上海市网络安全月报

2018 年第 1 期

发布单位：上海市通信管理局

支持单位：国家计算机网络应急技术处理协调中心上海分中心

发布日期：2018 年 2 月

目　　录

一、　概述.....1

二、　上海市网络流量监测情况.....2

1. 全网流量.....2

2. 跨地域流量.....3

三、　上海市网络安全威胁监测情况.....5

1. 木马僵尸网络.....5

2. “飞客”蠕虫.....6

3. 网页篡改.....7

4. 网站后门.....7

5. 移动互联网恶意程序.....8

四、　电信和互联网行业安全管理动态.....9

1. 网站备案管理.....9

2. 违法违规信息处置.....9

3. 网络安全信息上报.....10

4. 网络安全事件通报.....11

5. 网络安全“回头看”检查通报会.....11

五、　重要网络安全威胁公告.....13

六、　安全要闻回顾.....17

版权声明.....19

一、 概述

根据《网络安全法》《公共互联网网络安全突发事件应急预案》等有关法律法规，上海市通信管理局负责组织、指挥、协调上海地区公共互联网网络安全突发事件的预防、监测、报告和应急处置工作；国家计算机网络应急技术处理协调中心上海分中心（以下简称上海互联网应急中心）作为支撑单位，具体负责监测、报告上海地区公共互联网网络安全突发事件和预警信息，为应急工作提供决策支持和技术支撑；上海市各基础电信企业、域名机构、互联网企业负责本单位网络安全突发事件预防、监测、报告和应急处置工作，为其他单位的网络安全突发事件应对提供技术支持。

2018 年 1 月，在上海市通信管理局的指导下，上海互联网应急中心直接参与处理的事件共计 273 起，其中：网页仿冒 1 起，网页篡改 112 起，网站后门 157 起，移动互联网恶意程序 2 起，拒绝服务攻击 1 起。来自上海市各基础电信企业、域名机构、互联网企业上报以及上海互联网应急中心处置的安全事件共计 1224 起。其中涉及运营单位 IP 网事件 1 起，权威域名解析服务器事件 5 起，递归服务器事件 24 起，计算机病毒事 3 起，蠕虫事件 6 起，木马事件 78 起，僵尸网络事件 9 起，域名劫持事件 43 起，网络仿冒事件 573 起，网页篡改事件 118 起，网页挂马事件 7 起，拒绝服务攻击事件 64 起，后门漏洞事件 261 起，非授权访问事件 11 起，其他网络安全事件 21 起。上海市公共网络总体稳定，未出现大规模网络攻击事件。

二、 上海市网络流量监测情况

1. 全网流量

2018 年 1 月，上海地区全网流量峰值为 4,217Gbps，环比上升 33.0%。峰值出现时间为 2018 年 1 月 22 日 20:55，每日 20:45 至 23:10 流量较高。全网流量谷值为 643.8Gbps，环比下降 31.6%。谷值出现时间为 2018 年 1 月 29 日 04:20，每日 04:20 至 05:25 流量较低。全网流量均值为 2,020.7Gbps，环比上升 2.1%。

