NSFOCUS
THREATS REPORT 2012
2012绿盟科技威胁态势报告

NSFOCUS

执行摘要

2012 年是信息安全多样化的一年。网络攻防战场的从通用网络向专用网络延伸，甚至提前开始了“主场”的争夺；除了黑客个人和犯罪团伙，宗教团体和政治势力也开始使用网络武器；攻击目标不再限于主机和服务器，虚拟机、移动终端、平板电脑都被卷入，而原本用于提供保障的安全机制，有时也会成为攻击者的猎物。

通用网络环境中漏洞的逐年增长已经成为常态，并不令人意外。毕竟软硬件种类的极大丰富提供了广阔的温床。在这样的环境下，跨平台漏洞尤其引人注目，8 月份被披露的 Oracle Java 0 Day 漏洞（CVE-2012-4681）同时会影响 Windows、OS X 及 Linux 平台的多种浏览器。而一些专用网络环境也渐渐被挖掘者视为“潜力股”，尤其在 IPv6 和 SCADA 网络中，近来漏洞数量呈爆发性增长。每个人都知道竞争中的主场优势，政治势力也不例外。美国众议院报告称华为、中兴对美国国家安全构成威胁，正是在争夺未来战争中的网络“主场”。

对大部分企业用户来说， Web 应用依然最易受到攻击。分析显示，页面中出现 Web 漏洞的比率接近一半，其中“安全配置错误”和“跨站脚本”占较大比重，而“注入”类漏洞数量低于预期。与此同时，攻击目标也展现了多样性，虚拟机病毒和 MacOS 病毒接连出现；更高明的黑客甚至瞄准了“安全供应链”，入侵 Adobe 公司并用其数字证书签署恶意工具是其中的典型案例。

大部分攻击者的目是窃取和破坏。前者在 2012 年可谓沸沸扬扬，最具代表的有 LinkedIn 网站 650 万用户数据泄露事件和 VMware ESX 源码泄露事件，而后者在 2012 年正在默默的改变。首先，HTTP FLOOD 成为了最主要的 DDoS 攻击方式；其次，短期多次的攻击方式开始出现；最后，广东成为了中国的重灾区，国内近半数攻击针对该地。

不同类型的攻击者各具特色。有组织的势力以此来实现政治目的，DuQu, Wiper, Flame, Gauss 接连出现，中东地区已经成为网络武器的演练场。宗教团体的冲突敏感而激烈，一段 Youtube 视频引发了“燕子行动”，美国多家银行遭受连续的攻击。黑客行动主义不甘寂寞，Anonymous 甚至发布“年终总结”来彰显其“成果”。最常被作为攻击发起点的是僵尸网络和恶意网页， 前者在国内异常活跃，每类僵尸网络平均每天发起攻击 12.2 次；而后者看似沉默却危害巨大，其中包括的木马下载器最多。

总之，2012 年是信息安全多样化的一年。我们处于更复杂的战场中，需要保护的对象越来越多。而敌人，正变得更加狡猾，更加强大。

正文目录

方法和对象 4

背景：漏洞的变化趋势 5

观点 1：漏洞数量逐年上升，其中拒绝服务居第二位，占五分之一，信息泄露、未授权数据库操作类漏洞数增长显著 5

观点 2：云及虚拟化系统漏洞多与市场主流系统相关；新增漏洞数在 2012 年翻倍，且拒绝服务类漏洞接近五分之二 7

观点 3：工业控制系统相关漏洞近两年急剧增加，越权执行漏洞占六成 9

目标：众矢之的-Web 应用 12

观点 4：Web 站点中，每个页面的 Web 漏洞出现率接近一半，“安全配置错误”，“跨站脚本”等数量较多，“注入”类漏洞不再居主要地位 12

观点 5：Web 应用中同样存在主机漏洞，其中“远程信息泄露”数量最多，而“远程拒绝服务”增幅最大 13

手段：危险的 DDoS 攻击 14

观点 6：HTTP FLOOD 成为最主要的 DDoS 攻击方式，占总数的四成 14

观点 7：DDoS 攻击开始出现短期多次的特点，九成以上攻击发生在半小时内，同时半数目标被攻击多次。攻击的平均峰值达到 166.6 Mbps 15

观点 8：广东省成为重灾区，近半 DDoS 攻击指向该地，电信网络占四分之三 17

来源：活跃的僵尸网络和沉默的恶意网页 19

观点 9：国内活跃的僵尸网络，平均每天发起攻击 12.2 次，每天更新僵尸程序 1 次，每周跳转地址 0.25 次。此外，僵尸服务器使用的控制端口中 25 %是借用系统端口 19

观点 10：国内主要僵尸网络的控制服务器近半数位于国外，境内的则集中在浙江、江苏和河北等省市，其中四分之一以上在浙江省台州。运营商网络中，电信占七成以上 21

观点 11：国内的恶意网页中，近半数活跃度较低。从所处地域来看，北京、浙江和广东共占一半 23

观点 12：恶意代码中八成以上是动态库形式，而木马下载器占一半以上 25

热点：主要安全事件 26

事件 1：DuQu, Wiper, Flame, Gauss 接连出现，中东地区成为网络武器的演练场 26

事件 2：Oracle Java 惊现 0 Day 漏洞(CVE-2012-4681)，影响巨大 27

事件 3：LinkedIn 网站 650+万用户数据泄露事件 28

事件 4：黑客入侵 Adobe 公司并用 Adobe 数字证书签署恶意工具 28

事件 5：黑客行动主义盛行，依然活跃的 Anonymous 29

事件 6：Mac OS X 史上最严重的病毒 Flashback 29

事件 7：美国众议院报告称华为中兴对美国国家安全构成威胁 30

事件 8：Bank of America 等多家金融机构接连遭遇 DDoS 攻击 30

事件 9：VMware ESX 源码泄露事件 31

事件 10：首例可感染虚拟机的恶意程序 Crisis 出现 31

作者和贡献者 32

图目录

图 1 2005-2012 年收录的漏洞情况分析 6
图 2 漏洞威胁的分类统计与分析（2005-2012） 7
图 3 2010-2012 年间，漏洞按威胁分类的统计分析 7
图 4 2005-2012 年间收录的云及虚拟化相关漏洞情况分析 8
图 5 云及虚拟化系统漏洞的威胁分类分析 9
图 6 云及虚拟化漏洞按系统的分布情况 9
图 7 工业控制系统公开漏洞数量的年度统计分析 10
图 8 公开漏洞按威胁类型分布的统计分析 11
图 9 公开漏洞所涉及的主要 ICS 系统厂商 12
图 10 远程漏洞扫描服务和渗透测试服务发现的漏洞分布 13
图 11 Web 应用中的主机漏洞 14
图 12 DDoS 攻击的种类和分布 15
图 13 DDoS 的攻击持续时间 16
图 14 被攻击目标遭受的 DDoS 攻击次数 16
图 15 DDoS 攻击的峰值流量（Mbps） 17
图 16 DDoS 攻击目标的国家分布 17
图 17 国内 DDoS 攻击目标的省份分布 18
图 18 遭受 DDoS 攻击的运营商 19
图 19 僵尸网络每日攻击频率 20
图 20 僵尸网络每日更新频率 20
图 21 僵尸网络的每周跳转频率 21
图 22 僵尸网络控制端国际分布 22
图 23 僵尸网络控制端境内分布 22
图 24 僵尸网络控制端的运营商分布 23
图 25 恶意页面监测次数 24
图 26 恶意页面的国际分布 24
图 27 恶意页面的国内分布 25
图 28 恶意代码的文件类型 25
图 29 恶意代码的种类 26

表目录

表 1 可能的预设攻击时间 16
表 2 DDoS 受害城市排名 18
表 3 僵尸网络控制端常用端口 21
表 4 僵尸网络控制端集中的城市 23

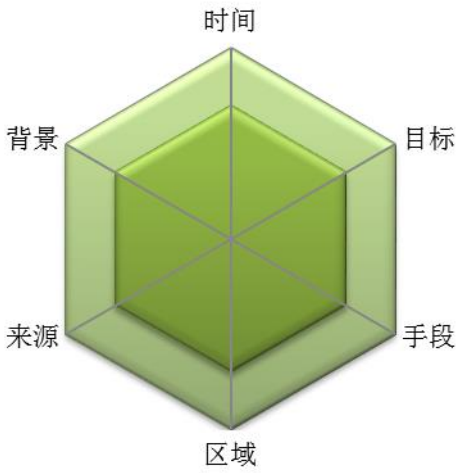
方法和对象

茫茫大漠，一位将军奉命驻守营地。傍晚时分，风云突变，天空中乌云蔽日，伸手不见五指。突然，营地边响起一声惨叫，敌人不知何时已经潜入。将军命令全营戒备，数只精锐小队赶去支援，入侵者却已不见踪影。入夜，敌人时而虚张声势，时而乘乱抢攻，忽东忽西，变幻莫测。他们使用的武器也古怪异常，士兵们只能勉强应对。黎明终于到来，筋疲力尽的将士们，看到的却是远处敌军主力正滚滚而来……

孙子曰：“知己知彼，百战不殆”。战争中，情报的重要性毋庸置疑。战场的气候变化、地理环境，敌人的组织方式、武器装备，以及战略战术目标，都会对胜负产生重要的影响。

企业的 CISO（首席信息安全官）们，面对的也是一场战争。想利用有限的资源获得胜利，除了部署装备和组建团队，及时准确的情报同样至关重要。最近的新漏洞多吗？有没有特别危险的？重要的补丁是不是都经过验证并及时部署了？攻击者中在流行什么新工具？攻击者眼中的价值点都有哪些？哪类操作系统或应用服务经常被侵入？当前流行的恶意软件传播媒介是什么？每个 CISO 都需要一个强大的情报渠道。

绿盟科技威胁响应中心的重要使命之一，就是为企业用户提供打赢信息安全战争所需的情报，而《2012 绿盟科技威胁态势报告》是其中的重要一环。报告将诸多因素组织成了四个维度：背景、目标、手段和来源（我们称之为 STAS 框架）。“背景”描述所处的战场；“目标”阐述敌人的目的；“手段”分析攻击者的武器；“来源”讲解威胁的源头。再加入对“时间”和“区域”两个因素，报告的每个章节都会依照这一框架进行分析。



文中观点均来自与对真实数据的分析，这些数据从绿盟科技的产品、服务和研究中获得，包括 21928 条记录的绿盟漏洞库，376 次渗透测试服务，4890 次远程漏洞扫描服务，82505 次 DDoS 攻击监测，19 类僵尸网络的 4624452 次行为跟踪， 5928537 次恶意网页行为监测，以及 211 人参与的“2012 年 10 大安全事件” 评选。

所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在报告中。

背景：漏洞的变化趋势

本章主要基于绿盟科技漏洞库信息来分析漏洞的变化趋势。截至到 2012 年 12 月，绿盟科技漏洞库已收录 21928 条漏洞信息。为了更好地反映漏洞近年来的变化趋势，我们主要选择 2005 至 2012 年间的漏洞数据进行统计分析；而且还专门对云计算及虚拟化系统、工业控制系统这两个业内热点领域的漏洞情况进行了具体的分析研究。

