



二零卫士安全公告

2012 第 2 期

(总六十一期)

上海二零卫士信息安全有限公司

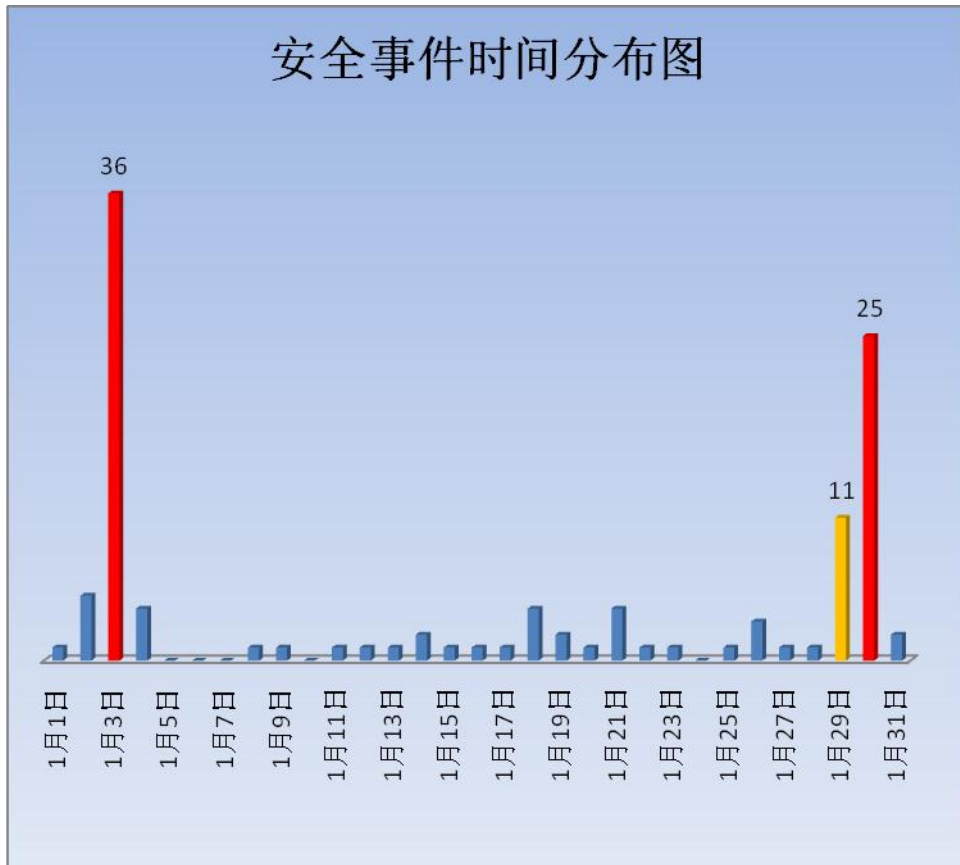
2011-2-6

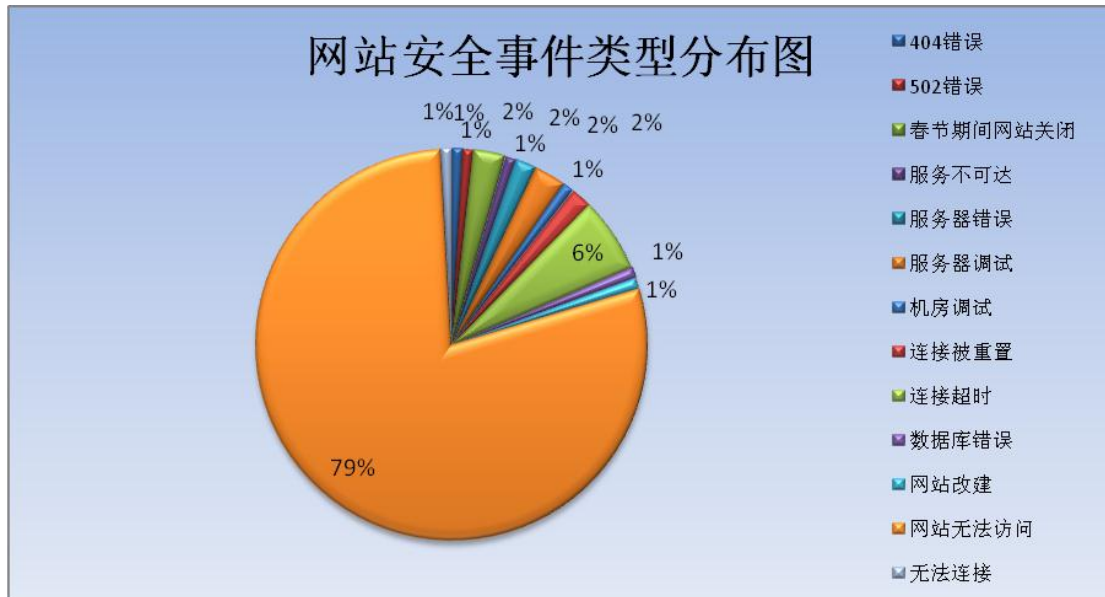
1. 网站监控分析

本月三零卫士监控中心对上海市各区门户网站及下属子网站进行监控。并根据监控情况进行分类统计和汇总。

整体安全情况良好。

从事件类型分析本月三零卫士监控中心所监控的上海市区县网站均较平稳，无严重安全事件。根据本月监控中心汇报，1月3日和1月25日网站事件较多，由于网站分布的服务器较为集中造成只要单台服务器出现故障则有可能出现大面积的网站不可访问，建议采用双机热备方式来缓解此类现象的产生。