周一至周五工作日全网流量分布如图 2.1 所示。

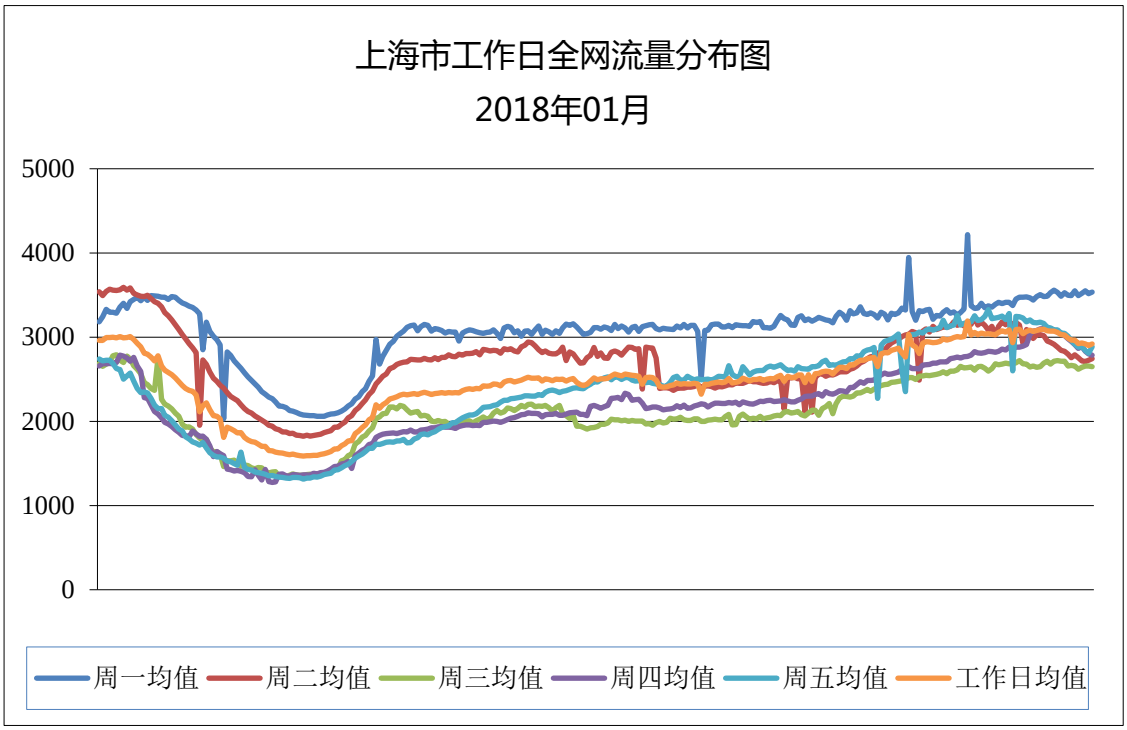

图 2.1：工作日全网流量分布图（单位：Gbps）

周六与周日双休日全网流量分布情况如图 2.2 所示。

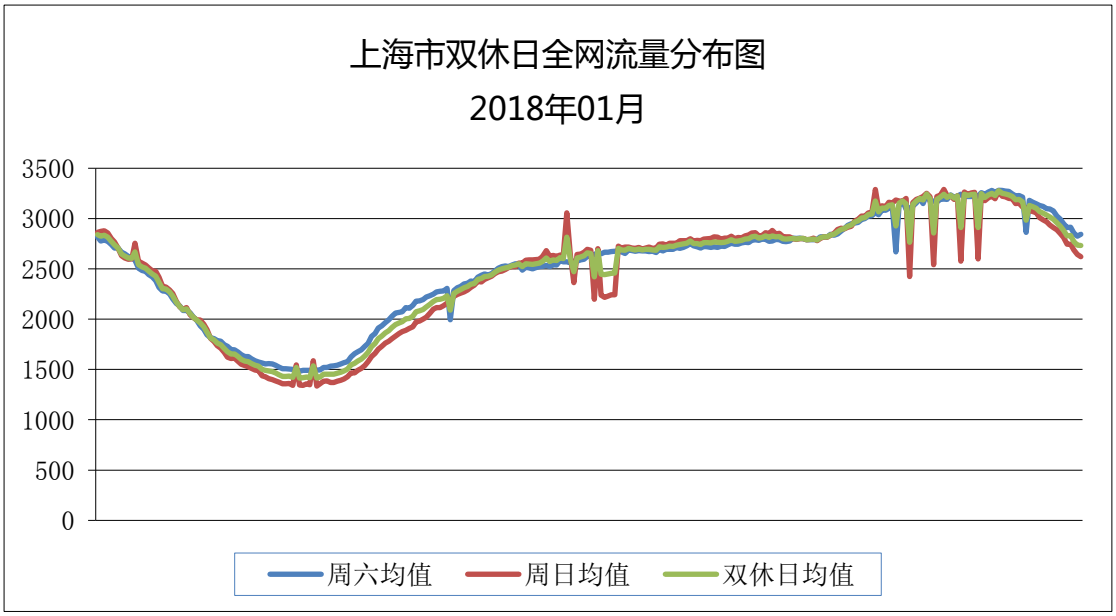

图 2.2：双休日全网流量分布图（单位：Gbps）

2. 跨地域流量

2018 年 1 月，从外省流入上海地区的流量分布情况如图 2.3 所示，最多的地区分别为江苏（38.1G，约占 14.2%）和浙江（31.3G，约占 11.7%），最少的地区为西藏（0.1G，约占 0.04%）。

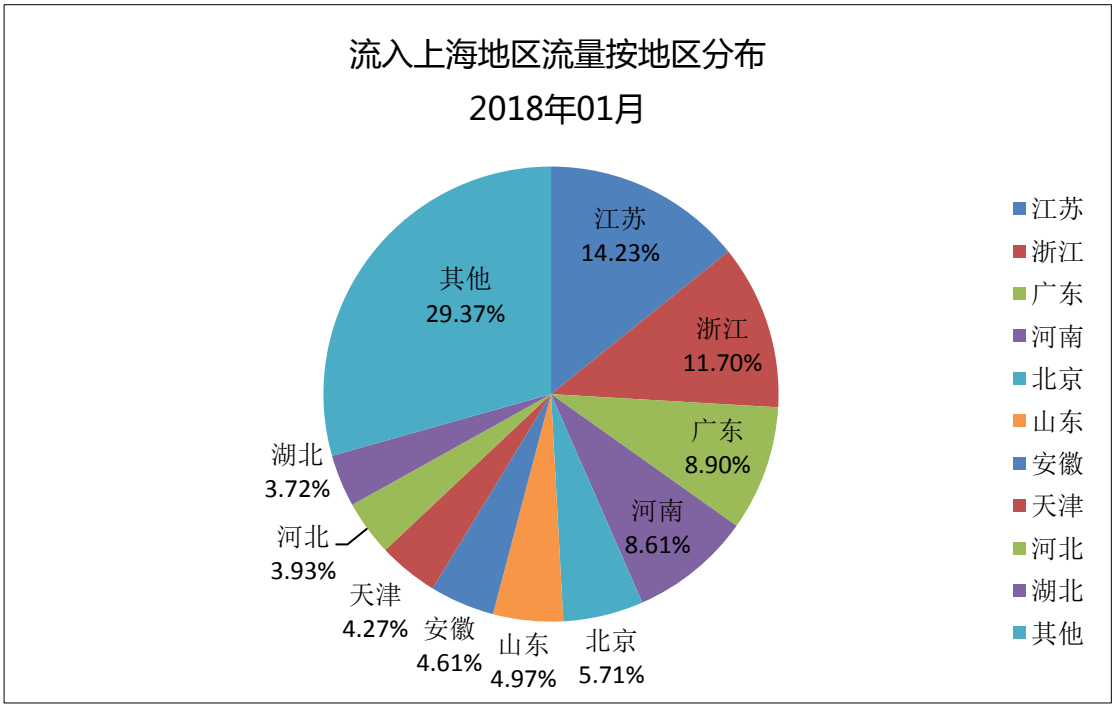

图 2.3：流入上海地区流量地区分布图

上海地区流出至外省的流量分布情况如图 2.4 所示，最多的地区分别为江苏（76.0G，约占 26.8%）和浙江（43.3G，约占 15.3%），最少的地区为西藏（0.04G，约占 0.01%）。