观点 1：漏洞数量逐年上升，其中拒绝服务居第二位，占五分之一，信息泄露、未授权数据库操作类漏洞数增长显著

通过统计分析 2005 年至 2012 年公布漏洞情况，可以发现每年公布的新增漏洞数目总体呈上升的趋势，而且 2012 年所公布的漏洞数，相对于往年增势明显，如图 1 所示。

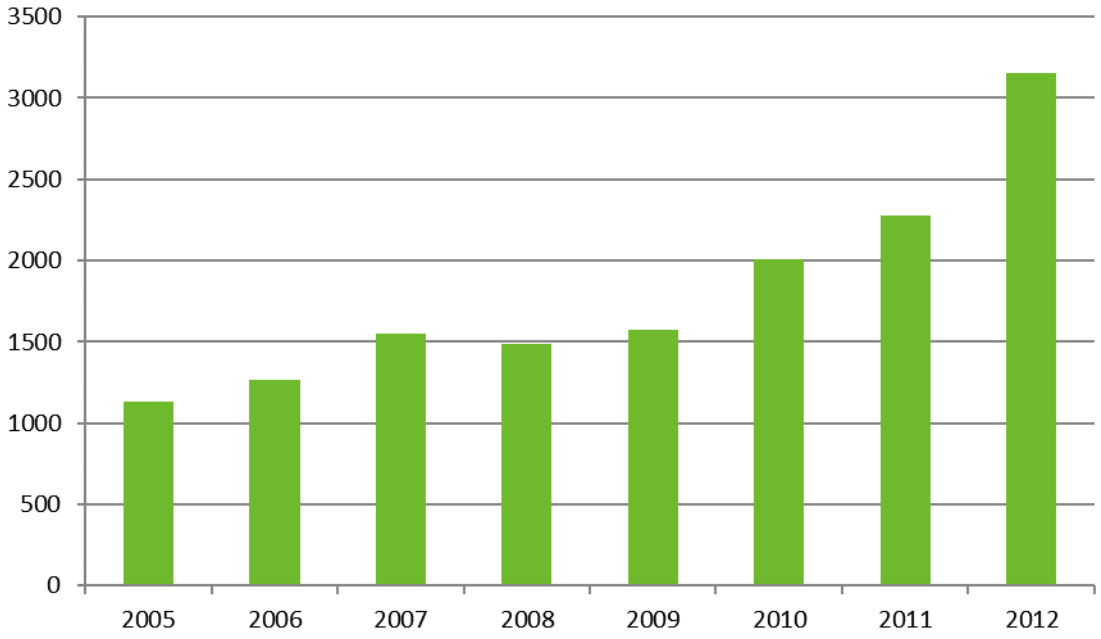


图 1 2005-2012 年收录的漏洞情况分析

通过对 2005-2012 年间发布的漏洞按漏洞威胁进行分类统计，分析结果（图 2）表明：获取普通用户权限、拒绝服务攻击、获取管理用户权限、信息泄露相关的漏洞占据主导地位。但从图 3 所示的 2010-2012 年间的漏洞威胁分类的趋势分析结果来看，在每年的新增漏洞中，获取普通用户权限类漏洞数量持续占据优势地位；拒绝服务类漏洞数则是逐年稳步增长，约占总体漏洞数的五分之一，并在近两年持续保持第二的位置。

值得注意的是，信息泄露及未授权数据库操作相关的漏洞数在 2012 年间有了飞速的增长，无论是新增漏洞的数量还是在 2012 年内所有新增漏洞数中所占的比例，与往年相比都增长显著；目前已经分别跃居第三和第五的地位（图 3）。

信息泄露及非授权数据库操作相关的漏洞数快速增加的原因，可能与 2011 年以来频繁发生的信息泄露事件相关。

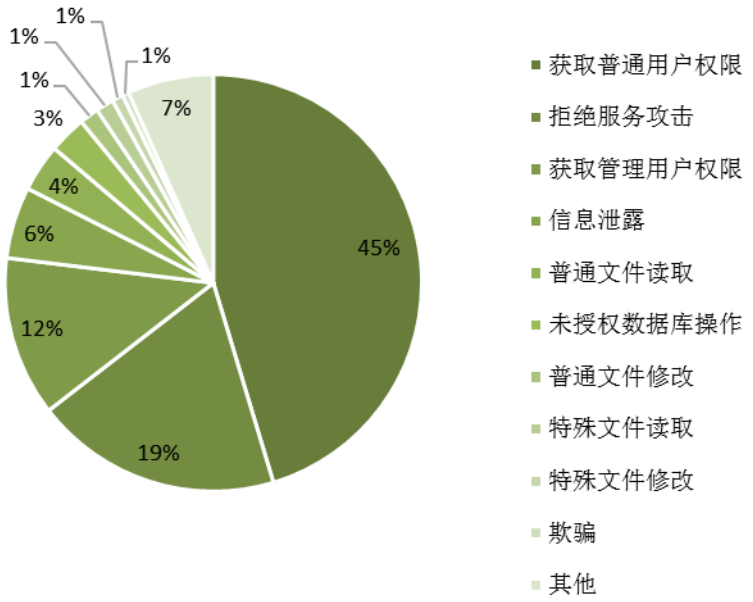


图 2 漏洞威胁的分类统计与分析（2005-2012）

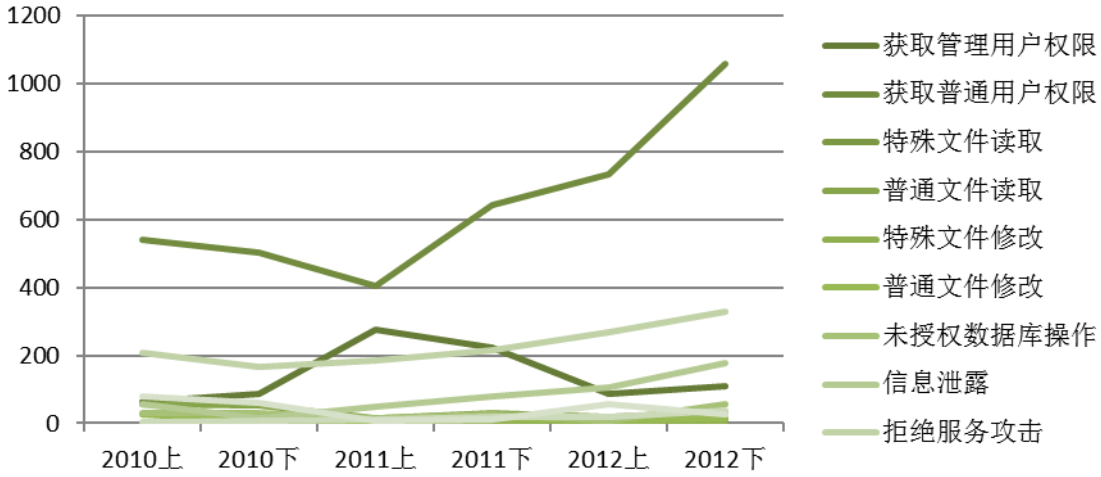


图 3 2010-2012 年间，漏洞按威胁分类的统计分析

观点 2：云及虚拟化系统漏洞多与市场主流系统相关；新增漏洞数在 2012 年翻倍，且拒绝服务类漏洞接近五分之二

随着云计算和虚拟化技术的快速发展与应用，云计算及虚拟化系统的安全问题在近几年也得到了业内的持续关注与研究。在此背景下，为了更好地了解当前云计算和虚拟化系统的

脆弱性，我们对云计算和虚拟化系统相关的漏洞进行了专门的整理与统计分析，分析结果如下：

根据历年新增漏洞数的统计结果（图 4）可知：2007 年之前公布的云计算和虚拟化系统相关漏洞很少；在 2007 至 2011 年，每年的新增漏洞数大致保持在 60 个左右；而在 2012 年新增漏洞数（137）却是显著增长，与前几年相比超过了一倍还多。

出现这种情况的原因可能是 2007-2011 年期间，云和虚拟化领域还主要处在具体应用的探索期，可供研究分析的云计算及虚拟化系统或应用软件相对较少，因此在这段时间内每年所能发现的漏洞数差别不大。而近两年随着云计算和虚拟化的应用服务的进一步发展，能够供研究、分析的云服务类产品的数量及种类也逐步增多，这可能是造成 2012 年云和虚拟化相关漏洞的突发式增多的主要原因。

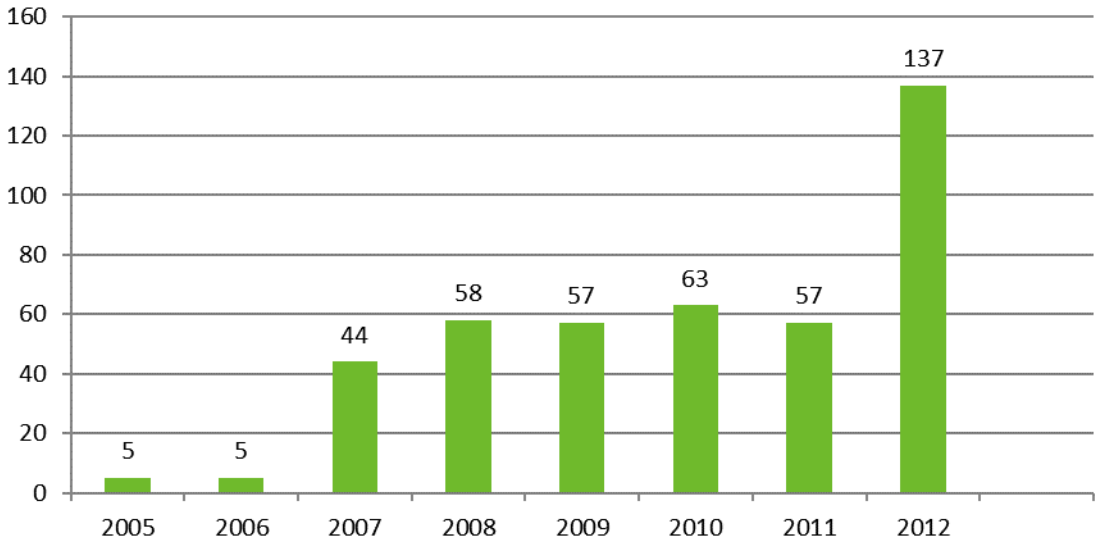


图 4　2005-2012 年间收录的云及虚拟化相关漏洞情况分析

从云计算及虚拟化系统的漏洞威胁分类分析结果来看，获取普通用户权限、拒绝服务攻击、获取管理用户权限、信息泄露相关的漏洞同样占据主导地位（如图 5 所示）。但通过对比图 2 与图 5 的内容可知，在云计算及虚拟化系统的相关漏洞中，拒绝服务类漏洞的所占比例明显偏高（27.5%），而在 2012 年新增的相关漏洞中，拒绝服务类的漏洞更是占到了 38%，接近五分之二。

