞的整体形势可以从两个角度分析：一是网站安全检测的自动扫描结果统计，二是网站被报告漏洞情况的统计。本章将从自动扫描角度，以 360 网站安全检测与防护相关产品的统计结果为依据，分析 2017 年 1-10 月中国网站的安全漏洞情况。

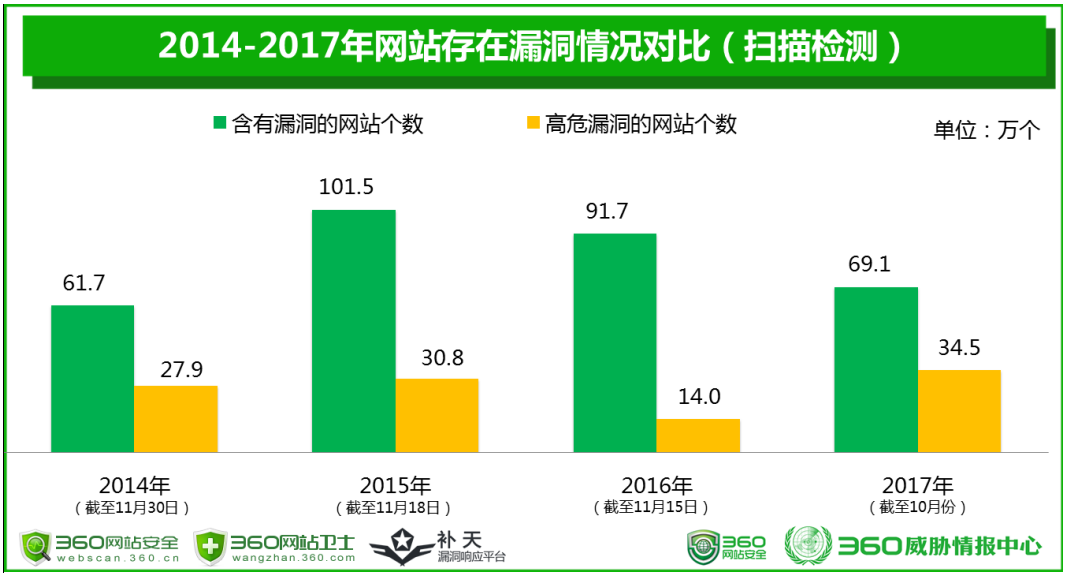
一、　漏洞数量概况

2017 年 1-10 月，360 网站安全检测平台共扫描检测网站 104.7 万个，其中，扫出存在漏洞的网站 69.1 万个（全年去重），占比为 66.0%，共扫描出 1674.1 万次漏洞。

从高危漏洞的检测情况来看，扫出存在高危漏洞的网站 34.5 万个（相比 2016 年的 14.0 万个网站漏洞，增长了约 2.5 倍），占扫描网站总数的 32.9%，共扫描出 247.0 万次高危漏洞。

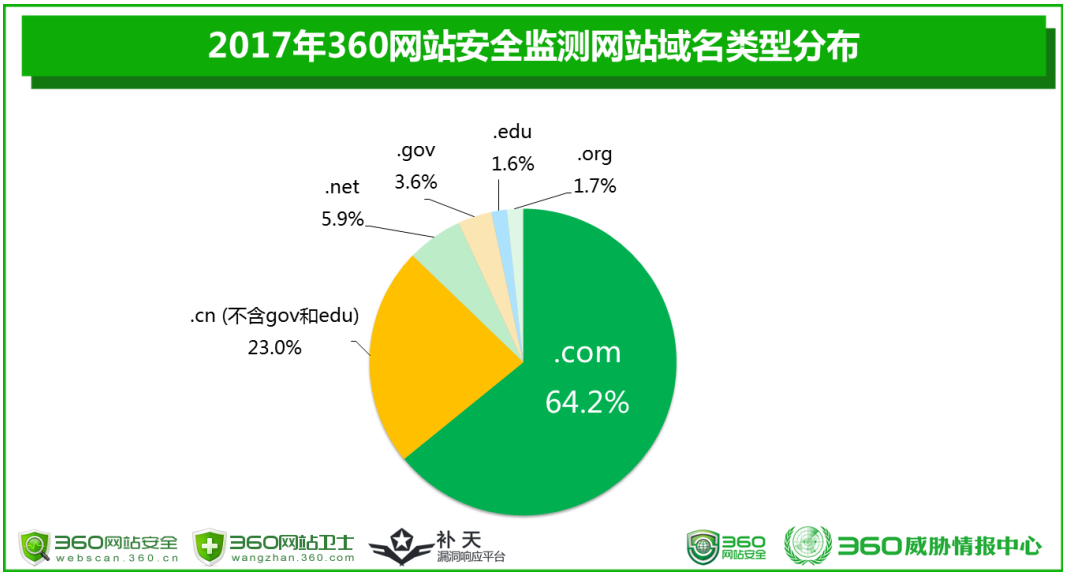


2014 年至 2017 年，虽然存在漏洞的网站数量呈现下降趋势，但是含有高危漏洞的网站数却在不断上升。高危漏洞更容易被病毒、木马、黑客等侵入，导致软件崩溃或者盗取重要信息、密码等，其危害性更大，影响更深远。下图给出了 2014 年至 2017 年网站存在漏洞的情况对比。



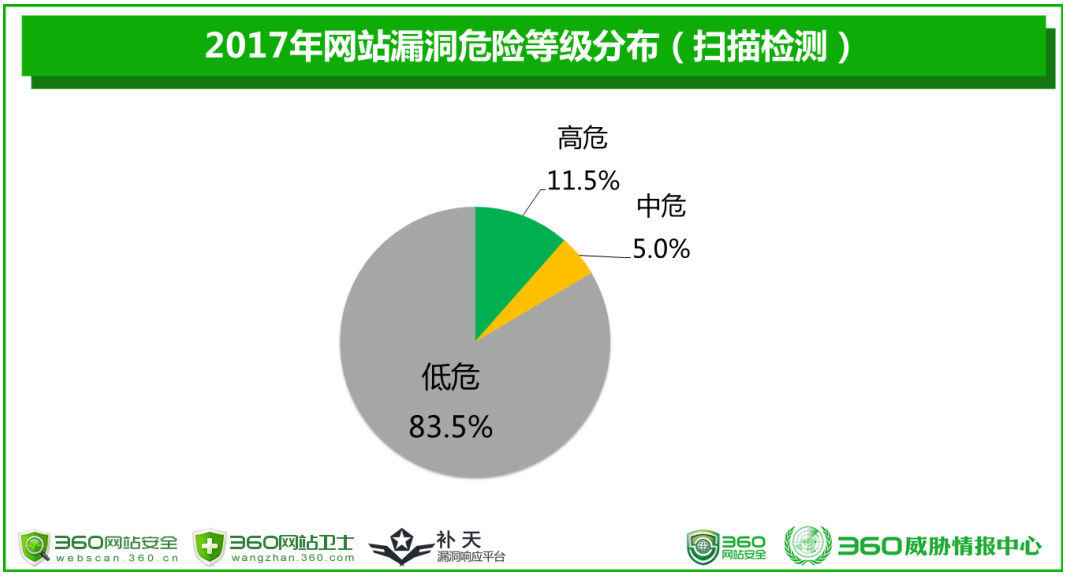
二、 扫描网站介绍

从域名类型统计来看，全球通用域名中.com 域名最多，占比为 64.2%；其次是.cn（23.0%）、.net（5.9%）；作为本土化域名，.gov 占比为 3.6%，.edu 占比为 1.6%。具体分布情况如下图所示。

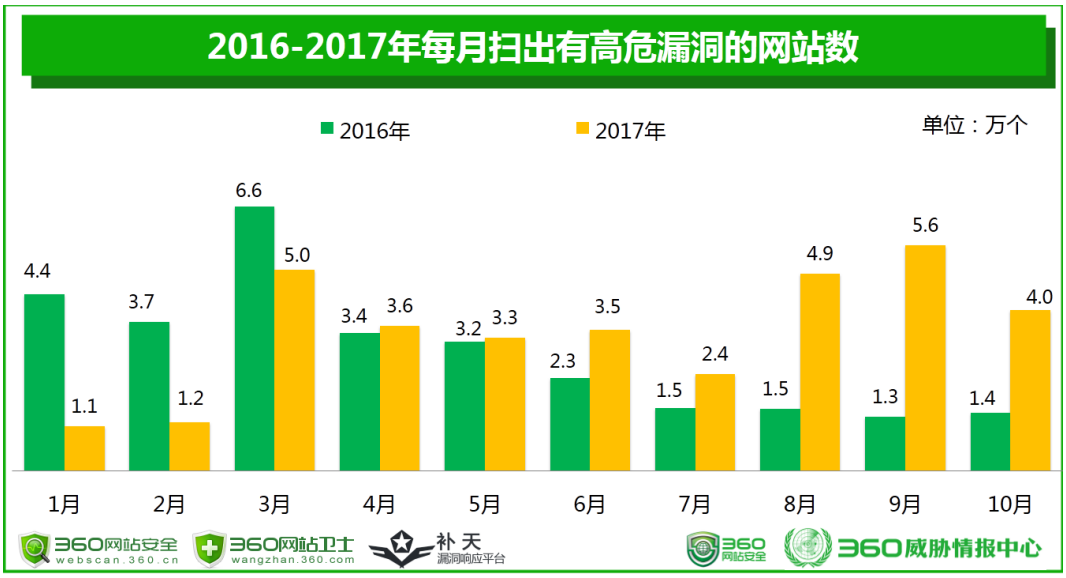


三、 漏洞危险等级情况

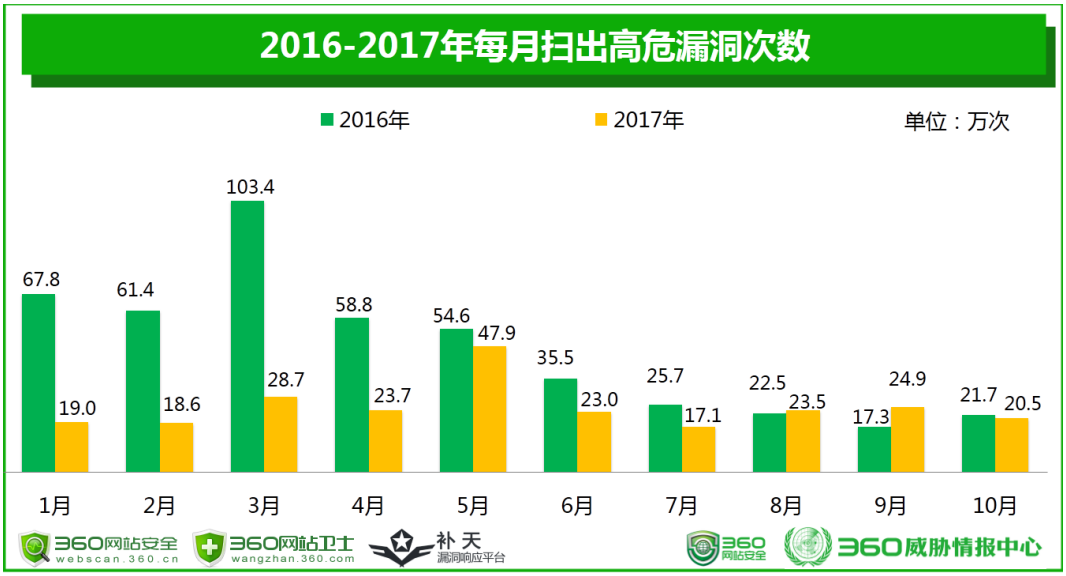
从网站检测出漏洞的危险等级来看，2017 年高危漏洞数量占比为 11.5%，中危漏洞占比为 5.0%，低危漏洞占比为 83.5%。具体如下图所示。



下图给出了 360 网站安全检测平台每月扫描出存在高危漏洞的网站个数（当月去重）。其中，在全年各月中，9 月扫出的有高危漏洞的网站数量最多，为 5.6 万个。与 2016 年 3 月后稳定下降相比，2017 年每月的变化还是很明显的。



360 网站安全检测平台全年共扫描发现网站高危漏洞 247.0 万次，较 2016 年 480.8 万次降低了 48.7%，平均每天扫出高危漏洞约 8097 次。下图给出了 2017 年每月扫描出网站高危漏洞的次数。整体基本保持平稳，其中 5 月份是扫出高危漏洞最多的月份，数量达到 47.9 万次。



四、 漏洞类型分析

根据 360 网站安全检测平台扫描出高危漏洞的情况，跨站脚本攻击漏洞的扫出次数和漏洞网站数都是最多的，稳居排行榜榜首。其次是 SQL 注入漏洞、SQL 注入漏洞（盲注）、PHP 错误信息泄露等漏洞类型。下表给出了 2017 年 1-10 月份高危漏洞 TOP10。

漏洞名称	扫出次数(万)	漏洞网站数（万）
跨站脚本攻击漏洞	91.7	7.6
SQL 注入漏洞	18.8	1.7
SQL 注入漏洞（盲注）	18.0	2.3
PHP 错误信息泄露	9.2	0.7
数据库运行时错误	5.3	0.5
跨站脚本攻击漏洞(路径)	3.7	1.1
使用存在漏洞的 JQuery 版本	3.7	1.8
MS15-034 HTTP.sys 远程代码执行	1.8	0.9
发现 SVN 版本控制信息文件	1.5	0.2
跨站脚本攻击漏洞（文件）	1.3	0.2

表格 1 1-10 月份高危漏洞 TOP10

根据各类网站安全漏洞被扫出次数的统计情况。应用程序错误信息（287.7 万次）、发现敏感名称的目录漏洞（184.1 万次）和异常页面导致服务器路径泄露（122.7 万次）这三类安全漏洞是占比最高的网站安全漏洞，三者之和超过其他所有漏洞检出次数的总和。

值得一提的是，“应用程序错误信息”漏洞等前四名都是低危漏洞，改变了前两年高危漏洞稳居排名第一的局面。下表给出了被扫出次数最多的十大类典型网站安全漏洞。

漏洞名称	漏洞级别	扫出次数（万）	漏洞网站数（万）
应用程序错误	低危	287.7	8.9
发现敏感名称的目录漏洞	低危	184.1	16.1
异常页面导致服务器路径泄漏	低危	122.7	8.0
X-Frame-Options 头未设置	低危	105.7	36.8

跨站脚本攻击漏洞	高危	91.7	7.6
发现 robots.txt 文件	低危	68.7	28.7
WEB 服务器启用了 OPTIONS 方法	低危	64.9	25.7
IIS 版本号可以被识别	低危	43.9	18.4
Cookie 没有 HttpOnly 标志	低危	30.3	10.1
IIS 短文件名泄露漏洞	低危	24.0	9.6

表格 2　2017 年扫描出数量最多的 10 类网站漏洞

五、　不同行业网站漏洞扫描情况

360 网站云监测主要通过云端发现企业网站的安全问题，是一款基于云的安全服务产品，依靠 360 强大的云端资源，为政府机构、大型国企等用户提供服务。

2017 年全年，360 云监测平台共对 7.94 万个网站进行扫描检测，扫出存在漏洞的网站 6.35 万个，占比为 80.0%，共扫描检测出 2428.8 万次网站漏洞，平均每个网站扫描出约 382 个漏洞。其中，扫描出高危漏洞网站 2.24 万个，共扫描出 121.3 万次高危漏洞，平均每个网站扫描出约 54 个高危漏洞。

从 2017 年云监测扫描检测的网站中，人工挑选出十个行业进行分析。教育培训类网站是检测出网站漏洞最多的行业，总计为 555.3 万次网站漏洞，其次是政府机构的网站，共检测出 455.9 万次网站漏洞，事业单位的网站，共检测出 92.0 万次网站漏洞。具体分布如下表所示。

行业	扫描检测网站总数	扫描出漏洞的网站个数	网站扫描出漏洞次数	平均每个网站检测出的漏洞个数
教育培训	13721	12512	5552554	444
政府机构	17209	15004	4559052	304
事业单位	2057	1920	920320	479
公检法	1483	1231	322029	262
金融	1643	1402	312212	223
交通运输	1347	1273	306436	241
媒体	1172	1143	265246	232
医疗卫生	718	640	205496	321
央企	640	584	121230	208
协会团体	145	138	60247	437

表格 3　不同行业网站漏洞扫描情况

进一步对不同行业网站扫出的高危漏洞进行分析，我们发现，政府机构网站扫描出高危漏洞次数最多，为 31.76 万次，其次为教育培训类网站，共扫描检测出高危漏洞 16.89 万次。

特别值得注意的是协会团体虽然只有 66 个网站扫描检测出高危漏洞，但是竟然扫描出了 5028 次高危漏洞，平均每个网站约扫描出 76 次高危漏洞。具体分布如下表所示。

行业	扫描检测网站总数	扫描出高危漏洞的网站个数	网站扫描出高危漏洞次数	平均每个网站检测出的高危漏洞个数

教育培训	13721	4040	168818	42
政府机构	17209	5434	317580	58
事业单位	2057	915	35823	39
公检法	1483	361	7365	20
金融	1643	394	9307	24
交通运输	1347	507	7898	16
媒体	1172	294	8646	29
医疗卫生	718	263	7796	30
央企	640	199	3447	17
协会团体	145	66	5028	76

表格 4　不同行业网站扫描出高危漏洞的分布情况

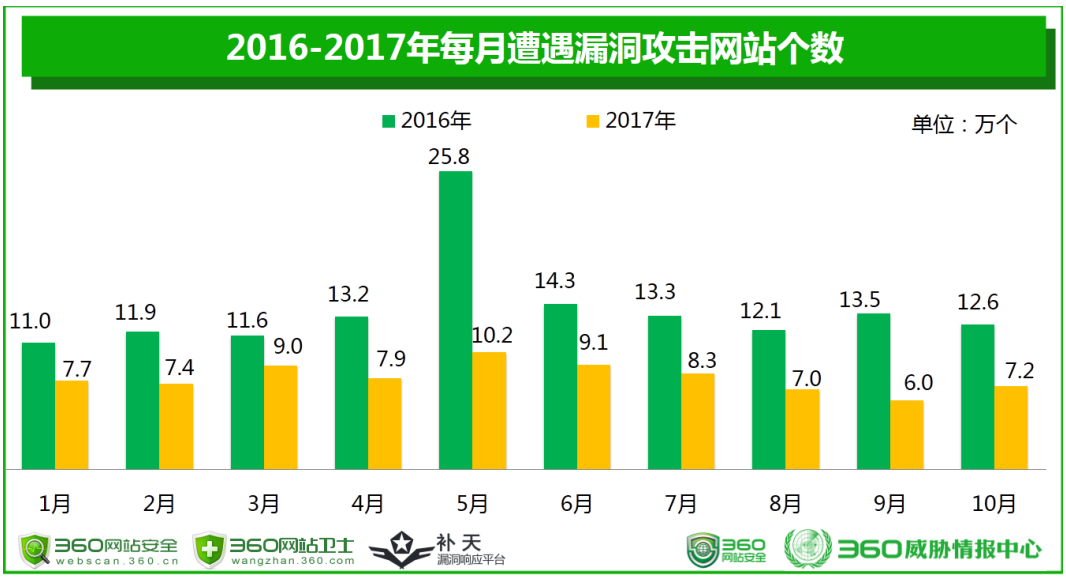
第二章　网站漏洞攻击分析

黑客对网站发动攻击一般有两种方式，一种方式是利用漏洞入侵网站，另一种方式是对网站发动流量攻击。本章将主要介绍分析 360 网站卫士针对各种漏洞攻击的拦截情况。

一、　漏洞攻击数量统计

2017 年 1-10 月，360 网站卫士共为 187.5 万个网站拦截各类网站漏洞攻击 26.4 亿次，较 2016 年 17.1 亿次，增长 54.4%，平均每天拦截漏洞攻击 868.9 万次。3 月、4 月是 2017 年攻击量最大的两个月，三月达到最高 6.3 亿次。网站每月遭遇漏洞攻击情况如下图所示。

截止到 2017 年 10 月，全年遭到漏洞攻击的网站共计 79.8 万个（全年去重），占 360 网站卫士覆盖总量（187.5 万）的 42.5%。平均每月约有 8.0 万个网站遭遇各类漏洞攻击，同比下降 44.2%。相比 2016 年每月遭遇漏洞攻击网站个数，2017 年整体趋于平稳。



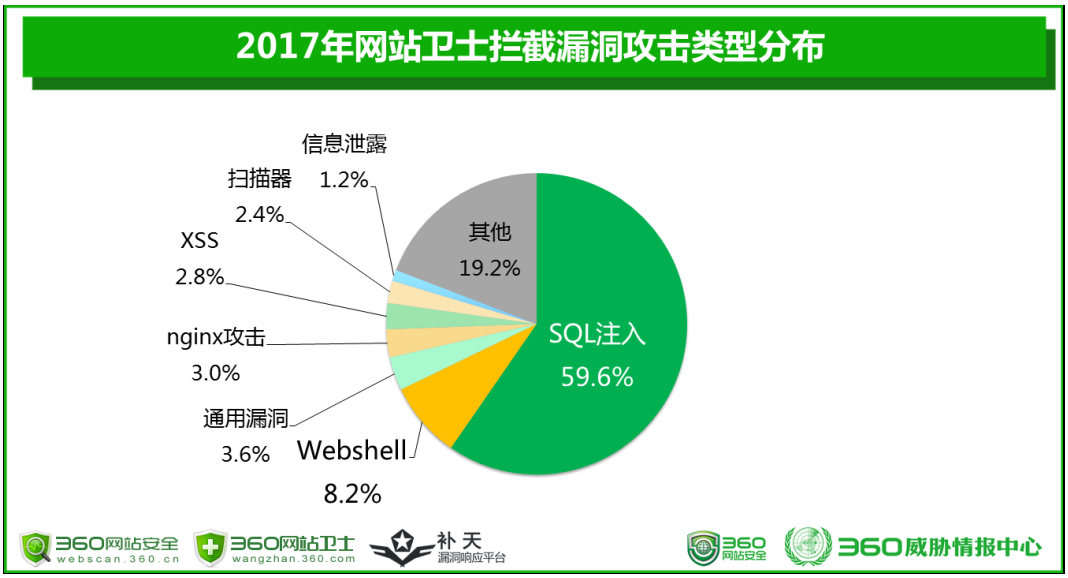
二、 漏洞攻击类型分析

下表给出了 360 网站卫士拦截漏洞攻击次数最多的 10 个漏洞类型。这十个类型共遭到攻击 22.0 亿次，占到漏洞攻击拦截总量的 83.4%。具体如下表所示。

TOP10	漏洞攻击类型	拦截次数（万）
1	SQL 注入	157682.9
2	Webshell	21615.1
3	通用漏洞	9402.9
4	nginx 攻击	7849.0
5	XSS	7491.3
6	扫描器	6385.4
7	信息泄露	3139.1
8	代码注入	2520.9
9	本地文件包含	2260.0
10	文件备份探测	2075.0

表格 5　漏洞攻击拦截量 Top10 的漏洞及其拦截次数

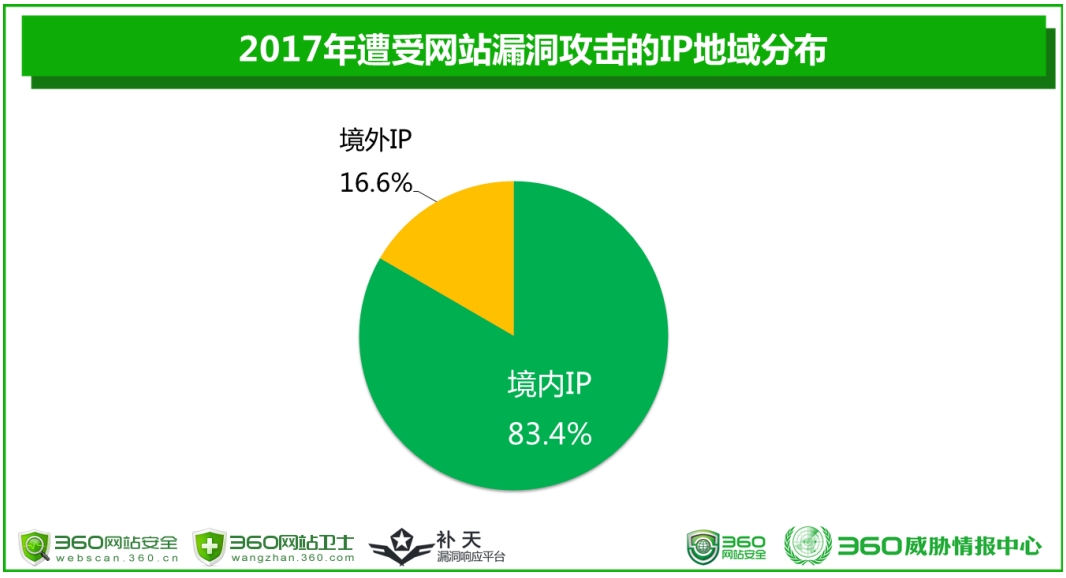
360 威胁情报中心监测显示，59.6%的网站漏洞攻击类型都为“SQL 注入”，稳坐第一。其次为“Webshell”和“通用漏洞”，占比分别为 8.2%和 3.6%。下图给出了网站漏洞攻击类型的具体分布情况。