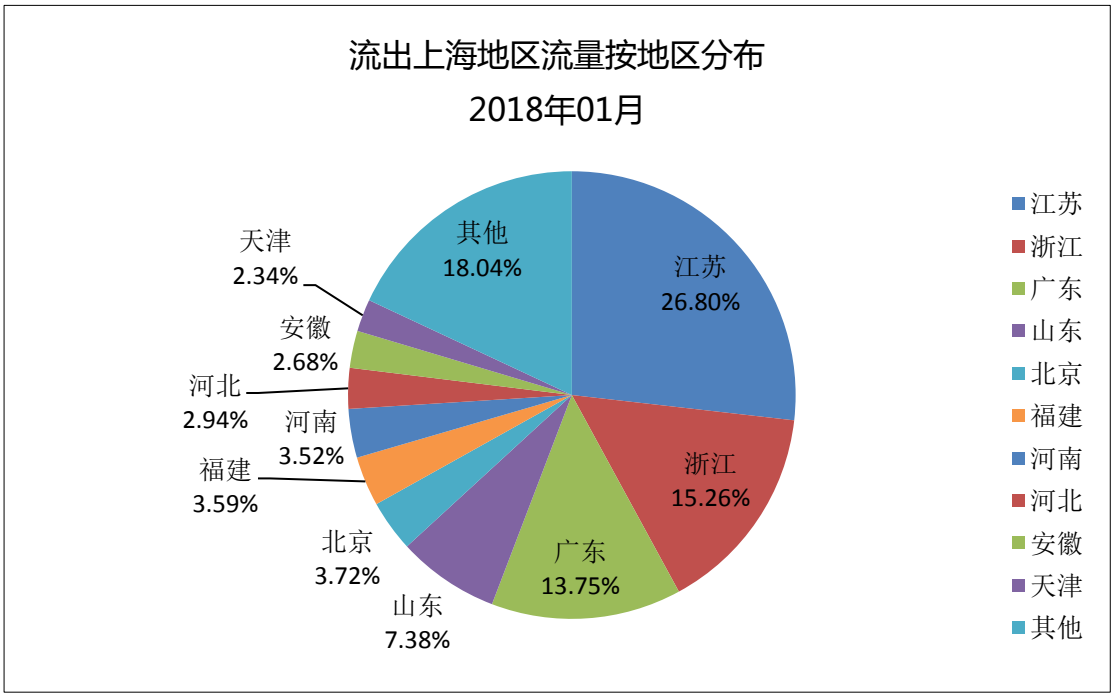

图 2.4：上海地区流出流量地区分布图

三、 上海市网络安全威胁监测情况

1. 木马僵尸网络

2018 年 1 月，国家计算机网络应急技术处理协调中心（以下简称 CNCERT/CC）对木马僵尸的活动状况进行了抽样监测，发现上海市有 5,407 个 IP 地址对应的主机被通过木马或僵尸程序秘密控制，同比减少 78.5%，环比增加 12.4%，约占全国总数的 1.0%，排名全国第二十五，较上月下降 1 位。近半年来月度分布情况如图 3.1 所示。

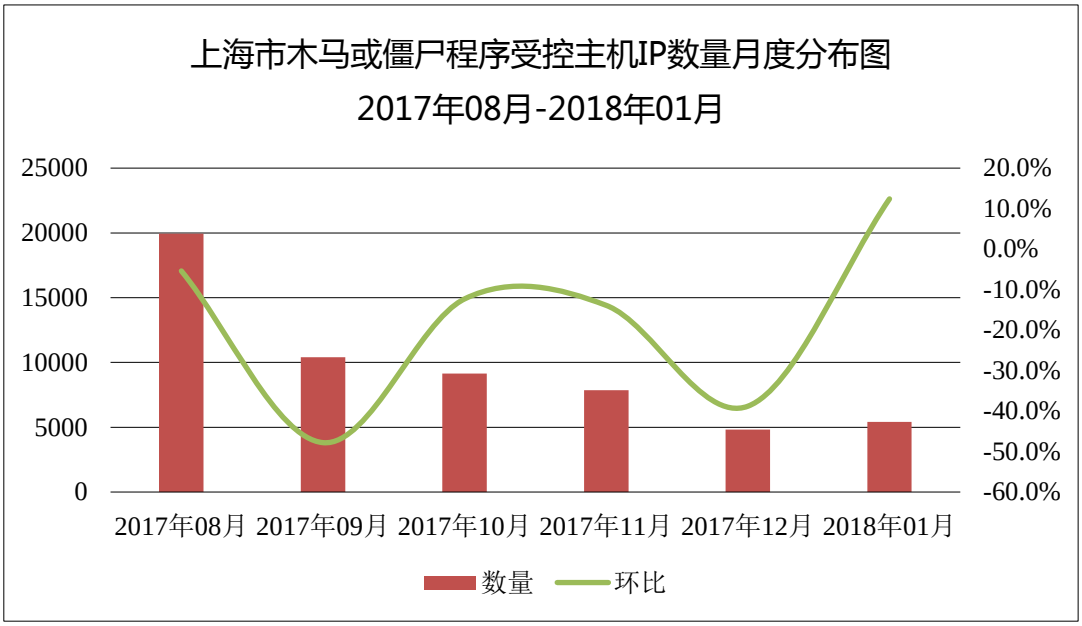

图 3.1：上海市木马或僵尸程序受控主机 IP 数量月度分布图

上海市 137 个 IP 地址对应的主机被利用作为木马或僵尸程序控制主机，同比减少 50.5%，环比增加 63.1%，约占全国总数的 5.9%，排名全国第四，较上月上升 2 位。近半年来月度分布情况如图 3.2 所示。