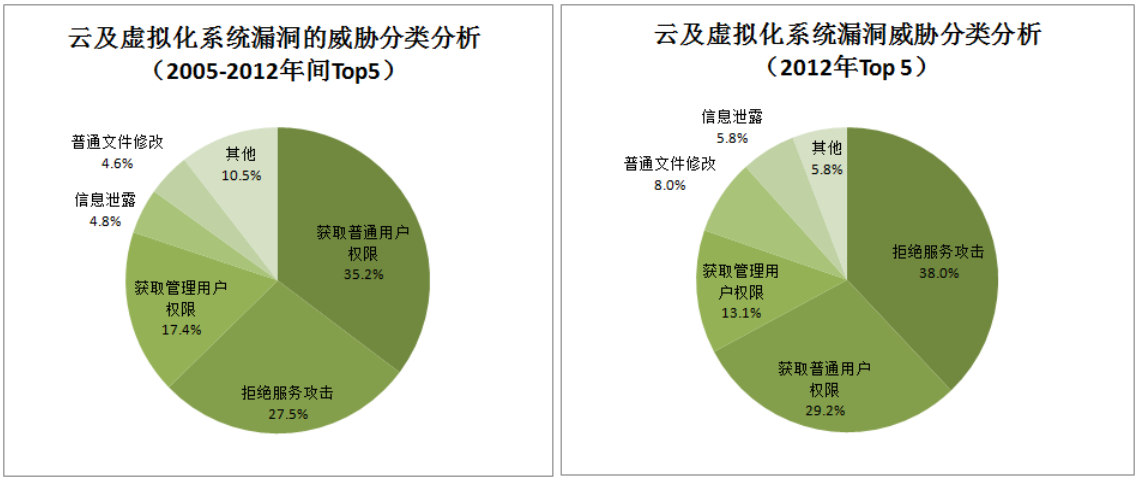


图 5 云及虚拟化系统漏洞的威胁分类分析

图 6 的统计分析结果则表明，目前已发现公布的云计算及虚拟化漏洞主要是业内主流云计算及虚拟化系统，诸如 VMware、Xen\Citrix 中存在的漏洞。

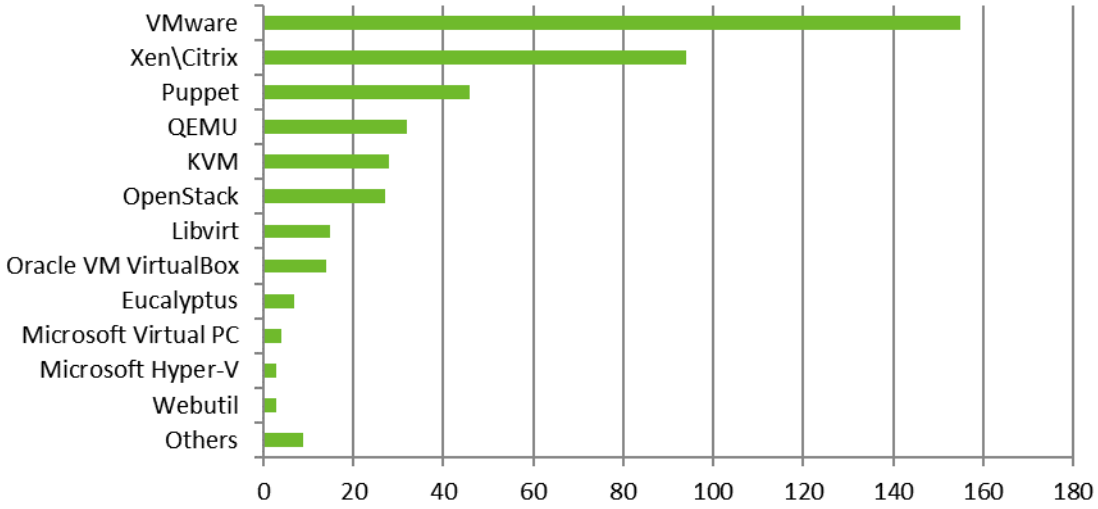


图 6 云及虚拟化漏洞按系统的分布情况

观点 3：工业控制系统相关漏洞近两年急剧增加，越权执行漏洞占六成

截止到 2012 年 11 月底，绿盟科技安全漏洞库中共收录到 216 个与工业控制系统相关的漏洞，在这里我们主要按发布时间、威胁类型、厂商分布等几个角度对这些漏洞进行统计分析，结果如下：

图 7 给出了从 2007 年到 2012 年 11 月之间所发布的工业控制系统公开漏洞按年度进行统计分析的结果。从图中可以很明显地看出：在 2011 年之前，公开披露的工业控制系统相关漏洞的数量相当少。但在 2011 年出现了井喷现象，并持续到 2012 年。这可能和 2010 年的 Stuxnet 蠕虫引起大家对工业控制系统安全问题的广泛关注有关。我们预计至少在未来一段时间内，工业控制系统仍然将是漏洞研究者们感兴趣的话题。

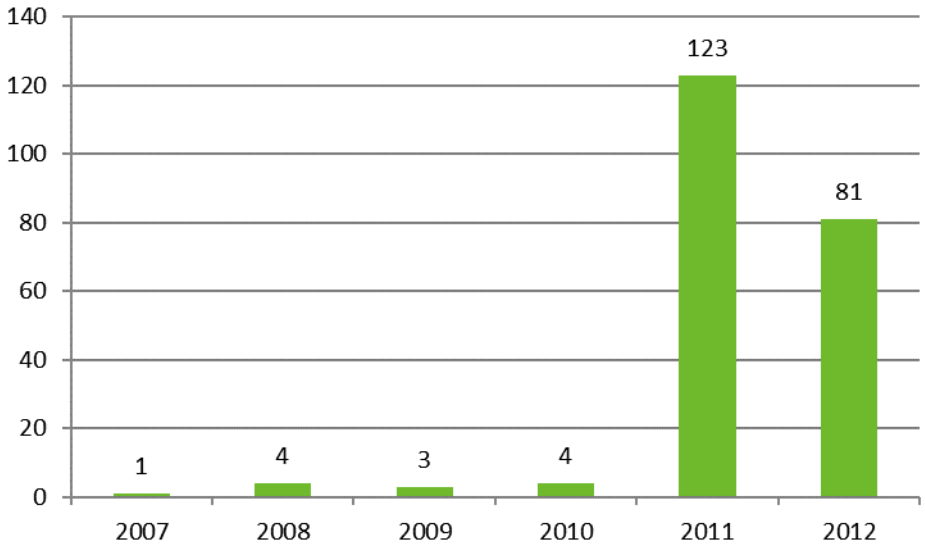


图 7 工业控制系统公开漏洞数量的年度统计分析

由于工业控制系统更加强调对系统的控制能力，因而它所关注的安全问题多是防止违规的越权操作以及避免业务的中断，保障控制系统的实时、正常运行。因此我们在分析工业控制系统漏洞的时候，采用了新的威胁分类标准。按照漏洞可能造成的危害，分为越权执行、越权写入、越权读取、拒绝服务四大类威胁：

- 越权执行，指的是缓冲区溢出、命令执行、SQL 注入等可以直接对系统造成较大程度控制的漏洞。
- 越权写入，指的是能以某种方式在系统上写入文件、修改用户密码和系统配置等，但无法直接执行代码的漏洞。
- 越权读取，指的是能读取指定或任意文件、内存信息等的漏洞。
- 拒绝服务，指的是可导致进程崩溃、死锁等，使软件无法正常工作的漏洞。

图 8 即为我们按威胁类型对工业控制相关漏洞进行分析的结果。分析结果表明：越权（执行、写入、读取）类漏洞占据了绝大多数，而其中危害最严重的越权执行类漏洞数量也是最多的，约占全部漏洞的 61.6%。

通过对越权执行类漏洞的详细分析发现：这类漏洞又以缓冲区溢出类漏洞最多，约占该类漏洞的一半以上。从整体上看，近年来缓冲区溢出类漏洞无论是绝对数量还是相对比例都呈下降趋势，而在工业控制系统领域却出现较多缓冲区溢出类漏洞的现象，我们认为其主要原因可能是因为以前研究者对此类漏洞关注较少，所以很多软件中累积了大量此类漏洞，而当研究者们开始对这些软件进行检查时，积累多年的漏洞就暴露了出来。

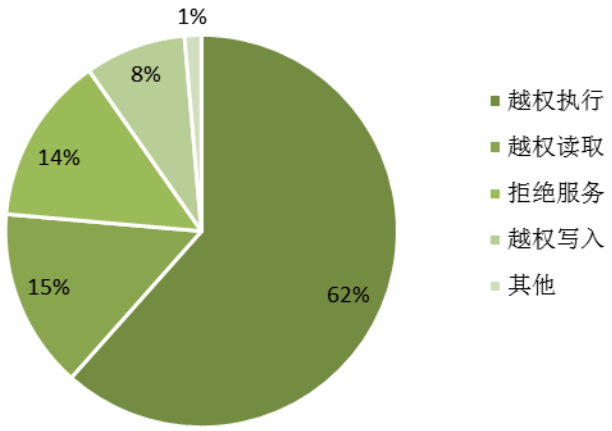


图 8 公开漏洞按威胁类型分布的统计分析

图 9 给出了公开漏洞所涉及的主要工业控制系统厂商以及各厂商的相关漏洞所占的比例。

但需要说明的是：各厂商产品的漏洞数量不仅与产品自身的安全性有关，也和厂商的产品种类、产品的复杂度以及受研究者关注的程度等多种因素有关。所以，我们并不能简单地认为，公开漏洞数量越多的厂商，其产品就越不安全。

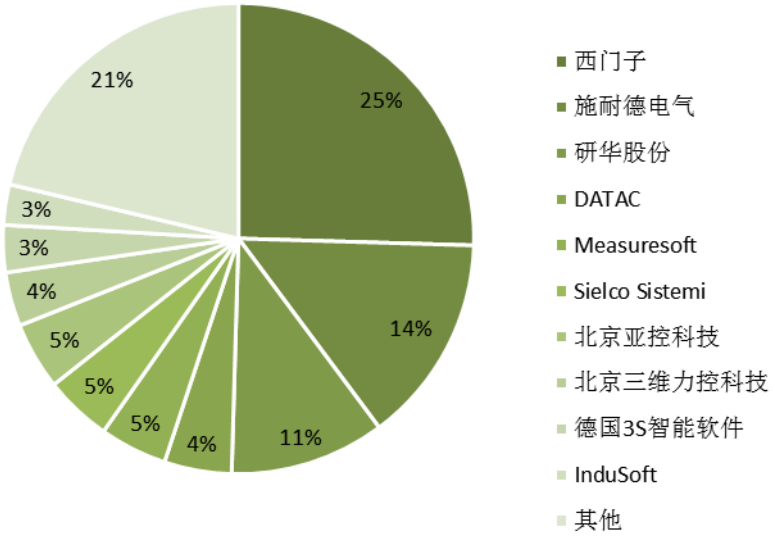


图 9 公开漏洞所涉及的主要 ICS 系统厂商

目标：众矢之的-Web 应用

2012 年 11 月末，据报道淘宝和天猫营业额达到 1 万亿元，相当于中国 GDP 的 2%。同期，新浪微博用户超过 4 亿，智能手机用户达到 2.7 亿，网络的繁荣给用户带来了诸多便利。然而，巨大的利益也蕴含着巨大的风险。在这一年中，网络信息窃取和金融欺诈事件层出不穷，从 LinkedIn 的信息泄露，到美国金融机构连续遭受攻击，每一次都让人惊心动魄。Web 应用正成为一座金矿，既引来了淘金者，也引来了窃贼和强盗。绿盟科技威胁响应中心对 376 次渗透测试服务和 4890 次远程漏洞扫描服务的统计数据进行分析，并得出以下观点。