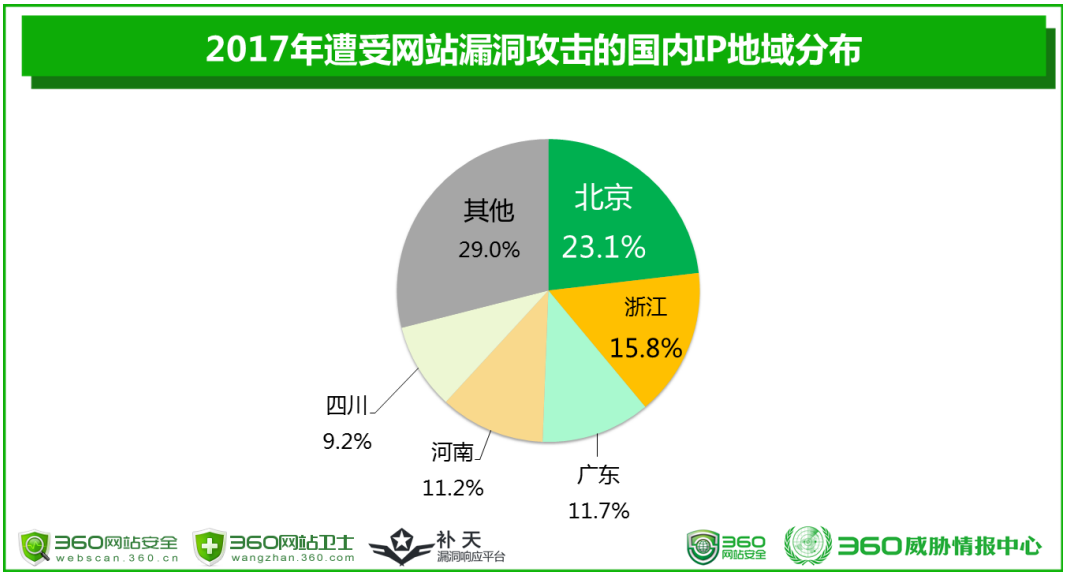
三、 漏洞攻击地域分析

（一）遭到漏洞攻击地域分析

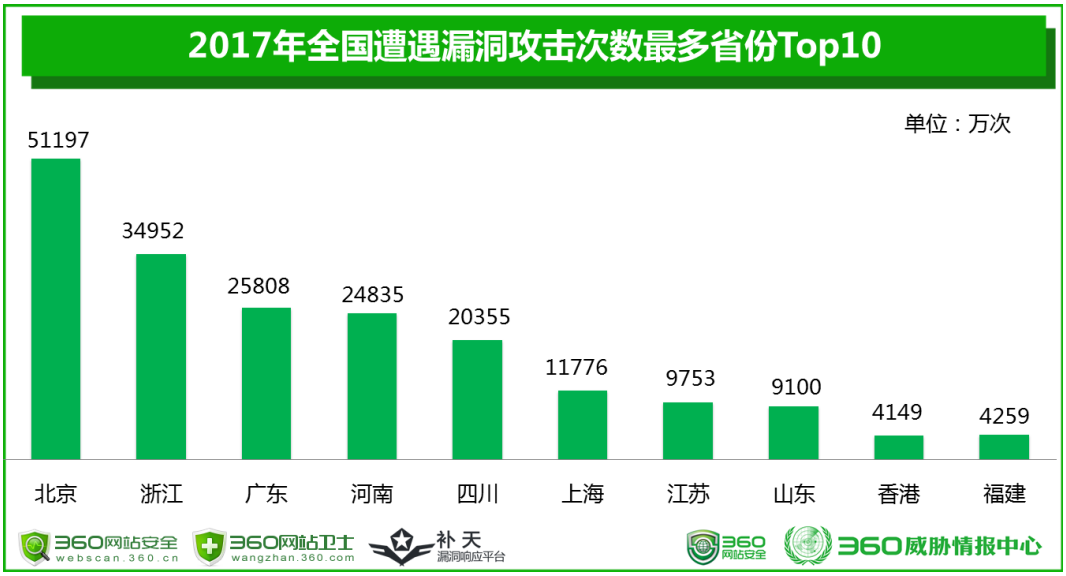
从遭到漏洞攻击网站服务器 IP 的地域分布来看，83.4%受害者 IP 来自境内地区 IP，境外的受害者仅为 16.6%。



从境内受害者的 IP 地域分布来看，23.1%来自北京，居于首位；其次分别为浙江（15.8%）、广东（11.7%）、河南（11.2%）、四川（9.2%）等。



下图给出了 2017 年遭到漏洞攻击的十大省份，其中，北京遭到攻击的 IP 最多，高达 5.1 亿次，相比去年 1.2 亿次上涨了 325%，居于全国首位；其次是浙江（3.5 亿次）、广东（2.6 亿次）。具体如下图所示。

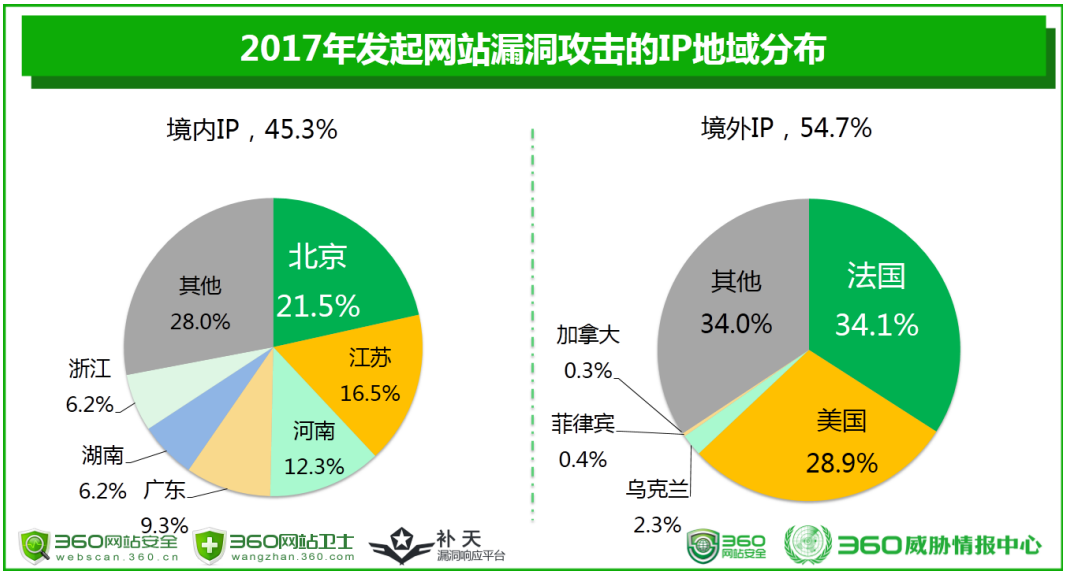


（二）发起漏洞攻击地域分析

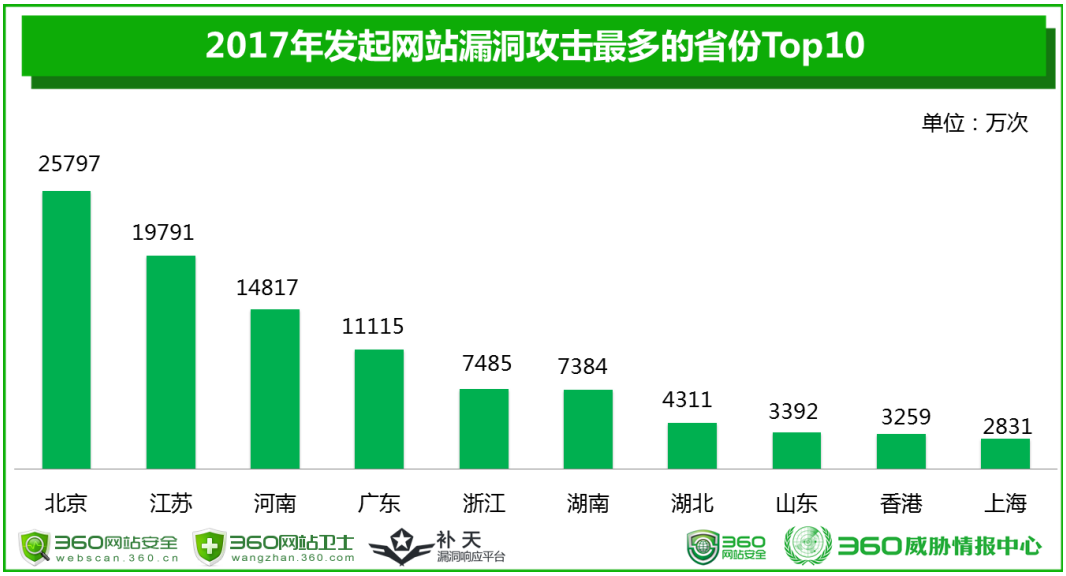
从发起漏洞攻击 IP 的地域分布来看，45.3%的攻击者 IP 来自境内地区，来自境外的攻击占比为 54.7%。境外攻击来源占比相较 2016 年的 23.4%足足增加了 31 个百分点。从侧面说明，来自境外的网站攻击呈现日益严重之势。

从境内攻击者的 IP 地域分布来看，21.5%来自北京，居于首位；其次分别为江苏（16.5%）、河南（12.3%）、广东（9.3 %）、湖南（6.2%）、浙江（6.2%）等。

从境外攻击者的 IP 地域分布来看，34.1%来自法国。其次是美国（28.9%）、乌克兰（2.3%）等。

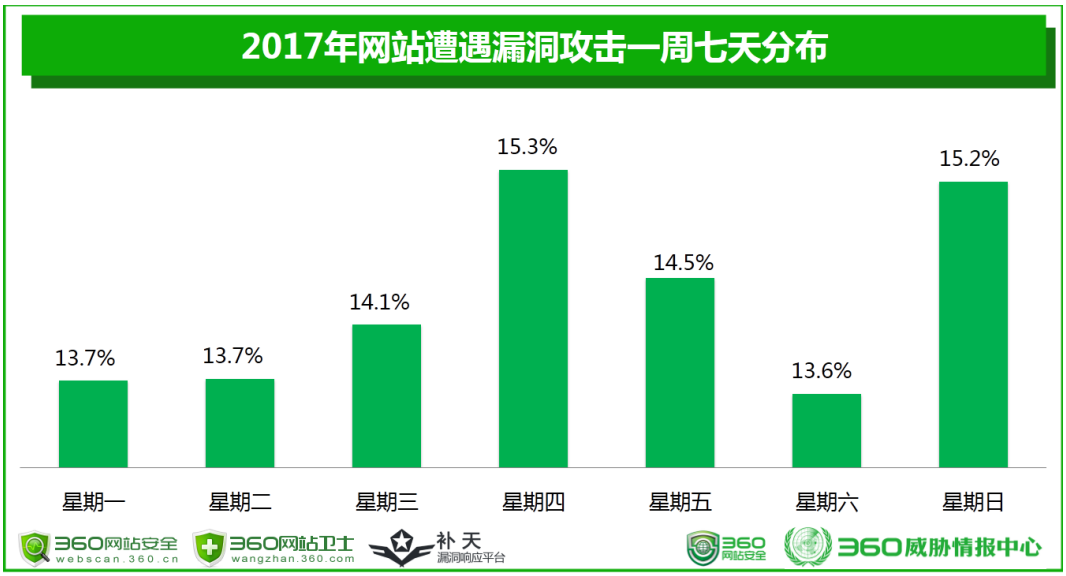


下图给出了 2017 年发起漏洞攻击最多的十大省份。其中，从北京发起漏洞攻击的 IP 最多，高达 2.6 亿次，居于全国首位，相比 2016 年居于全国首位的南京（5.0 亿次）有大幅的下降；其次是江苏（2.0 亿次）、河南（1.5 亿次）、广东（1.1 亿次）、浙江（7485 万次）、湖南（7384 万次）等。

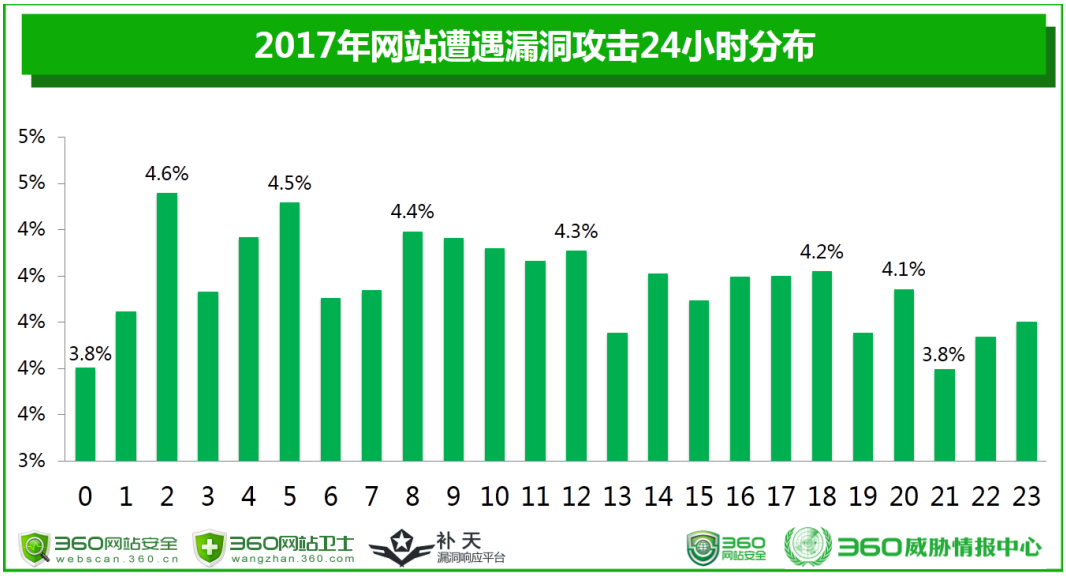


四、 漏洞攻击时域分析

下图给出了漏洞攻击在一周之内的分布统计。其中，每天的比例数字表示这一天的攻击量在一周总攻击量中的平均占比情况。从图中可以看出，星期四是一周中漏洞攻击最为集中的一天，占总攻击量的 15.3%，周日仅居其次，为 15.2%，而周五的攻击量则相对最少，仅占总攻击量的 14.5%。就平均性而言，周一周二周六较安全，而周四、周日最危险。



下图给出了一天之内漏洞攻击的分布统计。其中，每个小时的比例数字表示这一小时内的攻击量在当天总攻击量中的平均占比情况。从图中可以看出，一天的攻击分布基本平稳，漏洞攻击多集中于上午。


2017年网站遭遇漏洞攻击24小时分布
5%
5%
4%
4%
4%
4%
4%
3%
3.8%
4.6%
4.5%
4.4%
4.3%
4.2%
4.1%
3.8%
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
360网站安全 webscan.360.cn
360网站卫士 wangzhan.360.com
补天 漏洞响应平台
360网站安全
360威胁情报中心

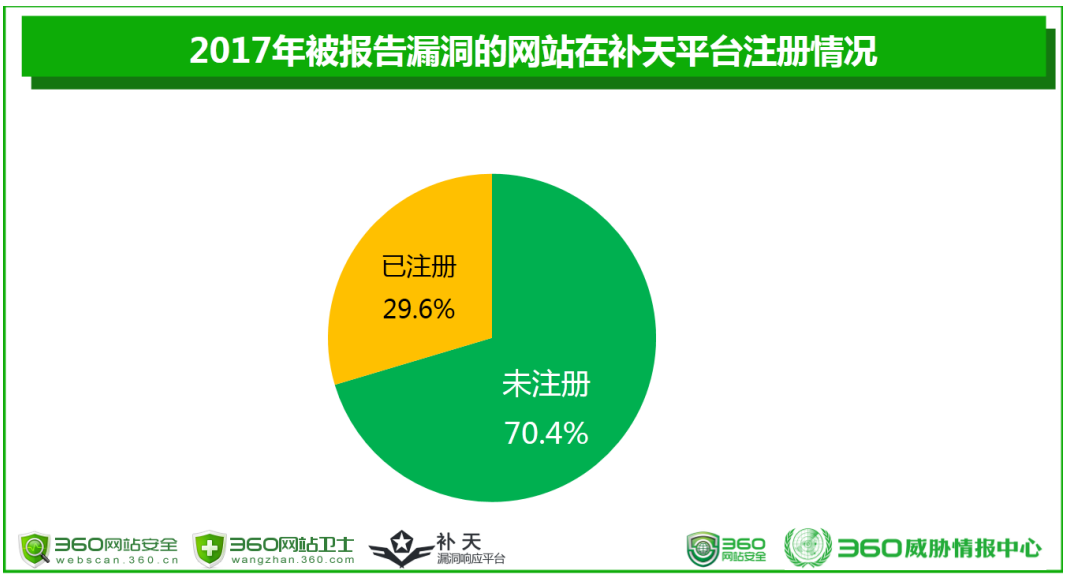
第三章　人工挖掘漏洞分析

本章从人工挖掘角度，对网站漏洞情况进行分析。主要根据补天平台公开征集收录白帽子提交的漏洞信息，结合平台自身对漏洞的研究积累，从而分析 2017 年全年，存在漏洞且被白帽子关注的全国数万个网站的安全状况。

一、　漏洞报告数量

2017 年全年，补天平台 SRC 共收录各类网站安全漏洞报告 22706 个，共涉及 14416 个网站。其中，3 月份收录的网站漏洞数量最多，为 3338 个。具体如下图所示。

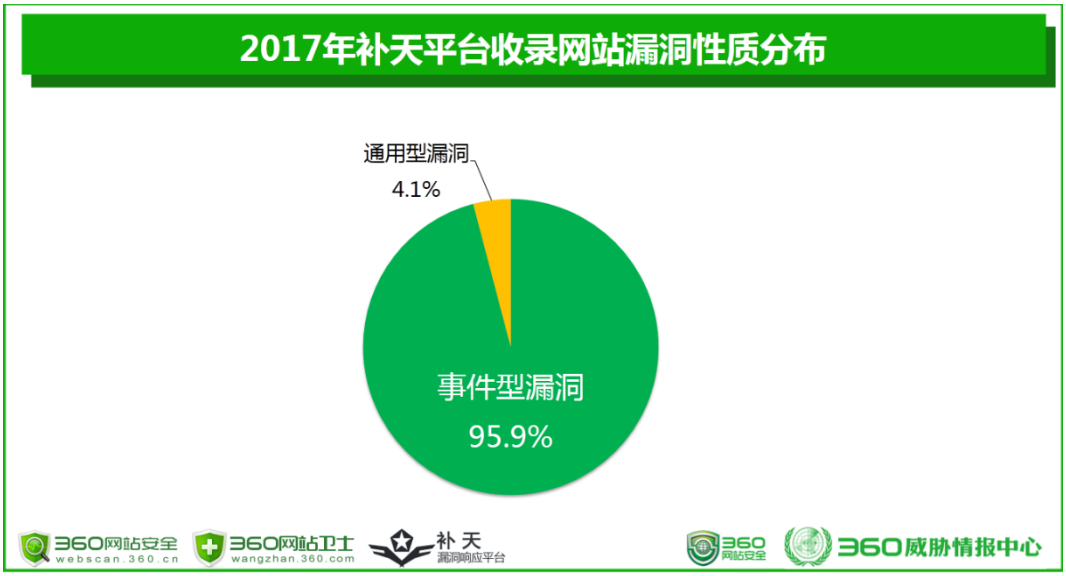
在补天平台被报告漏洞涉及的政企机构中，平均约有 29.6%的网站已注册加入补天平台。漏洞对应的网站政企机构注册加入补天平台，这通常意味着网站会安排专人对补天平台报告的漏洞进行响应和处理，在一定程度上反应了网站对安全漏洞的重视程度。



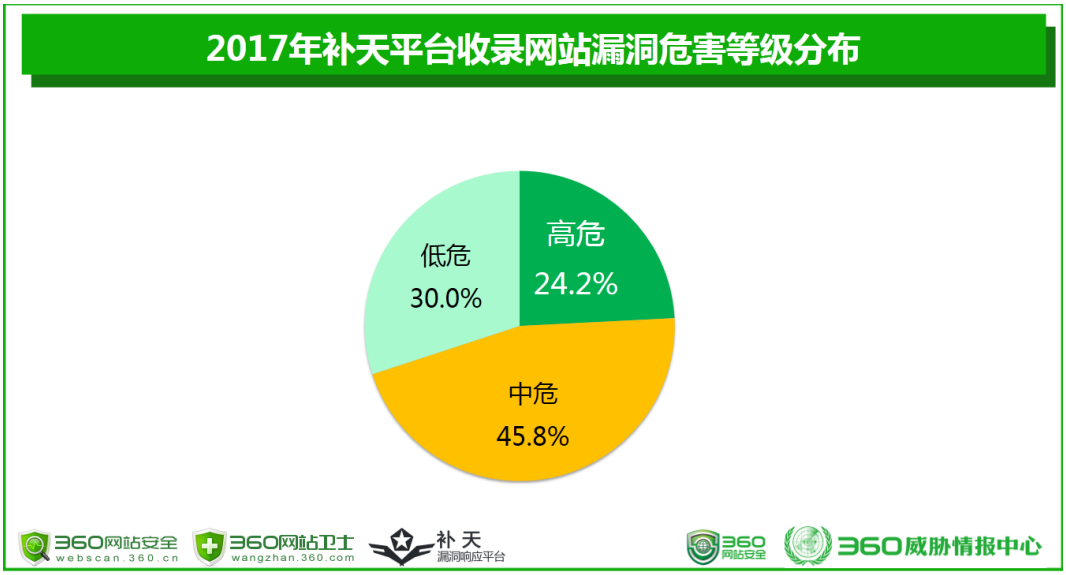
二、 漏洞类型分析

从补天平台收录网站漏洞的性质来看，通用型漏洞比例很低，仅为 4.1%，95.9%的网站漏洞都为事件型漏洞。

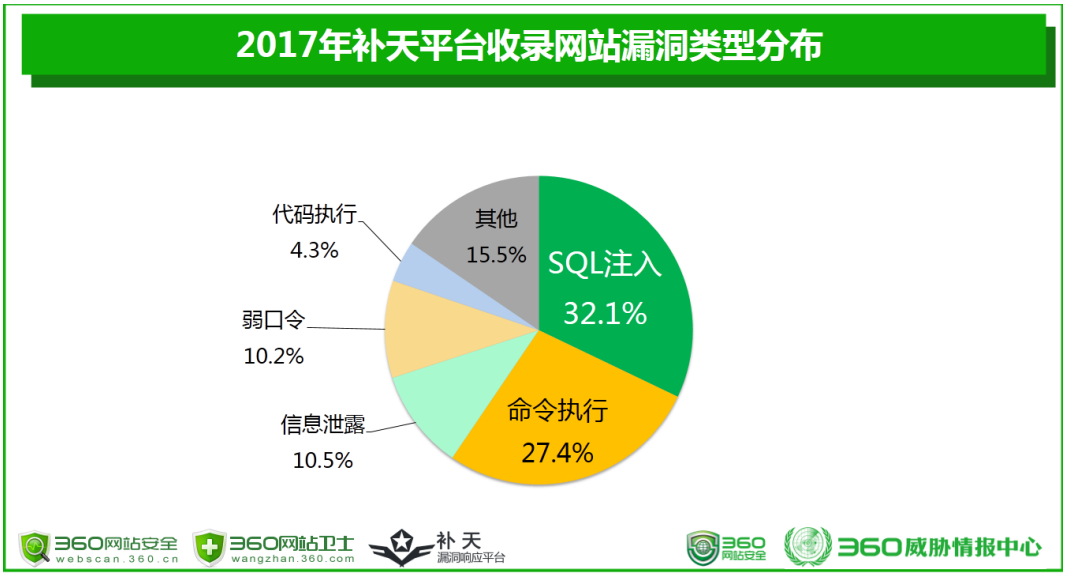
鉴于多数通用型漏洞属于可以检测的已知漏洞，而事件型漏洞则存在一定的偶发性和不可预测性。但从另一个角度来看，网站存在大量的事件型漏洞，这也就意味着：仅仅通过一般的、通用的安全检测手段并不足以及时的发现网站潜在的安全问题。第三方平台对网站漏洞的收集和报告，对于正规的网站来说尤为重要。



从补天平台收录网站漏洞的危害等级来看，高危漏洞占比为 24.2%，中危漏洞占比为 45.8%，低危漏洞占比为 30.0%。下图给出了补天平台收录的网站漏洞的危险等级情况。



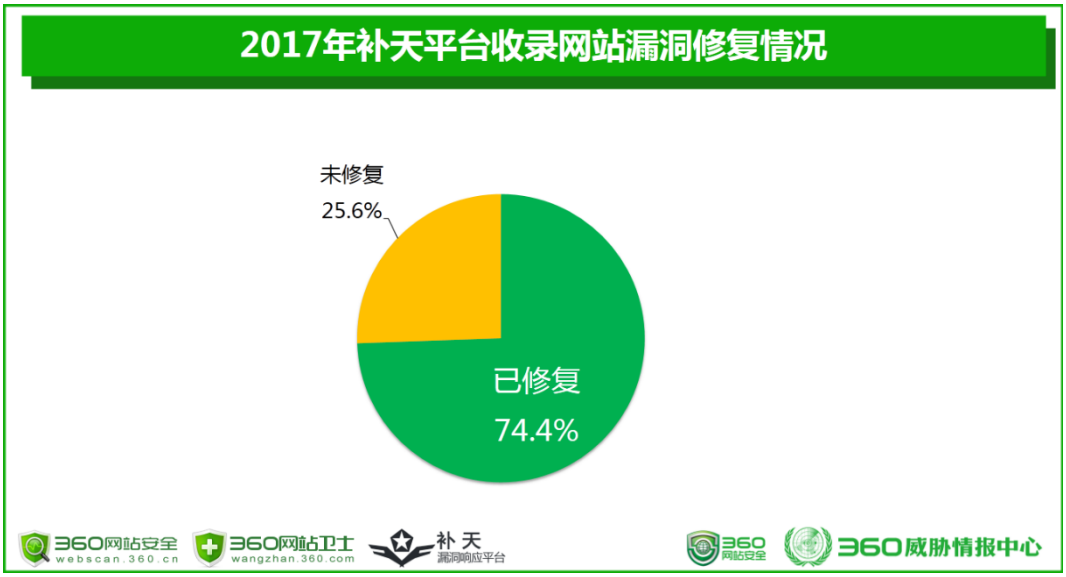
从补天平台收录网站漏洞的具体类型来看，SQL 注入漏洞最多，占比为 32.1%，其次是命令执行和信息泄露，占比分别为 27.4%和 10.5%。占比较高的还有弱口令（10.2%）、代码执行（4.3%），具体漏洞类型分布请见下图。



三、 漏洞修复情况

补天平台会不定期进行人工复核，以了解漏洞的修复情况，一般采取抽样人工验证的方式，本章将主要对政府机构及事业单位、教育培训、互联网、IT 信息技术、金融、通信运营商、医疗卫生、交通运输、制造业、传媒机构的十个行业网站修复情况进行分析。

