网络病毒的宏观性统计方法

肖新光 1 吴冰 2 邱永良 3 张晓兵 4

（1、2、3 安天实验室 哈尔滨 898 邮政信箱 150001；4 哈尔滨工业大学 哈尔滨繁荣街 130 号 150001）

摘要：

网络病毒已经成为了互联网的首要安全威胁，所以对网络病毒进行监测并进行宏观性统计，是维护互联网的重要的手段。由于网络病毒事件是基于复杂巨系统的分布式事件，因此描述网络病毒的宏观情况成为一个课题。本文课题组通过病毒样本统计、病毒分布统计、病毒网络测量等手段，形成了一套综合统计分析体制。

关键词：网络病毒、宏观性统计、网络评估计算、 感染节点

Macroscopical Statistics of Network Viruses

Xiao Xinguang1 Wu bing2 Qiu Yongliang3 Zhang Xiaobing4

(1、2、3 Antiy Labs Harbin P.O.Box 898 150001; Harbin Institute of Technology Harbin Fanrong Street 150 150001)

Abstract

The net-viruses are threatening China network.Therefore, in order to protect the network, we should monitor and count the net-virus roundly.In fact, because the virus incident of the network is scattered、base on hugeness system,so virus macroscopic statistical method of the network is a question for discussion，out team could well count the virus situation by analyzing virus sample distributing、virus-map distributing、net-virus measure and so on. It already became a statistical system.

Key Words：Network virus ,macroscopical statistics ,computing of network evaluation, infected nodes

引言

网络病毒的爆发是一种严重而频繁的网络安全事件，网络安全事件基本上符合摩尔定理，每十八个月数量翻一番。与此同时，网络安全事件也符合梅特卡夫定理，即网络的效率是与用户数量的平方成反比，这表明，互联网作为一个开放的复杂巨系统，不可避免地要发生安全事件，所以对网络病毒进行监测并进行宏观性统计，是掌握网络病毒发展趋势、维护互联网正常运转必不可少的技术手段。

网络病毒统计的主要难度是网络病毒事件的海量性和离散性。

网络病毒宏观性统计的目的

1、掌握网络病毒感染态势

通过对网络病毒的宏观统计，可以对每个区域的病毒泛滥情况形成完整的了解，从而为制定下一步的病毒防治方案提供了重要的数据依据。

2、控制网络病毒疫情

在掌握了网络病毒的整体态势之后，我们就可以针对病毒情况进行有的放矢。如，在网内，发现 Worm.Win32.Blast(冲击波)病毒，由于该病毒的大面积感染，网络中大部分带宽都被该病毒占据，依据这一情况，我们就可以采取病毒专杀工具定点投放的策略或者其它有效的方法来全面对抗网络中的病毒，从而很好地控制网络中的病毒疫情。

3、 预测病毒发展的趋势

当我们以某个区域子网为数据集，以该网络内的病毒发作次数或种类为 Y 坐标轴，以时间为 X 轴，我们就可以得出一个病毒的曲线图，只要变换一下关键量，就可以得到任意的关于病毒的统计图表，然后对该图表进行分析，就可以得出病毒的流行趋势，再加上一些经验因素，就可以对未来一段时间的病毒走势做出一个科学的预测，从而掌握病毒发展的趋势。

样本/入库审计方法

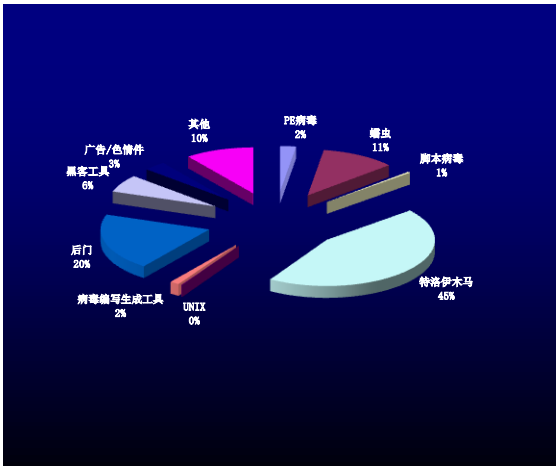
在对病毒整体趋势的分析过程中，样本/入库审计是最传统和最基本的方法。

对于网络病毒的统计，要采用两维分析的方法，病毒的一个发展维度是深度，即新的病毒种类的产生，另一个发展维度是广度，指的是某一种病毒在他的生命周期内所能传播的范围。样本/入库审计是对病毒发展深度的一种统计方法。一般反病毒公司都会根据样本流入情况和特征入库的审计来确定新病毒的种类，而这种病毒主要采用来自中毒用户的上报、合作公司之间的样本交换等途径。