观点 4：Web 站点中，每个页面的 Web 漏洞出现率接近一半，“安全配置错误”，“跨站脚本”等数量较多，“注入”类漏洞不再居主要地位

统计显示，平均每个站点包含页面 489.4 个，每个页面中 Web 漏洞出现率为 46.9%，高危 Web 漏洞出现率为 1.9%。

如下图所示，远程漏洞扫描服务发现的漏洞中“安全配置错误”最多，其次是“失效的身份认证和会话管理”和“没有限制 URL 访问”。而渗透测试服务中发现的漏洞以“跨站脚本”最多，其次是“安全配置错误”和“失效的身份认证和会话管理”。无论从哪个角度来看，“注入”类漏洞不再居主要地位。

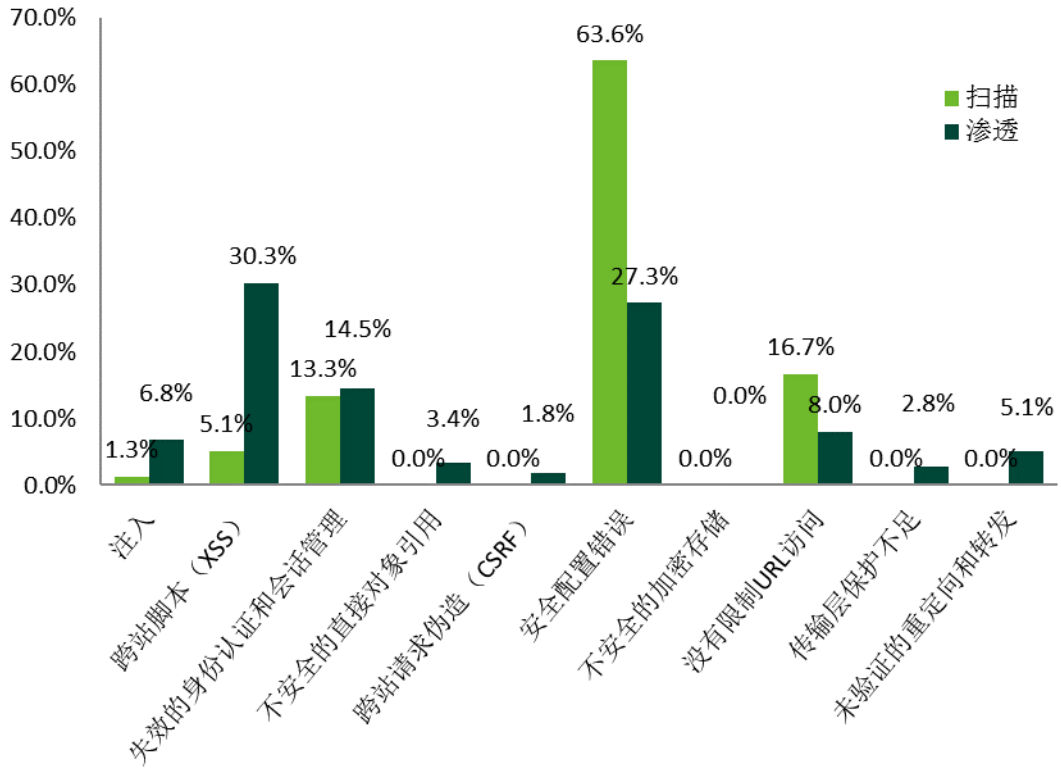


图 10 远程漏洞扫描服务和渗透测试服务发现的漏洞分布

观点 5：Web 应用中同样存在主机漏洞，其中“远程信息泄露”数量最多，而“远程拒绝服务”增幅最大

Web 应用的宿主机也面临被攻击的危险，他们中存在大量的普通漏洞，可能被攻击者利用。其中“远程信息泄露”数量最多，占 68.6%，与上半年相比增加 0.9%。其次是“远程拒绝服务”，占 17.3%，与上半年相比增加 5.1%，增幅最大。

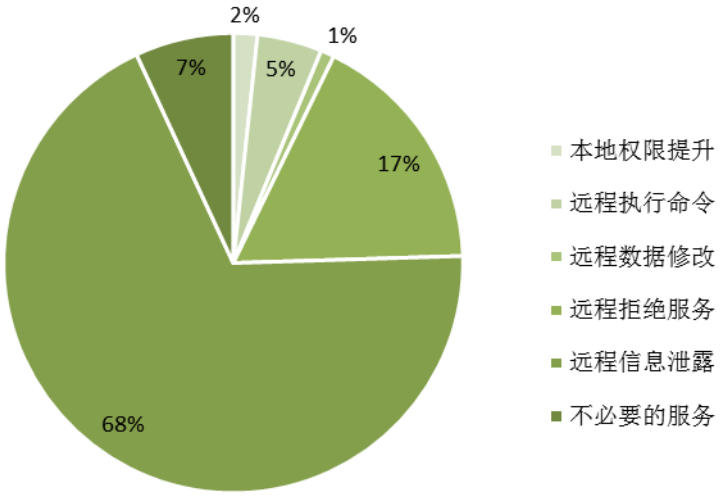


图 11 Web 应用中的主机漏洞

手段：危险的 DDoS 攻击

一般来说，攻击者的直接目的往往非常单纯：窃取或破坏。窃取的手段复杂多变；破坏的方法则分化为以下两类。首先，对于少数机密目标，需要使用 APT 才能接触到核心资产；其次，对于大部分公开目标，简单粗暴的 DDoS 攻击就成了最佳选择。2012 年的 DDoS 攻击中，HTTP FLOOD 终于跃居榜首，短期多次的间歇攻击越来越普遍，而地域性也更加明显。绿盟科技威胁响应中心与合作伙伴，对 2012 年发现的 82505 次 DDoS 攻击进行分析，并得出以下观点。

观点 6：HTTP FLOOD 成为最主要的 DDoS 攻击方式，占总数的四成

根据最新统计结果，从数量上看，HTTP FLOOD 成为了最主要的 DDoS 攻击方式，共占 42.7%；其次是 TCP FLOOD（包括 SYN FLOOD，PSH FLOOD 等）攻击，占 28.9%；DNS FLOOD 攻击则占

21.4%。另一个值得关注的现象是混合 DDoS 攻击，由于其组成复杂多样，这里并未给出相关数据。但在研究中我们发现，同时利用多种 DDoS 方法攻击单个目标的现象越来普遍。

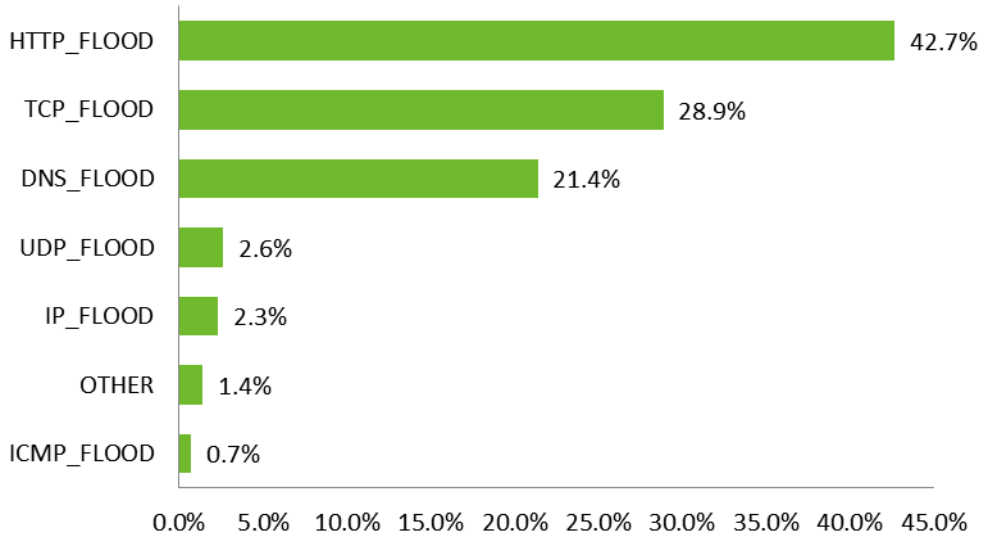


图 12 DDoS 攻击的种类和分布

观点 7：DDoS 攻击开始出现短期多次的特点，九成以上攻击发生在半小时内，同时半数目标被攻击多次。攻击的平均峰值达到 166.6 Mbps

一半以上的 DDoS 攻击只持续很短时间（十分钟以内），而三十分钟之内的攻击占到了 93.2%。同时，也有的攻击会持续很长时间，甚至超过 96 小时。此外，数据显示，持续时间为特定长度的攻击，数量明显超过同类， 包括 5 分钟、20 分钟、30 分钟、60 分钟、500 分钟和 5000 分钟。这可能表示一些攻击者使用了类似的攻击工具，以及预设的攻击持续时间。下表给出了一些典型预设时间的攻击出现次数。

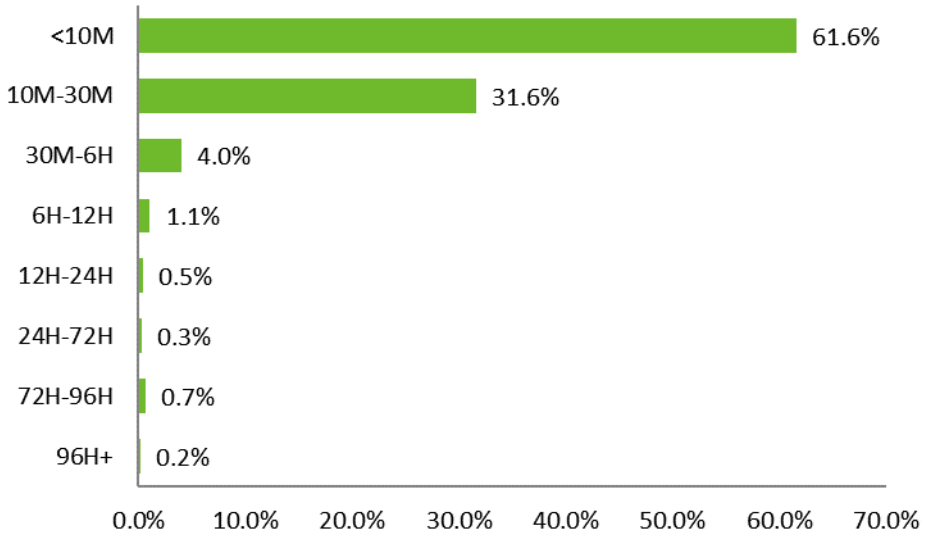


图 13 DDoS 的攻击持续时间

持续时间（分钟）	攻击次数
5	1695
20	208
30	22886
60	111
500	196
5000	337

表 1 可能的预设攻击时间

攻击者往往会对同一目标发起多次攻击。如下图所示，49.3%的被攻击对象在 2012 年遭受过不止一次 DDoS，而 5.2%的被攻击对象甚至遭受到超过 10 次 DDoS。