在补天平台收录网站漏洞中，74.4%的网站漏洞已经进行了修复，25.6%的网站漏洞未进行修复。



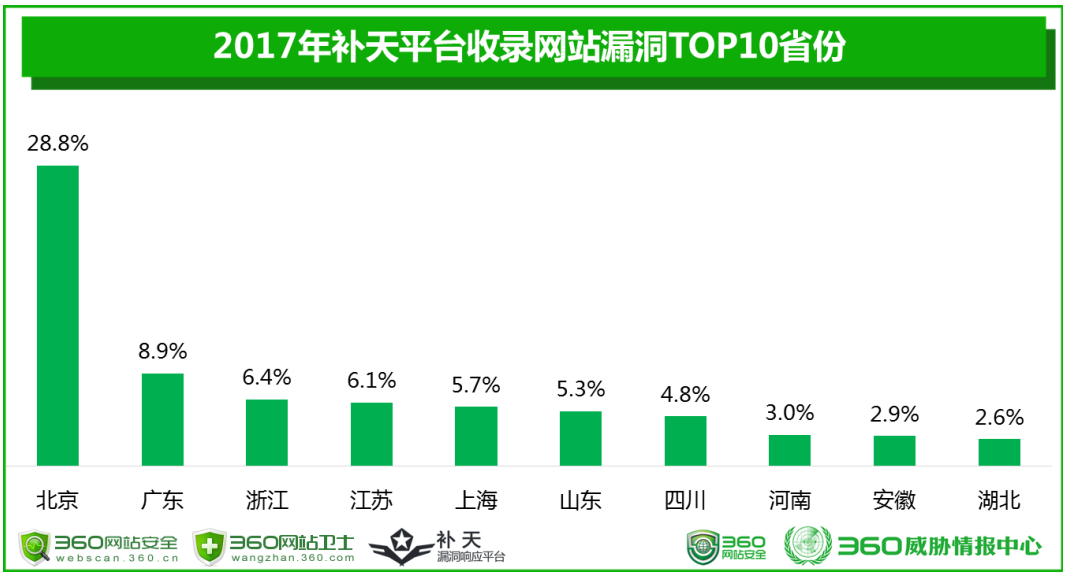
补天平台看到的漏洞修复情况，和抽样调查的结果略有不同。由于部分网站的安全负责人在修复网站漏洞后未及时在补天平台上进行登记，所以，补天平台上站长标记的修复情况会与上述统计有一定的出入。

另一方面，补天平台也没有强制标注的要求。补天平台在收到白帽子报告的网站安全漏洞后，都会在第一时间通知相关网站，但是对涉及政企机构，没有明确规定必须在修复漏洞之后及时标注漏洞状态信息。

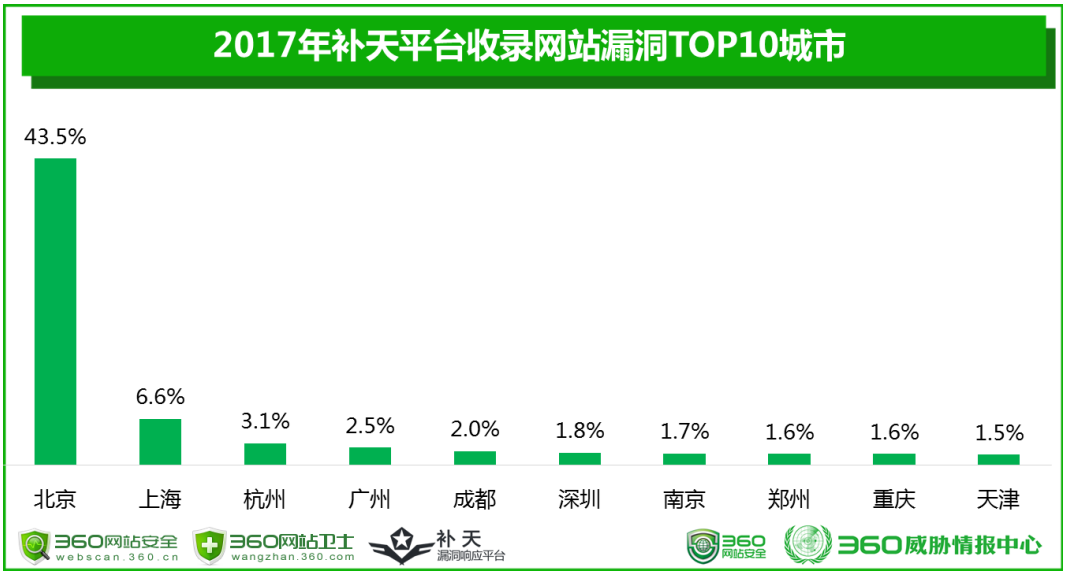
四、 有漏洞网站地域分布

本报告中地域划分主要根据 IP 地址查询其网站服务器归属地，可能与实际主管机构的行政归属地存在一定的差异。

从省级地域分布来看，补天平台收录网站漏洞最多的十个省份占到了总量的 74.5%。其中，IP 地址在北京的网站漏洞最多，占比为 28.8%，其次广东省为 8.9%，浙江省为 6.4%。具体如下图所示。



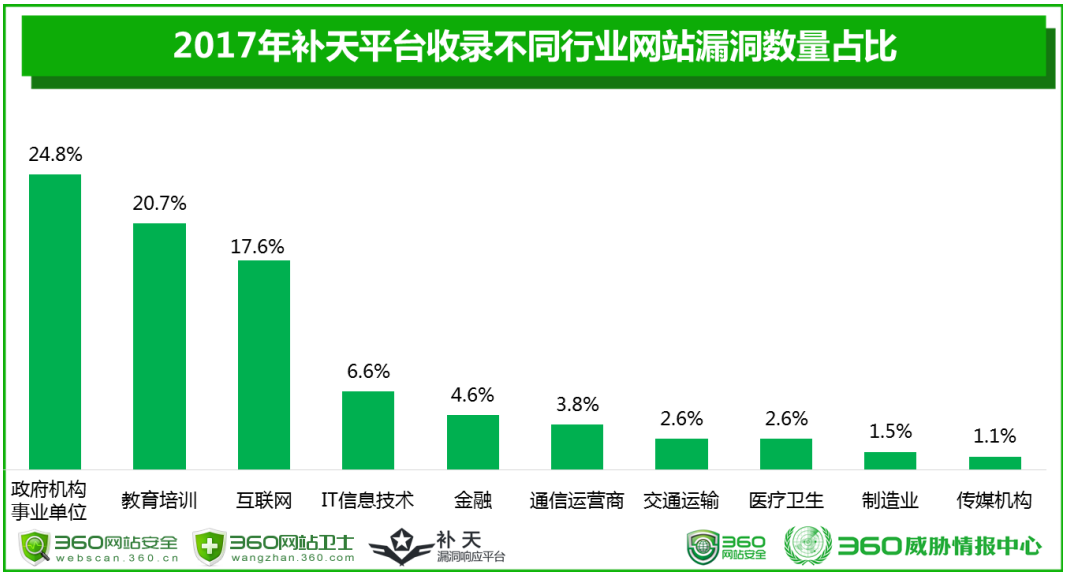
从城市地域分布来看，补天平台收录网站漏洞最多的十个城市占总量的 66.0%。其中，IP 地址在北京市的网站漏洞最多，高达 43.5%，其次上海市为 6.6%，杭州市为 3.1%。具体如下图所示。



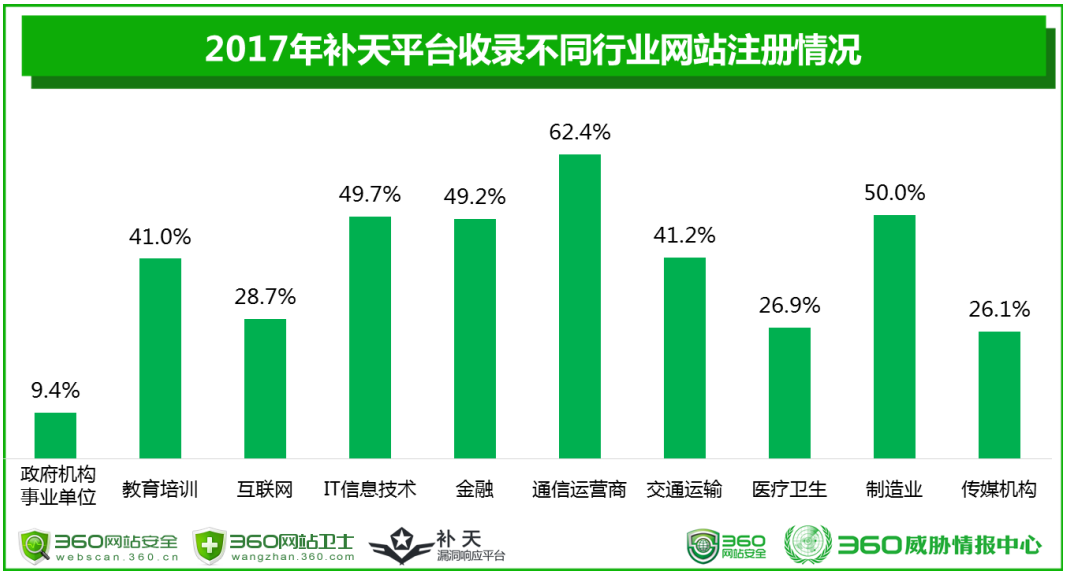
五、 不同行业网站漏洞情况

在所有网站中，我们在能够明确的确认其所属行业的网站中选择了政府机构及事业单位、教育培训、互联网、IT 信息技术、金融、通信运营商、医疗卫生、交通运输、制造业、传媒机构十个行业网站进行了分类，重点研究这十个行业网站的安全状况。

补天平台收录的网站漏洞中，政府机构及事业单位网站的漏洞数量是最多的，占比为 24.8%；其次，教育培训网站漏洞为 20.7%，互联网行业为 17.6%。每个行业的网站漏洞分布情况，具体如下图所示。



被报告漏洞涉及的不同行业网站中，通信运营商行业网站注册率最高为 62.4%，其次，制造业网站注册率为 50.0%，IT 信息技术行业网站注册率为 49.7%。



从高危漏洞网站来看，通信运营商和 IT 信息技术的网站高危漏洞占比最多，均为 45.4%，其次是金融网站高危漏洞为 43.1%。具体如下表所示。

行业	高危	中危	低危
政府机构、事业单位	18.5%	46.9%	34.6%
教育培训	17.1%	48.2%	34.6%
互联网	23.6%	45.8%	30.5%
IT 信息技术	45.4%	34.7%	19.9%
金融	43.1%	31.4%	25.5%
通信运营商	45.4%	38.7%	15.8%
交通运输	29.0%	45.9%	25.1%
医疗卫生	25.8%	49.6%	24.6%
制造业	28.6%	47.2%	24.1%
传媒机构	25.1%	46.7%	28.1%

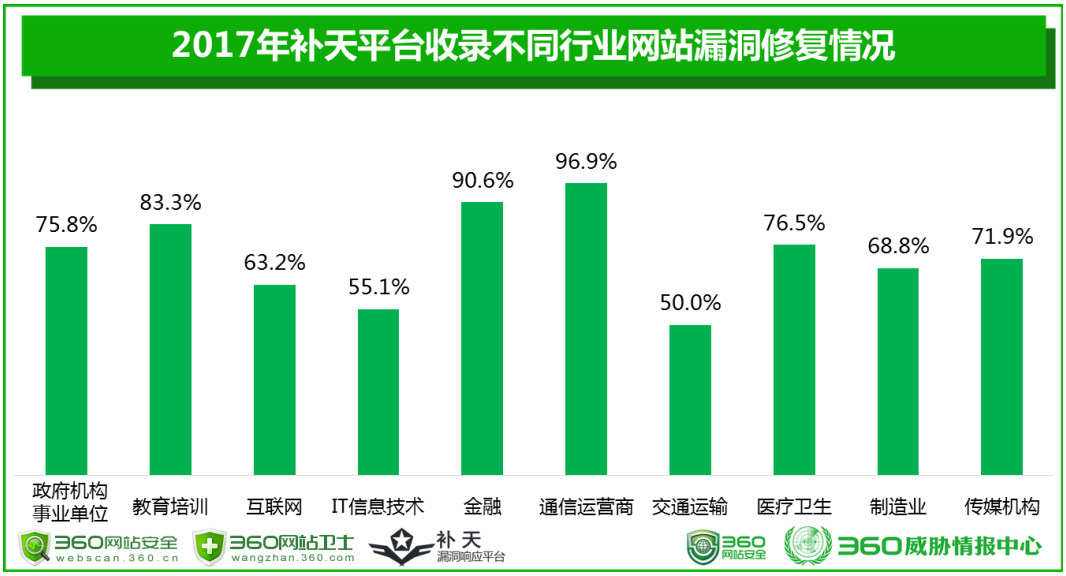
表格 6　不同行业的网站漏洞等级情况

政府机构及事业单位、教育培训、互联网、IT 信息技术、金融、通信运营商、医疗卫生、交通运输、制造业、传媒机构网站漏洞类型分布，如下表所示。我们可以看出，“SQL 注入”和“命令执行”漏洞类型无论是从总体角度还是从各行业网站漏洞类型均名列前茅。

行业	SQL 注入	命令执行	信息泄露
政府机构、事业单位	33.7%	34.3%	7.1%
教育培训	38.3%	18.6%	13.8%
互联网	30.2%	23.1%	13.2%
IT 信息技术	38.4%	16.5%	9.5%
金融	9.2%	45.8%	10.4%
通信运营商	7.5%	51.8%	5.8%
交通运输	23.0%	35.5%	8.8%
医疗卫生	37.2%	22.0%	8.9%
制造业	27.6%	24.8%	13.8%
传媒机构	33.2%	21.6%	12.6%

表格 7　不同行业的漏洞类型分布

对本次报告选取的十个行业进行抽样调研回访，我们发现，96.9%的通信运营商网站漏洞都进行了修复，其次，90.6%的金融行业的网站漏洞进行了修复，83.3%的教育培训网站进行了修复。


2017年补天平台收录不同行业网站漏洞修复情况
75.8%
83.3%
63.2%
55.1%
90.6%
96.9%
50.0%
76.5%
68.8%
71.9%
政府机构
事业单位
教育培训
互联网
IT信息技术
金融
通信运营商
交通运输
医疗卫生
制造业
传媒机构
360网站安全
webscan.360.cn
360网站卫士
wangzhan.360.com
补天
漏洞响应平台
360网站安全
360威胁情报中心

第四章　网络扫描

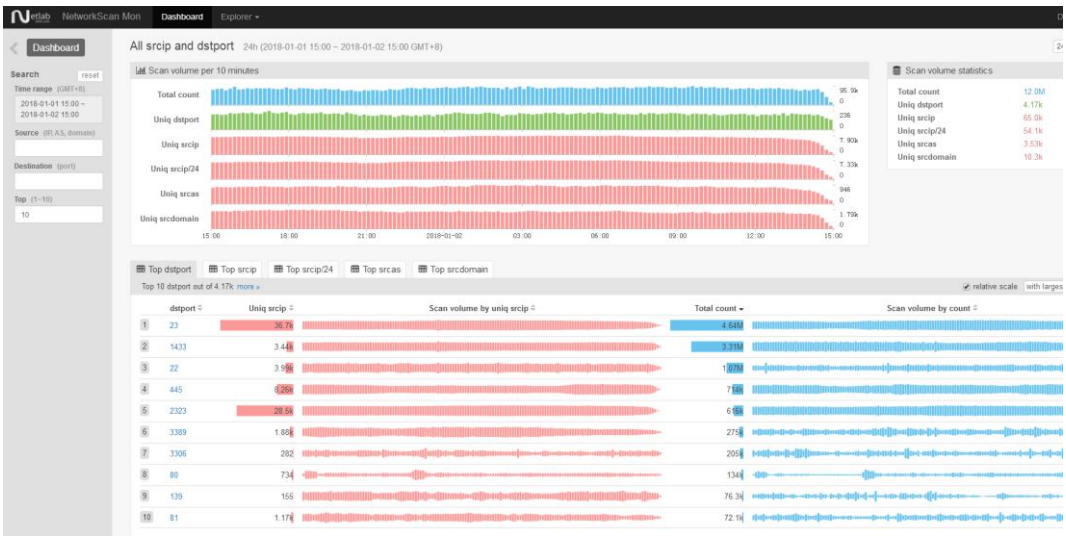
扫描行为通常处于情报搜集阶段，使用自动化程序对未知主机进行批量检测，根据主机返回的信息判断其运行状态。通常用于判断主机运行的服务类型、服务程序及版本，是否存在漏洞等信息，进而有针对性执行攻击手段。

一、　全网扫描活动监测概况

扫描事件是指在一定时间内，具有相同或相似特征的扫描行为的集合。2017 年全年，360 威胁情报中心在全球范围内共监测发现扫描源 IP 1400 万个，累积监测到扫描事件 3.93 亿次。全球平均每日活跃的扫描源 IP 大约有 13.3 万个，对应的日均扫描事件约 107.6 万起。

扫描器是一类自动检测本地或远程主机安全弱点的程序，它能够发现扫描目标存在的漏洞并将扫描结果提供给使用者。其工作原理是扫描器向目标计算机发送数据包，然后根据对方反馈的信息来判断对方的操作系统类型、开发端口、提供的服务等敏感信息。在互联网上，活跃的扫描器背后往往是活跃的黑客组织和潜在的危险。对全网扫描器及其扫描活动的监测、发现与防范，是网络系统安全运维所需的，重要的威胁情报信息。

360 威胁情报中心对全球网络扫描活动的监测，是通过全球首套，面向全球开放的，全球网络扫描器实时监测系统（http://scan.netlab.360.com/）实现的。这套系统以 360 安全大数据为基础，可以实时分析当前及过去 30 天内，发生在全球互联网上的扫描器扫描行为，分析精度最高可以精确到 10 分钟级。



该系统不仅可以分析扫描器活动的时域统计特征，还可以分别从扫描目标端口号（target ports）、扫描源 IP 地址（source IPs）、扫描源所属网段（source IP/24s）和扫描源所属的网络系统（source ASs）等 4 个维度进行分类分析和升降排序。同时该系统还可以支持攻击源的 IP、网段和所属网络等信息的查询检索服务，以及攻击目标的端口号查询服务。

二、 不同类型的扫描活动

网络扫描活动的具体技术方法多种多样，但从扫描的具体目的来看，主要可以分为三种类型：常规恶意扫描、针对性突发扫描和安全监控扫描。

1）常规恶意扫描

常规恶意扫描是攻击者针对一般性、常见性的网络安全问题进行的扫描活动，其主要目的是为了发现存在已知安全漏洞的网络设备，并进而对相关设备发动攻击。进行常规恶意扫描活动的攻击者遍布全球。从长期监测来看，常规恶意扫描活动每天的活动频率与整体规模都变化不大，形成了整个网络扫描活动监测过程中的“背景流量”。

常规恶意扫描针对的主要端口包括：远程控制端口（如 22/ssh， 3389/微软远程桌面），数据连接服务端口（如 1433/mssql，3306/mysql），以及 Web 服务端口（80/8080/http）等。

2）针对性突发扫描

针对性突发扫描是攻击者针对某些新出现的，特定的安全问题而突然发起的扫描活动，这种现象通常出现在重大的 0day 漏洞被披露之后的一段时间内。这里所说的 0day 漏洞，有的是被黑客组织或第三方研究人员披露的，而有的则是在软硬件供应商发布了安全公告或安全补丁之后，被攻击者逆向分析定位出来的。针对性突发扫描可以使攻击者在 0day 漏洞被修复之前，获得一个短暂的攻击间隙，在这个间隙中，尚未修复相关漏洞的网络设备或系统会百分之百的中招。

例如，2016 年 11 月 7 日，独立安全研究员 Kenzo 通过博客发布了家用路由器设备 TR-069/TR-064 的一个新的安全漏洞。而到了 11 月 26 日，mirai 僵尸网络就开始针对这一漏洞，对 7547 端口进行了大规模的扫描。结果到了 11 月 28 日的扫描高峰，就有大约 90 万台德国电信用户家中的 TR-069/TR-064 路由器因 mirai 的扫描活动而死机，形成了一次较大规模“断网”事件。

再比如，2017 年，世界著名漏洞军火商 Zerodium 最近表示愿意出价 150 万美元购买一套完整的 iPhone（iOS）持续性攻击的远程越狱漏洞，即在没有任何用户交互的情况下，远程感染目标设备。凭借这些信息，攻击者可以针对目标特性调整他们的开发方式，交付一个不太敏感的“1-day”或“N-day”的漏洞，而不是被誉为“皇冠上的宝石”的“0-day”漏洞。

类似于 Turla、ofacy 和 Newsbeef 这样的 APT 组织已把这类分析技术运用得相当熟练，其他的 APT 组织也以其自定义的分析框架而闻名，比如多产的 Scanbox。由于分析框架的普遍性和零日漏洞的高昂代价，我们可以估计在 2018 年使用“BeEF”之类的分析工具包将会增加，更多的黑客团队可能采用公共框架，或者自己开发工具包。

3）安全监控扫描

安全监控扫描是由安全机构或安全研究人员，出于安全监控或安全研究的目的，对网络设备发起的扫描活动，主要被用来发现有潜在安全风险的设备，以便实施更加有效的安全策略。从技术方法来看，安全监控扫描与前述两种恶意扫描活动并没有太大的差别，因此从被扫描者的角度来看，善意的扫描与恶意的扫描通常是无法区分的。只不过安全机构发起的扫描活动，通常不会利用恶意代码对相关设备发动实质性的恶意攻击。

三、 扫描活动扫描的主要端口

通过对 2017 年全年网络扫描器扫描的端口分析发现，扫描器扫描的端口主要为具备远程控制能力的端口和存在信息泄露的端口。从具体的端口号来看，被扫描次数最多的端口是 23 端口和 2323 端口，约 61.8%的网络扫描事件会扫描 23 端口，约 23.9%的网络扫描事件会扫描 2323 端口。

特别的，永恒之蓝勒索蠕虫（WannaCry 病毒）的特征之一就是会扫描 445 端口，所以，每一台感染 WannaCry 病毒电脑也会成为一个针对 445 端口的扫描器。而该病毒在 2017 年的爆发，使得针对 445 端口的扫描活动也异常活跃，以至于针对 445 端口的扫描器数量在 2017 年排名进入了前十名。而在 2016 年，被扫描最多的十个端口中并没有 445 端口。

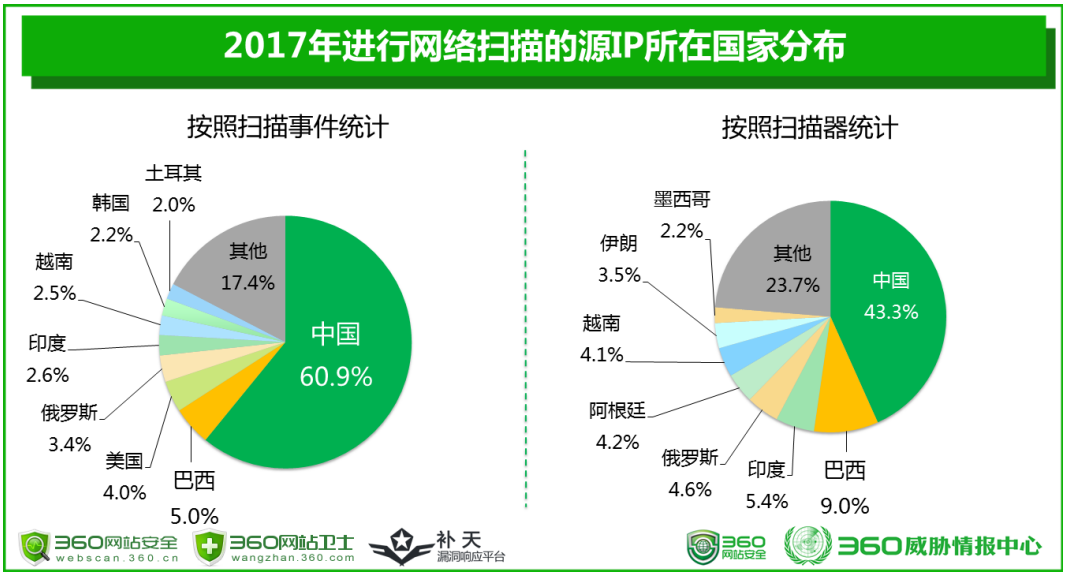
下表给出了 2017 年网络扫描事件扫描最多的十个网络端口及其对应的常用服务、潜在危害说明。其中，“扫描事件覆盖率”表示对相关端口进行扫描的扫描事件占全部扫描事件的比例情况。需要特别说明的是，扫描事件与漏洞、端口并非是一一对应的。一次网络扫描事件可能会只针对一个网络端口或只针对一个安全漏洞，但也有可能会同时针对多个网络端口或多个安全漏洞。所以，在下表中，仅排名前十的网络端口号对应的扫描事件覆盖率之和就已经大于了 100%。

端口	常用服务	潜在危害	扫描事件覆盖率
23	#telnet & #mirai	远程控制	61.8%
2323	#mirai	远程控制	23.9%
1433	#SQL server	信息泄露	15.0%
22	#ssh server	远程控制	6.2%
80	#http server	远程控制	4.1%
23231	#mirai	远程控制	2.5%
6789	#mirai	远程控制	2.0%
445	#windows network share	信息泄露	1.7%
7547	#TR-069 & #mirai	远程控制	1.7%
5358	#wsdapi-s	信息泄露	1.5%