2. 网站漏洞分析

本月三零卫士监控中心对上海各区门户网站及下属子网站进行网站漏洞扫描。并根据扫描情况进行分类统计和汇总。

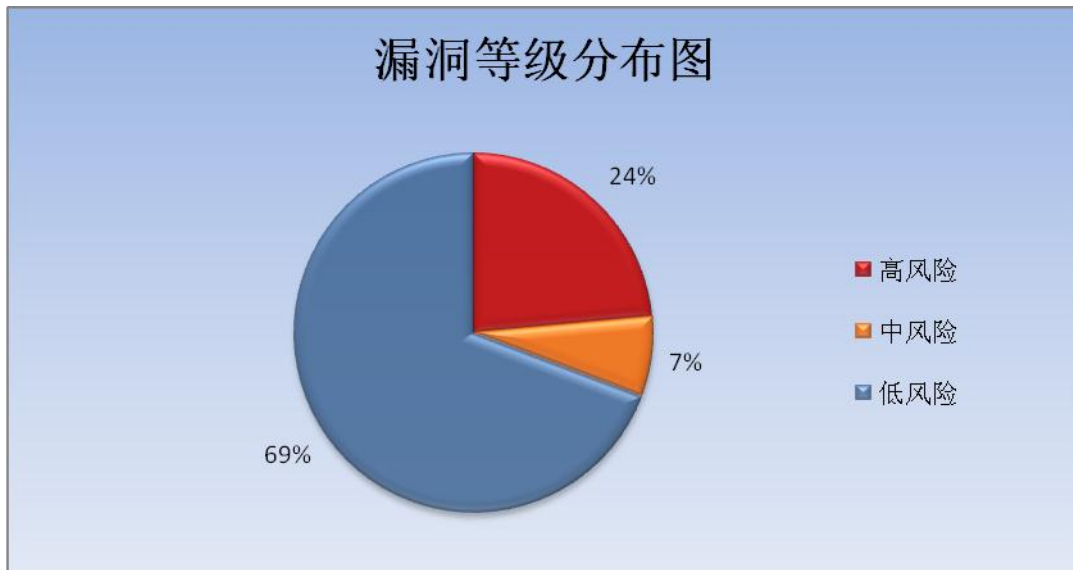
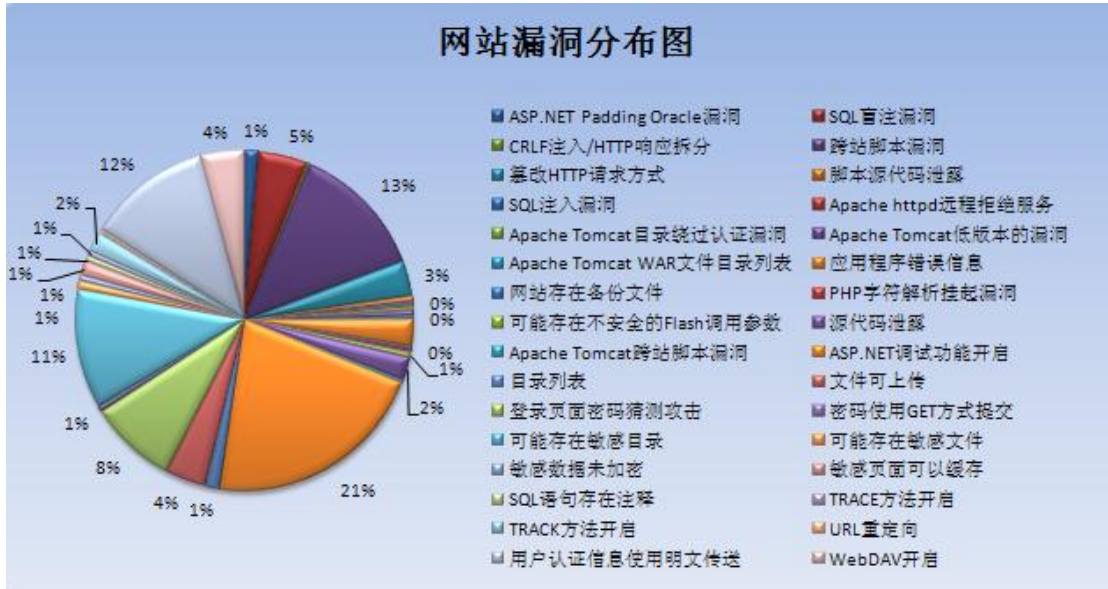
本月三零卫士监控中心为提供扫描服务的网站进行了扫描。各区县委办局门户网站总体情况较好。从本月的扫描可以发现政府网站的高风险主要还是以跨站脚本漏洞（占总漏洞数 13%）、ASP.NET Padding Oracle 漏洞占总漏洞的（占总漏洞数 5%）、篡改 HTTP 请求方式漏洞（占总漏洞数 4%）这三个高风险漏洞为主。