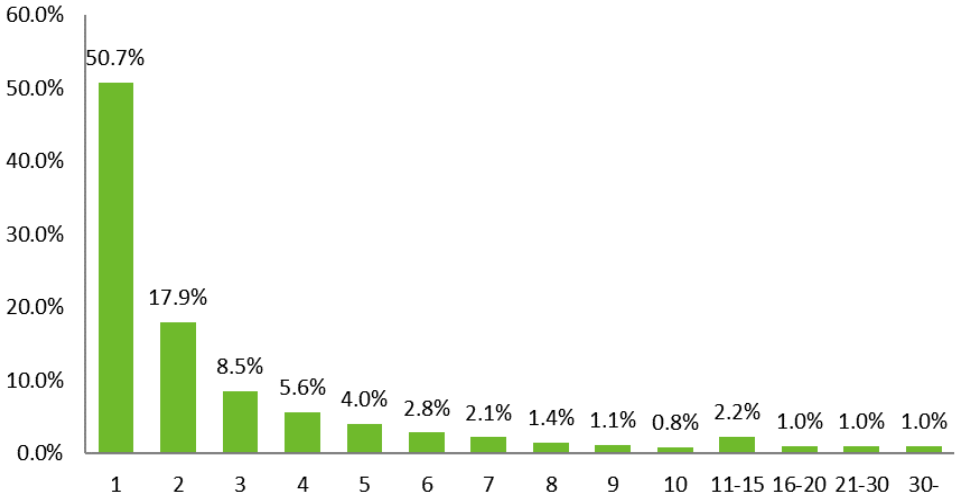


图 14 被攻击目标遭受的 DDoS 攻击次数

对于持续时间较长的 DDoS 攻击，我们统计了其峰值流量。此类攻击的最低峰值 34 Mbps，最高峰值 23.8 Gbps，平均峰值 166.6 Mbps。70%的峰值在 50 Mbps 以下。需要注意的是，由于类型不同，并不是攻击流量越大，带来的伤害就越大。

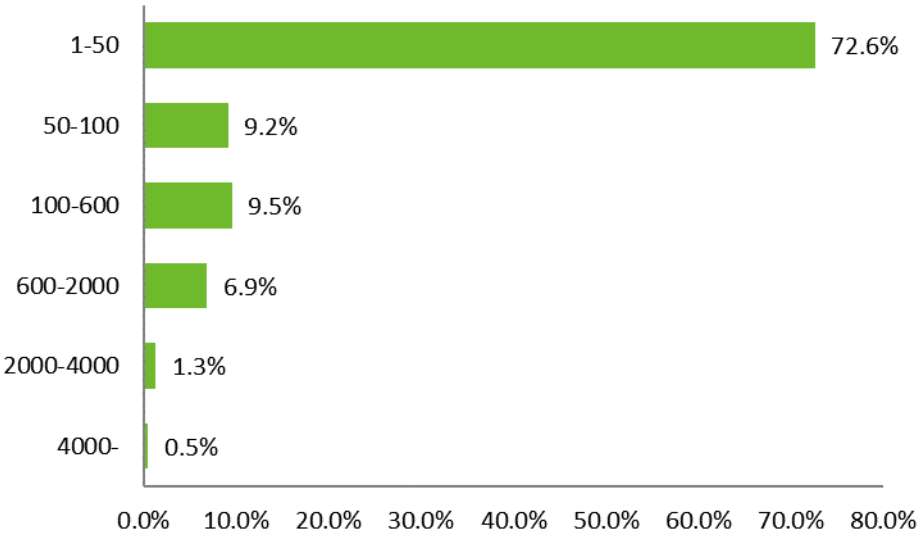


图 15 DDoS 攻击的峰值流量（Mbps）

观点 8：广东省成为重灾区，近半 DDoS 攻击指向该地，电信网络占四分之三

我们监测的范围主要是中国大陆地区，所以发现的 DDoS 攻击也大多针对这一区域，大约占总数的 84.8%。此外，也有部分攻击针对其他国家和地区，主要目标位于美国、香港、韩国、土耳其等地。

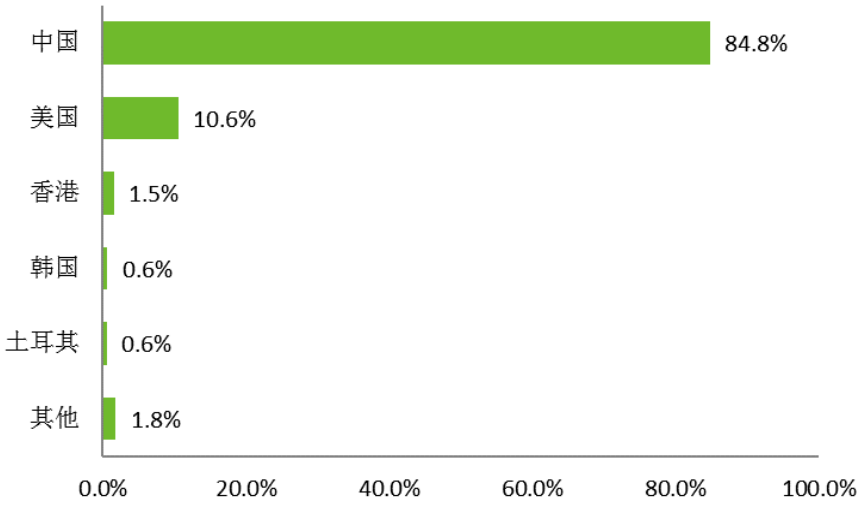


图 16 DDoS 攻击目标的国家分布

中国大陆地区各省中，广东受到 DDoS 攻击数量最多，占 48.3%，其次是浙江、江苏、湖南等地。北京和上海仅占 3.1%和 1.0%。

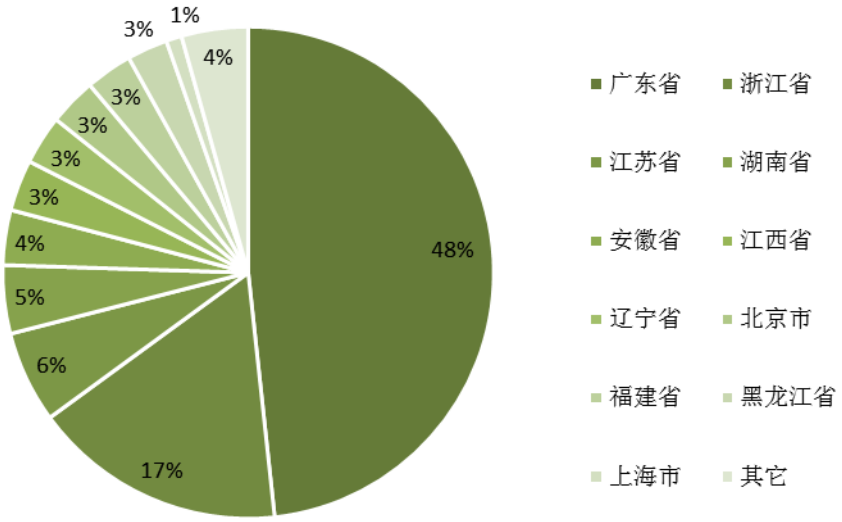


图 17 国内 DDoS 攻击目标的省份分布

本期监测区域包括了全国 204 个城市和地区，其中受害最严重的是广东东莞、湛江、深圳、茂名，以及浙江绍兴、杭州等地。下表列出了受害最多的 10 个城市。

省份	地市	受攻击数量
广东省	东莞市	6013
广东省	湛江市	5857
广东省	深圳市	4365
浙江省	绍兴市	4197
浙江省	杭州市	2080
湖南省	长沙市	2040
广东省	茂名市	1784
北京市	北京市	1695
江西省	南昌市	1348
辽宁省	大连市	1319

表 2 DDoS 受害城市排名

所有攻击中，目标位于电信网络中的占 75.6%，联通网络中的占 20.4%。其他提供商主要包括网联光通、景安计算机网络、中国万网、阿里巴巴等。根据 CNZZ 的一份统计显示，用户中使用电信互联网接入服务的占总数一半以上，这可能是造成以上现象的原因之一。

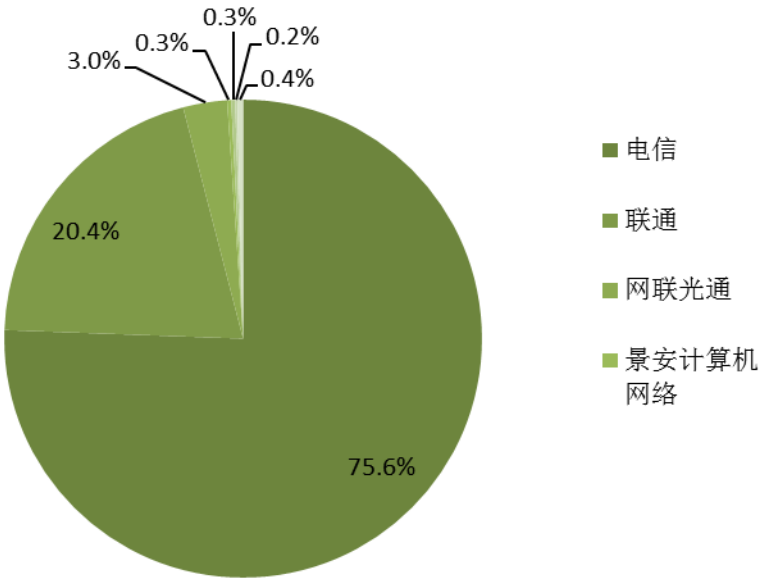


图 18 遭受 DDoS 攻击的运营商

来源：活跃的僵尸网络和沉默的恶意网页

近年来，攻击者表现出两个明显的变化趋势。首先，逐利性的加强使得黑客更多地考虑时间成本和实际收益间的关系；其次，技术的发展使得他们的隐蔽性和攻击性更强。为了获取更多地猎物，猎人会利用陷阱，以较高的性价比随机捕获小型猎物；同时，也会长期追踪大型猎物，寻找时机用猎枪一击必杀。优秀的攻击者像猎人一样狡猾，他们用恶意网页布置陷阱，而僵尸网络就是他们手中的猎枪。绿盟科技威胁响应中心 2012 年一方面利用蜜网系统监测了 5928537 次恶意网页行为，另一方面跟踪了中国境内的 19 类主流僵尸网络的 4624452 次行为记录。