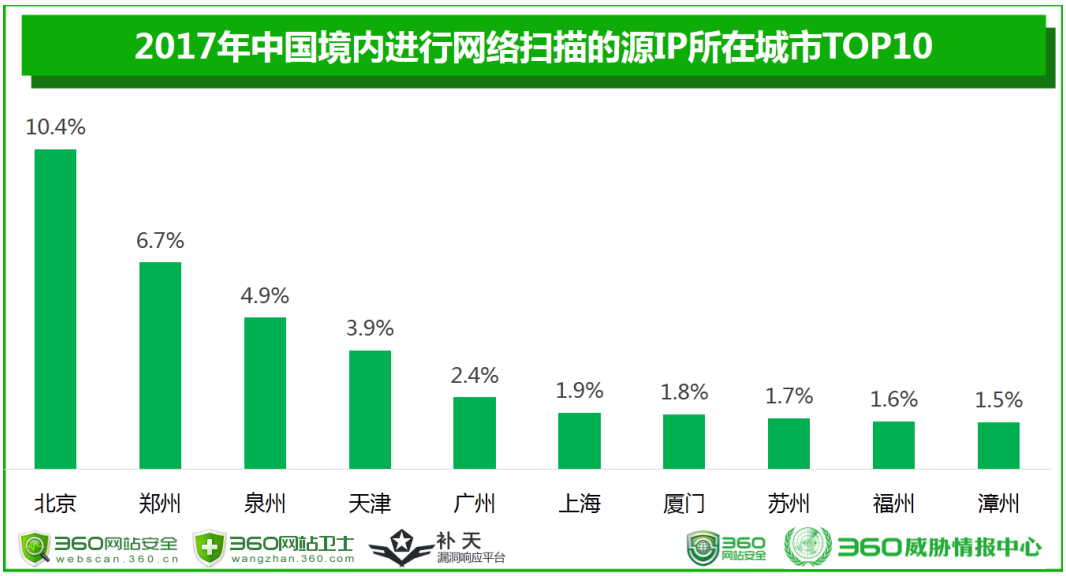
表格 8　2017 年扫描器扫描最多的十个端口

四、 扫描源 IP 地域分布

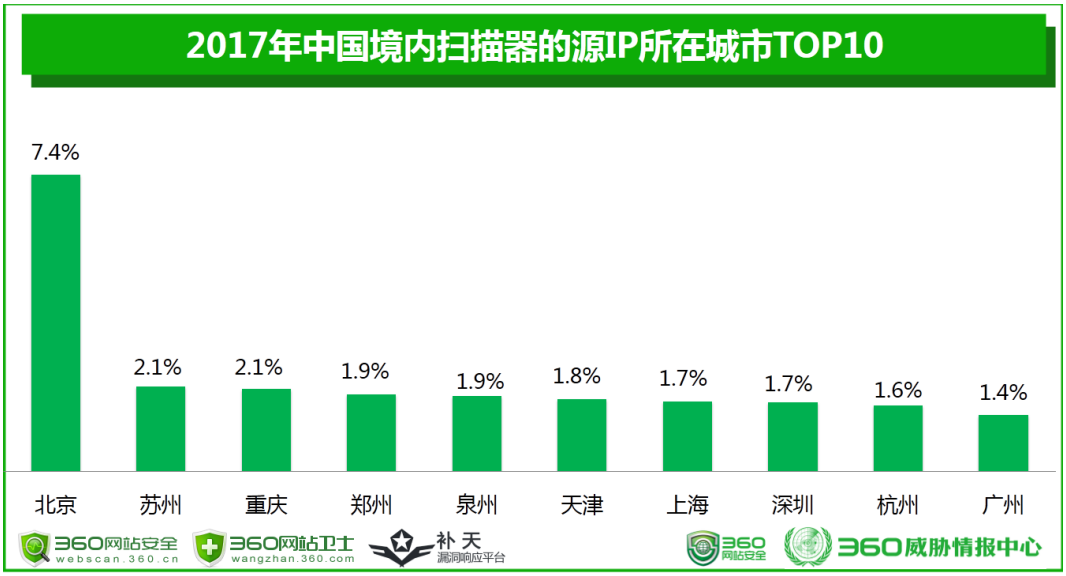
统计显示，在 360 威胁情报中心监测到的所有网络扫描活动中，从扫描事件的数量来看，60.9%的网络扫描事件是从中国大陆发起的，5.0%是从巴西发起的，而美国、俄罗斯和印度位列其后，占比分别为 4.0%、3.4%和 2.6%。而从扫描器的数量来看，43.3%的扫描源 IP 位于中国大陆境内；9.0%的扫描源 IP 位于巴西；印度、俄罗斯、阿根廷分列三到五位，比例分别为 5.4%、4.6%和 4.2%。相比 2016 年，越来越多的扫描源 IP 集中在中国大陆（这主要是由于我们能够看到的数据来源主要来源于中国大陆），同时中国大陆发起的网络扫描事件数量也大幅增长。



对 IP 地址属于中国的网络扫描源进行进一步的地域分析发现，位于北京的扫描器数量最多，扫描源 IP 占全国总量的 10.4%；其次是郑州，占比为 6.7%，排在三到五位的城市分别是泉州、天津和广州，占比分别为 4.9%、3.9%和 2.4%。



而如果从发起扫描事件的数量来看，在国内，IP 属于北京的扫描器发起的扫描事件最多，占境内扫描器发起的所有扫描事件的 7.4%，其次是苏州，占 2.1%，排在三到五位的城市分别是重庆、郑州和泉州，占比分别为 2.1%、1.9%和 1.9%。


2017年中国境内扫描器的源IP所在城市TOP10
7.4%
2.1%
2.1%
1.9%
1.9%
1.8%
1.7%
1.7%
1.6%
1.4%
北京
苏州
重庆
郑州
泉州
天津
上海
深圳
杭州
广州
360网站安全 webscan.360.cn
360网站卫士 wangzhan.360.com
补天 漏洞响应平台
360网站安全
360威胁情报中心

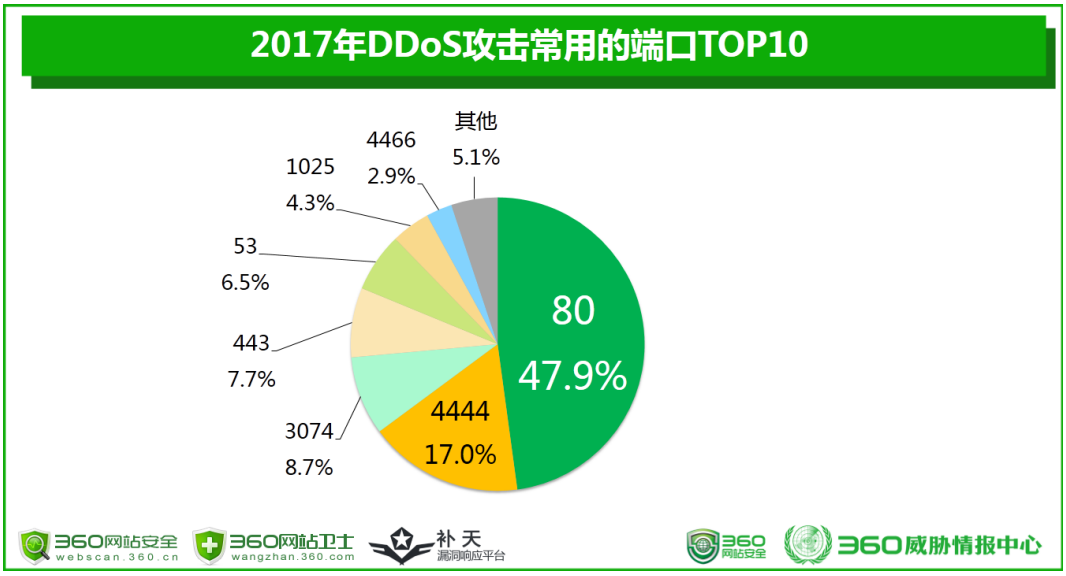
第五章　网站 DDoS 攻击情况

DDoS 攻击仍然是全球最大的互联网安全威胁之一，根据 DDosMon 网站（https://ddosmon.net/insight/?last=365）数据显示，在过去一段时间内每天检测到大约 2 万次攻击。本章包含由 DDoS 和僵尸网络追踪系统检测到的各种 DDoS 攻击的观察结果和见解。它代表了网络攻击趋势的独特视角，包括针对最新 DDoS 攻击统计数据和行为趋势。

一、　DDoS 攻击情况

2016 年 12 月 5 日至 2017 年 12 月 5 日，360 威胁情报中心监测到 626.2 万个 IP 在过去一年曾遭到过 1064.3 万次攻击。

2017 年，360 威胁情报中心监测显示，针对 DDoS 攻击的端口中，80 端口是 DDoS 攻击最常用的端口，占比为 47.8%，其次为 4444 端口（17.0%）、3074 端口（8.7%），具体分布情况如下图所示。

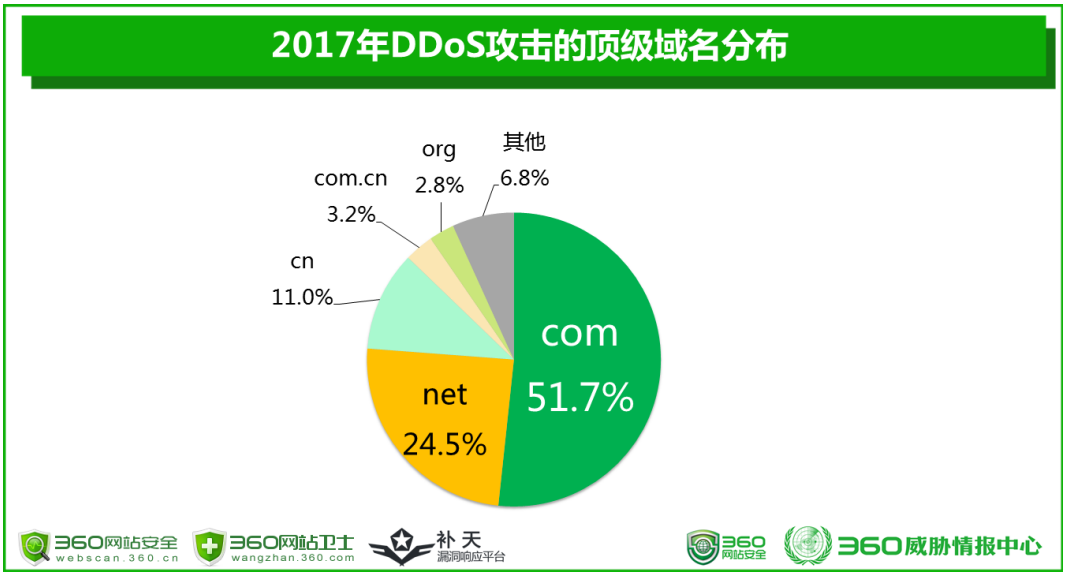


下表是对上图中 DDoS 攻击常用端口的简单介绍。

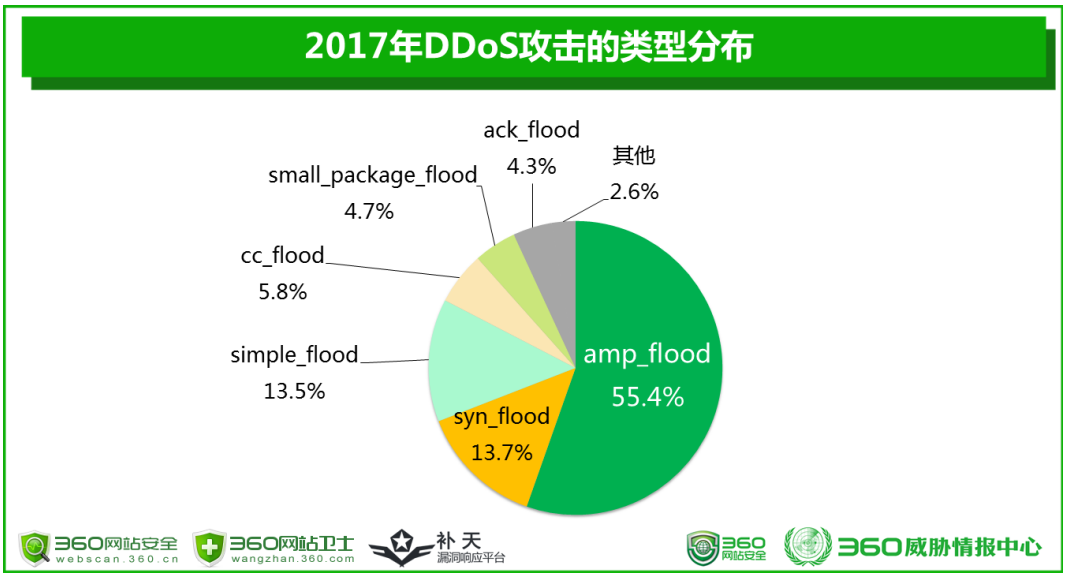
端口	常用服务
80	HTTP 服务端口
4444	Metasploit 的默认监听端口，有些恶意程序也会使用该端口进行远程入侵
3074	xbox game 服务端口
443	HTTPS 服务端口
53	DDNS 服务端口

表格 9　2017 年 DDoS 常用端口介绍

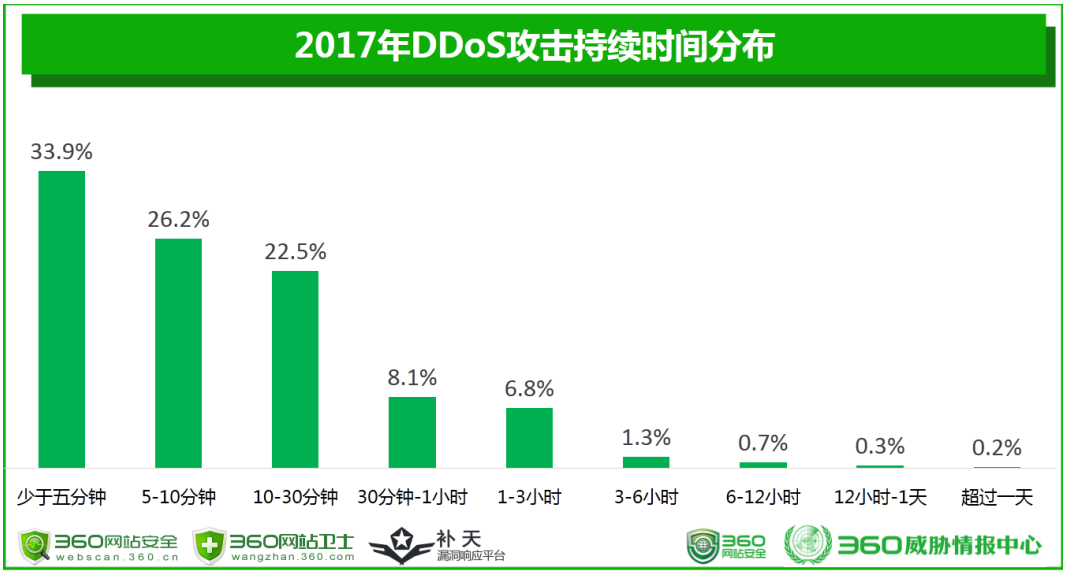
2017 年，360 威胁情报中心监测显示，DDoS 攻击的网站域名中，51.7%为.com 域名，其占据了半壁江山。其次是.net 和.cn 域名，占比分别为 24.5%和 11.0%。具体分布情况如下图所示。



2017 年，360 威胁情报中心监测显示，DDoS 攻击类型中，amp_flood 类型最多，占比为 55.4%，其次为 syn_flood 和 simple_flood，占比分别为 13.7%和 13.5%。具体分布情况如下图所示。



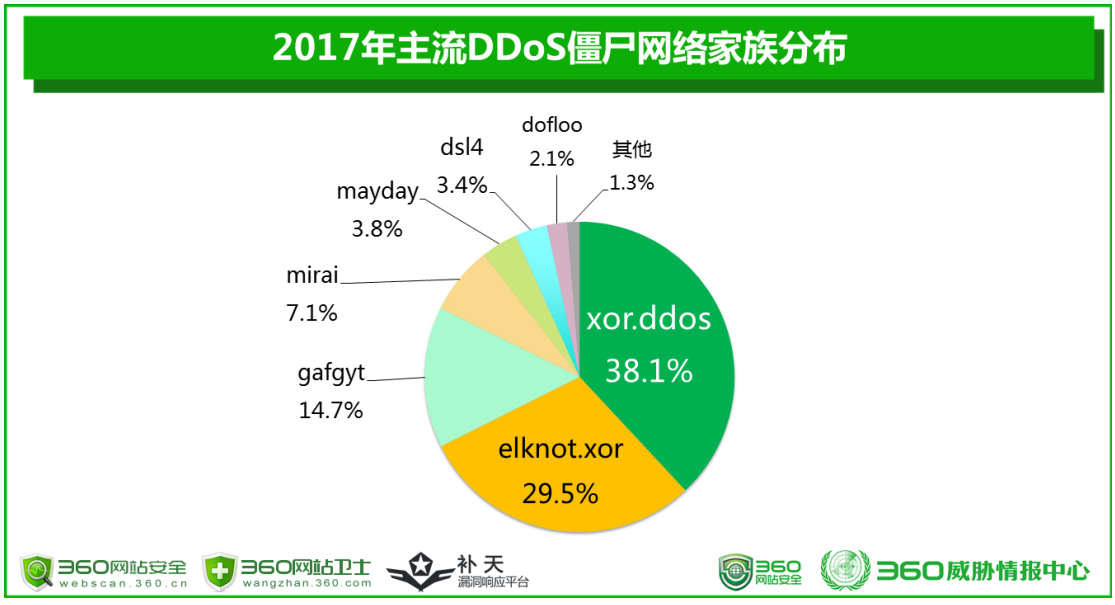
从攻击时长来看，超过五成的 DDoS 攻击持续时间小于 10 分钟，而持续时间在 10 分钟至 30 分钟的攻击占比约为 22.5%，30 分钟至 1 小时的攻击占比约为 8.1%，持续时间超过 1 小时的攻击占比不足 10%。总体而言，短时、小量的攻击仍然是 DDoS 攻击的主流。下图给出了 DDoS 的攻击持续时间分布。



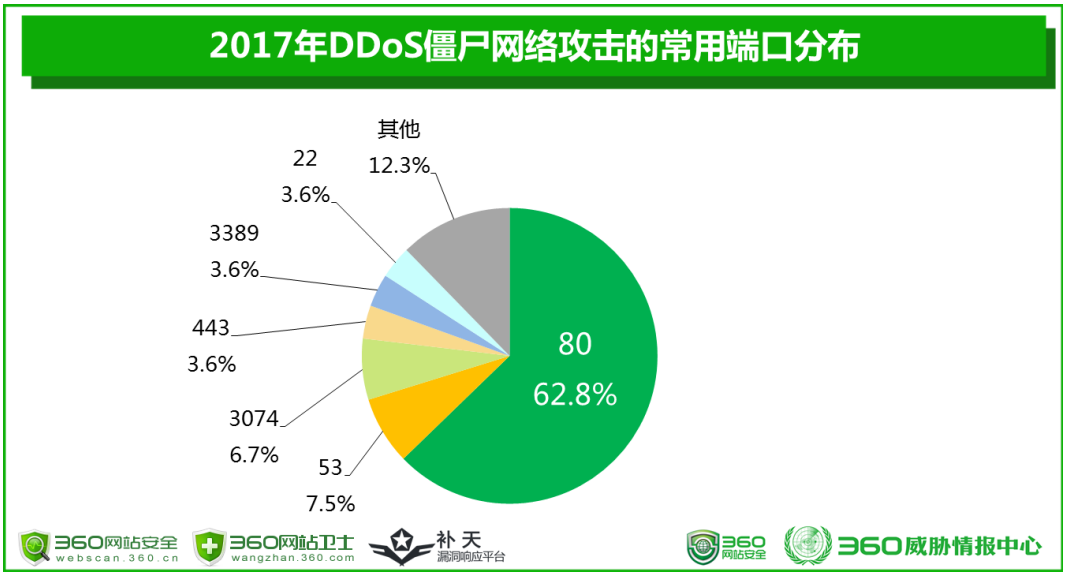
二、 DDoS 僵尸网络

僵尸网络 Botnet 是指采用一种或多种传播手段，将大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。攻击者通过各种途径传播僵尸程序感染互联网上的大量主机，而被感染的主机将通过一个控制信道接收攻击者的指令，组成一个僵尸网络。之所以用僵尸网络这个名字，是为了更形象地让人们认识到这类危害的特点：众多的计算机在不知不觉中如同中国古老传说中的僵尸群一样被人驱赶和指挥着，成为被人利用的一种工具。

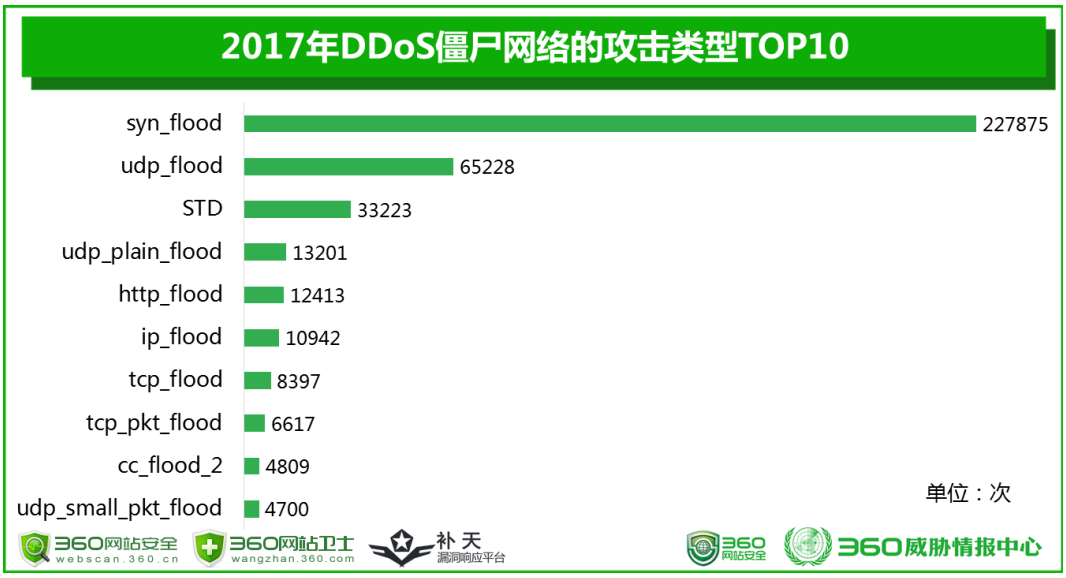
DDoS 攻击主要由受控的僵尸网络发动。统计显示，xor 家族是最为活跃的 DDoS 僵尸网络家族，占比为 38.1%；elknot 家族紧追其后占比为 29.5%；而 gafgyt 家族占比为 14.7% 位居第三。下面给出了 2017 年流行的僵尸网络的家族分布。



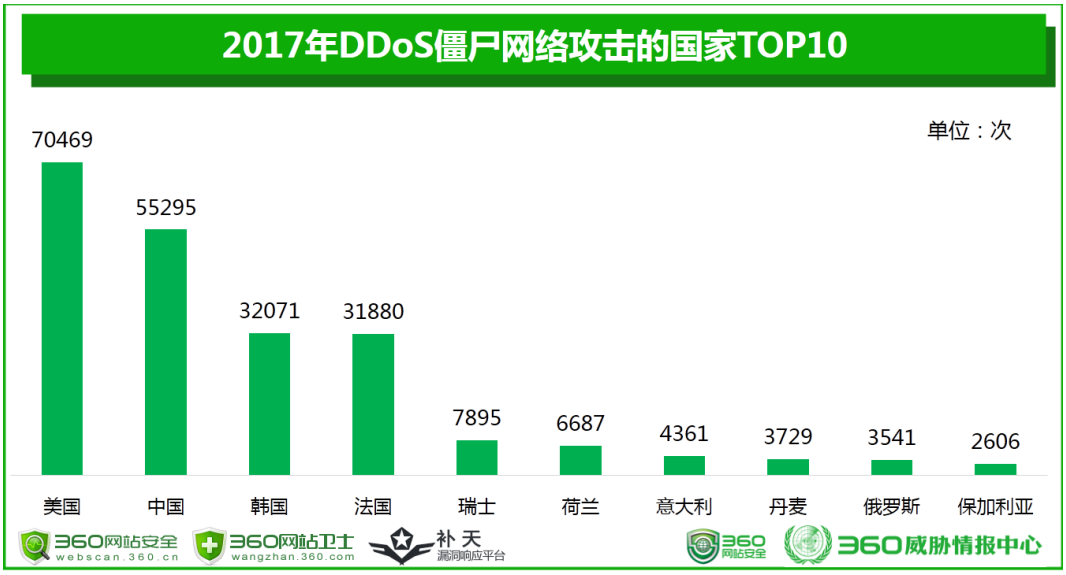
僵尸网络攻击的端口也很受大家的关注。80 端口仍是大多数僵尸网络攻击的主要目标，占比为 62.8%，其次是 53 端口为 7.5%，3074 端口为 6.7%。具体分布如下图所示。



下图给出了 2017 年十大僵尸网络攻击类型对比。从中可以看出，在 2017 年的 DDoS 僵尸网络攻击中，syn_flood 攻击次数达到 22.8 万次，其次是 udp_flood 6.5 万次、STD 为 3.3 万次等。



从 DDoS 僵尸网络攻击国家的地域分布来看，2017 年，DDoS 僵尸网络攻击的国家中，美国是重灾区（7.05 万次）。中国排名第二（5.53 万次），其次为韩国和法国，分别为 3.21 万次和 3.19 万次。具体分布情况如下图。



三、 DDoS 攻击造成的经济损失

360 威胁情报中心的监测数据显示，2017 年全年，国内共有 626.2 万个网站 IP 地址遭到了 1064.3 万次 DDoS 攻击。平均每天发生 DDoS 攻击 2.9 万次。可见，DDoS 攻击是互联网上一种常态攻击。

鉴于 DDoS 攻击的主要原因是恶意竞争和敲诈勒索，所以被攻击的网站，即便只是中小网站，通常也是具有相当程度的商业价值。因此，结合前述统计，我们可以大致通过下面方法来评估 DDoS 攻击给整个互联网造成的经济损失。

若我们按照平均每个网站的搭建成本为 1 万元（包括网站设计、制作、设备、运维、推广等基本投入），商业价值为 10 万元（由广告收入、用户缴费收入等评估的网站资本价值）的较低水平来估算，2017 年遭到攻击的网站数量为 626.2 万个，约 23%的网站被攻击后受到致命影响，面临停服风险，那么 DDoS 攻击全年给这些网站的经营者造成的经济损失至少为：

投入成本损失：1 万元×626.2 万×23%≈144.0 亿元

商业价值损失：10 万元×626.2 万×23%≈1440.2 亿元

四、 2017 年新型僵尸网络

（一）我国发现新型物联网僵尸网络 HTTP81

在去年 mirai 僵尸网络攻击造成美国东海岸大面积断网事件之后，2017 年 5 月，国内也出现了控制大量 IoT 设备的僵尸网络。该僵尸网络是由 360 威胁情报中心率先发布公告，披露了一个名为 http81 的新型 IoT 僵尸网络。

http81 僵尸网络的幕后操控者远程入侵了大量没有及时修复漏洞的网络摄像头设备，在这些摄像头中植入恶意代码，只要发出指令就可以随时向任何目标实施 DDoS 攻击。由于网络摄像头属于长期在线的设备，普遍拥有比较高的带宽，相比由电脑组成的僵尸网络具备更强的杀伤力。此外，http81 僵尸网络借鉴了 mirai 的端口嗅探手法和部分基础代码，但是

对比僵尸网络的关键特性，http81 在传播、C2 通信协议、攻击向量等方面与 mirai 完全不同，属于新的僵尸网络家族。

http81 僵尸网络在中国已经感染控制了超过 5 万台网络摄像头。如果按照每个活跃 IP 拥有 10Mbps 上行带宽测算，http81 僵尸网络可能拥有高达 500Gbps 的 DDoS 攻击能力，足以对国内互联网基础设施产生重大威胁。此安全事件告诫我们：国内的网络摄像头等设备大多缺乏安全更新维护，从事物联网行业的运维人员应该尽可能更新维护，及时清除恶意代码。