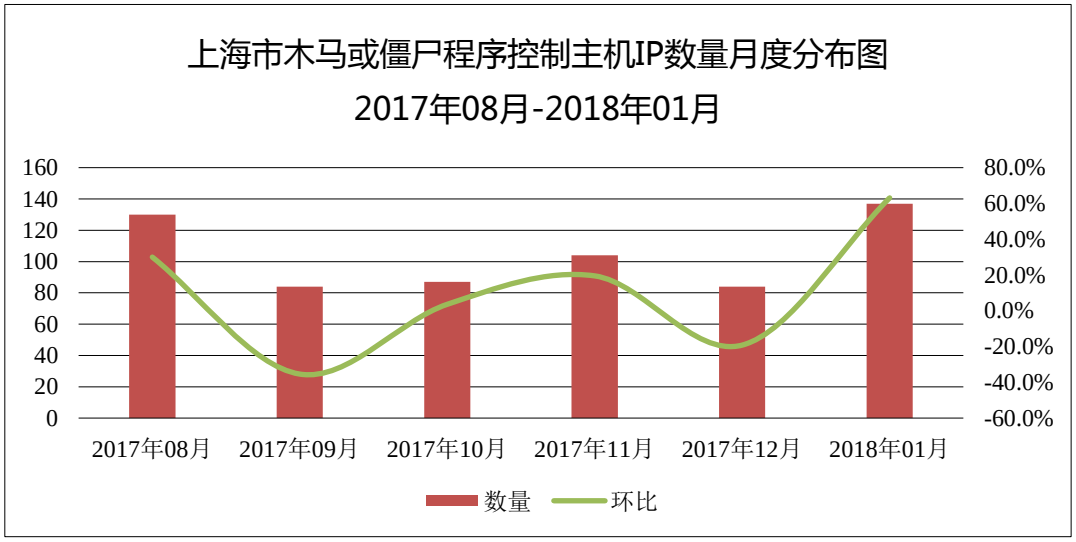

图 3.2：上海市木马或僵尸程序控制主机 IP 数量月度分布图

2. “飞客”蠕虫

2018 年 1 月，CNCERT/CC 对“飞客”蠕虫的活动状况进行了抽样监测，上海市有 13,519 个 IP 地址对应的主机感染“飞客”蠕虫，同比减少 45.5%，环比减少 8.9%，约占全国总数的 4.4%，排名全国第五，较上月持平。近半年来月度分布情况如图 3.3 所示。

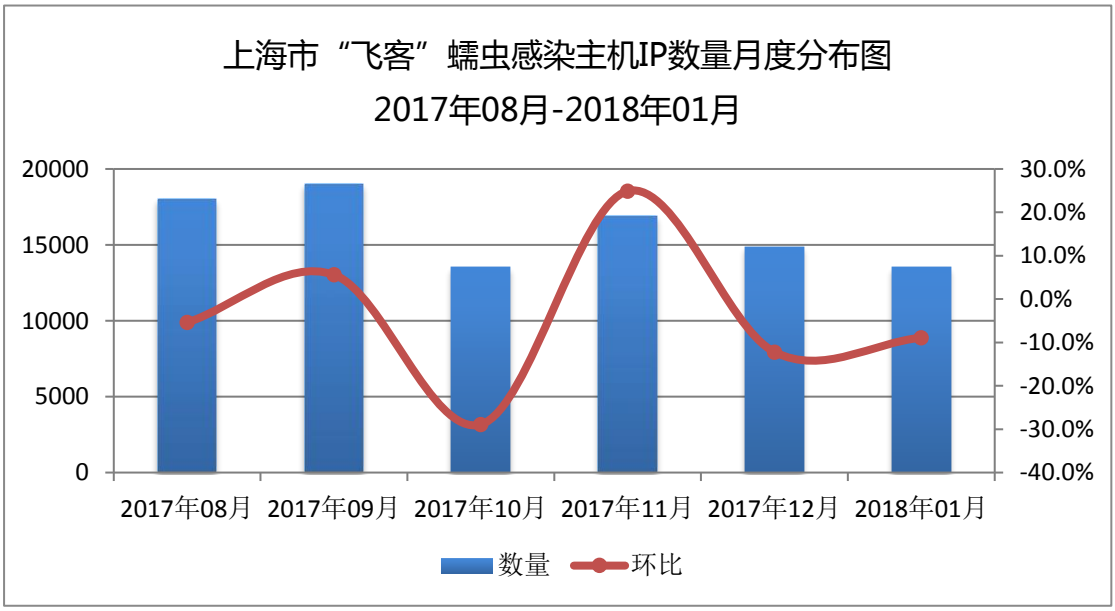

图 3.3：上海市感染飞客蠕虫的主机 IP 数量月度分布图

3. 网页篡改

2018 年 1 月，CNCERT/CC 监测发现主机位于上海地区的被篡改网站数量为 232 个，同比减少 12.1%，环比增加 0.9%，约占全国总数 5.7%，排名全国第四，较上月上升 1 位。近半年来月度分布情况如图 3.4 所示。

