NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

网站安全之痛

杜跃进　博士
国家网络信息安全技术研究所　所长
CNCERT/CC　副总工

2012.1.6　YOCSEF 北京

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

内 容

* 网站安全的重要性
* 我国网站安全形势
* 问题根源
* 出路所在

网站安全：从“脸面”问题到“中枢”问题

* 早期的网站安全：主要是“面子”问题
  * 2001年的“中美黑客大战”
* 趋利敲诈
* 钓鱼设套
* 挂马
* 后台数据

随着HTTP一统天下，网站在整个信息化社会中扮演的角色不断深化，网站安全已不再是“脸面”问题；网站在成为几乎各种信息服务“门户”的同时，也成为实施攻击的主要“门户”或“中枢”

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

我国的网站安全问题突出

* 网页篡改问题依然严重
* 总体趋势有所改善
  * 特别是政府网站的安全水平

但是，这些数据并不反映全貌，很多隐蔽攻击尚不具备发现能力

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

问题根源：为什么？

* 意识淡薄：不重视或不知该怎么重视
  * 讨论安全时，领导们在哪？
  * 当联系到“问题网站”时，对方不以为然
* 技术短板：代码安全能力薄弱
  * 赖不着微软了，赖谁？
  * “自主”了？“可控”吗？
* 制度缺陷：定位太低强制要求不足
  * 合规性方面的法律要求？
  * 安全工作三阶段之第三阶段？

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

出路所在：做什么

- 重新认识：时代已不同于2008奥运期间
  - 既然不仅仅是面子问题，就必须真正重视起来
  - 尤其是重要的或大型网站安全，需要按照更高标准要求
- 政府层面的工作至关重要
  - 政府 VS 互联网安全，从来不该是旁观者
  - 法律、政策、标准；监督、检查、执法
  - 战略制定、个人信息保护、代码安全要求，etc
- 企业要有长远战略与社会责任
- 安全界和第三方提升服务能力
- 用户安全意识的不断提高