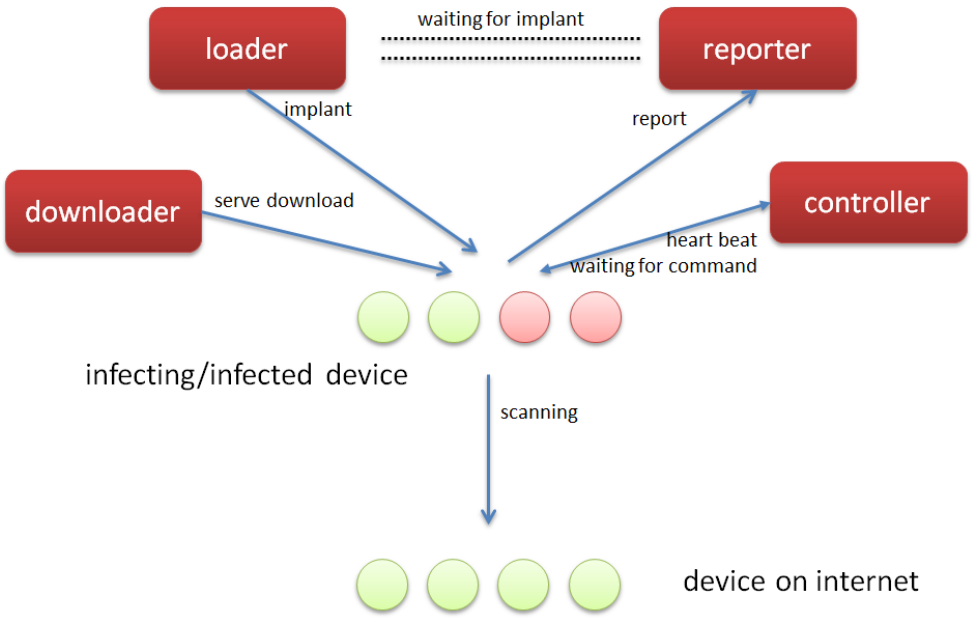
（二）IoT_reaper：快速扩张的新 IoT 僵尸网络

2017 年 9 月 13 日，360 威胁情报中心捕获到一个新的针对 IoT 设备的恶意样本。在随后的这个一个多月时间里，该 IoT 僵尸网络家族不断持续更新，开始在互联网上快速大规模的组建僵尸网络军团。

该僵尸网络脱胎于 mirai，但其在诸多方面比 mirai 更进一步提升攻击能力，特别是开始放弃弱口令猜测，完全转向利用 IoT 设备漏洞收割被控设备。我们将之命名为 IoT_reaper（IOT 收割者）。

IoT_reaper 规模较大且正在积极扩张，例如根据之前监测的数据（10 月 19 日），在我们观察到的多个 C2 中，其中一个 C2 上活跃 IP 地址去重后已经有 10k 个，此外还有更多的易感设备信息已经被提交到后台，由一个自动的 loader 持续植入恶意代码、扩大僵尸网络规模。

根据监测情况，IoT_reaper 最主要传播的恶意代码位于特定 URL 上，由于这个 URL 上的样本之间内聚关系比较强，我们称为 S 簇。S 簇的 C2 布局、感染机制等请参考下图。



上图中各主要环节功能介绍如下：

1） Loader：负责通过漏洞植入恶意代码

2） downloader：提供恶意代码下载

3） reporter：接收 bot 扫描到的易感染设备信息

4） controller：控制 bot、发送控制指令

在 reporter 和 loader 之间，我们猜测有一个队列，reporter 会将收集到的易感染设备信息推入队列，等待 loader 处理。

（三）Satori 及其后续变种 Satori.Coin.Robber

2017 年 12 月 5 日，360 威胁情报中心注意到 Satori（一个 mirai 变种）的新版本正在端口 37215 和 52869 上非常快速的传播，最快时感染速度达到 12 小时 26 万台，成为史上传播速度最快的僵尸网络。这个新变种有两个地方与以往 mirai 有显著不同：

1） bot 不再完全依赖以往的 loader/scanner 机制进行恶意代码的远程植入，而是自身有了扫描能力。这是一个类似蠕虫的传播行为，值得引起注意；

2） bot 中增加了两个新的漏洞利用，分别工作在端口 37215 和 52869 上。考虑到 bot 类似蠕虫的行为，我们建议安全工作者关注端口 37215 和 52869 上的扫描行为。

2018 年 1 月 8 日，360 威胁情报中心检测到 Satori 的后继变种正在端口 37215 和 52869 上重新建立整个僵尸网络。值得注意的是，新变种开始渗透互联网上现存其他 Claymore Miner 挖矿设备（一个流行的多种代币的挖矿程序，并提供了远程监控和管理的接口，而且互联网上较多设备都是基于 Claymore Miner 进行挖矿的），通过攻击其 3333 管理端口，替换钱包地址，并最终攫取受害挖矿设备的算力和对应的 ETH 代币。我们将这个变种命名为 Satori.Coin.Robber。

这是我们第一次见到僵尸网络通过利用肉鸡渗透并攫取其他现存挖矿设备的算力和代币。这给对抗恶意代码带来了一个新问题：即使安全社区后续接管了 Satori.Coin.Robber 的上联控制服务器，那些已经被篡改了钱包地址的挖矿设备，仍将持续为其贡献算力和 ETH 代币。

第六章　白帽子与安全人才

本章主要针对 2017 年全年在补天平台提交过漏洞的白帽子的获奖情况进行分析。并对白帽子的性别和年龄数据进行抽样调查，统计分析。

一、　白帽子获奖情况

2017 年全年，共有 4199 名白帽子向补天平台提交有效漏洞 2.27 万个，总计获得奖金 489 万元。

2017 年获补天平台奖金最多的三位白帽子分别是 lakes、depy 和 jkgh006。从报给补天平台并被收录的漏洞总数来看，挖洞最多的是 carry_your，共贡献 695 个漏洞，大约每天挖洞 2 个。而获得奖金最多的是 lakes，共获得 49.3 万元。

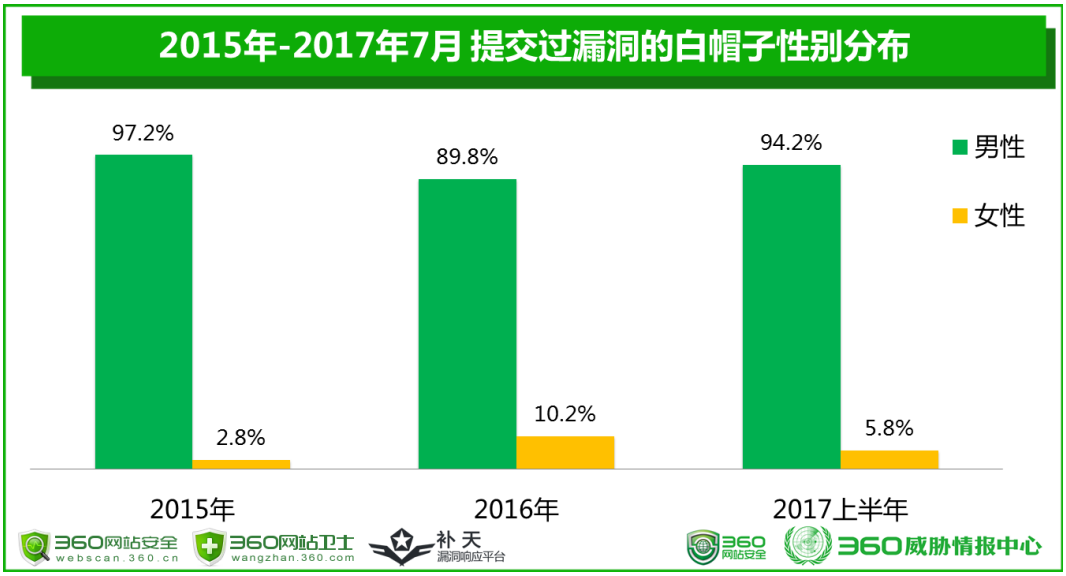
获奖金最多的白帽子 Top10 排名，以及挖洞情况具体见下表。

名次	网名	挖漏洞个数	获奖金额（万元）
冠军	lakes	454	49.3
亚军	depy	312	33.6
季军	jkgh006	365	24.8
第 4 名	carry_your	695	18.3
第 5 名	holoboy	89	17.5
第 6 名	xcold	186	16.5
第 7 名	dell	251	15.1
第 8 名	少司命	160	13.8
第 9 名	飞扬风	201	13.6
第 10 名	西沟里	69	8.0

表格 10　2017 年补天平台获奖金最多白帽子 Top10

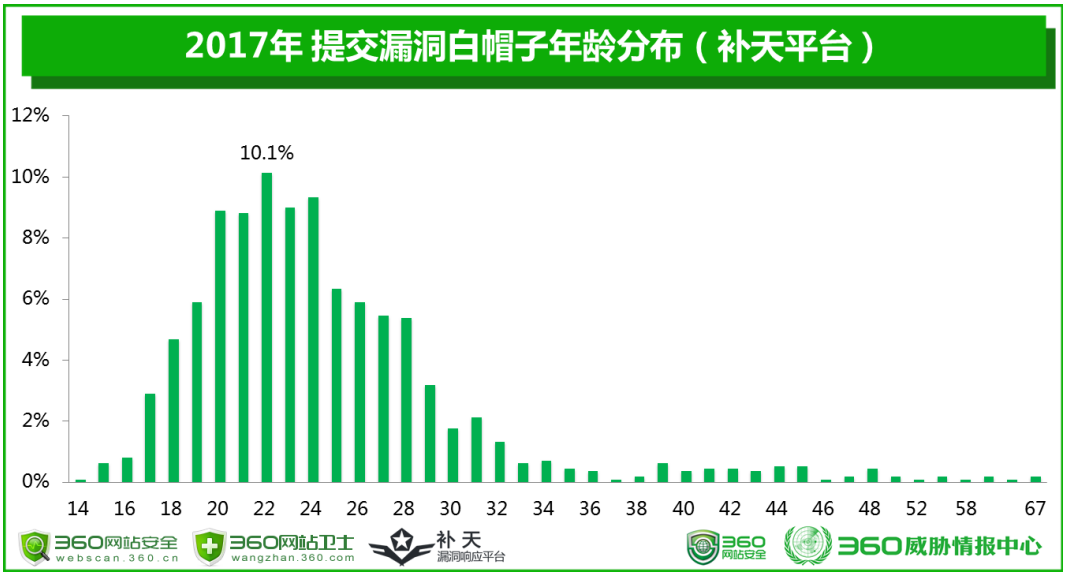
二、　白帽子性别分布

黑客的世界，一向被认为是男人的世界，而白帽子当中的女生更是凤毛麟角。2017 上半年，向补天平台提交漏洞的白帽子中，女性白帽子占比仅为 5.8%，男性白帽子占比为 94.2%。相比 2016 年 10.2%的女性白帽子在补天平台提交漏洞，有一定的下降趋势，可见女性白帽子依然是稀缺资源。



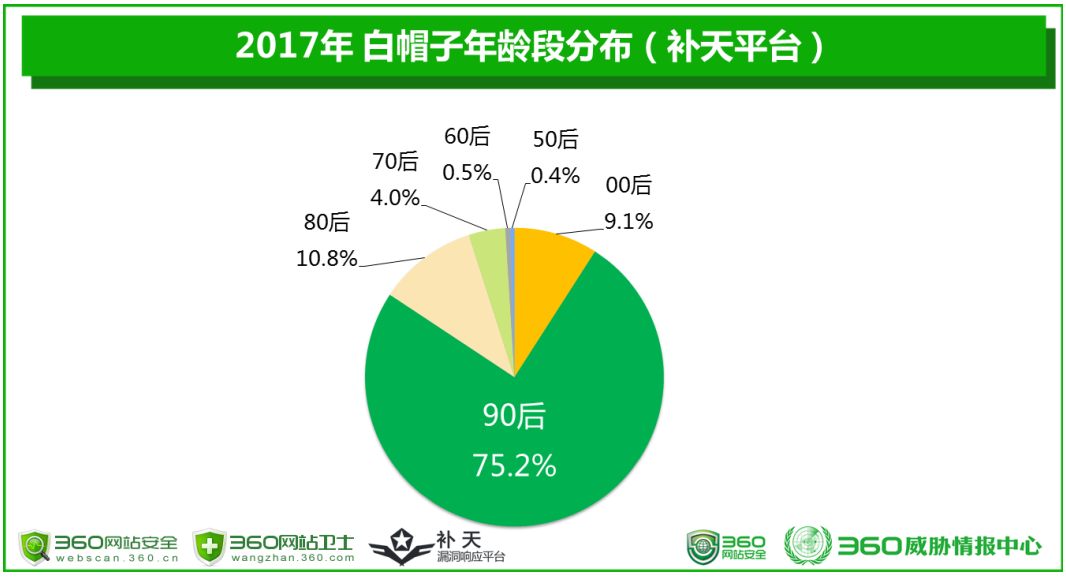
三、 白帽子年龄分析

根据白帽子的注册信息统计，在 2017 年上半年向补天平台提交漏洞的白帽子中，年龄最小的 14 岁，年龄最大的 67 岁。其中，18 岁-28 岁之间的白帽子数量最多，约占总数的 79.9%。下图给出了向补天平台提交漏洞白帽子的年龄分布。



而从年龄段来看，延续了 2016 年的趋势，年轻的“90 后”目前仍然是白帽子的绝对主力，占白帽子总量的 75.2%，“80 后”次之，占 10.8%，00 后正在崛起，占比为 9.1%。

值得注意的是，相比 2016 年“00 后”白帽子仅占 2.6%，今年约有 9.1%的白帽子是 17 岁及以下的青少年，比例和数量都大为提高。这与政府机构和高校的的助推密不可分，网信办在 2017 年发布了《关于加强网络安全学科建设和人才培养的意见》，上百所高校也设立了网络安全相关专业带来实际人才的输出。


2017年 白帽子年龄段分布（补天平台）
60后
0.5%
50后
0.4%
70后
4.0%
00后
9.1%
80后
10.8%
90后
75.2%
360网站安全
webscan.360.cn
360网站卫士
wangzhan.360.com
补天
漏洞响应平台
360威胁情报中心

第七章　网站安全的典型案例

一、　挖矿木马攻击与响应典型案例

挖矿木马是 2017 年非常流行的一种针对网络服务器进行攻击的木马程序，此类木马程序通过自动化的批量攻击感染存在漏洞的网络服务器，并控制服务器的系统资源，用于计算和挖掘特定的虚拟货币。由于挖矿木马长期占用 CPU 率达 100%，因此，服务器感染挖矿木马后最明显的现象，就是服务器响应非常缓慢，出现各种运行异常。如果挖矿木马攻击的整个云服务平台，则平台上所有网站和服务系统都会受到严重影响。

（一）　某社会管理服务机构被植入挖矿木马

场景回顾

2017 年 3 月，某社会管理服务机构的网站管理员发现其网站服务器存在恶意脚本，清除该恶意脚本后不久，平台又会重新被感染，同时，系统还存在其他一些异常情况。360 安服团队收到该机构求助后，第一时间到达该平台中心机房进行排查。

疫情分析

现场排查显示，该平台服务器感染的木马程序是 2017 年非常流行的挖矿木马。而之所以删除木马程序后又会被反复感染，主要原因是攻击者在服务器系统中写入了一个定期执行的计划任务，每隔一段时间，就会自动检测服务器上是否运行了挖矿木马，如果没有，则自动联网再次下载一个挖矿木马程序，并释放到系统中。所以，要彻底清除木马，首先必须删除该计划任务。

进一步调查显示，该服务器之所以能被攻击者写入恶意计划任务，主要是因为该服务器存在明显的安全配置漏洞。调查显示，该平台使用了 Redis 数据库，并且采用缺省的配置模式，即并未开启密码验证功能，且监听的端口绑定了 0.0.0.0 地址，表示可接受任意的 IP 访问，且权限为 root 启动。因此攻击者利用这一 Redis 配置漏洞，匿名登陆了 Redis 数据库，并写入 SSH 公钥，进而获得了系统的 root 权限，并在系统中增加了这样一条恶意计划任务。

处置方案

安服人员对 Redis 添加密码验证功能，更改绑定地址，对运行用户进行降权，建议不采用 root 权限进行启动；删除攻击者写入的计划任务及木马程序；加强攻击检测以及拦截功能；建议采用全流量监控设备从而有效发现木马攻击以及对攻击行为进行溯源。

（二）　某大型云平台被植入挖矿程序

场景回顾

2017 年 11 月，某大型云平台运维人员发现其云平台约 200 台租户虚拟机的 CPU 占用异常，同时租户的主机也受到了影响。平台运维人员分析发现服务器被植入挖矿程序，删除后仍会自动下载运行。

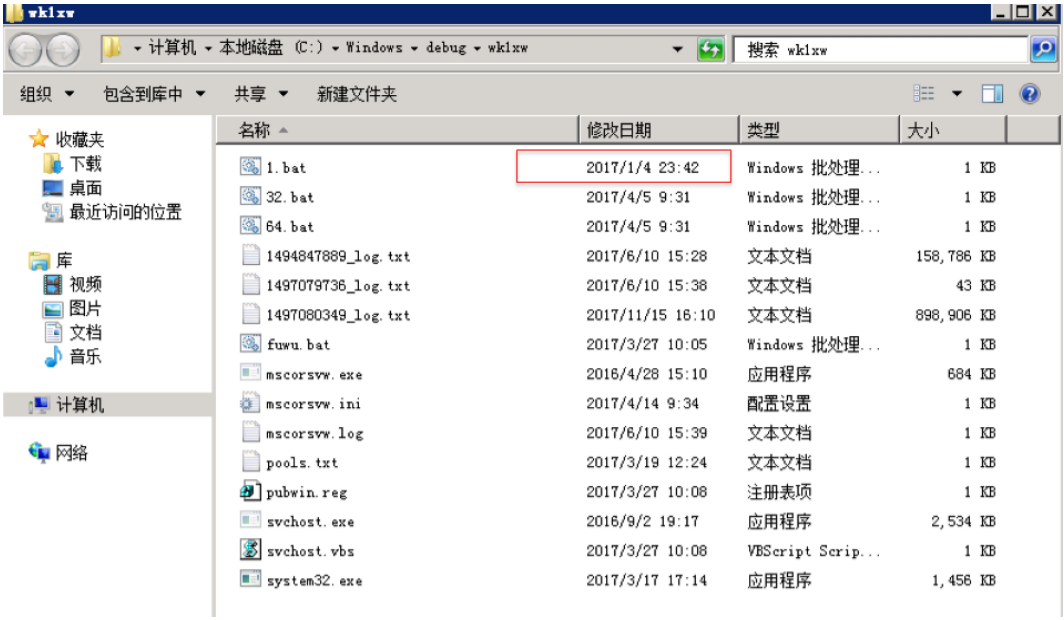
疫情分析

根据 360 安服人员现场排查发现，该云平台租户的虚拟机 CPU 占用异常，确实是由于被植入了挖矿木马程序。挖矿程序删除后仍会自动下载运行是由于攻击者在植入挖矿程序的同时，在计划任务中写入了一段定时启动挖矿程序的脚本。每隔规定时间（5 分钟）该程序就会自动运行扫描虚拟机是否在执行挖矿程序，若执行则继续，若未执行则下载新的挖矿任务并启动。

该云平台向 360 安服人员提供了五台中招测试机的登录权限，根据测试机进行查杀分析，由于用户进行交付时普遍存在默认口令，且为弱口令，租户与租户之间的虚拟机也没有阻断策略。这使得攻击者可以通过弱口令爆破和应用配置漏洞，自动化扫描。

从过程来看，如下图所示，通过对历史数据的复查，攻击者最早在 2017 年 1 月就入侵了云平台，挖矿程序很可能在该云平台存在长达十个月之久。

通过对挖矿木马样本的分析发现，由于挖矿木马可大量扫描传播的特性，攻击者为了加大利益，会肆意大幅对虚拟机 CPU 占用，即使被发现或删除，也可以在过段时间后重新执行新的挖矿指令。进行自动扫描和传播。



处置方案

1） 删除木马相关所有脚本程序；

2） 并针对漏洞建议平台运维人员立即修改操作系统用户密码，同时密码应严格使用复杂口令，避免密码的重用情况，避免规律性，定期进行修改；

3） 加强访问控制策略，开启 SSH 证书登录；定期对系统日志进行备份，避免攻击者恶意删除相关日志文件，阻断溯源能力；

4） 同时加强日常安全巡查，防范于未然。

（三） 某事业单位管理员用户被删除

场景回顾

某事业单位（副部级）运维人员于 2017 年 9 月发现公网邮件服务器 root 用户被删除，导致管理员无法正常登录邮件服务器，同时相关配置存在异常。该运维人员在发现异常之后，对服务器进行修复，添加正常 root 用户，并更新其他系统用户密码，随后向 360 安服团队发出求助。

疫情分析

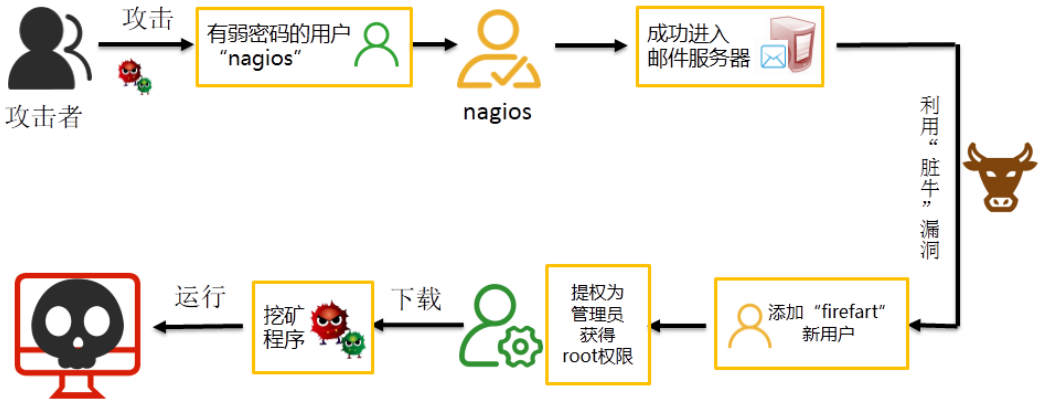
安服人员对对外开放的邮件服务进行分析，未发现可疑进程和连接，但发现一个名叫“nagios”的普通低权限用户的命令历史中存在可疑操作。此类用户是为了性能监控需求，用于监控系统性能资源而存在。针对这个用户，安服人员进行了调查。

该用户从位于越南的远程服务器下载了可疑文件并解压运行。根据文件和执行命令初步判断为 miner 挖矿程序。攻击者利用 nagios 的弱口令，通过 SSH 登录该用户，由于用户“nagios”存在多个 IP 登录记录，对这些 IP 地址监控，其中一个 IP 通过一个非正常业务系统账号“firefart”进行登录，进一步分析，找到攻击者利用“脏牛”漏洞（一个 Linux 系统中从 2007 年就被发布的已经存在的漏洞）运行提权工具，添加了 firefart 账号并覆盖了正常的 root 用户记录，使原 root 用户无法正常登录。然后利用管理员权限，下载了挖矿程序并建立了定时计划任务，定期运行挖矿程序。

对用户 nagios 的命令进行分析，从过程中来看，攻击者已在该事业单位内网潜伏长达十个月，从攻击者进入服务器渠道来看，都是使用 SSH 服务从公网直接连接登录。在攻陷主机后，建立新用户，提升用户权限，后续使用高权限帐号进行登录。并在进入服务器后，下载相关挖矿程序（如下图）运行于后台，使用计划任务定期激活程序。

该事件充分暴露了普通用户即便是系统的低权限用户也可能对系统造成重大威胁

过程图解



处置方案

1） 立刻修复“脏牛”漏洞、修改相关操作系统用户密码，同时密码应严格使用复杂口令，并能定期进行修改；

2） 禁止公网直接访问 SSH 服务；开启 SSH 证书登录，避免直接使用密码进行登录，同时禁止 root 用户直接远程登录；

3） 对于需要 root 权限的操作，定期对系统日志进行备份，避免攻击者恶意删除相关日志文件，

4） 同时加强日常安全巡查，防范于未然等操作。后续需要结合业务情况，移除上述可疑非业务程序。禁止远程对服务管理系统的访问。

（四） 挖矿木马小结

总结起来看，网站之所以会被挖挖矿木马攻击，主要是由于两方面的原因：首先是因为没有做好隔离保护措施，将内部服务或管理端口暴露在了互联网上，为攻击者留下了“靶子”；第二是因为网站存在明显的安全漏洞，包括弱口令、配置漏洞以及其他一些安全漏洞等。

需要特别说明的是，挖矿木马追求的是能够控制资源的总体规模，而并不太在意个别服务器的得失。因此，挖矿木马的攻击者通常不会对特定服务器发起定向攻击，而是利用系统漏洞进行批量攻击。所以说，本小节前面所介绍的三个典型案例中，相关系统漏洞的存在都不是偶然现象，而是普遍存在的安全问题。

二、 某大型机构门户网站的服务器被恶意篡改

场景回顾

2016 年 10 月某大型机构技术人员发现，该机构门户网站的发布服务器上，页面内容存在被恶意篡改行为，即有恶意程序试图在该服务器上非法创建文件。360 安服团队收到求助，应急响应小组进行排查。

（网站发布服务器是指管理网站页面内容的服务器，用于控制和发布网站内容。即网民访问某个网站看到的文字、图片、音视频文件及程序，都是由发布服务器来呈现。）

疫情分析

经排查，安服人员追踪查找到了试图篡改网站首页内容的木马，但该机构的门户网站发布服务器不与互联网连接。攻击者借助内网的一台服务器，将木马复制到网站发布服务器。但这台内网服务器也不与互联网连接，而仅仅是一个中间跳板，真正让黑客进入内网的主机是一台 MAS 系统（Media Asset System）服务器。

MAS 为某商业公司推出的应用软件，是一个方便用户管理多媒体素材资源的服务系统，例如用户可以通过它上传、编辑和分发图片、音视频等文件，管理网站页面内容素材。

攻击者首先在外网环境下，通过弱口令以管理员账号身份登入了 MAS 主机，以添加皮肤的名义，上传了 zip 类型的木马文件包，其中包含若干恶意的脚本木马，不断对内网资源进行访问，熟悉和摸清攻击路线。