观点 9：国内活跃的僵尸网络，平均每天发起攻击 12.2 次，每天更新僵尸程序 1 次，每周跳转地址 0.25 次。此外，僵尸服务器使用的控制端口中 25 %是借用系统端口

僵尸网络的活跃程度主要体现在三个方面。第一，发动攻击的频率，表现出僵尸网络的攻击性，我们称之为“攻击频率”；第二，僵尸程序的更新频率，每次更新意味着该网络具

备了更强的攻击能力或隐蔽能力，我们称之为“更新频率”；第三，僵尸控制端会不断改变自身的 IP 地址来隐藏自身，防止跟踪，我们称之为“跳转频率”。

根据我们的监测，对于国内主流僵尸网络，每个控制端的活跃期内，其平均攻击频率为每天 12.2 次。其中以 neglemir 最为活跃，达到了每天 87.2 次。攻击频率最高的五类僵尸网络如下图所示。

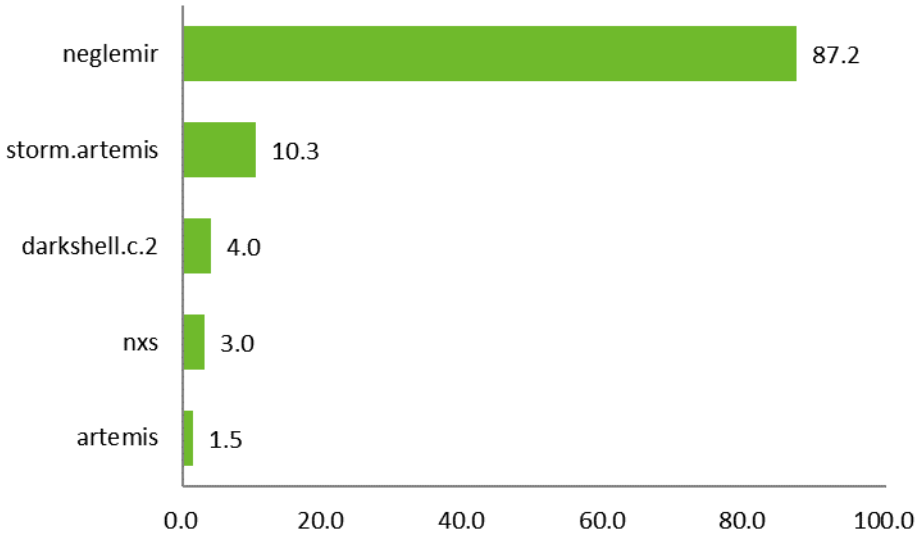


图 19 僵尸网络每日攻击频率

国内主流僵尸网络的每个控制端的活跃期内，平均更新频率为每天 1 次。其中以 darkshell.c.2 最为活跃，达到了每天 2.5 次。更新频率最高的五类僵尸网络如下图所示。

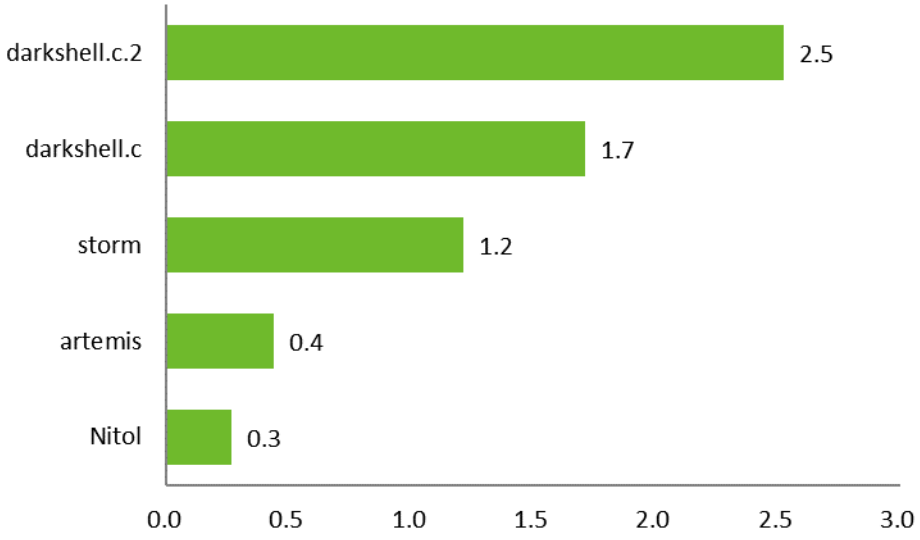


图 20 僵尸网络每日更新频率

国内主流僵尸网络的每个控制端的活跃期内，平均跳转频率为每周 0.25 次。其中以 flyboy 最为活跃，达到了每周 0.56 次。跳转频率最高的五类僵尸网络如下图所示。

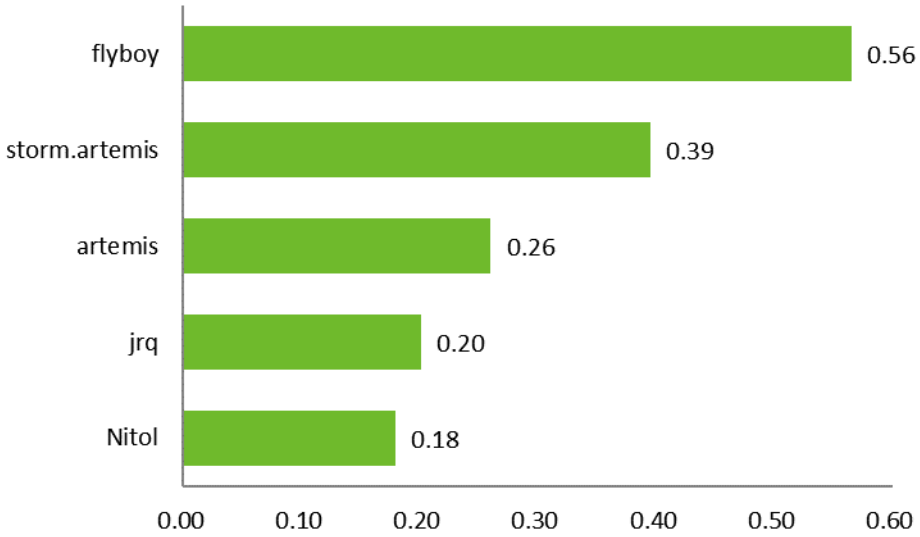


图 21 僵尸网络的每周跳转频率

僵尸网络控制端所使用的端口中，25%是借用了小于 1023 的系统端口，其余则是自定义端口。使用次数最多的是 75 号端口，最为频繁的 5 个如下表所示。

端口	百分比
75	12.7%
7777	8.3%
8888	7.9%
8000	7.1%
1234	4.8%

表 3 僵尸网络控制端常用端口

观点 10：国内主要僵尸网络的控制服务器近半数位于国外，境内的则集中在浙江、江苏和河北等省市，其中四分之一以上在浙江省台州。运营商网络中，电信占七成以上

虽然监测对象主要是境内的僵尸网络，但其控制服务器并不集中在中国。有近半数位于海外，其中以美国、英国、日本等地为主。

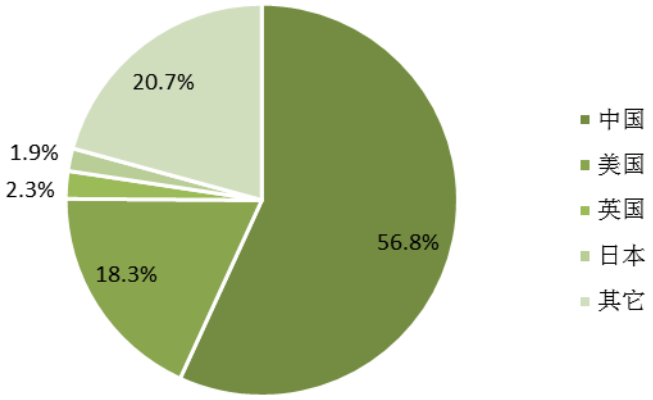


图 22 僵尸网络控制端国际分布

在中国境内的控制服务器中，以浙江、江苏和河北最多。根据工信部相关报告显示，2011 年完成的电子信息产业固定资产投资方面， 以上三省均名列前十，而上海和北京则位于在第 12 和第 22。可见信息产业快速发展的地区，往往更需要加强信息安全防护。

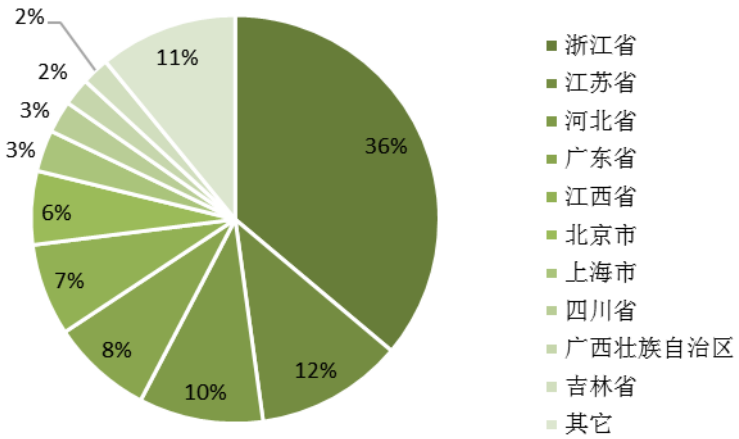


图 23 僵尸网络控制端境内分布

就单一城市而言，最为集中的是浙江省台州市，占总数四分之一以上的控制服务器集中于此地。排名前十的城市列表如下：

省份	城市	所占比例
浙江省	台州市	27.4%
河北省	邢台市	6.6%
北京市	北京市	5.8%
广东省	深圳市	4.7%
江西省	景德镇市	4.7%
浙江省	金华市	4.7%
江苏省	镇江市	4.7%
江苏省	扬州市	3.3%
上海市	上海市	3.3%
河北省	沧州市	2.2%

表 4 僵尸网络控制端集中的城市

从控制服务器所属的运营商来看，电信占据了七成以上，其次是联通和移动。根据 CNZZ 的一份统计显示，用户中使用电信互联网接入服务的占总数一半以上，这可能是造成以上现象的原因之一。