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

谢　谢

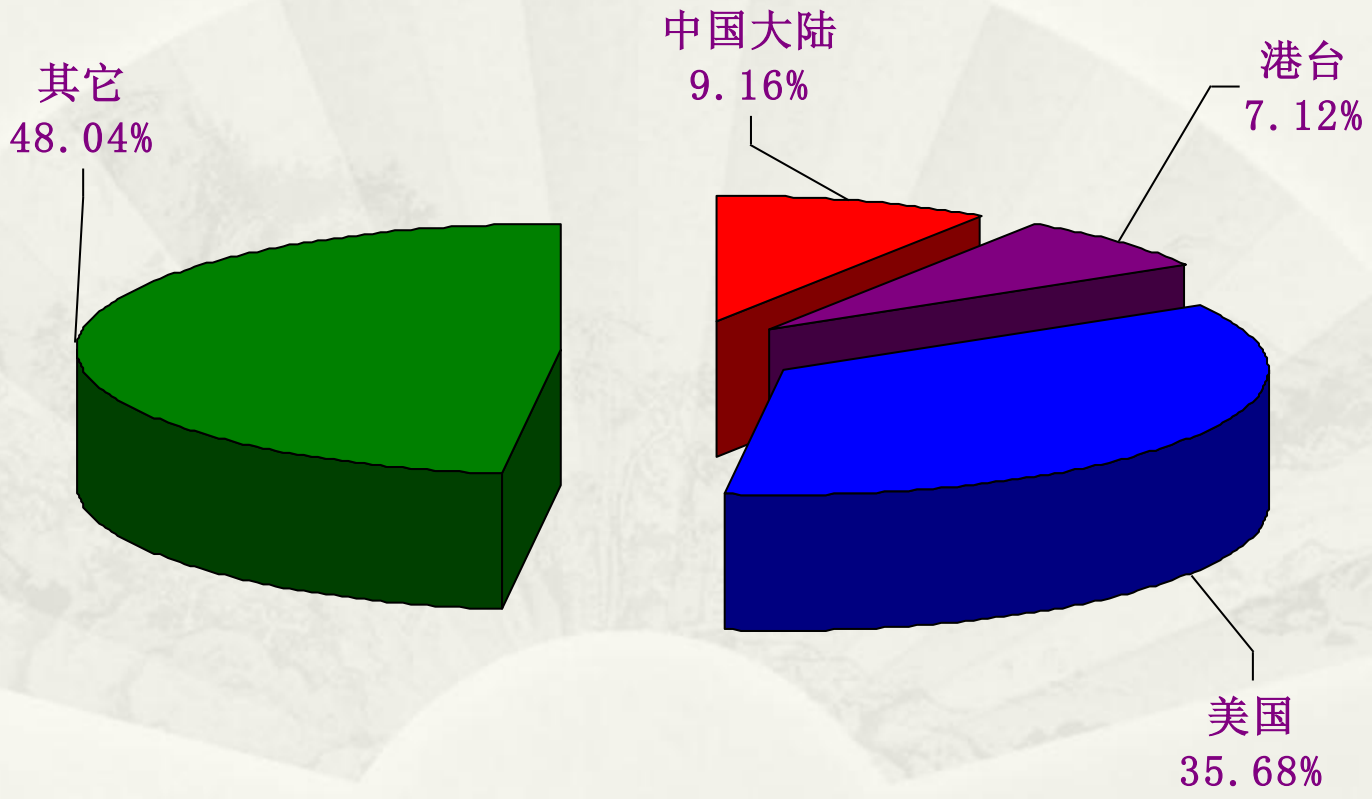
欢迎探讨

2001年所谓“中美黑客大战”