所有扫描的网站中存在高风险网站的数量达到 **51.2%**，基本上每 2 个政府网站即存在 1 个高风险的网站，形式不容乐观。但各区县和市委办局一级门户网站未发现存在高风险漏洞。

由于跨站脚本漏洞（又名：**XSS**）并不像 SQL 注入漏洞那样“立竿见影”，但是跨站脚本漏洞带来的危害也不可小视。它最直接的 3 种危害为：

- 窃取 Cookie，Cookie 一般控制着对 Web 应用程序的访问，如果攻击者偷窃了受害用户的 Cookie，那么攻击者就可以使用受害者的 Cookie 来完全控制受害者的帐户。
- 在受害用户面前假冒成 Web 应用程序，通过假冒 Web 应用程序，攻击者可以将 XSS 用于社会工程。XSS 攻击得手后，攻击者能够完全控制 Web 应用程序的外观。这可用于丑化 web，例如攻击者在页面上放置一个无聊的图片。其中有部分钓鱼攻击使用 XSS 漏洞进行。

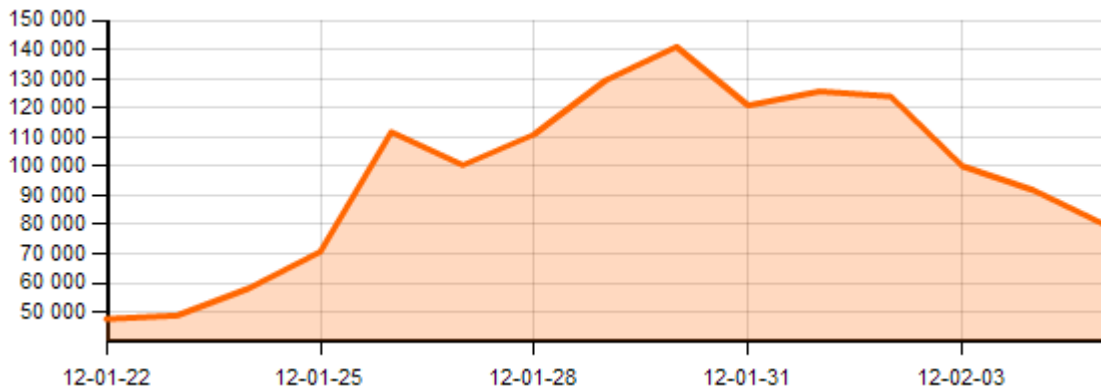
- 在 Web 应用程序面前假冒成受害用，XSS 对 Web 应用程序最大的影响在于，黑客能够通过它假冒成 Web 应用程序的合法用户。