而具体的审计工作内容则是病毒上报数量的统计、新病毒名字的统计等。其中上报数量统计能够对病毒感染严重程度做出一个相对的分析，新病毒名字的统计，能对阶段性病毒产生情况和整体病毒库情况做出统计。

例如，安天实验室利用这种方法，得出了 2004 病毒产生的情况。2004 年，安天实验室共向病毒库中添加了 20,047 个新的独立病毒名称（含变种）。2004 年各类病毒的产生数量如下：

PE 病毒	478
UNIX/Linux 系统病毒	33
蠕虫	2239
脚本病毒	81
特洛伊木马	8969
后门工具	4010
黑客工具	1241
病毒编写工具	279
广告/色情件	668
其他	2049



通过上述数据，我们可以清楚地看到，2004 年，在全部产生的新病毒中， 特洛伊木马、后门、黑客工具类病毒占据了 77%的份额，蠕虫病毒占据了 11%、广告/色情插件类病毒以 3%的份额位居第三，经过对这些数据的分析，可以了解新病毒产生的趋势。

样本审计的对照分析

传统反病毒企业的 TOP 10 蠕虫/病毒的列表一般是依照单位时间上报次数的对比形成的，按照宏观的观点，上报次数的多少是感染节点数量多少的真实反应，对照评估的方法同样适用于其他的方法，例如，安天通过这一方法，得出了 2004 年用户感染的扫描型蠕虫 TOP 10 的列表（图 2）：

根据病毒的名字处理可以进行数据合并，例如，对某一病毒家族的统计等，下图展示的就是 2004 年 BOT 病毒家族的 TOP10：

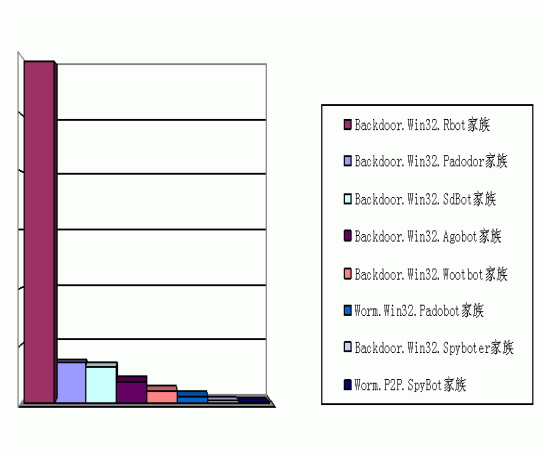


图 2：2004 年扫描型蠕虫 TOP 10（安天数据）

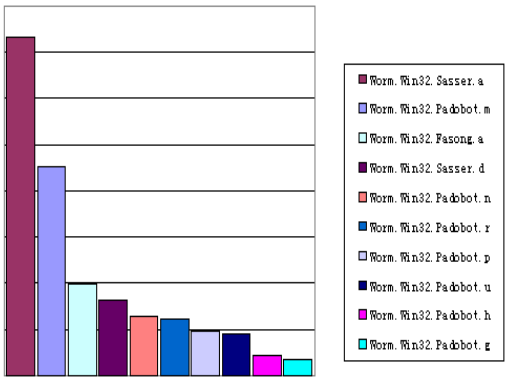


图 3：2004 年 BOT 病毒家族的 TOP10（安天数据）

网络蠕虫检测与压力评估计算

1、现状

传统的对于网络病毒的监测一般都是在本地节点或路由节点上进行的，无法评价病毒对网络节点设备和整个网络的压力情况。课题组设计了一种基于旁路监听的骨干网网络病毒监测系统（VDS）。VDS 可以监控病毒的扫描、传输、攻击等行为，并测量病毒产生的网络流量对网络的影响。通过对测量设备获得的数据进行采集和挖掘，得出网络病毒对网络出口、网关和交换设备、周转节点和最终节点产生的压力的计算方法，最终定量地评估网络病毒对互联网和节点设备的影响，为网络病毒的控制与遏制提供必要的基础数据。