- 四月-五月初，近600个中国网站被成功攻击，网页被篡改
- 五月一日至七日，中美两国网页篡改的数量明显增强

- 结论：
  - 发生了中美之间集中的网页篡改攻击
  - 政治影响恶劣

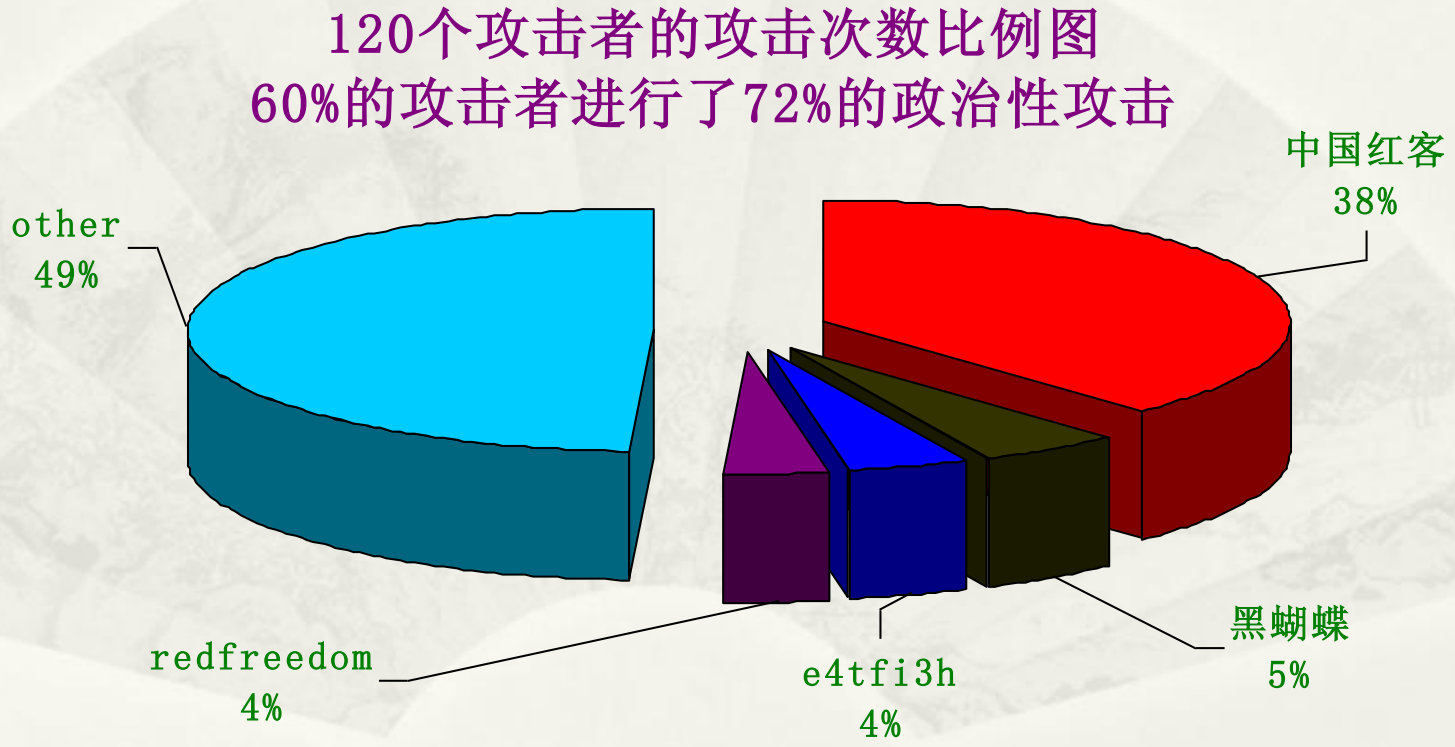
五月1-7日中美被攻态势



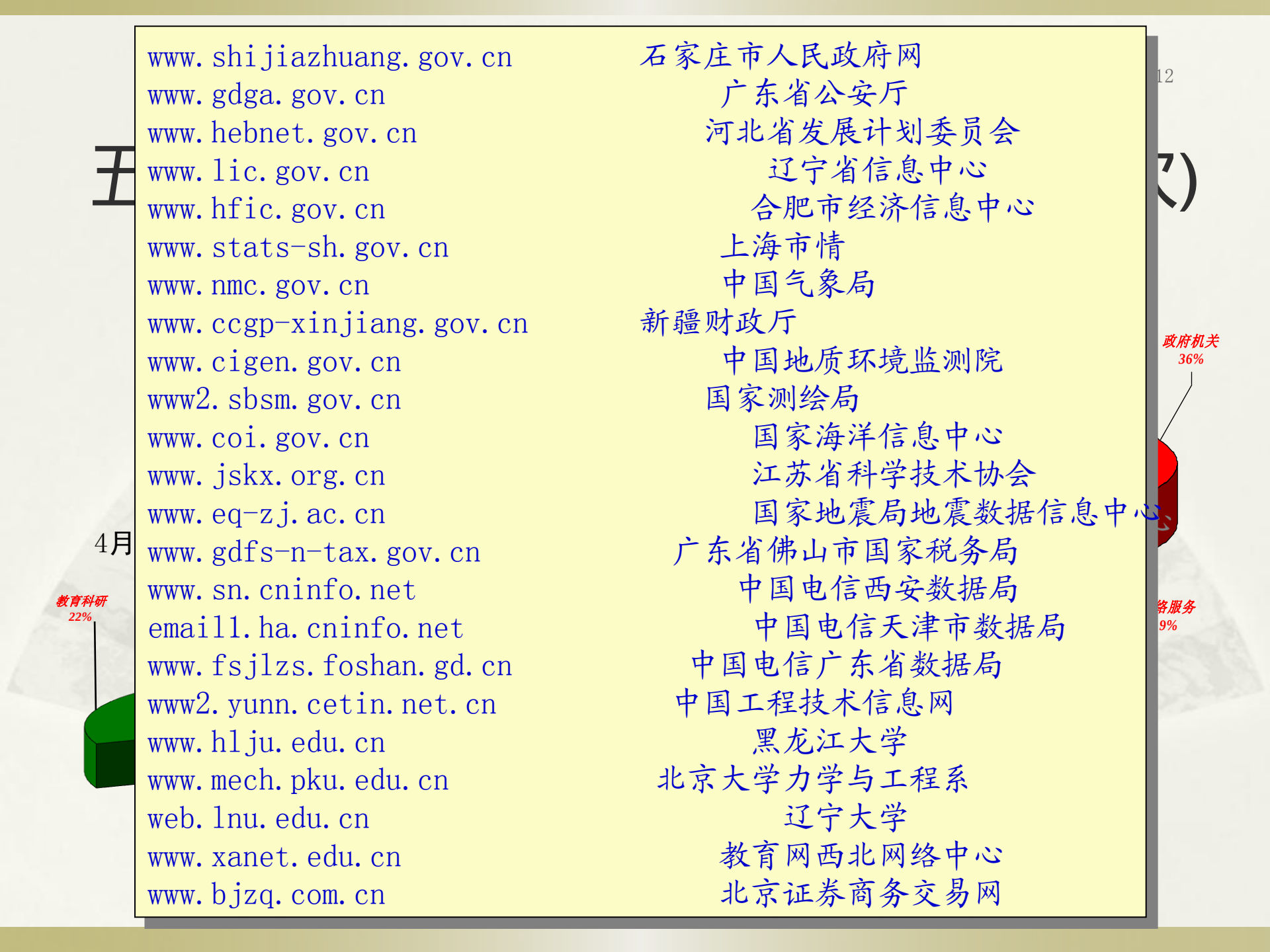
五月1-7日对美国网站的攻击(1041次)

www.deland.org	DeLand Community Development (DELAND2-DOM)
130.39.100.123	Louisiana State University (LSU-DOM)
philadox.phila.gov	City Of Philadelphia (PHILA-DOM)
www.alacoyotes.org	Arizona Lutheran Academy (ALACOYOTES-DOM)
63.230.120.233U S	WEST Communication Services (USWEST2-DOM)
www.kernfcu.org	Kern Federal Credit Union (KERNFCU2-DOM)
199.249.165.170	Northwestern University (NUNET2-DOM)
131.230.182.144	Southern Illinois University (SIU-DOM)
outlook.das.state.or.us	Oregon State Government
202.128.71.246	Guam Community College
www.naval-air.org	MUSEUM NAMVALAVIATION
www.apo.data.faa.gov	Federal Aviation Administration (FAA-DOM)
www.gmcu.org	Gateway Metro Credit Union (GMCU-DOM)
www-staging.t-bird.edu	Thunderbird, The American Graduate School of International