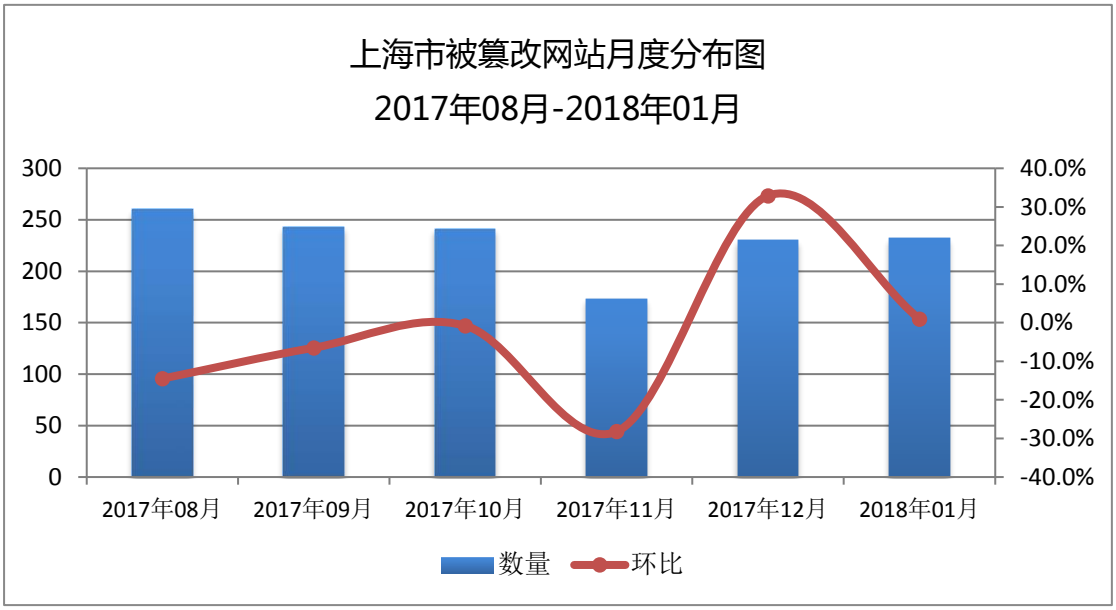

图 3.4：上海市被篡改网站数量月度分布图

4. 网站后门

2018 年 1 月，CNCERT/CC 监测发现主机位于上海地区的被植入后门的网站数量为 101 个，同比减少 38.8%，环比减少 35.7%，约占全国总数 3.9%，排名全国第六，较上月下降 2 位。近半年来月度分布情况如图 3.5 所示。

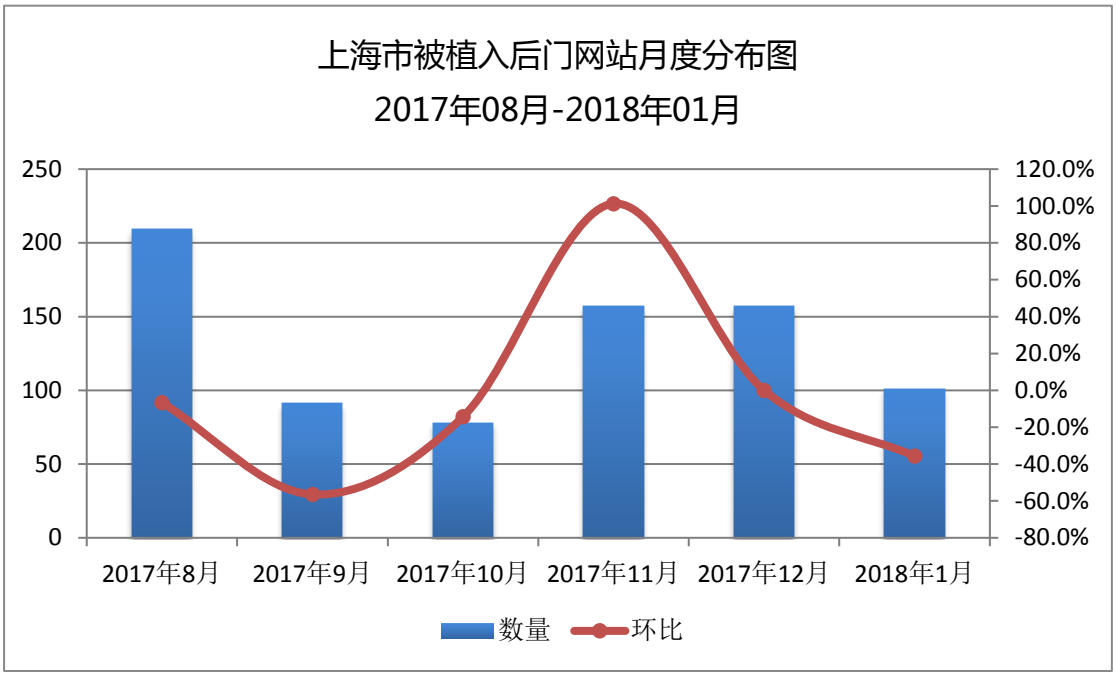

图 3.5：上海市被植入后门网站数量月度分布图

5. 移动互联网恶意程序

2018 年 1 月，CNCERT/CC 监测发现，上海地区传播服务器数量为 2 个，环比减少 90.5%，约占全国数据 0.9%，排名全国第二十二，较上月下降 6 位名。传播服务器分布情况如图 3.6 所示。