之后借助 MAS 主机的内网权限，并使用特定文件传输服务，成功将木马复制到同一 IP 段内的某台内网服务器上。然后再次利用上述文件传输服务将木马上传到真正的目标——网站发布服务器。最终木马在试图创建非法文件及篡改文件时，引发告警。

处置方案

根据本次应急响应服务，360 安服团队成功发现网站所存在的安全漏洞并还原复现了攻击场景，给出了修复建议。第一，MAS 主机不应暴露在外网环境，禁止外部 IP 登录访问。第二，修改 MAS 管理员账号密码，杜绝弱口令。第三，加强控制内部服务器相互访问控制策略，采用白名单机制只允许特定 IP 访问特定的服务器端口。

后续建议加强对网站系统的安全监控，并定期举行信息安全意识培训，这样才能与时俱进的做好信息安全防范工作，建立更完善的信息安全防护体系结构。

三、 某知名软件公司的服务器遭恶意部署

场景回顾

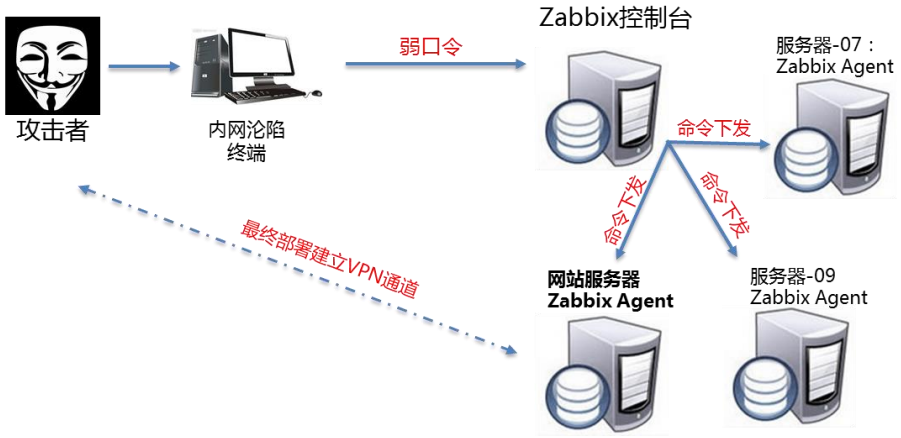
2017 年 4 月某知名软件系统公司运维人员发现，内部网络发生非法外联现象，不明 IP 地址的访问者可能已成功进入企业内部，在 360 安全服务团队协助下，应急响应技术人员对

其网站服务器及内网进行了检测排查。

疫情分析

经过检测，该公司内部较早之前已经存在一台被入侵 PC，攻击者通过它的内网 IP，利用弱口令漏洞，间接获得了访问内部 zabbix 控制台的权限，从而在网站服务器上恶意部署 VPN 通道，导致攻击者成功通过 VPN 方式直接拨号进入到服务器内网，并可能已造成内网敏感信息数据泄露。

注：zabbix 控制台是一种监控内网服务器运行状态的分布式监控程序，一般会在被监控服务器主机上安装 zabbix Agent，对内部服务器统一监管。



在网站服务器上安装 VPN 程序，需要相对较高的权限。安服人员进一步排查，该公司内网安装了 zabbix 控制台，它拥有对所有安装有 zabbix Agent 的服务器下发任意系统命令的权限。

通过分析 zabbix Agent 日志发现，攻击者至少从 zabbix 控制台推送三个关键命令到各个 Agent 服务器，为其进行一系列的恶意操作做准备。第一，执行特定系统命令，获得远程交互权限；第二，下载某个.Bat 文件，把恶意代码加载到内存；第三，下载 VPN 文件并部署在服务器上，为后续攻击建立通道。

处置方案

安服人员根据网站日志还原网站攻击事件，找到了应用的漏洞与攻击源地址。并针对漏洞提出修补建议。首先，做好终端防护，需对内网 PC 做全面的安全检查，尽早消灭终端安全隐患。其次，对内部服务器系统进行弱密码检查，及时修改弱口令，避免被恶意利用。

四、 某事业单位门户网站疑似被 CC 攻击

场景回顾

2017 年 11 月，某事业单位门户网站发现在 2 天时间里，针对某个查询页面的总请求访问量超过 900 万次，最终服务器资源压力过高，致使业务异常，整个网站页面无法正常访问。技术人员怀疑遭到 CC 攻击。360 安服团队接到客户应急请求，应急响应小组第一时间赶赴现场，进行排查。

注：CC 攻击是一种针对特定应用程序的持续、高频次恶意访问，目的是消耗 Web 服务

器资源，破坏业务应用的正常运行。广义上，CC 攻击属于 DDoS 流量攻击的一种，和 DDoS 的手段相比，CC 攻击更具针对性、手段更精细化，攻击效率也更高。

疫情分析

通过初步分析，在服务器上的并未发现异常进程以及恶意木马程序，也排除了 CC 攻击。随后，通过该机构部署的 360 网站安全监测设备，以及结合客户端访问行为数据，技术人员认为前述 900 万次，属于“合法”的页面请求。

但进一步分析发现，这些“合法”的页面访问来自若干个特定的 IP 地址，并在短时期内发出大量的访问请求，而且这些访问请求主要查询网站内容中特定的公告消息和特定的字段数据。因此，可以判断网站遭到了恶意的网络爬虫行为。（网络爬虫，又称网络蜘蛛，是指一种自动抓取网页内容信息的网络程序，也是互联网搜索引擎广泛采用的技术之一。）

技术人员还发现，之所以机器爬虫访问行为没有被阻止，是因为该网站的查询验证机制存在漏洞，使得攻击者只要通过一次人机验证，就可以持续发起查询请求却不被阻止。而且该网站在每次接收查询请求时，也没有对发起者 IP 地址进行限制，从而让机器爬虫程序有机可乘。

处置方案

查明原因后，安服人员首先协助关停相关查询功能业务，使网站访问恢复正常，建议网站运维人员在相关代码更改完毕后，再完全恢复查询业务。

其次，针对目前的网络爬虫的遍历爬取数据行为没有根除办法，但可以通过加强人机验证措施进行抑制。例如在查询页面的代码里增加人机验证程序，并且每次验证之后刷新验证码，以及限制单个 IP 访问次数、频率，抬高网络爬虫程序的攻击门槛。

五、 某监管机构被上传添加注册人员命令

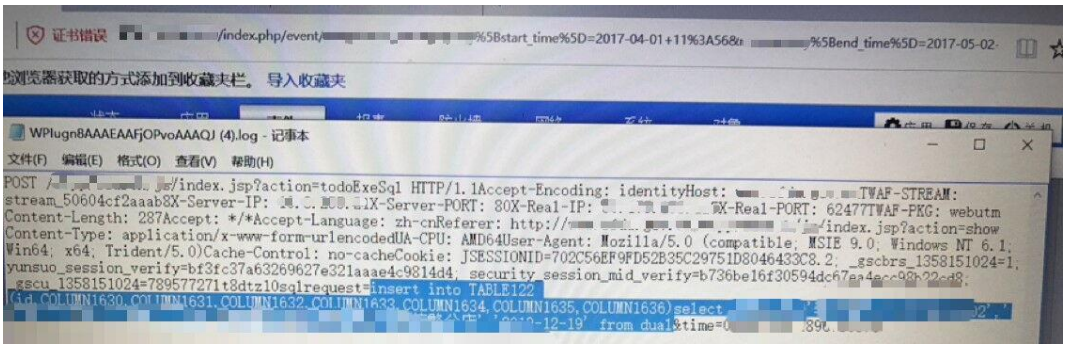
场景回顾

2017 年 5 月，某监管机构防火墙收到告警，拦截到一条含有敏感信息的 SQL 注入信息指令，疑似对系统内容进行篡改。360 安全服务团队收到求助，应急响应小组进行排查。

疫情分析

安服人员到达现场后发现，该机构为某地政府机构网站，可对外提供某特定职位的注册信息查询服务。

通过对日志以及样本进行分析，初步推断：该监管机构被植入了脚本木马，拥有执行系统命令、文件操作、数据库操作等功能，木马可以把信息篡改到网站上，但攻击者发送的语句被防火墙拦截（如下图所示）。经调查，该语句实际是发送给一个已经长期寄存在该网站上的木马。如果该语句未被拦截。木马收到该指令后会将编辑好的虚假的从业人员信息写入网站服务器，可在外部查到该新增的虚假信息。故判定，此次事件为利用某黑产产品办理假证的团伙所为。提供为社会人员制办假证的服务。进一步排查发现，相关木马程序已经被植入长达四个月之久。同时相对于木马程序，该网站上可能存在弱口令、SQL 注入漏洞，以及 Struts2 远程命令执行漏洞等问题。攻击者疑似利用上述相关漏洞，向网站植入了恶意木马。



用户表后台用户账号密码可能已经泄露。因此推测 WEBSHELL 此前已被成功上传，且网站历史上遭遇多个黑客多次入侵并长期控制。

处置方案

对后续此类事件的安全防护方案和漏洞修补建议：

1） 立刻修改弱口令；

2） 加强攻击监控；延长日志轮询保存时间，同时日志备份不应该备份在本地服务器，建议把备份日志上传到远程服务器；

3） 对应用系统进行渗透性测试以及源代码安全审计，挖掘目前所存在的应用程序漏洞；加强访问控制权限；

4） 涉及的服务器进行重装并修改密码，涉及的后台用户密码全部修改；

5） 严格限制后台发布系统的访问策略等。

六、 某国家单位服务器存在后门

场景回顾

2017 年 4 月，某国家单位接到安全通报，发现两条境外恶意 IP 访问了该机构的内部网络以及其 2 台服务器存在 WebShell 后门。要求该机构进行排查。360 安服团队收到求助，应急响应小组进行排查。Webshell 用于控制网站。同时登录访问 Webshell 需要经过密码验证。

疫情分析

通过分析原始流量记录，发现被通告的两个恶意 IP 确实同黑客组织有关。两条 IP 早在四天前便通过弱口令直接登陆了 weblogic 管理后台，并在至少两台服务器上放置了 webshell 后门，获得了该网站的管理员权限，以管理员身份登录网站，方便进行恶意操作。安全人员分析，该团伙疑似已经窃取了网站内部大量机密信息。但攻击者并未进行拖数据、内网渗透等高危操作，无法溯源。进一步调查显示，攻击者之所以能在服务器放置 webshell 后门是由于其 weblogic 管理员账号使用了弱密码。（WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的应用管理平台，具有单独的管理后台界面，管理员输入密码后可登陆管理后台控制网站运行）

随后，攻击者利用上传的 webshell 后门操作服务器注册表，试图开启服务器的远程桌面服务。通过对攻击者 IP 进行分析，发现本次攻击涉及的 IP 基本上是通过批量扫描弱口令以及常见的 web 漏洞来进行批量攻击，并非针对性攻击。

处置方案

鉴于攻击者曾将获得过管理员权限，很可能对服务器做出了篡改可能存在尚未发现的安全隐患，安服人员提出建议：

1） 及时更新 Weblogic 到最新版；

2） 更改 weblogic 管理端口令要求密码强度为 8 位以上，包含数字、字母、特殊字符；

3） 为每隔服务器设置新的 weblogic 口令，不能为弱口令。

七、 某新闻门户网站被攻击，下载恶意木马

场景回顾

2018 年 1 月，某新闻门户网站收到监管部门通报，称其遭受到 weblogic 最新反序列漏洞攻击。360 安服团队接到客户应急响应请求。

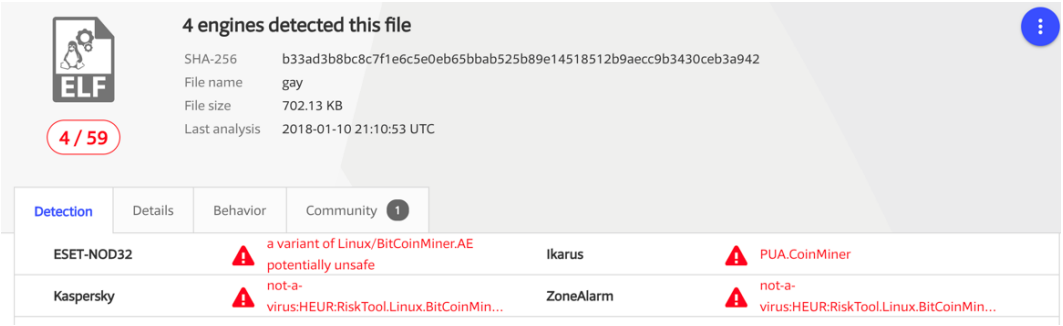
疫情分析

此次事件是 2017 年末自 CVE-2017-10271 漏洞发布后，360 安服团队在国内接到的首起基于该漏洞的 weblogic 反序列漏洞攻击。2017 年末，国外已有黑产团体利用 weblogic 反序列化漏洞对全球服务器发起大规模攻击的事件。该漏洞的利用方法较为简单，攻击者只需要发送精心构造的 HTTP 请求，就可以拿到目标服务器的权限，潜在危害巨大。可能出现攻击事件数量激增，大量新主机被攻陷的情况。

安服人员对 6 台服务器进行了排查，发现该网站遭受了 weblogic 反序列攻击，下载了挖矿木马程序。目前暂未对服务器造成影响。

由于服务器并未及时更新 Weblogic 补丁，导致网站遭受到远程代码执行漏洞攻击，攻击者通过该漏洞执行远程下载命令，主要为下载挖矿木马到本地运行，但由于远程病毒文件已经不存在，导致无法正常下载，因此并未造成实际的影响。

后续 360 应急响应人员通过访问黑客服务器地址，成功下载了该恶意木马，通过在线杀毒平台对该恶意木马进行查杀，初步确定为虚拟货币挖矿木马。



处置方案

安服人员到达后排查服务器找出并关闭异常进程，更新 Weblogic 补丁并禁止外联后，重新部署恢复应用系统业务。溯源攻击路线并制定了缓解措施以及后续防护方案：

1） 相关的用户杜绝使用弱口令；

2） 禁止服务器主动发起外部连接请求，对主动连接 IP 范围进行限制；

3） 加强安全溯源能力；对相关使用口令进行登录的服务，加入防爆破策略；

4） 定期进行全面扫描，加强入侵防御能力等。

八、 某关键基础设施公共服务器被加密

病毒简介

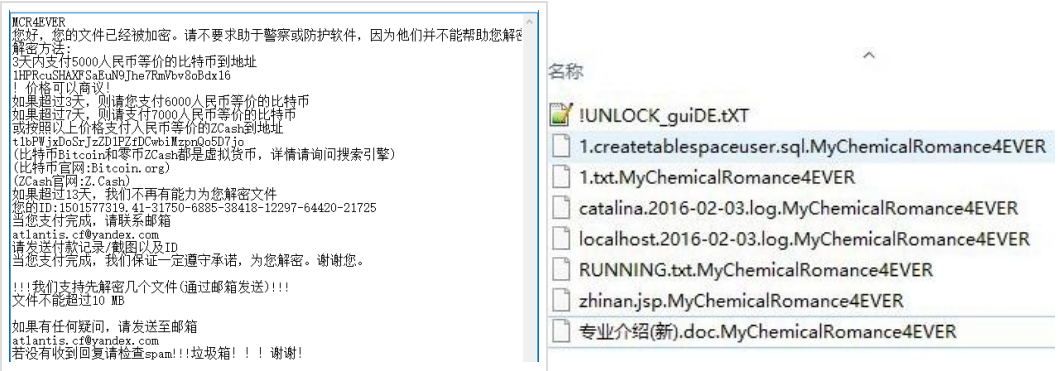
勒索病毒是个舶来品，无论是英文版的勒索信息，还是比特币这一赎金交付方式，都透漏着浓浓的国际化味道。而最近，360 威胁情报中心却发现一款国产化的勒索病毒。该病毒为国内黑客制造，并第一次以乐队名字 MCR 命名，即称该病毒为 MCR 勒索病毒。该病毒在 2017 年 7 月底首次出现，采用 python 语言编写。

该病毒加密文件后，文件扩展名会变为“.MyChemicalRomance4EVER”。而扩展名中的“My Chemical Romance”，其实是源自一支美国新泽西州的同名朋克乐队。该乐队成立于 2002 年，十一年后的 2013 年宣告解散。朋克这种充满了叛逆与不羁的音乐风格向来深受年轻人的喜爱。

该勒索软件的特点是：在加密的文件类型列表中，除了大量的文档类型外，还包括有比特币钱包文件和一些较重要的数据库文件。而另一个更大的特点则是，该木马不同于以往的勒索软件使用不对称加密算法，而是采用了 AES 对称加密算法，并且用于加/解密的密钥则是硬编码在脚本中的：“MyChemicalRomance4EVER_tkfy_lMCR”中。因为使用对称加密算法，并且密钥可以从脚本中获得。所以在不支付赎金的情况，被加密的文件资料也可以比较容易的被解密恢复。

场景回顾

2017 年 8 月 5 日，某公共服务系统单位的工作人员在对服务器进行操作时，发现服务器上的 Oracle 数据库后缀名都变为了“.MyChemicalRomance4EVER”，所有文件都无法打开。该 IT 人员怀疑自己的服务器被勒索软件进行了加密，因此向 360 安全监测与响应中心进行求助。



疫情分析

安全人员现场勘测发现，该公共服务系统感染的是 MCR 勒索病毒。该病毒名字起的很“朋克”，但传播方式却颇为老套，即伪装成一些对广大网民比较有吸引力的软件对外发布，诱导受害者下载并执行。比如我们现场截获并拿来分析的这个样本，就自称是一款叫做“VortexVPN”的 VPN 软件。除此之外，还有类似于 PornDownload、ChaosSet、BitSearch 等，基本都是广大网友都懂得的各种工具软件。

而与众不同的是，这款病毒竟然是用 Python 语言编写了木马脚本，然后再打包成一个.exe 的可执行程序。首先，木马会判断自身进程名是否为 systern.exe。如果不是，则将自身复制为 C:\Users\Public\systern.exe 并执行。之后，木马释放 s.bat 批处理脚本，关闭各种数据库和 Web 服务及进程。接下来，就是遍历系统中所有文件并加密且留下勒索信息了。当然，为了避开敏感的系统文件，代码有意避开了“C:\Documents and Settings”和“C:\Windows”两个目录。最终木马会调用系统的 wevtutil 命令，对系统日志中的“系统”、“安全”和“应用程序”三部分日志内容进行清理，并删除自身，以求不留痕迹。

处置方案

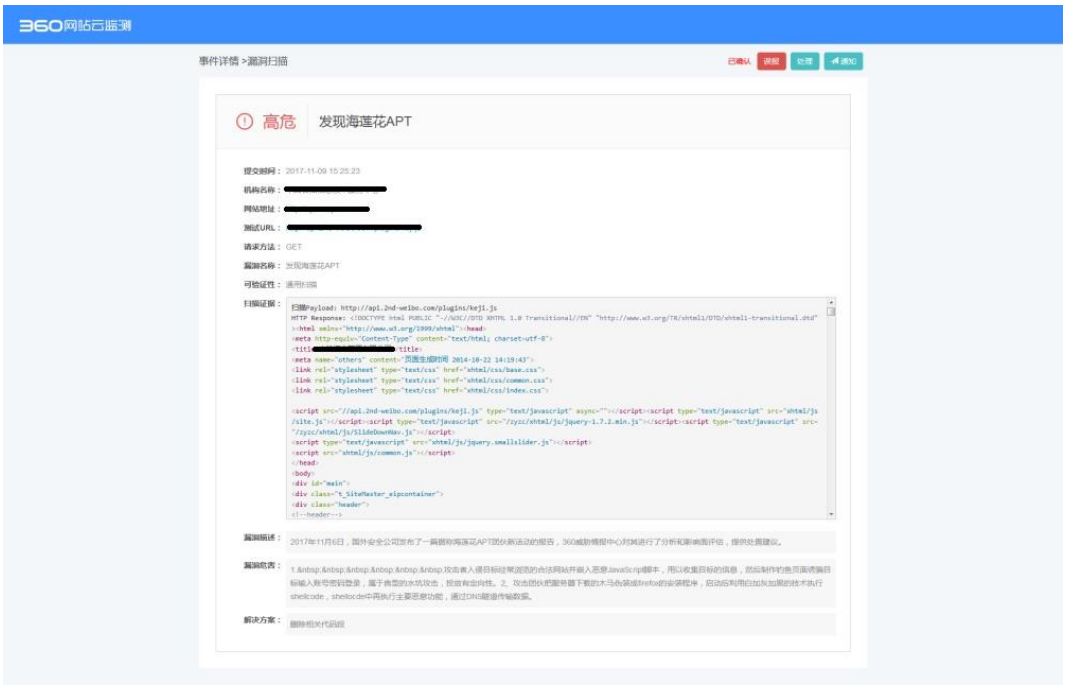
安服人员发现该勒索软件程序写的有漏洞，可直接利用 360 解密工具恢复数据。因此，在未向黑客支付一分钱的前提下，360 帮助该单位成功的恢复了所有被加密的文件。建议该企业员工：不要从不明来源下载程序；安装杀毒软件并开启监控；更不要相信所谓外挂、XX 工具、XX 下载器一类的程序宣称的杀软误报论。

九、 某大型能源企业网站遭遇 APT 入侵

海莲花（OceanLotus）是首个由国内安全机构（360 威胁情报中心，2015 年 5 月）披露的 APT 组织。2012 年 4 月起至今，该境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。该组织主要通过鱼叉攻击和水坑攻击等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播专用木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。

场景回顾

2017 年 11 月，云监测发现，某大型能源企业被海莲花 APT 组织攻陷。我们认为网站是整个组织暴露在外的非常关键的入口，这是 360 云监测第一次发现 APT 与网站入侵直接相关的国内案例。



疫情分析

该大型能源企业被海莲花 APT 组织攻陷，云监测发现其采取的是“水坑攻击”方式，并且目前网站首页上存在海莲花 APT 水坑域名相关的 js。攻击者团伙入侵网站后，不仅破坏网站的安全性，还会收集所访问用户的系统信息。如果确认感兴趣的目标，则会执行进一步的钓鱼攻击获取敏感账号信息或尝试植入恶意程序进行秘密控制。

处置方案

1） 建议该企业及时清理被篡改的相关页面。

2） 该企业与 360 合作，展开全面调查。

第八章　网站安全威胁前沿趋势

一、　不当信息公开导致大量政府网站信息泄露

2017 年，国内发生了一系列的政府机构泄露信息事件。让人惊讶的是，这些事件大多是由于政府网站在政务公开环节，不必要的公开了相关人员完整的、详细的身份信息而造成的，被不当公开的信息包括完整的身份证号码，联系电话等信息。

比如：2017年10月10日，江西省宜春市财政局在宜春市政府信息公开网（xxgk.ycf.gov.cn）发布的《关于公布 2017 年会计专业技术初级资格无纸化考试宜春考区合格人员名单的通知》中，公布了相关人员详细的个人身份证号码的人员名单，910 名合格考生的证书编号、准考证号、身份证号码、姓名等信息予以公开。2017 年 10 月 31 日，江西省景德镇市政府信息公开网（xxgk.jdz.gov.cn）曾发布了《第二批大学生一次性创业补贴公示》。其中，可供公众下载的文件公布了学生姓名、完整身份证号以及联系电话等。此外，景德镇市人社局官网也可获取上述公示信息。

这些信息泄露事件的发生，主要是由于有关部门的相关负责人缺乏最基本的网络安全常识，缺乏最基本的公民信息保护意识而引发的“完全不必要的”网络安全事件，而与任何网络攻击技术或网站安全漏洞无关。这也不得不让我们对很多中小城市的网络安全建设水平感到担忧。我们有理由认为，类似的事情在全国各地可能非常的普遍，媒体报道出来的相关情况可能也只是冰山一角。

同时，关于政务公开、重大事件公示等必要的行政措施，与公民个人信息保护之间可能存在的矛盾问题也值得我们进行更深入的思考。表面上看，我们似乎总是可以找到一个平衡点来平衡公开公平与隐私保护之间的关系。但实际上，此类问题涉及法律法规、技术手段、公众认知、公职人员办事能力等多方面的复杂因素，很难在短时间内得到全面有效的解决。

二、　勒索软件大量入侵服务器

2017 年，勒索软件的攻击进一步聚焦在高利润目标上，其中包括高净值个人、连接设备和企业服务器。特别是针对中小企业网络服务器的攻击急剧增长，已经成为 2017 年勒索软件攻击的一大鲜明特征。据不完全统计，2017 年，约 15%的勒索软件攻击是针对中小企业服务器发起的定向攻击，尤以 Crysis、xtbl、wallet、arena、Cobra 等家族为代表。

客观的说，中小企业往往安全架构单一，相对容易被攻破。同时，勒索软件以企业服务器为攻击目标，往往也更容易获得高额赎金。例如：针对 Linux 服务器的勒索软件 Rrebus，虽然名气不大，却轻松从韩国 Web 托管公司 Nayana 收取了 100 万美元赎金，是震惊全球的永恒之蓝全部收入的 7 倍之多。Nayana 之所以屈服，是因为公司超 150 台服务器受到攻击，上面托管着 3400 多家中小企业客户的站点。这款勒索病毒的覆盖面有限，韩国几乎是唯一的重灾区。

三、　挖矿木马的疯狂敛财暗流

在 2017 年这个安全事件频发的年份，除了受到全世界关注的“WannaCry”勒索病毒的

出现之外，一大波挖矿木马也悄然崛起。不同于勒索病毒的明目张胆，挖矿木马隐蔽在几乎所有安全性脆弱的角落中，悄悄消耗着计算机的资源。由于其隐蔽性极强，大多数 PC 用户和服务器管理员难以发现挖矿木马的存在，这也导致挖矿木马数量的持续上涨。

挖矿机程序运用计算机强大的运算力进行大量运算，由此获取数字货币。由于硬件性能的限制，数字货币玩家需要大量计算机进行运算以获得一定数量的数字货币，因此，一些不法分子通过各种手段将挖矿机程序植入受害者的计算机中，利用受害者计算机的运算力进行挖矿，从而获取利益。这类在用户不知情的情况下植入用户计算机进行挖矿的挖矿机程序就是挖矿木马。挖矿木马最早出现于 2013 年。由于数字货币交易价格不断走高，挖矿木马的攻击事件也越来越频繁，不难预测未来挖矿木马数量将继续攀升。对于挖矿木马而言，选择一种交易价格较高且运算力要求适中的数字货币是短期内获得较大收益的保障。