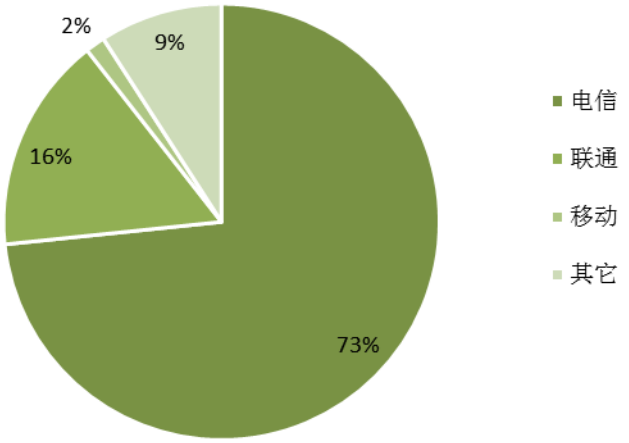


图 24 僵尸网络控制端的运营商分布

观点 11：国内的恶意网页中，近半数活跃度较低。从所处地域来看，北京、浙江和广东共占一半

绿盟科技威胁响应中心监测的恶意网页主要指被监测到恶意行为的 URL，包括挂马页面和恶意软件下载页面，范围以中国大陆地区为主。其中 47.8%的恶意页面仅被监测到一次或两次恶意行为，而 1.8%的页面有一千次以上恶意行为被记录。

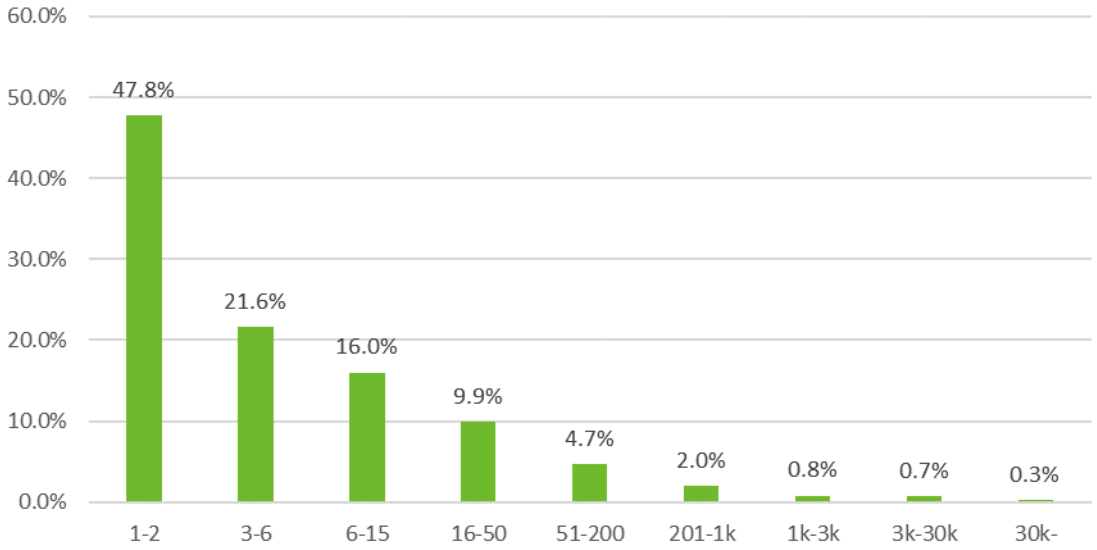


图 25 恶意页面监测次数

从恶意网页的分布来看，由于监测范围的关系，其中 79.6%位于中国大陆地区，其次是美国占 15.4%，再次是加拿大、香港、马来西亚等地。

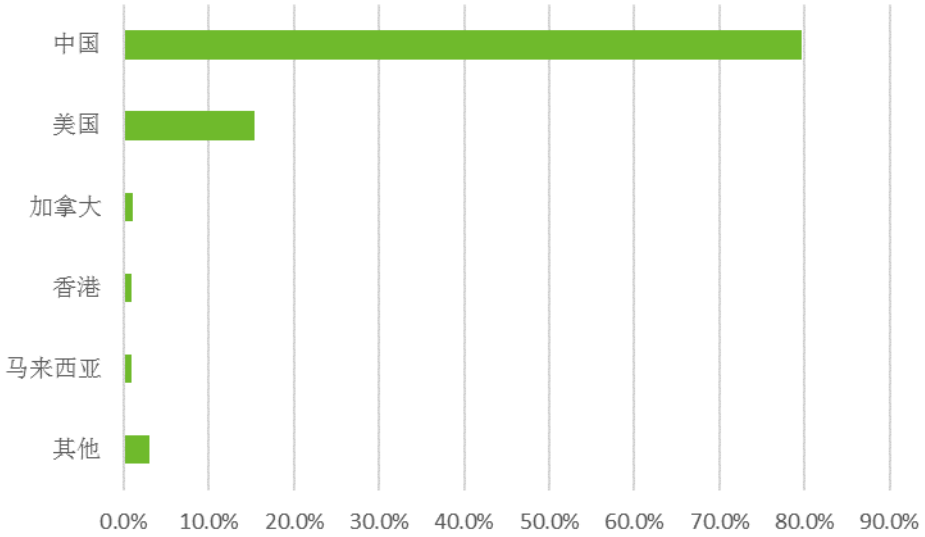


图 26 恶意页面的国际分布

在中国境内的恶意网页中，以北京、浙江和广东最多，共占 50.3%。与上半年相比变化较为显著的是，天津市由第九升至第四，而江苏省由第三降至第六。

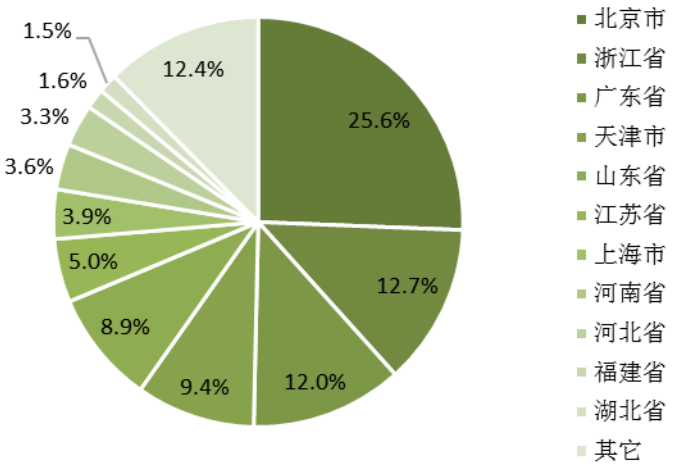


图 27 恶意页面的国内分布

观点 12：恶意代码中八成以上是动态库形式，而木马下载器占一半以上

2012 年来自恶意网页捕获的恶意代码中，DLL 格式的动态链接库最多，占 84.7%，其他主要包括执行文件、临时文件、图形文件、系统文件等。

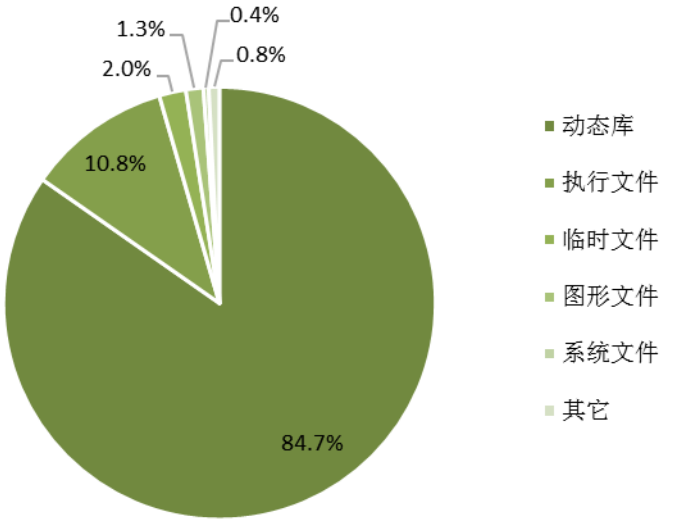


图 28 恶意代码的文件类型

恶意代码中，TrojanDownloader 数量最多，占总数的一半以上，其它依次是 Trojan、TrojanSpy、TrojanPWS、Worm 和 Backdoor 等。

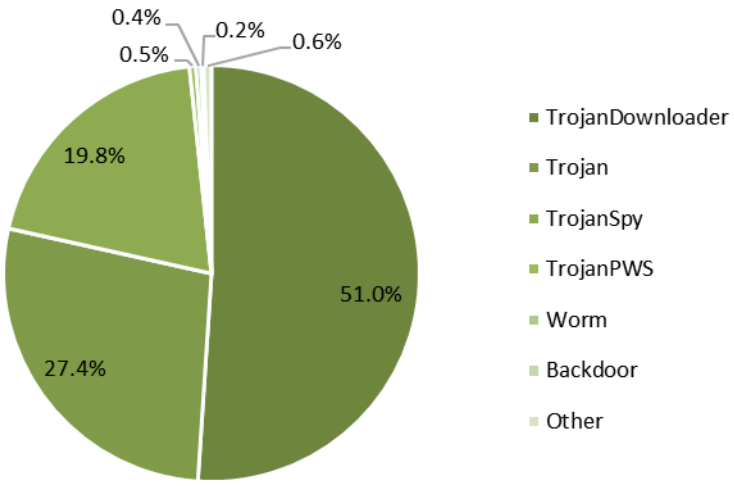


图 29 恶意代码的种类

热点：主要安全事件

2012 年发生了很多重要的安全事件，其中一些现在只受到小部分人关注，但随着时间流逝，却可能会对安全行业，甚至整个世界造成持续的影响。为了选取出最具影响力的事件，绿盟科技威胁响应中心通过问卷调查的方式，由 211 位参与者，对所有候选事件进行评判，本章给出了其中的 Top10。

事件 1：DuQu，Wiper，Flame，Gauss 接连出现，中东地区成为网络武器的演练场

摘录来源：Kaspersky，Symantec

原文链接：

http://www.symantec.com/connect/blogs/new-duqu-sample-found-wild
http://www.symantec.com/connect/blogs/shamoon-attacks
http://365.rsaconference.com/servlet/JiveServlet/previewBody/3697-102-1-4855/BR-208_Bencsath.pdf
http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons

热点简介：

2012 年之前，全世界已知的网络武器只有 Stuxnet 和 Duqu 两种，其攻击目标是伊朗。2012 年网络武器的部署范围已经覆盖到同伊朗接壤的其它中东地区国家。根据 Kaspersky 统计数据表明网络武器同中东地区具有明显的地域关联。

Duqu 最早于 2011 年 9 月被发现，在安全厂商对 Duqu 开始调查分析后，Duqu 幕后操纵者销毁所有活动的痕迹。2012 年 2 月 Symantec 在伊朗发现了一款 Duqu 新版本驱动，但这款新版本的核心模块一直未被检测到。

Wiper 于 2012 年 4 月底开始在伊朗大范围传播。Wiper 恶意软件的编写者采取所有可能措施，并销毁所有可能被用于分析它的数据。所以，Wiper 攻击结束后，几乎任何关于这款恶意程序活动的痕迹都未留下。

Flame 于 2012 年 5 月被曝光，它是目前为止所知道的最复杂网络武器。Flame 是一款木马同时具有蠕虫特征的恶意软件。

miniFlame 于 2012 年 6 月初被检测到，miniFlame 和 Flame 基于同一个架构平台。它既能够做为独立的网络间谍程序执行特定功能，又能够做为 Flame 或 Gauss 的组件执行恶意功能。