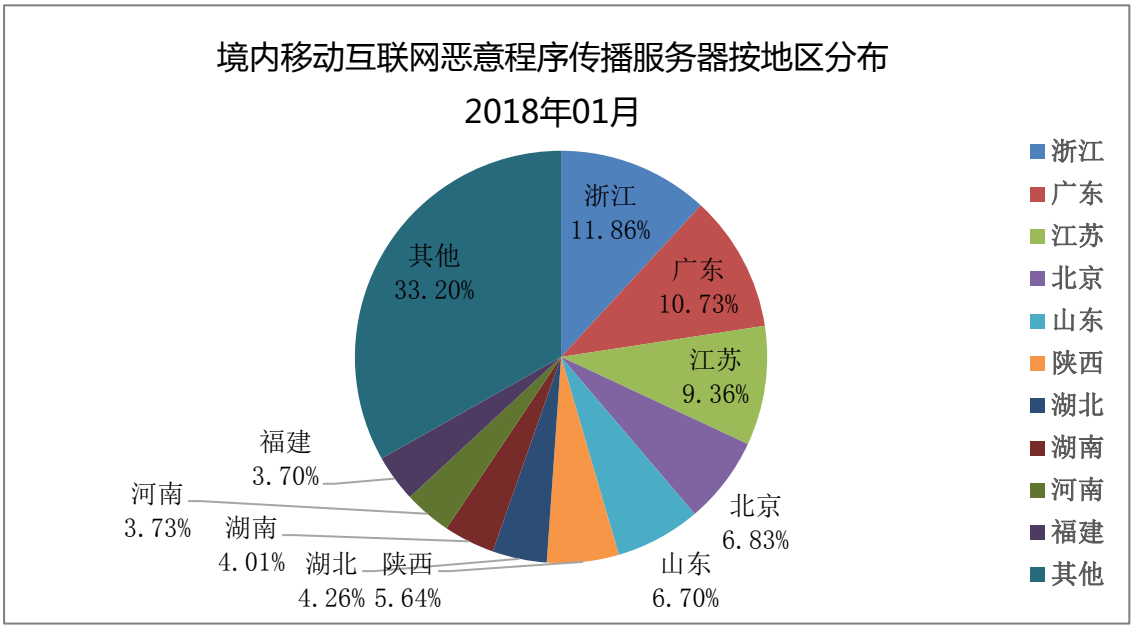

图 3.6：境内移动互联网恶意程序感染用户按照地区分布

四、 电信和互联网行业安全管理动态

1. 网站备案管理

2018 年 1 月，上海市通信管理局共审核网站备案信息 9771 条，其中审核通过 8708 条，审核通过率为 89.1%。截至 2018 年 1 月 31 日，本市已备案网站总数达 40.5 万个，备案主体总数达 28.8 万个。目前，市通管局备案管理系统中尚有存量空壳类数据 4425 个，较上月（1782 个）相比增加了 2643 个。

2. 违法违规信息处置

2018 年 1 月，上海市通信管理局自主、联合和配合市网信办等职能部门进一步加强网络空间治理，关闭违法违规网站共计 6 个。其中违规医疗器械 5 个，虚假备案 1 个。违法违规网站处置按类型分布情况如图 4.1 所示。

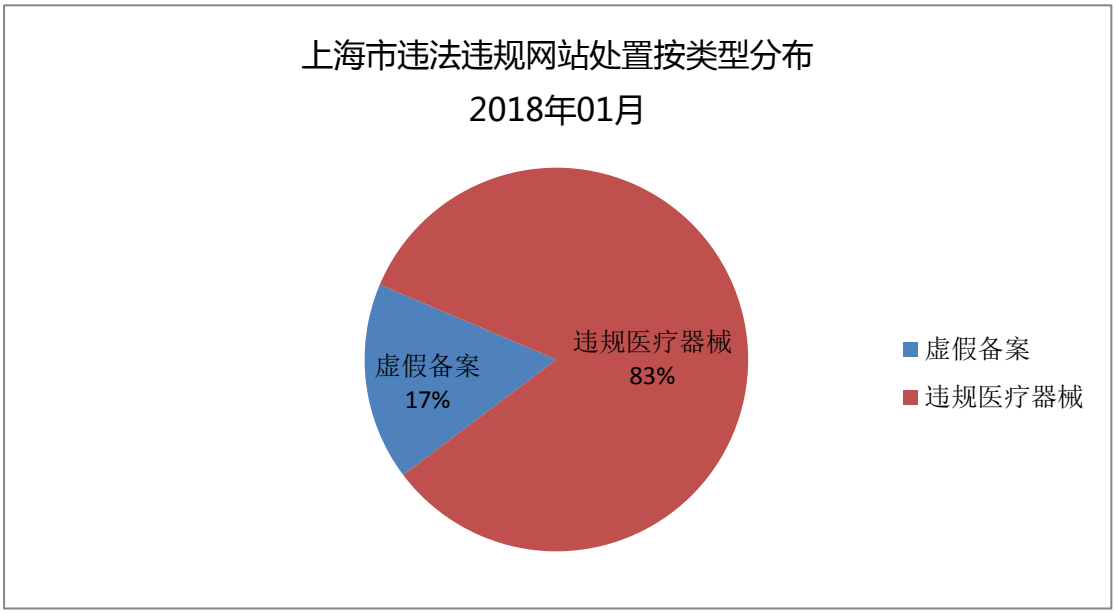

图 4.1：上海市违法违规网站处置按类型分布

根据工业和信息化部《公共互联网网络安全威胁监测与处置办法》《移动智能终端应用软件预置和分发管理暂行规定》，上海互联网应急中心在上海市通信管理局的指导下，对备案在上海的应用商店、游戏平台、云平台、广告平台等网站上传播的移动互联网智能终端应用开展监测和处置工作。2018 年 1 月，共协调 2 家单位下架移动互联网恶意程序 15 个。移动互联网恶意程序传播源处置情况如表 4.1 所示：