3. 恶意网站分析

恶意拦截排名

排名	网站	今日拦截
1	http://hj688.**222.org	2716
2	http://porschedesign.**666.o...	2400
3	http://88788.**222.org	2188
4	http://jincheng2012.**222.org	1800
5	http://lmysb.**222.org	789



从本周拦截的恶意网站数量来看，本月的恶意网站数量有上升的趋势。

4. 本月热门病毒

病毒名称	警惕程度
Worm.Win32.FakeFolder.c (蠕虫病毒)	高
Trojan.PSW.Win32.Agent.exw (木马病毒)	高
worm_autorun.deep (蠕虫病毒)	高
Trojan.Win32.Generic.129A4F1D (木马病毒)	高
Trojan.Win32.FakeIME.d (木马病毒)	高

本月发现木马型蠕虫病毒。较之早先的以破坏为主的病毒，木马型蠕虫更具有隐蔽性更具破坏性。

5. 本月安全新闻

- **HTC 承认其 Android 手机漏洞或泄露 WiFi 密码**

北京时间 2 月 2 日消息，宏达电 (HTC) 日前承认该公司的部分手机处理特定 Android

请求的方式存在漏洞，可能从而暴露这些手机所连接的 WiFi 网络的安全凭证。

研究人员克里斯·赫斯(Chris Hessing)及布雷特·乔丹(Bret Jordan)发现，在受影响的宏达电手机上，带有 `android.permission.ACCESS_WIFI_STATE` 权限的任何 Android 应用都能够调用 `WifiConfiguration` 上的 `toString()` 指令，查看无线网络的所有安全认证。

如果结合 `android.permission.INTERNET` 权限，黑客就可以获得相关的详细信息，并通过互联网发至远程服务器。

该漏洞影响下列手机：

Desire HD-Versions FRG83D, GRI40

Glacier-Version FRG83

Droid Incredible-Version FRF91

Thunderbolt 4G-Version FRG83D

Sensation Z710e-Version GRI40

Sensation 4G-Version GRI40

Desire S-Version GRI40

EVO 3D-Version GRI40

EVO 4G-Version GRI40

● 卫星电话加密算法被破解

德国的一组研究人员看起来已经破解了被许多卫星电话使用的 `GMR-1` 和 `GMR-2` 加密算法。传统的 `GSM` 和 `UMTS (3G)` 制式手机是与运营商的基站通信，其覆盖距离在几百米和几十公里之间，在大多数情况下已经够用。

卫星电话提供了更广阔距离的通信网络，适合在偏远地区等环境下使用。德国研究人员逆向工程和破解了 `GMR-1` 和 `GMR-2` 加密算法，这意味着对使用这两种算法的卫星电话通话拦截和窃听将成为可能。研究人员的演示系统用了半小时破译了一次通话，表示更强大的计算机将能实时窃听。

电商成黑客敛财新手段 90%电商用户数据外泄

● Diggity 攻击

Stach & Liu 的研究人员 Fran Brown 和 Rob Ragan 编写了一系列工具“Diggity”，能够加快通过 Google 或 Bing 搜索检测安全漏洞的过程。目的是让企业比黑客更快地发现其服务器中的这些漏洞：SQL 注入、跨站脚本漏洞等。

在进行 Google Hacking 通常需要搜索一个域，当你面对企业数百个域时，这根本不足一提。Brown 表示，Diggity 工具类似于嗅探出已知攻击的入侵防御系统，这些工具是基于已知谷歌和 Bing 攻击数据库、Foundstone 的搜索引擎攻击资料库和 Stach & Liu 自己的已知漏洞和攻击数据库。

它的工作原理是这样的：当攻击发现一个潜在攻击时，它们会向企业发送一个谷歌提醒，随后谷歌会停止索引，这给企业时间来修复漏洞。

6. 二零三零服务

网站渗透测试

采用完全模拟入侵者可能使用的攻击技术，利用专家经验对网络中常用的应用系统等进行非破坏性质的模拟攻击，发现系统最脆弱的环节。给执行人员、管理层、技术人员提供一份全面的安全报告，以辅助进行系统信息安全风险管理的相关决策。

咨询热线：800-820-5530 (400-820-5530)

地址：上海市徐汇区龙吴路 777 号 11 号楼 3 楼

网址：<http://www.30wish.net>

邮件：30services@30wish.net

传真：021-54363095

或下述地区

上海请拨打：021-55313030

南京请拨打：025-86210976

杭州请拨打：0571-28913098

广州请拨打：020-38288430

武汉请拨打：027-88612165