Guass 于 2012 年 7 月被检测到，它具有模块化结构，支持远程部署新功能。通过 Guass 模块名称分析发现其模块的命名似乎是为了纪念多个著名数学家和思想家，包括 Kurt Gödel(哥德尔)，Carl Friedrich Gauss(高斯)与 Joseph Louis Lagrange(拉格朗日)。

Shamoon 于 2012 年 8 月中旬攻击全球最大的石油企业 ARAMCO(沙特阿美石油公司)从而被披露，Kaspersky 认为 Shamoon 是在模仿网络武器 Wiper。资讯安全公司给予 Shamoon 的评价有:amateurish(业余)与 copycat(抄袭)。

事件 2：Oracle Java 惊现 0 Day 漏洞(CVE-2012-4681)，影响巨大

摘录来源：FireEye

原文链接：

http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html
https://community.rapid7.com/community/metasploit/blog/2012/08/27/lets-start-the-week-with-a-new-java-0day

热点简介：

2012 年 8 月 26 日，资讯安全公司 FireEye 披露 CVE-2012-4681 漏洞，该公司安全研究员 Atif Mushtaq 发现 CVE-2012-4681 漏洞最初的利用代码是部署在网站 ok.XXX4.net。当用户通过电子邮件等方式引导连结到该网站时，网页内含的 Java 程序能够绕过 Java 的沙盒保护机制，并下载安装恶意程序 dropper（Dropper.MsPMs）。8 月 27 日经 Rapid 7 公司验证，该漏洞利用代码可影响 Windows、OS X 及 Linux 平台的多款浏览器。

事件 3：LinkedIn 网站 650+万用户数据泄露事件

摘录来源：LinkedIn

原文链接：

http://www.dagensit.no/article2411857.ece
http://nakedsecurity.sophos.com/2012/06/06/millions-of-linkedin-passwords-reportedly-leaked-take-action-now/
http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/

热点简介：

2012 年 6 月 6 日，挪威 IT 网站 Dagens IT 率先报道经 SHA-1 散列的 LinkedIn 网站用户密码出现在俄罗斯一个黑客论坛，并且攻击者正寻求帮助以试图加快破解密码的速度。随后 Sophos 高级技术顾问 Graham Cluley 在 Sophos 博客中称一个包含 6,458,020 个 unsalted SHA-1 散列密码的文件(不包含邮箱地址)已在网上流传，Sophos 已经确认该文件至少部分包含 LinkedIn 网站用户密码。同日,在社交网站 LinkedIn 担任 Director 职位的 Vicente Silveira 在该网站官方博客上发表声明证实 LinkedIn 用户账户的密码已被泄露。

事件 4：黑客入侵 Adobe 公司并用 Adobe 数字证书签署恶意工具

摘录来源：Adobe

原文链接：

http://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html

热点简介：

2012 年 9 月 27 日，Adobe 产品安全与隐私高级总监 Brad Arkin 在 Adobe 官方博客上发表声明，Adobe 公司发现攻击者利用该公司的数字证书将两个恶意程序伪装成 Adobe 开发的软件，第一个是恶意工具"pwdump7 v7.1"，该工具主要用于提取 Windows 系统密码的散列值；第二个恶意程序是一个 ISAPI 过滤器"myGeeksmail.dll"。Adobe 在 2012 年 10 月 4 日废除相关的数字证书，Windows 平台的 Adobe 软件与 3 个 Mac/Windows 平台的 Adobe Air 应用受到影响需要升级。

事件 5：黑客行动主义盛行，依然活跃的 Anonymous

摘录来源：AnonNews

原文链接：

http://anonnews.org/press/item/2004/

热点简介：

Anonymous 于 2012 年 12 月 30 日在 Youtube 发布 Anonymous 2012 年"年终总结"视频(Expect Us in 2013)，回顾 Anonymous 在 2012 年一系列的攻击事件，其中详细介绍因反对查封文件共享网站 MegaUpload，Anonymous 而强力出击对美国司法部(DOJ)、联邦调查局(FBI)、环球音乐(Universal Music)和美国电影协会(MPAA)网站进行一系列的 DDoS 攻击。Anonymous 在声明中指出视频中的这些行动只是部分"案例"而已，还有更多不为人知的行动，其中一些行动仍在继续继续进行，例如#OpSyria。

事件 6：Mac OS X 史上最严重的病毒 Flashback

摘录来源：F-Secure

原文链接：

http://www.f-secure.com/weblog/archives/00002341.html

http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_Confirms_Flashfake_Flashback_Botnet_Infected_more_than_600_000_Mac_OS_X_Computers_Describes_Ramifications_and_Remedies

热点简介：

2012 年 4 月 2 日，F-Secure 威胁研究组成员 Brod 在 F-Secure 官方博客向 Mac OS X 用户发出警告，恶意程序 Flashback 的新变种 Flashback.K 利用了 Mac 系统中尚未修补的 Java 漏洞 CVE-2012-0507。一旦 Flashback.K 执行将提示用户输入管理员密码，无论用户是否输入管理员密码，该恶意程序都会试图感染系统，只是根据是否输入密码该恶意程序会选择不同的感染方式。Brod 在文中强调 Oracle 在 2 月份已经发布 Windows 平台该漏洞的补丁，但是截至 Brod 发稿时 Apple 公司仍未发布对 OS X 进行升级。据 Kaspersky 公司 4 月 9 日估计 Flashback.K 感染 Mac 系统数量高到 60 万台。

事件 7：美国众议院报告称华为中兴对美国国家安全构成威胁

摘录来源：U.S. House of Representatives

原文链接：

http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf

热点简介：

2012 年 10 月 8 日，美国众议院发布报告《Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE》，该报告称众议院情报委员会发起这项调查旨在了解长期以来对于中国电信公司华为、中兴与中国政府之间的关系。然而,两家公司在情报委员会调查期间都未能对他们与中国政府的关系提供详细的信息。基于此次调查结果，众议院情报委员会提出 5 点下建议，其中包括：强烈建议美国私营部门慎重考虑与华为、中兴进行设备或服务业务往来的长期安全隐患，强烈建议美国网络提供商或系统开发商寻求其它的合作厂商。

事件 8：Bank of America 等多家金融机构接连遭遇 DDoS 攻击

摘录来源：Arbor

原文链接：

http://pastebin.com/mCHia4W5
http://pastebin.com/E4f7fmB5
http://ddos.arbornetworks.com/2012/12/lessons-learned-from-the-u-s-financial-services-ddos-attacks/

热点简介：

从 2012 年 9 月 18 日，以抗议诋毁伊斯兰教先知穆罕默德的电影《Innocence of Muslim》为导火索,Izz ad-Din al-Qassam Cyber Fighters 黑客组织对美国金融机构发起代号为"Operation Ababil"的大规模 DDoS 攻击，攻击带宽有时甚至达到 60 Gbps。2012 年 12 月 10 日该组织在 Pastebin 网站声称"Operation Ababil"进入第二阶段，其攻击对象包括 U.S. Bancorp, JPMorgan Chase&co, Bank of America, PNC Financial Services Group, SunTrust Banks, Inc 在内的美国金融机构，Izz ad-Din al-Qassam Cyber Fighters 声称"Operation Ababil"第二阶段 DDoS 攻击无论是攻击范围还是攻击数量都将会有明显增加。

事件 9：VMware ESX 源码泄露事件

摘录来源：VMware

原文链接：

http://blogs.vmware.com/security/2012/04/vmware-security-note-2.html
http://blogs.vmware.com/security/2012/11/vmware-security-note-3.html

热点简介：

2012 年 4 月 24 日，VMware 公司安全响应中心总监 Iain Mulholland 在 VMware 官方博客上发表声明称该公司于 4 月 23 日获悉 VMware ESX 的一个源代码文件被公开泄露，并且未来可能有更多相关源码文件被公开。根据代码及其注释可确定泄露的是 2003 年-2004 年时间段内的源代码。Iain 在声明中强调 VMware ESX 源代码被公开分享并不意味会对 VMware 用户增加任何风险。2012 年 11 月 4 日 Iain 在 VMware 官方博客上发表 2012 年度第二次 VMware ESX 源代码泄露声明，称 11 月份泄露的 VMware ESX 源代码与 4 月份泄露的 VMware ESX 源代码之间有关联。这两份声明中有一句大意相同的"预测": "It is possible that more related files will be posted in the future"。

事件 10：首例可感染虚拟机的恶意程序 Crisis 出现

摘录来源：Intego,Symantec

原文链接：

http://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/
http://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines

热点简介：

2012 年 7 月 24 日反病毒厂商 Intego 报道 OS X 平台的木马程序 Crisis(OSX/Crisis)。8 月 20 日 Symantec 报道 Crisis 木马程序的 Windows 版 W32.Crisis，并指出 W32.Crisis 可通过 3 种方式传播:1).复制 W32.Crisis 和 autorun.inf 文件到可移动磁盘;2).复制 W32.Crisis 到 VMware 虚拟机映像文件;3)使用 Remote Application Programming Interface(RAPI)将 W32.Crisis 所属模块复制到 Windows Mobile 设备。Symantec 安全研究员 Takashi Katsuki 称 W32.Crisis 在搜索到 VMware 虚拟机映像文件后，使用 VMware Player 将恶意软件自身复制到该映像文件中，并认为 W32.Crisis 可能第一个试图感染 VMware 映像文件的恶意软件。

作者和贡献者

作者：

鲍旭华，绿盟科技

Email：baoxuhua@nsfocus.com

博士，绿盟科技战略研究部研究员，主要研究领域为信息安全事件分析、安全智能和态势感知。

李鸿培，绿盟科技

Email：lihongpei@nsfocus.com

Blog：http://www.i170.com/user/falcon

博士、高级工程师，绿盟科技研究院战略师。研究方向主要涉及网络安全、可信网络体系架构、安全信息智能处理技术及工业控制系统安全研究等

赵刚，绿盟科技

Email：zhaogang@nsfocus.com

主要研究领域为信息安全事件分析，始终专注于安全攻防技术研究。

贡献者：

刘亚，绿盟科技

Email：liuya@nsfocus.com

李政，绿盟科技

Email：lizheng@nsfocus.com

杨丽，绿盟科技

Email：yangli@nsfocus.com

于旸，绿盟科技

Email：yuyang@nsfocus.com

洪海，绿盟科技

Email：honghai@nsfocus.com

谭荆利，绿盟科技

Email：tanjingli@nsfocus.com

董阳，绿盟科技
Email：dongyang@nsfocus.com

周素华，绿盟科技
Email：zhousuhua@nsfocus.com

何坤，绿盟科技
Email：hekun2@nsfocus.com

王洋，绿盟科技
Email：wangyang2@nsfocus.com

关于绿盟科技 http://www.nsfocus.com/

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 30 多个分支机构，为政府、运营商、金融、能源等行业客户，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顺畅运行。

NSFOCUS
THREATS REPORT 2012

2012绿盟科技威胁态势报告

NSFOCUS