另外，1 月 8 日，我们第一次见到 Satori.Coin.Robber 僵尸网络利用“肉鸡”扫描正在挖矿的设备，并通过篡改其挖矿设备的算力和代币，致使其挖掘的虚拟货币流向自己的口袋。

四、 反人工检测技术大范围流行

2013 年时，我们就曾经监测到过不发分子在正常网站中植入一段判断代码，该网页自动判断访问者是人还是搜索引擎爬虫，如果是人就跳转回正常页面，如果是搜索引擎爬虫就继续访问非法网站，给不法分子带来流量，从中非法获益。但是，此后却很少看到不法分子使用这种方法，直到 2017 年，我们又重新监测到了大量的实际案例。

不法分子们为了使自己私自搭建的非法网站存活时间更长久，更加难以被发现，也在不断地改进其手法，使其更加具有迷惑性。当我们用正常手段访问网页时，网页自身显示没有问题，并且由于隐蔽性较高，我们第一时间通过肉眼难以观察到不正常现象。

不法分子之所以这样做的主要目的是，希望网站拥有者（不懂技术的人），访问之后认为自己的网站没有问题，但是实际上自己的网站正在被黑产利用产生效益。不法分子采用这种手法的优点如下：

1） 保证了对黑产 SEO 的优化效率。

2） 网站管理者很难及时发现黑链并将其删除。

3） 隐蔽性极高，甚至网站管理者知道存在这种情况，也可能因为没有能力找不到。

4） 保持了黑链的存活时间，拥有更久的存活率。

5） 即便是接到了领导机构或第三方机构通报，网站运维人员也很难发现。

五、 物联网威胁的更加突出

物联网时代，网络安全形势非但没有减弱，相反越来越严峻。一是连接的设备更多，预防更加困难；二是物联网和互联网将虚拟世界和现实世界连在一起，未来发生在网络世界的攻击可能变成物理世界真实的伤害。信息安全、物理安全、人身安全是可以跨界且融合贯通的，这些智能硬件设备如果存在安全漏洞或缺陷，被恶意利用，那么发生在网络世界的攻击就有可能伤害到人身安全。这也使得个人信息、数据面临的网络安全挑战变得空前巨大。

2017 年 5 月，http81 僵尸网络的幕后操控者远程入侵了大量没有及时修复漏洞的网络摄像头设备，在这些摄像头中植入恶意代码，只要发出指令就可以随时向任何目标实施

DDoS 攻击。统计显示，http81 僵尸网络在中国已经感染控制了超过 5 万台网络摄像头。

2017 年 8 月 3 日，印度多地发生 BrickerBot 网络攻击事件，影响了 Bharat Sanchar Nigam Limited（BSNL）和 Mahanagar Telephone Nigam Limited（MTNL）这两家印度国有电信服务提供商的机房内的调制调解器以及用户的路由器，事件导致印度东北部、北部和南部地区调制调解器丢失网络连接，预计 6 万台调制调解器掉线，影响了 45%的宽带连接。

六、 Weblogic 反序列化漏洞攻击可能爆发

2017 年 12 月末，国外安全研究者 K.Orange 在 Twitter 上爆出有黑产团体利用 Weblogic 反序列化漏洞对全球服务器发起大规模攻击。有大量企业服务器已失陷且被安装上了 watch-smartd 挖矿程序。近期，我们安服人员在应急响应过程中也发现了几起利用 Weblogic 反序列化漏洞攻击的相关事件。

该漏洞的利用方法较为简单，攻击者只需要发送精心构造的 HTTP 请求，就可以拿到目标服务器的权限，潜在危害巨大。推测在 2018 年可能会出现，利用 Weblogic 漏洞攻击的事件大幅增涨，大量新主机被攻陷的情况。

这种攻击我们在实践中遇到的较少，但鉴于新的反序列化攻击的出现及近期虚拟货币疯涨的利益驱动力，我们预计未来攻击规模可能呈上升趋势，需要引起高度重视。

第九章　网站安全技术前沿趋势

一、　HTTPS 的大量普及

HTTPS 的全称是 Hyper Text Transfer Protocol over Secure Socket Layer，是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版，即 HTTP 下加入 SSL 层，简称为 HTTPS。现在越来越多的网站和 APP 都已经向 HTTPS 方向发展。例如：苹果公司强制所有 iOS App 在 2017 年 1 月 1 日前全部改为使用 HTTPS 加密，否则 APP 就无法在应用商店上架。谷歌从 2017 年 1 月推出的 Chrome 56 开始，对未进行 HTTPS 加密的网址链接亮出风险提示，即在地址栏的显著位置提醒用户“此网页不安全”。腾讯微信小程序的官方需求文档要求后台使用 HTTPS 请求进行网络通信，不满足条件的域名和协议则无法请求。

Google 在透明公开报告中公布了 HTTPS 网页使用数据，显示到今年 10 月底为止，Chrome OS 的 HTTPS 网页造访比例以 68%居冠，其他依序是 macOS 的 62%、Linux OS 的 57%、Windows 的 53%，以及 Android 的 42%。

Google 在公开报告（Transparency Report）中新增 HTTPS 网页使用数据，显示透过 Chrome 桌面浏览器载入的 HTTPS 网页比例已超过 50%，与 Mozilla 日前公布的 Firefox 数据相呼应。大力推广 HTTPS 加密传输的 Google，目前旗下已有 85%的服务采用 HTTPS，并在去年 12 月宣布 Google 搜寻引擎将优先索引 HTTPS 网页。

二、　政务云推动云安全技术升级

2017 年上半年海南、福建厦门、辽宁辽阳政务云相继招标完成，浙江嘉兴等地政务云扩容招标也陆续展开。12 月国家在贵州正式授牌建立国家电子政务云数据中心体系（试点示范）建设项目南方节点，也是首个开建的三大国家级骨干节点之一。据 IDC 统计，65%的省市都已正式建设运行政务云，且中国云计算市场正在以 30%左右的增速高速发展，而政务云正是云市场需求的主力。

国家及各省市区、地区政务云系统及应用建设热火朝天，云计算基础设施的快速建设，促进政府部门数据资源的集中，必将对云安全技术提出更高要求。政务云带来技术部门安全运维和管理的集中，也冲击原有的内部安全监督管理的角色和责任分工的格局。例如，某市政府的门户网站使用公有云服务的模式，那么政府相关负责人上传到门户网站 Web 首页的图文内容，及其管理账户，已经不再靠自身独立负责，其控制权与安全责任，转变为其自身和云服务商双方“各自分担”的安全责任。

而云计算系统的安全和“云”的虚拟化架构特征紧密相关，解决虚拟化系统的安全控制与管理问题，首先，需要解决虚拟机与宿主机权限边界问题，避免虚拟机逸出。其次，建立云控制器，实现云安全的调度管理，打造云安全的“智慧大脑”。第三，构建持续的、智能化的安全运营体系。第四，解决虚拟化环境下的数据安全与隐私保护。

目前中国乃至全球范围内，云计算平台建设规模越来越大，应用更加广泛。国际上有专业机构建议不要用分散的安全技术来应对多样化的安全需求，需要体系化的建设网络、终端、应用的全方位感知能力，在检测、响应、预测方面持续投入，并降低防御投入。

三、 IPv6 促进安全技术革新

2017 年 11 月中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》（下文简称计划）。以此为标志，IPv6 将在技术和政策两方面迎来新的发展期，“我国五年内要做到世界上最大的 IPv6 用户网络”。所谓 IPv6，相对 IPv4 而言，是 IP 协议版本的升级，但也在 IP 地址数量、安全性、稳定性、可扩展性等方面大大提升。

创新技术、设备和应用。目前 IPv6 领域的创新技术和应用，是 IPv6 技术大规模工程实施的基础和优势，可高效支撑移动互联网、物联网、工业互联网、人工智能等新兴领域快速发展，不断催生新技术新业态，但 IPv6 越来越广泛部署，即对未来安全技术发展带来利好，同时也将对网络安全能力提出新的挑战和要求。

首先，网络架构升级到 IPv6 之后，其本身增加的溯源能力、加密传输能力、抗扫描威胁能力等，和现有网络安全技术应用结合，将加快传统的网络信息安全建设加速创新和发展。

其次，IPv6 为解决已知的网络安全问题提供了新平台、新思路。未来，架构在 IPv6 网络之上的安全解决方案，将在全网安全、主干网 DNS 安全、主干网路由安全、网络管理安全、故障检测与自愈等关键技术方面，寻找破解风险与威胁的新途径。

第三，IPv6 加速推进，接入互联网的设备和终端，融入更多专门、专用的拓扑网络，这将使未来网络结构更加复杂，网络环境开放程度提高，容纳各类信息能力增大，从而客观上增大了海量数据安全保护、网络应用管控和流量监控的难度，这对于未来网络安全产业而言，既是挑战，也是机会。

第十章　2017 网络安全制度建设要点与趋势

一、　确立关键信息基础设施

世界各国都将关键信息基础设施列为重点保护对象，中国也不例外。网络安全法三易其稿，最终敲定了具有代表性的七大领域：公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等，作为关键信息基础设施，要求必须“在网络安全等级保护制度的基础上，实行重点保护”。

而《国家网络空间安全战略》则进一步补充教育、科研、工业制造等三个领域，并将《网络安全法》中公共服务进一步具体化为医疗卫生、社会保障。此外《国家网络空间安全战略》还单独强调了重要互联网应用系统，这一点也值得互联网从业者重点关注。（重要互联网应用系统：应当属于公共通信和信息服务中的一个组成部分）

关键信息基础设施安全保护条例（征求意见稿）在《网络安全法》和《国家网络空间安全战略》的基础上，增加了环境保护、国防科工、大型装备、化工和食品药品等科研领域的基础设施。某些方面还细化了具体内容，如“重要互联网应用系统”，上述条例中特别提到“提供云计算、大数据和其他大型公共信息网络服务的单位”。

从安全业界实践层面看，网络安全首要考虑的保护对象就是关键信息基础设施（CII）。国家在这一领域投入重大资金进行安全保护的同时，也在逐步建立国家级的 CII 清单——即纳入被保护对象的最为重要的基础网络或信息应用系统。

关键信息基础设施清单的明确和公布之后，对 CII 安保责任主体提出了更为严格和高标准的要求。《网络空间安全战略》针对关键信息基础设施的保护，提出“坚持技术与管理并重，保护与威慑并举”的原则，要求“着眼识别、防护、监测、预警、响应、处置等环节，建立关键基础设施保护制度”。

关键信息基础系统的安全保障建设，可对一般性网络设施或信息应用系统的安全建设起到示范和标杆作用，在一定程度上将提高网络信息系统责任主体的安全意识，以及在人力、物力、财力等方面的投入，对于普遍提升整个互联网的安全水平有积极效应。

二、　督促提升安全漏洞防护能力

在面对网络空间形形色色的威胁时，确保网络责任主体，强化安全制度与能力建设非常重要。2016-2017 年出台的相关政策也对切实督促企事业单位或组织机构提升漏洞响应与防护能力做了相应规范。尤其是在漏洞监测、通报、修补上做了明确规定。

例如，网络安全法第三章第二十二条明确规定，网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当及时告知用户并采取补救措施，并按照规定及时告知用户并向有关主管部门报告。

上述条款在网络安全法草案中还没有出现，但在 2016 年的三审稿中新增写入，并最终成为律条，说明网络安全漏洞已经引起越来越多业内政府部门以及企业机构专家学者的关注和重视。

漏洞防护进入立法者视野，也从侧面反映出业内出现的第三方漏洞监测、通报收录平台，以及安全企业围绕漏洞修复而初步探索出的“自动扫描+人工挖掘”模式得到了业界认可。后续在帮助提升信息基础设施、企业网站、开放信息系统、公共服务系统的漏洞监测水平，降低潜在风险，消除漏洞威胁等方面，将发挥重要作用。

例如补天平台发起的公益项目公有 SRC、针对高安全标准需求提供的私有 SRC 以及“补天众测”项目，就是在落实法律对漏洞安全管理的相关规范原则，也给业界在如何更好的落实上述法律法规带来启发。

需要补充说明的是，从法治角度讲，在现有法律规定不完善的情况下，立法从正向引导和限制边界这两个角度进一步明确了“白帽子”挖掘漏洞行为。例如，从引导角度看，法律应该真正将“白帽子”和众测平台通过适当的衡量标准纳入到安全产业当中，切实给予他们合法地位。同时，对于不能触碰的关键基础设施和信息应用系统，也需给出较为清晰的界定，并明确“白帽子”的行为边界，让第三方漏洞收录平台及提交者遵守法律法规时心中有数。

三、 强化网络运营者与监管部门各自责任

2017 年，网络运营者这一概念在网络安全法中正式确立，其内涵是指网络的所有者、管理者和网络服务提供者。在明确定义的基础上，法律对网络运营者提出一系列责任底线。与此同时，“网信部门”也是首次以法律词汇的形式出现在国家法律中，并与公安部门等其他政府机构作为网络安全的监管方。

从国家出台的一系列政策文件看，一方面在强化网络运营者的安全保障责任，另一方面也强调网信、公安，甚至社会服务相关机关部委等监管部门的被监督义务。

网络运营者安全责任与义务

网络运营者的安全责任在网络安全法第三、四、五章中有详细的描述，与此前各类相关法律法规相比，变化较大的包括但不限于以下几点：

第一，信息安全等级保护制度升级为网络安全等级保护制度，其主体内容预期将出现一些变化，特别是威胁情报、态势感知等概念可能会更多出现在高级别的安全保护等级规范中。

其次，在网络安全等级保护基础上，法律对网络运营者提出一些新的要求。例如网络日志必须留存 6 个月以上；确保运营业务或产品的连续性等问题。

第三，网络运营者也要接受社会监督。发生网络安全事件除了需要立即启动应急预案、采取技术和其他必要措施，消除安全隐患防止危害扩大等之外，还必须及时向社会、公众发布有关警示信息。该条款体现出：法律要求网络运营者对社会、对广大网民担当企业责任。

第四，依法配合有关部门调查执法。重大安全事件向主管部门报告，而且有义务和责任为公安及国家安全机关依法维护国家安全和侦察犯罪的活动提供技术支持和协助等。

监管部门接受社会监督

针对近年来网络监管执法过程中出现的问题，相关部门探索积累的一些约束机制，国家逐步形成了对监管部门的监察和执法的相关规范。与此前各类相关法律法规相比，变化较大的包括但不限于以下两点：

第一，网信、公安和有关部门履行网络安全保护职责中获取的数据，必须按规定使用，不能用于维护网络安全之外的用途。（网络安全法三十条）

第二，监管部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私、商业秘密严格保密，不得泄露出售或非法向他人提供。

上述规定无疑对政府部门在网络安全执法监督履职过程中提出了规范的要求，也是保证网络运营者和广大网民合法利益的必要手段。实际上，有些政府部门既是网络运营者，又是网络安全监管者。例如监管部门的内网和官方网站安全工作，就是运营者需依法履行的职责。

总体看，不论是对网络运营者的高标准要求，还是对监管者的严肃纪律、依法行政，其落脚点是有利于激发和促进包括政府、企业、个人，以及其他网络组织在内的各方力量，规范严格、强化责任，协同起来，共同维护网络空间安全。

四、 严格实施个人信息保护

2017 年正式实施的《网络安全法》有一个突出的亮点就是，首次在国家层面开始高度重视对个人信息的保护，法案中给出了几个非常重要的原则。

第一，任何互联网企业/网站在收集和使用公民信息时，必须遵循“合法、正当、必要”这三个原则，网络运营者不得收集与其提供的服务无关的公民个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用公民个人信息，而且网络运营者收集、使用公民个人信息，应当公开其收集、使用规则。

第二，它间接承认了个人对自身的信息享有被遗忘权和更正权。法案第 37 条中指出“公民发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正”。

第三，在严格规范网络运营者的数据保护责任方面，法律也明确要求一旦发生泄漏、毁损、丢失的情况时，如网站注册用户信息遭拖库，网站方必须及时采取有效措施降低危害，或采取技术等手段及时补救，并且“按照规定及时告知用户并向有关主管部门报告”。

同时，在针对侵害、非法获取及出售个人信息的惩处罚责上也做出了严格的规定。例如对于构成犯罪的交检察机关起诉，对于尚不构成犯罪的，在没收违法所得的同时还可最高罚款至一百万元。

五、 政府网站集约化建设

2017 年 8 月，省政府办公厅印发《关于推进政府网站集约化建设的通知》，要求各市县政府、省政府各部门办公厅（室）组织对本市县、本部门政府网站进行全面摸底、查缺补漏，确定拟整合迁移和拟保留的政府网站名单，拟制集约化建设方案，于明年 3 月底前完成组织整合迁移，并明确网站运维责任。强调，省政府各部门原则上只允许开设 1 个政府网站。省政府部门下属单位不得单独开设政府网站，已开设的必须整合迁移至部门网站，开展政务公开，提供政务服务。

截至 2017 年 6 月 1 日，全国正在运行的政府网站有 3.7 万家，比第一季度集约上移 6227 家；相比 2015 年摸家底时的 8 万多个，精简近六成。其中，县级以下政府网站精简至 12265 家，市级部门政府网站数首次超过县级以下网站数，网站集约化建设成效显著。

附录1　2017 年重大网站安全漏洞

一、　CVE-2017-3248 ：WebLogic 远程代码执行

2017 年 1 月 27 日，WebLogic 官方发布了一个编号为 CVE-2017-3248 的漏洞。分析之前 WebLogic 漏洞 CVE-2015-4852 的补丁，发现 WebLogic 采用黑名单的方式过滤危险的反序列化类，但是这种修复方式很被动，存在被绕过的风险，只要发现可用并且未在黑名单之外的反序列化类，那么之前的防护就会被打破，系统就会遭受攻击。这次发布的 CVE-2017-3248 就是利用了黑名单之外的反序列化类，通过 JRMP 协议达到执行任意反序列化 payload。该漏洞影响 WebLogic 10.3.6.0，12.1.3.0，12.2.1.0，12.2.1.1 多个版本，并且官方仍未发布针对该漏洞的补丁，所以危害巨大。

二、　CVE-2017-5638 ：Struts2 远程代码执行（S2-045）

2017 年 3 月 7 日，该漏洞是 Apache strut2 最新的一个漏洞，CVE 编号 CVE-2017-5638.（基于 Jakarta plugin 插件的 Struts 远程代码执行漏洞），该漏洞会造成 RCE 远程代码执行，恶意用户可在上传文件时通过修改 HTTP 请求头中的 Content-Type 值来触发该漏洞，进而执行系统命令，可直接造成系统被控制。黑客通过 Jakarta 文件上传插件实现远程利用该漏洞执行代码。

（远程命令执行漏洞，用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许攻击者通过改变 $PATH 或程序执行环境的其他方面来执行一个恶意构造的代码。）

三、　CVE-2017-5638 ：Struts2 远程代码执行（S2-046）

2017 年 3 月 21 日，安全研究人员发现著名 J2EE 框架——Struts2 存在远程代码执行的漏洞（S2-046），与 S2-045 影响范围及组件完全相同，在上次的漏洞中升级过的 Struts2 组件不受影响。Struts2 是一个基于 MVC 设计模式的 Web 应用框架，它本质上相当于一个 servlet，在 MVC 设计模式中，Struts2 作为控制器(Controller)来建立模型与视图的数据交互。当上传文件的大小（由 Content-Length 头指定）大于 Struts2 允许的最大大小（2GB）或是在文件名内容构造恶意的 OGNL 内容时，Content-Disposition 请求中含有空字节，就可能会造成远程命令执行，导致系统被入侵。Struts2 的使用范围及其广泛，国内外均有大量厂商使用该框架，因此，该漏洞被安全服务团队风险评级为：严重。

四、　CVE-2017-3531 ：WebLogic 远程代码执行

2017 年 4 月 18 日，Oracle 融合中间件（子组件：Servlet 运行时）的 Oracle WebLogic Server 组件中的漏洞。受影响的受支持版本是 12.1.3.0，12.2.1.0，12.2.1.1 和 12.2.1.2。轻松“可利用”漏洞允许未经身份验证的攻击者通过 HTTP 访问网络，从而危害 Oracle WebLogic Server。虽然此漏洞位于 Oracle WebLogic Server 中，但攻击可能会对其他产品产生重大影响。此漏洞的成功攻击可能会导致未经授权的更新，插入或删除对部分 Oracle WebLogic Server 可访问数据的访问，以及未经授权的导致部分拒绝服务（部分 DOS）的 Oracle WebLogic

Server。CVSS 3.0 基本评分 7.2（完整性和可用性影响）。CVSS 向量：（CVSS：3.0 / AV：N / AC：L / PR：N / UI：N / S：C / C：N / I：L / A：L）。

五、 CVE-2017-1000353 ：Jenkins 远程代码执行

2017 年 5 月 1 日，Jenkins 的反序列化漏洞，攻击者使用该漏洞可以在被攻击服务器执行任意代码，漏洞利用不需要任何的权限。Jenkins 是一款持续集成（continuous integration）与持续交付（continuous delivery）系统，可以提高软件研发流程中非人工参与部分的自动化处理效率。作为一个基于服务器的系统，Jenkins 运行在 servlet 容器（如 Apache Tomcat）中，支持版本控制工具（包括 AccuRev、CVS、Subversion、Git、Mercurial、Perforce、Clearcase 以及 RTC），能够执行基于 Apache Ant、Apache Maven 以及 sbt 的工程，也支持 shell 脚本和 Windows 批处理命令。

该漏洞存在于使用 HTTP 协议的双向通信通道的具体实现代码中，Jenkins 利用此通道来接收命令，恶意攻击者可以构造恶意攻击参数远程执行命令，从而获取系统权限，造成数据泄露。

六、 CVE-2017-9791 ：Struts2 远程代码执行（S2-048）

北京时间 2017 年 7 月 7 日 apache 官方发布通告，在 Struts2 框架中存在漏洞代号为 S2-048（CVE-2017-9791）的远程命令攻击漏洞。Apache Struts2 是一种国内使用非常广泛的 Web 应用开发框架，被大量的 Web 网站所使用。当 Struts 2 中的 Struts 1 插件（默认不启用）启用的情况下，攻击者通过使用恶意字段值可能造成远程命令执行。这些不可信的输入数据被带入到 ActionMessage 类中的错误信息中，通过构建不可信的输入实现远程命令执行，被评价为高危漏洞。

七、 CVE-2017-9822 ：DotNetNuke 远程代码执行

2017 年 8 月 2 日，DNN 安全板块发布了一个编号 CVE-2017-9822 的严重漏洞，DNNPersonalization 是一个在 DNN 中是用于存放未登录用户的个人数据的 Cookie，该 Cookie 可以被攻击者修改从而实现对服务器任意文件上传，远程代码执行等攻击。漏洞报告者 Alvaro Muñoz 和 OleksandrMirosh 在 BlackHat USA 2017 上披露了其中的一些细节。据称，全球有超过 75 万的用户在使用 DNN 来搭建他们的网站，影响范围很大。360 CERT 跟进分析了该漏洞及其使用 XmlSerializer 进行序列化/反序列化的攻击利用场景，确认为严重漏洞。

八、 CVE-2017-9805 ：Struts2 远程代码执行（S2-052）

2017 年 9 月 5 日，千疮百孔的 Struts2 应用又曝出存在新的高危远程代码执行漏洞。该漏洞由 lgtm.com 的安全研究员汇报，编号为 CVE-2017-9805 ，漏洞危害程度为高危（Critical）。当用户使用带有 XStream 程序的 Struts REST 插件来处理 XML payloads 时，可能会遭到远程代码执行攻击。漏洞存在于非默认的插件中，首先确认应用是否使用了 REST 插件，如果没有使用，则不受此次漏洞影响。如果 WEB 应用的 WEB-INF/lib 目录下存在以“struts2-rest-plugin”开头的 jar 文件，且文件名不是“struts2-rest-plugin-2.5.13.jar”或者 “struts2-rest-plugin-2.3.34.jar”，则有可能存在漏洞。目前漏洞相关的技术细节和利用

代码已经公开，漏洞极有可能被积极利用获取对用户系统的控制，需要引起高度注意。

九、 CVE-2017-10366 ：PeopleSoft 远程代码执行

据 2017 年 10 月 19 日报道，该漏洞（CVE-2017-10366）允许攻击者在运行 PeopleSoft 软件的服务器上获得远程代码执行。ERPScan 的研究人员说，这个缺陷是核心引擎，意味着 PeopleSoft 产品的多种风格可能会受到影响。

此漏洞可以通过向 PeopleSoft 服务器发送不合法的 HTTP 请求和构造一个反序列化的 Java 对象来执行远程代码攻击，任何把 PeopleSoft 系统暴露在外网上的公司都有可能受到影响。值得注意的是，相较于 PeopleSoft 的 4 月的 16 个补丁和 7 月的 7 个补丁，在本月 Oracle 发布的 252 个补丁中，有 30 个属于 PeopleSoft。截止到 10 月，今年发布的 PeopleSoft 补丁已经有 76 个，相比 2016 年的 44 个和 2015 年的 29 个，补丁的数量有所上涨。

十、 CVE-2017-11283 ：Adobe ColdFusion 远程代码执行

据 2017 年 10 月 19 日报道，Adobe ColdFusion 在 2017 年 9 月 12 日发布的安全更新中提及到之前版本中存在严重的反序列化漏洞（CVE-2017-11283, CVE-2017-11284），可导致远程代码执行。当使用 Flex 集成服务开启 Remote Adobe LiveCycle Data Management access 的情况下可能受到该漏洞的影响，使用该功能会开启 RMI 服务，监听的端口为 1099。ColdFusion 自带的 Java 版本过低，不会在反序列化之前对 RMI 请求中的对象类型进行检验。

360CERT 经过分析验证，确认该漏洞确实存在，请相关用户尽快进行更新处理。

附录2　2017 年威胁网站安全的典型病毒

一、 暗云 III

2017 年 6 月 12 日，臭名昭著的暗云III病毒再次卷土重来，在全国范围内发起网络攻击。暗云III木马的恶意程序，伪装成“赤月传说”、“传奇霸业”等游戏微端进行补丁修复，通过各大下载站的下载器等各种传播渠道进行海量推广。暗云系列木马异常狡猾，此次突然爆发有很大可能会引发牵连范围极广的 DDoS 攻击。专家建议，除了安装安全软件，还要保持良好的上网习惯，不要运行来源不明或被安全软件报警的程序，不要下载运行游戏外挂、私服登录器等软件；定期在不同的存储介质上备份信息系统业务和个人数据。