2、网络病毒监控系统（VDS）的实现

VDS 所实现的是一个基于旁路监听、高速规则匹配结合的网络病毒检测平台，下图为系统结构示意图。

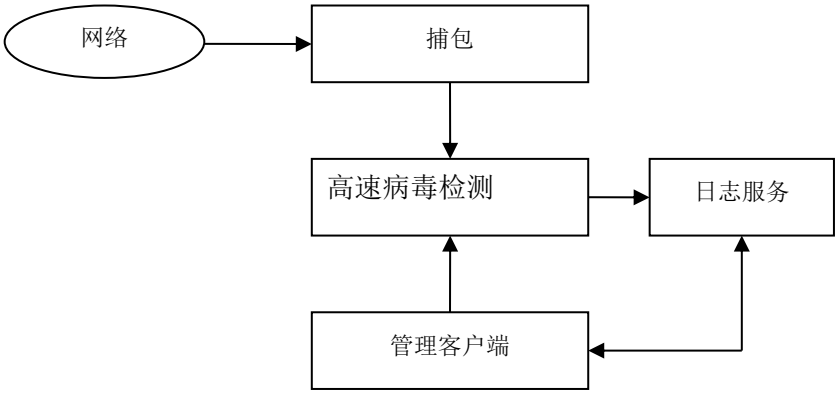


图 4：VDS 系统软件结构图

3 原始数据与统计

VDS 可以得出当前网络中活跃蠕虫的名称、相关行为、次数和流量等等，并能够直接得出部分统计结果。

4、活跃蠕虫的列表

利用 VDS 可以形成活跃蠕虫列表，并按照时限内传播次数进行排行，如图 9：

2003-7-7病毒扫描日志

统计数据:	
扫描数据流总数：	0
发现病毒体总数：	242573
发现已知病毒总数：	242573
发现未知病毒总数：	0

发现病毒体传输次数排行榜:

名次	病毒名	发现次数
1	I-worm.Klez.h	171267
2	I-Worm.Runouce.b	39661
3	I-Worm.Lentin.i	941
4	I-Worm.Lentin.m	167
5	I-Worm.Sobig.a	67
6	I-Worm.LovGate.f	54
7	I-Worm.Sobig.b	12
8	I-Worm.Sobig.c	2
9	I-Worm.Sobig	1
10	I-Worm.Tanatos.dam	1

发现病毒体传输次数统计图:

图 9：活跃蠕虫的 TOP10

（图片来源：VDS 1 .0 WEB 报表截图，数据来源：哈工大测试节点）

5、病毒流量压力排行

我们还可以利用这一方法来评估网络病毒的压力影响，对某一个病毒的病毒病毒流量进行统计，这一统计能够给网管们建设性的指导。 如图 10。

邮件病毒传输次数排行榜:

名次	病毒名	发现次数	病毒流量大小
1	I-Worm.NetSky.q	136	4021248
2	I-Worm.Runouce.b	37	4982124
3	I-Worm.LovGate.ad	33	4595712
4	I-Worm.NetSky.d	10	20510
5	I-Worm.NetSky.r	5	147840
6	I-Worm.LovGate.p	4	389120
7	I-Worm.Bagle.z	2	145266