表 4.1：移动互联网恶意程序处置情况表

网站名称	网站属性	恶意程序处置数量
360 缓存	应用商店	14
优刻得	云平台	1

3. 网络安全信息上报

2018 年 1 月，来自上海市各基础电信企业、域名机构、互联网企业上报以及上海互联网应急中心处置的安全事件共计 1224 起。其中涉及运营单位 IP 网事件 1 起，权威域名解析服务器事件 5 起，递归服务器事件 24 起，计算机病毒事 3 起，蠕虫事件 6 起，木马事件 78 起，僵尸网络事件 9 起，域名劫持事件 43 起，网络仿冒事件 573 起，网页篡改事件 118 起，网页挂马事件 7 起，拒绝服务攻击事件 64 起，后门漏洞事件 261 起，非授权访问事件 11 起，其他网络安全事件 21 起。上海市公共网络总体稳定，未出现大规模网络攻击事件。

上海电信、上海移动、上海联通、上海新觉信息科技有限公司、上海有孚计算机网络有限公司、游族网络股份有限公司、上海快网网

络信息技术有限公司、上海巨人网络科技有限公司等企业针对不同级别安全事件，做出了及时有效的处理措施，并积极上报市通信管理局，配合通信管理局有力维护了上海市公共互联网的安全稳定运行，予以肯定。

4. 网络安全事件通报

2018 年 1 月，市通信管理局接报发现，上海聚力传媒技术有限公司移动智能终端 APP 应用“PP 视频”存在安全漏洞，攻击者可利用漏洞进行敏感操作，危害用户信息安全。对此，市通管局约谈上海聚力传媒公司有关负责人，要求其迅速处置安全威胁，并进一步重视网络安全管理，加强各类互联网信息系统的网络安全防护工作。企业已及时制定上报整改方案，并向市通管局报告了有关网络安全防护情况。

5. 网络安全“回头看”检查通报会

为进一步宣贯明确《网络安全法》有关法律要求，总结通报网络安全“回头看”等前阶段网络信息安全工作情况，市通信管理局于 2018 年 1 月组织召开网络安全“回头看”检查通报会。会上，市通管局有关负责人通报了前阶段网络安全“回头看”、车联网业务安全评估、互联网新业务安全评估等重点工作情况，对 2017 年度网络信息安全工作表现突出的集体和个人进行了表扬，并简要部署了 2018 年度电信和互联网行业网络与信息安全工作任务。上海市各基础电信

企业、互联网企业、车联网企业、安全企业等 70 余家企业代表参加会议。

五、 重要网络安全威胁公告

2018 年 1 月部分互联网高危安全漏洞内容如下所示。请相关单位及时做好漏洞检测、补丁升级和主机加固工作，获取软件的最新版本，以提高自身及整体的安全防护能力。

✧ 关于 Android 平台 WebView 控件存在跨域访问高危漏洞的安全公告

2017 年 12 月 7 日，国家信息安全漏洞共享平台（CNVD）接收到腾讯玄武实验室报送的 Android WebView 存在跨域访问漏洞(CNVD-2017-36682)。攻击者利用该漏洞，可远程获取用户隐私数据（包括手机应用数据、照片、文档等敏感信息），还可窃取用户登录凭证,在受害者毫无察觉的情况下实现对 APP 用户账户的完全控制。由于该组件广泛应用于 Android 平台，导致大量 APP 受影响，构成较为严重的攻击威胁。

一、漏洞情况分析

WebView 是 Android 用于显示网页的控件，是一个基于 Webkit 引擎、展现 web 页面的控件。WebView 控件功能除了具有一般 View 的属性和设置外，还可对 URL 请求、页面加载、渲染、页面交互进行处理。

该漏洞产生的原因是在 Android 应用中，WebView 开启了 file 域访问，且允许 file 域对 http 域进行访问，同时未对 file 域的路径进行严格限制所致。攻击者通过 URL Scheme 的方式，可远程打开并加载恶意 HTML 文件，远程获取 APP 中包括用户登录凭证在内的所有本

地敏感数据。

漏洞触发成功前提条件如下：

1. WebView 中 setAllowFileAccessFromFileURLs 或 setAllowUniversalAccessFromFileURLs API 配置为 true；

2. WebView 可以直接被外部调用，并能够加载外部可控的 HTML 文件。

CNVD 对相关漏洞综合评级为“高危”。

二、漏洞影响范围

漏洞影响使用 WebView 控件，开启 file 域访问并且未按安全策略开发的 Android 应用 APP。

三、漏洞修复建议

厂商暂未发布解决方案，临时解决方案如下：

1. file 域访问为非功能需求时，手动配置 setAllowFileAccessFromFileURLs 或 setAllowUniversalAccessFromFileURLs 两个 API 为 false。（Android 4.1 版本之前这两个 API 默认是 true，需要显式设置为 false）