二、 Xshell 后门

2017 年 8 月 4 日 Xshell 开发公司 NetSarang 与卡巴斯基工程师发现 Xshell 软件中存在后门。恶意攻击者利用该后门可窃取用户服务器账号密码等信息，进一步可致整个服务器被攻击。在软件的开发阶段，程序员常常会在软件内创建后门程序，以便可以修改程序设计中的缺陷。但是，如果这些后门被其他人知道，或者在发布软件之前没有删除后门程序，容易被不法分子当成漏洞进行攻击，用户们的服务器会面临严重的威胁。此次黑客似乎入侵了 Xshell 相关开发人员的电脑，在源码植入后门，导致官方版本也受到影响。并且由于 dll 文件已有官方签名，众多杀毒软件依据白名单机制没有报毒。

三、 IoT_reaper 僵尸网络

2017 年 9 月，奇虎 360 公司研究人员首次发现 IoT 僵尸网络，命名为“IoT_reaper”。这款恶意软件不在依赖于破解弱口令，而是利用各种 IoT 设备中的漏洞进行攻击，并将其纳入僵尸网络。同时，CheckPoint 的研究人员也警告了这个 IoT 僵尸网络，他们取名为“IoTroop”，它已经感染了数十万个公司组织。根据 CheckPoint 的观点，IoTroop 恶意软件还利用了 GoAhead，D-Link，TP-Link，AVTECH，Linksys，Synology 等无线网络摄像机设备中的漏洞。

四、 BrickerBot 恶意软件

8 月 3 日，印度多地发生网络攻击事件，影响了 Bharat Sanchar Nigam Limited（BSNL）和 Mahanagar Telephone Nigam Limited（MTNL）这两家印度国有电信服务提供商的机房内的调制调解器以及用户的路由器，事件导致印度东北部、北部和南部地区调制调解器丢失网络连接，预计 6 万台调制调解器掉线，影响了 45%的宽带连接。

BrickerBot 是一款影响 Linux 物联网和联网设备的恶意软件。与其它囤积设备组成僵尸网络实施 DDoS 攻击等恶意软件不同的是，BrickerBot 重写 Flash 存储，使物联网设备变“砖”。大多数情况下，“砖化”效应可以逆转，但在某些情况下却会造成永久性的破坏。BSNL 几万台调制调解器使用了不受保护的 TR069（TR064）接口，允许任何人重新配置设备实施中间人攻击或 DNS 劫持。BSNL 和 MTNL 遭遇这起网络攻击的原因，还在于这两大 ISP 允许他人通过 7547 端口连接到它们的网络。

五、 Satori 僵尸网络

2017 月 12 月 5 日，奇虎 360 公司研究人员首先发现 Satori 僵尸网络，Satori 是 mirai 的变种，同样针对物联网设备，尤其以某品牌家用路由器为主。

Satori 的 bot（僵尸程序）不再完全依赖以往的 loader/scanner 机制进行恶意代码的远程植入，而是自身有了扫描能力，类似蠕虫的传播行为；另外，bot 中增加了两个新的漏洞利用，分别工作在端口 37215 和 52869 上，在过去的 12 个小时里，26.3 万个不同的 IP 在扫描端口 37215，以及 1.9 万个 IP 在扫描端口 52869，成为史上传播速度最快的僵尸网络。

六、 挖矿木马

挖矿木马是 2017 年非常流行的一种针对网络服务器进行攻击的木马程序，此类木马程序通过自动化的批量攻击感染存在漏洞的网络服务器，并控制服务器的系统资源，用于计算和挖掘特定的虚拟货币。由于挖矿木马对的 CPU 率一般为 100%，因此，服务器感染挖矿木马后最明显的现象，就是服务器响应非常缓慢，出现各种运行异常。如果挖矿木马攻击的整个云服务平台，则平台上所有网站和服务系统都会受到严重影响。

附录3　2017 年国内外重大网站安全事件

一、　黑客入侵 FBI 网站，公开 FBI 用户敏感信息

2017 年 1 月，黑客 CyberZeist 成功入侵了美国联邦调查局的官方网站 FBI.gov，并将该网站中的部分数据发布到了 Pastebin 上。此次泄漏的数据中包括 FBI.gov 的用户账号信息，其中包括账号的用户名、SHA1 加密的用户密码、SHA1 盐值、以及用户邮箱等信息。根据安全研究专家透露的信息，CyberZeist 从 FBI.gov 的服务器中发现了几个备份文件（acc_102016.bck、acc_112016.bck 和 old_acc16.bck 等等），并在这些备份文件中找到了大量用户数据。安全专家经过分析发现，此次入侵事件发生在 2016 年的 12 月 22 日，这名黑客利用了一个存在于 FBI.gov-Plone 内容管理系统中的一个 0 day 漏洞发动了此次攻击。

二、　普京的网站每天会遭到数千次黑客攻击

2017 年 1 月，一名俄罗斯官员最近表示，俄国每天会遭遇数百次甚至数千次的网络攻击，其中一部分来自美国。当美国方面声称俄国试图利用网络攻击干扰 2016 年总统大选时，俄罗斯联邦安全会议秘书长尼科 帕特鲁舍夫则表示俄罗斯自身也是黑客攻击的一个主要目标。他还在一份公开声明中称美国对俄罗斯的指控还无根据，缺乏真实性。他们还故意无视这一事实，那就是世界上的所有主要互联网服务器都在建立在美国国内，并被美国作为保持其主导地位的工具所利用。另外，帕特鲁舍夫还称最近俄罗斯所遭遇的网络攻击数量不断上升，有人试图攻入俄罗斯政府的电脑以窃取情报。俄罗斯总统普京的网站也是黑客攻击的一大目标，其每天遭到的黑客攻击次数已经超过一千次，其中大部分来自美国、欧洲、中国和印度。

三、　日本 10 万条信用卡信息泄露

2017 年 3 月，日本支付服务提供商 GMO Payment Gateway（GMO PG）公司证实，黑客利用其应用框架中的 Apache Structs2 漏洞对该公司的两大客户的网站发起攻击，并导致大量个人数据被泄。这两大客户为东京都政府和日本住宅金融支援机构。通过东京都政府网站泄露的数据量为 67.6 万条，包括 61.5 万条电子邮箱地址、6.2 万条信用卡号以及信用卡到期日。从日本住宅金融支援机构泄露信用卡信息为 4.4 万条，包括信用卡号、信用卡到期日、安全码、信用卡支付注册日期、地址、电子邮箱地址、姓名、电话、出生日期和支付加入日期。

四、　美国数个地方政府网站遭支持 IS 黑客攻击

2017 年 6 月，美国一些州政府和地方政府的网站遭黑客攻击，网站被黑后显示出支持极端组织“伊斯兰国”（IS）的信息。受影响最大的是俄亥俄州，州长卡西奇和州长夫人凯伦·卡西奇，以及州总监察长办公室、医疗补助计划部、州惩教局等部门网站均遭到黑客攻击。卡西奇的办公室说：“我们被告知情况后立即开始更正，我们将继续密切关注直到问题解决。”马里兰州霍华德县和纽约州布鲁克黑文的政府网站也遭到黑客攻击。据报道，一些网站已于当天晚些时候恢复，其他网站受到攻击后下线，直到 26 日凌晨仍未恢复。

五、 以太坊平台被盗走超过 15 万枚以太币

2017 年 7 月 21 日，据以太坊初创公司 Etherscan 的数据，约有 15.3 万枚以太币被黑客盗走，其中 4.4 万枚盗至贸易平台 Swarm City。按当天的价格计算，盗走的以太币价值超过 3000 万美元（约合人民币 2.03 亿元）。黑客利用了 Parity Multisig 代码中的一处漏洞，该漏洞令一个已知方从 Edgeless Casino、Swarm City、Aeternity 等多个平台盗走了超过 153000 枚以太币。当漏洞曝光后，以太坊社区的“白帽子黑客”挽救了超过 37.7 万枚以太币，方式是将这些货币从受影响的钱包转移到了其他地方。他们表示，将开发另一种多重签名技术，其设置与此前的多重签名技术相同，但移除了其中的漏洞。一旦开发完成，便把资金返还给用户。

六、 航运公司马士基遭遇勒索软件，损失数亿美元

2017 年 8 月，全球最大的集装箱航运公司马士基（AP Moller-Maersk）在线公布《2017 第二季度财务业绩报告 》，证实公司于 6 月遭受勒索软件 NotPetya 袭击后损失数亿美元。调查显示，公司收入损失源自重大业务中断，因被迫暂时关闭感染恶意软件的关键系统 Damco 与 APM 终端作为防御措施。据悉，由于该恶意软件只影响马士基集装箱相关业务，因此包括所有能源企业在内的九家公司中六家能够正常运营。此外，马士基还于攻击期间对所有船只进行全面检测，以确保所有员工运输安全。

七、 委内瑞拉遭遇网络攻击，700 万手机通讯瘫痪

2017 年 8 月，委内瑞拉政府表示，政府网站本周早些时候遭遇大规模网络攻击，导致 700 万手机用户无法使用通信服务。一支自称“The Binary Guardians”的组织宣称对此负责。攻击使委内瑞拉政府、最高法院和国会的网站关闭。科技部长胡格博 • 罗亚将这些攻击称为恐怖行动，称攻击者周三攻陷了运营商 Movilnet 的 GSM 平台，导致 700 万手机用户无法使用通信服务。罗亚表示，委内瑞拉本周一开始遭遇一波攻击，几十个政府和私企公司网站被黑。光纤网被切断，影响了 7 个州。罗亚表示，委内瑞拉仍在调查该事件。

八、 瑞典交通署信息系统遭攻击导致列车延误

2017 年 10 月，瑞典运输局 Transport styrelsen 官方网站遭遇多次 DDoS 攻击，致服务掉线，其 IT 系统遭攻击，导致了列车延误。据报道，今年 7 月，瑞典运输局的大量数据被误上传到了云服务器。这些数据含有该国几乎所有公民(包括军人和警察)的车辆和个人信息。尽管调查仍在进行中，初步检查发现，被暴露的数据包含：数百万公民的姓名、住址、照片，警车、公务用车和军车相关人员信息，瑞典空军战斗机飞行员的驾照记录，秘密部队军人的详细资料，以及包含道路和桥梁在内的瑞典关键基础设施数据。

九、 瑞典交通机构遭受 DDOS 攻击

10 月 11 日，黑客针对瑞典运输管理局（ Trafikverket ）展开 DDoS 攻击，导致该机构负责管理列车订单的 IT 系统瘫痪，以及电子邮件系统与网站宕机，从而影响了旅客预定或修改订单的情况。10 月 12 日，瑞典交通运输局（Transportstyrelsen），以及公共交通运营

商 Västtrafik 的 IT 系统遭到类似 DDoS 攻击。黑客发动的 DDoS 攻击主要针对服务提供商 TDC 和 DGC，其目的是影响机构的正常运营。

十、 运输局网站被黑，服务器文件三成被删

2017 年 11 月，萨克拉门托地区运输局（Sacramento Regional Transit，简称 SacRT）的网站遭到了黑客入侵。黑客删除了网站服务器中部分文件，并威胁称如果 SacRT 不向其支付一个比特币（约值 8000 美元），将制造更多的破坏。SacRT 首席运营官 Mark Lonergan 表示，黑客删除了服务器上 30%的文件，导致 SacRT 部分内部运营功能丧失但并没有数据被窃取，并正在努力确保其网站系统免受进一步的攻击。SacRT 在第一时间删除了其网页上的客户信息，并关闭了 Connect Card 上用于处理信用卡付款的系统，以防止收到黑客的侵害。目前，SacRT 的技术人员正在通过备份的数据进行系统功能重建。此外，SacRT 已经聘用了安全专家来对其网站系统进行漏洞审查，以确保类似的事件不会再次发生。

附录4　补天平台介绍

补天漏洞响应平台，原名为“库带计划”，成立于 2013 年 3 月，是国内首个现金奖励漏洞，专注于漏洞响应的第三方公益平台。2014 年 12 月 1 日 10 点更名为“补天漏洞响应平台”，简称“补天平台”。补天平台通过充分引导和培养民间的白帽力量，实现实时的、高效的漏洞报告与响应，守护企业网络安全，积极推动互联网安全行业的发展。

该平台于 2013 年 3 月份推出时，是一项针对开源建站系统漏洞的有奖征集项目。该项目通过现金奖励的方式，公开征集建站工具软件/系统存在的漏洞，以帮助软件公司和开发者及时修复漏洞，加强国内数百万家网站对黑客攻击的防范能力，并加强 360 网站安全产品的漏洞检测能力和攻击防御能力。该项目目前已陆续协助 ShopEx、Discuz！、ECShop、ShopEX、PHPWind、PHPCMS 等上百个知名建站和 IT 系统修复了安全漏洞。

从 2014 年 06 月开始，除了通用型漏洞外，补天平台也开始收到事件型漏洞的报告。事件型漏洞主要是指网站或应用的一个具体漏洞，只对该网站自身有影响。如某政府网站后台存在弱口令可进后台 GETSHELL，某著名企业门户网站存在重要信息泄露等。

面对复杂多变的网络安全态势和层出不穷的攻击手段，补天平台通过 SRC、众测等方式服务广大企业，以安全众包的形式让白帽子从模拟攻击者的角度发现问题，解决问题，帮助企业树立动态、综合的防护理念，维护企业的网络安全。

补天平台通过帮助企业建立 SRC（Security Response Center，安全应急响应中心），一方面，可以最大程度避免企业由于安全漏洞遭受损失；另一方面，尊重白帽子的劳动产出，让白帽子获得收益。

继 2014 年下半年提供专属 SRC 服务之后，2016 年 4 月补天平台又推出众测服务。补天众测是补天漏洞响应平台基于众包模式打造的互联网安全测试服务，通过集结国内顶尖的安全专家团队，采取真实环境进行渗透测试，帮助企业发现系统和业务中的漏洞及风险，为企业提供深度定制化的安全测试服务方案。

2017 年 9 月推出的漏洞情报服务，主要向企业提供第一手的面向不同行业精准的行业漏洞情报。补天平台 4 万余名白帽子及补天安全专家获得的漏洞数据，经过联合分析研判、协同挖掘和脱敏加工，最终形成深层次的行业漏洞情报。通过补天平台行业标签算法，第一时间向行业客户进行精准推送。补天平台希望将多种安全服务有机的整合起来，进一步提升企业的漏洞响应能力和积极防御能力。

截止 2018 年 1 月，平台注册白帽子已达 41,000 余名，发现的漏洞数量超过 258,226 个。被公安部、CNCERT、国测等机构评定为优秀技术支撑单位。

网聚安全力量，为社会提供准确、详实的安全情报，让全中国网络都实现漏洞的及时发现与快速响应是补天平台始终坚持并不断履行的社会使命。

附录5　补天白帽大会及校园行

2017 年 3 月，作为中国最大的网络漏洞报告与响应平台，“补天平台”发起并主办“补天白帽大会”。此次大会，吸引国内外多家知名企业 SRC（Security Response Center）联合支持举办，是首个面向全球白帽和技术精英开放的、专注于漏洞响应和防护的全球性安全行业大会。

大会秉承开放、协同的基本原则，广泛邀请国内外知名白帽、技术精英、安全爱好者，与网络安全相关主管机构和知名企业和机构的 CISO 共同参与，共同解读当前网络安全形势和安全威胁，探讨漏洞响应与防范方案，同时分享交流漏洞挖掘与安全攻防等前沿议题。

补天平台以协同保护全社会网络安全为使命，致力于为全社会提供网络漏洞报告与响应服务，通过补天白帽大会努力为不断成长的安全爱好者提供充满正能量的安全交流平台，帮助企业和机构建设安全可靠的网络环境！

自 2016 年起，补天平台开展校园安全活动，丰富多彩的校园行遍布全国 12 座城市和 30 余所信息安全相关的高校。通过一场场宣讲活动，将安全理念、网络安全、法律知识送到各地的高校，给学生们带来了行业最前沿的知识，开拓了学生的视野，提供了相互交流学习的平台，为积极投身网络安全建设打好坚实的基础。

在 2017 年，补天平台走进北京、天津、成都、重庆、青岛、太原、南昌和合肥等 8 座城市，在北京邮电大学、电子科技大学、四川大学、重庆邮电大学、青岛大学等 19 所信息安全相关的高校火热举办。校园活动区域逐渐扩大，让北上广深之外城市的网络安全爱好者

感受到补天平台白帽子的热情和一起分享技术知识交流的喜悦。

时间	地点	地点
2017-5-11	北京	北京航空航天大学
2017-5-16	天津	天津大学
2017-5-18	四川成都	成都信息工程大学
2017-5-18	北京	北京邮电大学-第一场
2017-5-19	四川成都	四川大学
2017-5-19	四川成都	电子科技大学
2017-5-20	四川成都	富力丽思卡尔顿酒店二层水晶厅
2017-5-21	山西太原	山西省太原市希望大厦
2017-5-21	重庆	重庆邮电大学
2017-5-22	重庆	重庆大学
2017-5-22	山东青岛	青岛大学
2017-5-23	北京	北京信息科技大学
2017-5-23	山东青岛	青岛科技大学
2017-5-25	北京	北京邮电大学-第二场
2017-6-3	北京	北京邮电大学-defcon010 专场
2017-6-7	江西南昌	江西理工大学
2017-6-7	江西南昌	江西警察学院
2017-6-8	江西南昌	江西财经大学
2017-6-8	江西南昌	江西科技师范大学
2017-11-2	安徽合肥	合肥师范学院
2017-11-3	安徽合肥	中国科学技术大学
2017-11-3	安徽合肥	合肥工业大学
2017-11-4	安徽合肥	丰大国际大酒店曼谷厅

表格 1　补天平台校园行活动

此外，北京邮电大学校园安全月还通过讲师进校，学生到公司参观学习的互动形式持续展开，不断为热爱信息安全的同学提供学习机会；成都走进三所高校之余还通过假面主题沙龙的形式，举办安卓议题专场，为当地的同学带了不一样的安全沙龙新体验。北京沙龙的新书签售会，更让许多莘莘学子见到了知名的业内大咖，技术大牛。

2017 年 9 月，全新推出补天安全人才培养计划，向全社会网络安全爱好者开放，将线上线下的优质内容整合，促进安全人才的技术创新和法律理念的互动交流。旨在为社会输送新鲜的安全人才血液，推动安全人才生态链的可持续发展。

通过沙龙课程录制与专题录制，共同构成补天安全人才培养计划的系列视频课程。通过线上课程补充白帽子技术培养，旨在帮助培养白帽子的网络安全能力，助力白帽子技能提升和成长，让更多白帽子获益，培养未来中国安全行业的领军人物！

人才是网络安全第一资源。补天平台将一如既往的响应国家政策号召，在创新网络安全人才培养机制和推动高等院校与行业企业合作育人、协同创新方面持续投入，为切实加强网络安全人才培养贡献一份力量。

附录6　360 网站安全云防护系统介绍

360 网站安全云防护系统，是集 DNS 解析、DNS 安全、DDoS 防护、Web 应用防护于一体的云安全防护平台，并提供缓存加速、安全数据分析等功能，辅助网站运营和安全管理。是一套辅助企业级用户保证其网站可用性、数据私密性和完整性的 Web 安全整体方案。360 网站安全云防护系统的用户，经过实名认证注册后，只需修改 DNS 解析将流量引流至网站卫士云防护系统即可获得以下安全、快速、稳定的隐身式安全服务：

Web 攻击防护：可以对黑客发起的针对网站的 SQL 注入攻击、命令注入攻击、跨站脚本攻击、Web 扫描攻击、Web Shell 上传、远程文件包含、目录遍历攻击、敏感信息泄露等各种攻击方式进行防护，使得网站免遭被拖库、被恶意篡改、跨站钓鱼、远程控制、被扫描通报等安全威胁。丰富的日志报表可以让用户整体性的了解自身网站的安全情况。

抗 DDOS 攻击防护：网站卫士云防护系统在全国多地分布有高防节点机房，可以将 DDOS 攻击流量智能调度到各个节点机房进行流量清洗，利用全国 300G 的储备带宽来有效抵御各种 DDOS 攻击，确保用户网站服务的持续可靠性。

CC 攻击防护：智能识别 CC 攻击行为，有效区分 CC 攻击和正常访问，通过 JS 验证、图片验证等多种方式验证疑似的攻击，并对攻击进行阻止。

高防 DNS：可以为用户提供 DNS 域名解析服务并对 DNS 服务器提供防护，使得 DNS 服务器免遭诸如 DNS Flood 攻击、DNS 反射攻击、DNS 缓存投毒、DNS 欺骗等攻击，确保安全的 DNS 解析，防止因 DNS 服务器被攻击而导致用户网站无法解析访问的情况发生。

缓存加速：可以对访问链路做智能负载解析，对访问用户的运营商接入情况和位置情况作出智能分析判断，根据网站管理员制定的网站缓存策略，由离访问用户最近的缓存机房向用户响应经压缩处理的缓存数据，避免跨运营商的路由慢的问题发生，极大的提高了网站数据的响应速度，提高了用户的访问体验。

截止 2017 年 12 月 31 号，360 网站安全云防护系统保护着全国 72 万个一级网站域名，176 万个二级网站域名，保护网站数量占中国互联网协会和国家互联网应急中心 2017 年统计全国网站数 526 万个的百分之十四，是全国规模最大、技术最专业的网站安全防护系统，对中国网站的整体安全水平的提高起着重要作用。 也正是由于 360 在“基于 SaaS 模式的 Web 安全及监测”方面的积累和投入，在 Web 安全领域具备明显的优势，被 IDC 评为国内技术先进性最高的安全厂商，并被排在领导者象限厂商区间。

360 网站安全云防护防护系统分为两种：一种是**免费版**的**网站卫士**，一种是**商业版**的**安域产品**。

360 网站安全云防护系统的前身网站卫士于 2012 年 2 月上线，该系统主要为政府科研机构、中小企业、电商、教育培训机构等单位及个人提供永久免费的网站安全防护服务。

“360 安域 Web 应用安全云防护系统”简称“安域”是 360 在 2014 年推出的为政府机构、大中型企业、互联网电商、高校、医疗、能源、金融、运营商等行业客户量身定制的网站安全云防护系统。与免费版的网站卫士相比，商业版的安域产品主要有以下特点：

1） 更好的节点服务质量

采用线路覆盖、地理位置更多、带宽资源储备更丰富的节点为商用客户提供服务，平台综合贮备带宽达 2T，有着更强智能解析能力和更高的回源质量。

2） 更大的防护能力

云端账号交付，产品涵盖了网站卫士的所有功能与能力，同时在 Web 攻击防护规则、DDOS 攻击防护能力、CC 攻击防护能力、安全策略条数、安全报表的丰富度及其他功能的丰富程度等方面都有大幅度的加强提高。

3） 更丰富的协议支持

除标准安域云防护支持的 HTTP 和 HTTPS 协议之外，安域产品系列的安域高防产品还支持 TCP 协议的防护，是 360 企业安全集团针对游戏、金融等 DDoS 高危客户推出的专业 DDoS 高防服务。高防产品不仅支持域名接入，还支持 IP 接入，能防护的 DDoS 攻击类型包括：

1. 网络层 DDoS 攻击，可有效几乎全类型 DDoS 攻击，具体包括以下类型：

SYN Flood 及其变种，例如 SYN-Payload 等攻击；

ACK Flood 及其变种（除上述 SYN Flood 之外的其它 TCP 标记位 Flood 型攻击均被记为 ACK Flood）；

UDP Flood 及其变种，例如 DNS 反射、NTP 反射等；

ICMP Flood；

IP Fragment Flood，含 Ping of Death；

Null Connection Exhaustion 攻击。

2. 应用层 DDoS 攻击，主要指 CC（Challenge Collapsar）攻击。

4） 更及时、有效的运营响应

提供 7*24 小时的电话支持服务以及故障应急响应支撑服务，同时售前可以提供免费测试及现场交流等。针对网站数量较多的用户，360 可以和用户共建独享式的私有化云防护节点。

附录7　360 网站安全监测平台介绍

360 网站安全监测平台，集网站漏洞扫描检测、网站可用性监控、网页篡改监测、黑词暗链监测、木马后门查杀等功能为一体的综合性的网站安全检测平台。此平台拥有全自动化的扫描器，可以对七千多种类别的 Web 安全漏洞做出有效的识别检测，这是 360 根据自身多年安全研究累积的全国最大的 Web 安全漏洞库。近年来，随着 360 企业安全集团的成立，依靠 360 的云端大数据资源，秉承“数据驱动安全”的理念，陆续又针对企业级客户打造出包含：未知资产监测、钓鱼/仿冒网站监测、DDoS 攻击监测和漏洞舆情监测等功能的全新版本。360 网站安全监测平台在网站监测方面优势主要得益于 360 强大的公司资源投入和安全数据积累。

监测平台内置的 webscan 漏洞扫描引擎，可以周期性的提供安全漏洞检测服务，自动更新补天及运营团队每日编写的检测规则，全面、快捷的识别网站存在的最新漏洞。可以将爬虫爬取的信息，通过分析模型及海量样本库加权判断网站是否被仿冒，网页是否被挂马，检测网页被篡改位置及内容，及时告警使其得到快速处理。同时可以通过 360 搜索引擎技术搜取更具有价值的相似页面，通过内容比对，上下文分析等技术为网站钓鱼提供判断依据。

网站安全监测平台现在全国拥有 40 余个可用性监测节点，监测频率最小能到 1 分钟。能 7x24 小时实时监测用户的网站的可用性情况。结合 360 的大数据分析平台，监测平台可以对网站的性能指标进行详细分析，为网站的运维和优化提供数据支撑，并可以结合海量的网络数据对 DDoS 攻击做出准确的安全分析监测。

360 拥有全国最大的也是唯一存在的 Web 漏洞响应平台“补天平台”，监测平台可获取全国的注册白帽子提交的通用性漏洞和事件型漏洞并进行分析，提炼出最为精准的 Web 特征库，并第一时间向客户推送相关漏洞舆情信息。

360 除了有为广大网站管理员免费提供服务的网站安全监测平台“webscan.360.cn”以外，还有专门为企业级客户提供服务的商业化监测平台“360 网站云监测系统”。

截止到 2017 年底，360 网站安全监测平台已经对全国 20 亿网站页面做出过漏洞扫描检测，并扫描出 2.2 亿的网站安全漏洞。

360 网站云监测系统运营示意图：