图 10：邮件病毒传输次数排行榜

（图片来源：VDS 2.0 WEB 报表截图，数据来源：2004 年 6 月 12 日哈工大测试节点。）

6、病毒阶段趋势统计

系统可以得到病毒的阶段趋势统计曲线，从而可以对未来的病毒疫情做出预测。如图 14。

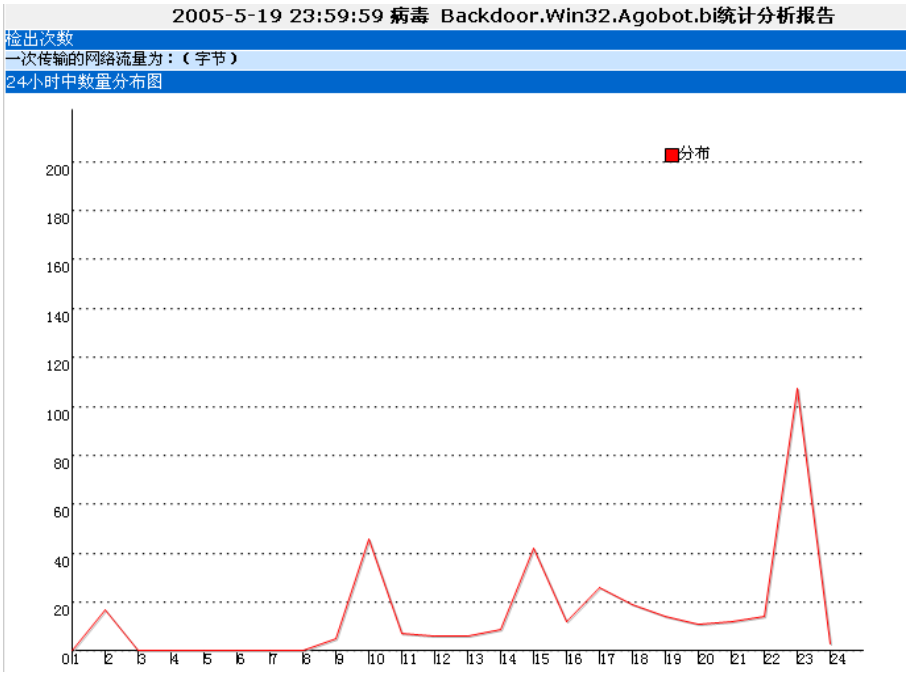


图 14：病毒时间发展曲线图

（图片来源：VDS 2.0 WEB 截图，数据来源：2004 年 8 月教育网测试节点）

地理性统计（Virus Map）

virus map 是病毒信息地理分布图，通过图表，用户可以很清楚地看到各个地区的病毒发作状况，这种方法对宏观掌握病毒的疫情，有着很重要的意义。传统的 virus map 是根据上报者的 IP 地址/电子邮件域归属以及在线杀毒用户的 IP 分配进行病毒分类统计，然后再映射到地理信息系统而形成的病毒活跃地图，如下图：

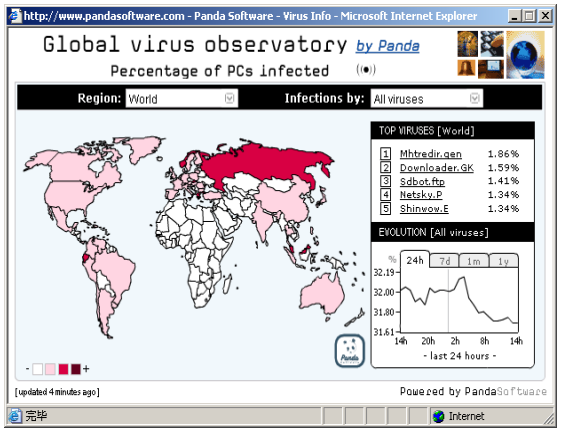


图 11：典型的 virus map 图

（图片来源：panda 反病毒网站）

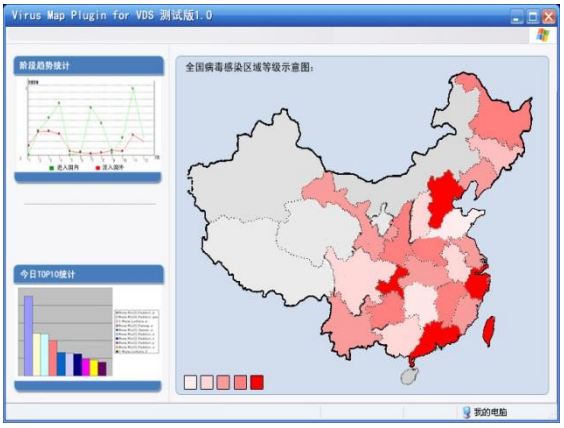


图 13： Virus Map 图

（图片来源：VDS 2.0VirusMap 插件截图）

这种方法虽然也可以得出病毒的分布情况，但是粒度不够细化。

采用 VDS 可以直接定位病毒的源节点：

当前位置：信息查询 → 按病毒名称

病毒名称（英）：netsky 查询

病毒名称	数量	源IP	目的IP	开始时间	结束时间
I-Worm.NetSky.r	1	210.46.70.153	61.136.62.73	2005-02-28 08:26:46	2005-02-28 08:27:00
I-Worm.NetSky.q	3	202.118.238.206	202.84.17.167	2005-02-28 08:25:53	2005-02-28 08:26:40
I-Worm.NetSky.r	1	218.104.83.140	202.118.224.153	2005-02-28 08:25:45	2005-02-28 08:26:00
I-Worm.NetSky.q	1	202.118.251.116	61.181.84.15	2005-02-28 08:25:24	2005-02-28 08:25:40
I-Worm.NetSky.r	1	218.58.71.174	202.118.224.153	2005-02-28 08:25:10	2005-02-28 08:25:20
I-Worm.NetSky.q	1	218.9.78.206	202.118.224.153	2005-02-28 08:24:54	2005-02-28 08:25:00
I-Worm.NetSky.q	1	211.93.37.15	202.118.224.153	2005-02-28 08:24:30	2005-02-28 08:24:40