2. 若需要开启 file 域访问，则设置 file 路径的白名单，严格控制 file 域的访问范围，具体如下：

（1）固定不变的 HTML 文件可以放在 assets 或 res 目录下，file:///android_asset 和 file:///android_res 在不开启 API 的情况下也可以访问；

（2）可能会更新的 HTML 文件放在/data/data/(app) 目录下，避

免被第三方替换或修改；

（3）对 file 域请求做白名单限制时，需要对“../../”特殊情况进行处理，避免白名单被绕过。

3. 避免 App 内部的 WebView 被不信任的第三方调用。排查内置 WebView 的 Activity 是否被导出、必须导出的 Activity 是否会通过参数传递调起内置的 WebView 等。

4. 建议进一步对 APP 目录下的敏感数据进行保护。客户端 APP 应用设备相关信息（如 IMEI、IMSI、Android_id 等）作为密钥对敏感数据进行加密。使攻击者难以利用相关漏洞获得敏感信息。

✧ 关于 OAuth 2.0 存在第三方帐号快捷登录授权劫持漏洞的安全公告

2018 年 1 月 21 日，国家信息安全漏洞共享平台（CNVD）接收了 OAuth 2.0 存在第三方帐号快捷登录授权劫持漏洞（CNVD-C-2018-06621）。综合利用上述漏洞，攻击者可通过登录受害者账号，获取存储在第三方移动应用上的敏感信息。由于 OAuth 广泛应用于微博等社交网络服务，漏洞一旦被黑客组织利用，可能导致用户隐私信息泄露。

一、漏洞情况分析

OAuth（Open Authorization）是一个关于授权的开放网络标准，允许用户授权第三方移动应用，访问用户存储在其他服务提供者上的信息，而无需将用户名和密码提供给第三方移动应用或分享数据的所有内容。

该漏洞利用 OAuth 第三方授权无需用户名和密码的特点，结合 redirect_uri 未指定授权目录引发用户劫持攻击。攻击者通过登录某种社交网络服务，修改链接 redirect_uri 参数值指向，将伪造后的用户授权链接发给目标用户，当目标用户点击或被欺骗访问上述授权链接进行登陆后，攻击者即可通过 referer 获取用户授权，快速登录目标用户账号，还可登陆该账号绑定的其他网站信息，查看敏感信息或执行授权操作，还可以利用受害人账号进行非法信息传播、诈骗等非法行为。

CNVD 对上述漏洞的综合评级为“中危”。

二、漏洞影响范围

上述漏洞影响采用第三方登陆授权方式的服务。

三、漏洞修复建议

CNVD 建议第三方应用平台采取如下措施进行漏洞的防范，同时请广大用户注意第三方授权链接，谨慎输入账号密码：

1. 在注册第三方授权时，redirect_uri 需要限制到指定网站的指定目录，比如 redirect_uri 注册为 passport.aaa.com/oauth/，而非 aaa.com 或者 passport.aaa.com。

2. 禁止非源跳转。通过增加网站跳转的判断条件，禁止对非本网站的链接进行跳转。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-01622

六、 安全要闻回顾

✧ 全国信息安全标准化技术委员会发布《网络安全实践指南—CPU 熔断和幽灵漏洞防范指引》

1 月 16 日消息 全国信息安全标准化技术委员会秘书处（以下简称“信安标委秘书处”）针对近期披露的 CPU 熔断（Meltdown）和幽灵（Spectre）漏洞，组织相关厂商和安全专家，编制发布了《网络安全实践指南—CPU 熔断和幽灵漏洞防范指引》(以下简称《防范指引》)。

信安标委秘书处相关负责人表示，熔断和幽灵漏洞影响范围覆盖主流 CPU，引发广泛的关注。相关厂商应及时应对，为产品提供必要的技术支持，有序开展补丁升级工作，引导用户提高安全意识，有效控制相关风险，维护用户利益。

据介绍，本次披露的漏洞属于芯片级漏洞，主要影响和风险包括窃取内存数据、造成敏感信息泄漏等。目前尚未发现利用上述漏洞针对个人用户的直接攻击。

《防范指引》就受熔断和幽灵漏洞威胁的四类典型用户，包括云服务提供商、服务器用户、云租户、个人用户等，给出了详细的防范指引，并提供了部分厂商安全公告和补丁链接。其中，云服务提供商和服务器用户应在参考 CPU 厂商和操作系统厂商建议的基础上，结合自身环境制定升级方案，综合考虑安全风险、性能损耗等因素，采取相关安全措施防范安全风险；云租户和个人用户应及时关注云服务提供商、操作系统厂商、浏览器厂商等提供的安全补丁，及时升级，避免受到漏洞的影响。《防范指引》全文可通过访问信安标委网站获

得（www.tc260.org.cn）。

✧ 正式成为法律 特朗普签署新 NSA 监控法

1 月 21 日消息 据外媒报道，当地时间 1 月 19 日，美特朗普总统宣布他已经在对《外国情报监控法（FISA）第 702 条修改再授权法》上签名，也就是说，这个备受争议的新监控条款成为法律。获悉，最新授权将在 2023 年 12 月到期。

特朗普在官方声明中表示，这份法案将能让情报机构收集关于美国外的国际恐怖分子、武器扩散者及其他重要外国情报人员目标的重要情报信息。另外他还表示，比起这样一份有时间期限的法案他更希望它是永久的。

据了解，这份法案于上周在众议院以 256 比 164 的投票结果通过，本周早些时候则以 65 比 34 在参议院通过，现在总统也在上面签上了字。

版权声明