图 12：病毒源节点定位

（图片来源：VDS 2.0 WEB 报表截图，数据来源：2004 年 8 月 28 日哈工大测试节点）

再与 Virus Map 系统相结合，就能够得出病毒的更准确的活跃地区的判断。

感染率和总感染量统计方法

病毒感染率和总感染量（节点数）的统计，是最为困难的统计。这种统计的目的是宏观地掌握一段时间内的病毒准确影响状况，从而对病毒的发展做出预测。

这种目前有抽样法、用户上报法、VDS 监控法和扫描探测法等四种手段。

抽样法是针对一个确定的用户群进行抽样，然后运用统计公式进行放大，从而得出结果，这种方法的统计难度大且误差较大。

用户上报法是用户上报的病毒进行分析、统计，然后对上报人群进行区域归属划分，从而得出感染量的一种方法。这种方法因为不能准确得出用户上报数量与实际感染数量的比例关系，难以转化成绝对数量。

VDS 监控法是利用网络病毒监控设备 VDS，对网络进行监控统计而得到的病毒信息数据，这种方法由于代理和邮件服务器的差异会造成一定的误差，尤其是内网用户，有些扫描蠕虫网络特征一致。

扫描探测法是利用高速网段扫描器，对已知端口进行扫描探测的一种方法。这种方法只

能针对具体漏洞，多数不能针对具体病毒。

感染节点数的计算方法

这一方法是利用扫描工具的统计报告，然后再加上经验数据，进行揉合而产生结果数据的一种方法。

例如，我们可以通过对邮件蠕虫传播次数排行和用户上报次数排行进行比较，从而得出以下结论。

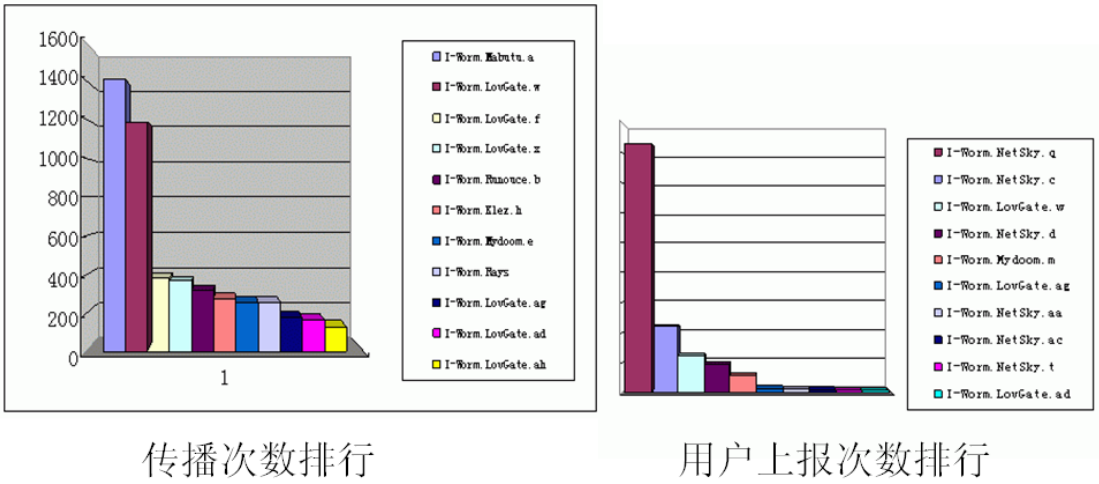


图 15：病毒传播次数排行和用户上报次数排行

分析结论如下：

传输次数是网络压力的反应，体现蠕虫的发信能力，用户上报是感染节点的反应。通过其不对应性可见，蠕虫发信能力与感染节点数没有必然联系。

基于信任链传播能造成更为有效的感染。

对于历史病毒有大量顽固节点存在，这些节点可能是 internet 上的无控节点。

结论

文中所描述的一系列方法，较为全面论述了病毒统计的各种方法，对课题组所作的工作进行了总结。

参考文献：

[1] Deng Hui ，Research of Internet Worm，Doctorial Paper，Nan kai University，2000

[图 1] Wu Bing, Yun Xiaochun, Xiao Xinguang， Backbone Network Worm Pressure Measurement System Based on Bypass Monitor，AVER 2004