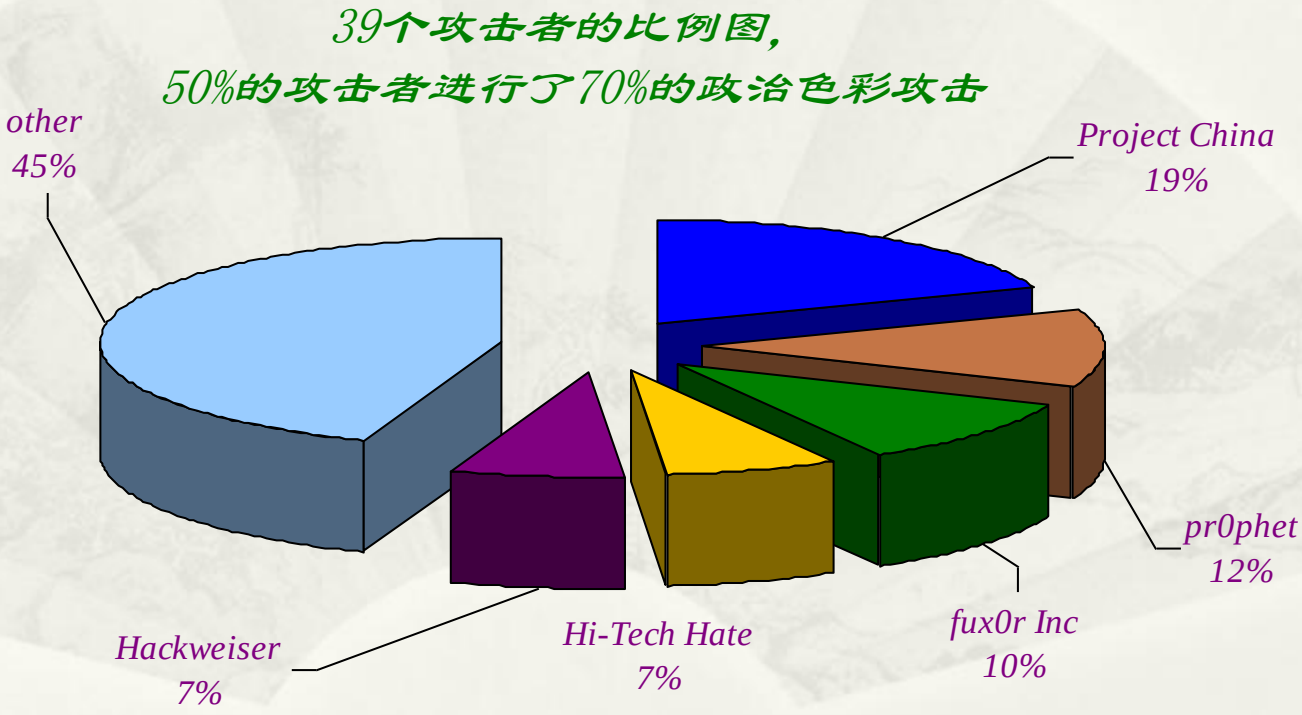
五月1-7日对美国网站的攻击来源



www.shijiazhuang.gov.cn	石家庄市人民政府网
www.gdga.gov.cn	广东省公安厅
www.hebnet.gov.cn	河北省发展计划委员会
www.lic.gov.cn	辽宁省信息中心
www.hfic.gov.cn	合肥市经济信息中心
www.stats-sh.gov.cn	上海市情
www.nmc.gov.cn	中国气象局
www.ccgp-xinjiang.gov.cn	新疆财政厅
www.cigen.gov.cn	中国地质环境监测院
www2.sbsm.gov.cn	国家测绘局
www.coi.gov.cn	国家海洋信息中心
www.jskx.org.cn	江苏省科学技术协会
www.eq-zj.ac.cn	国家地震局地震数据信息中心
www.gdfs-n-tax.gov.cn	广东省佛山市国家税务局
www.sn.cninfo.net	中国电信西安数据局
email1.ha.cninfo.net	中国电信天津市数据局
www.fsjlzs.foshan.gd.cn	中国电信广东省数据局
www2.yunn.cetin.net.cn	中国工程技术信息网
www.hlju.edu.cn	黑龙江大学
www.mech.pku.edu.cn	北京大学力学与工程系
web.lnu.edu.cn	辽宁大学
www.xanet.edu.cn	教育网西北网络中心
www.bjzq.com.cn	北京证券商务交易网



五月1-7日对中国网站的攻击来源



NINIS
NATIONAL INSTITUTE OF NETWORK AND INFORMATION SECURITY

网站

2011-12-19-25日

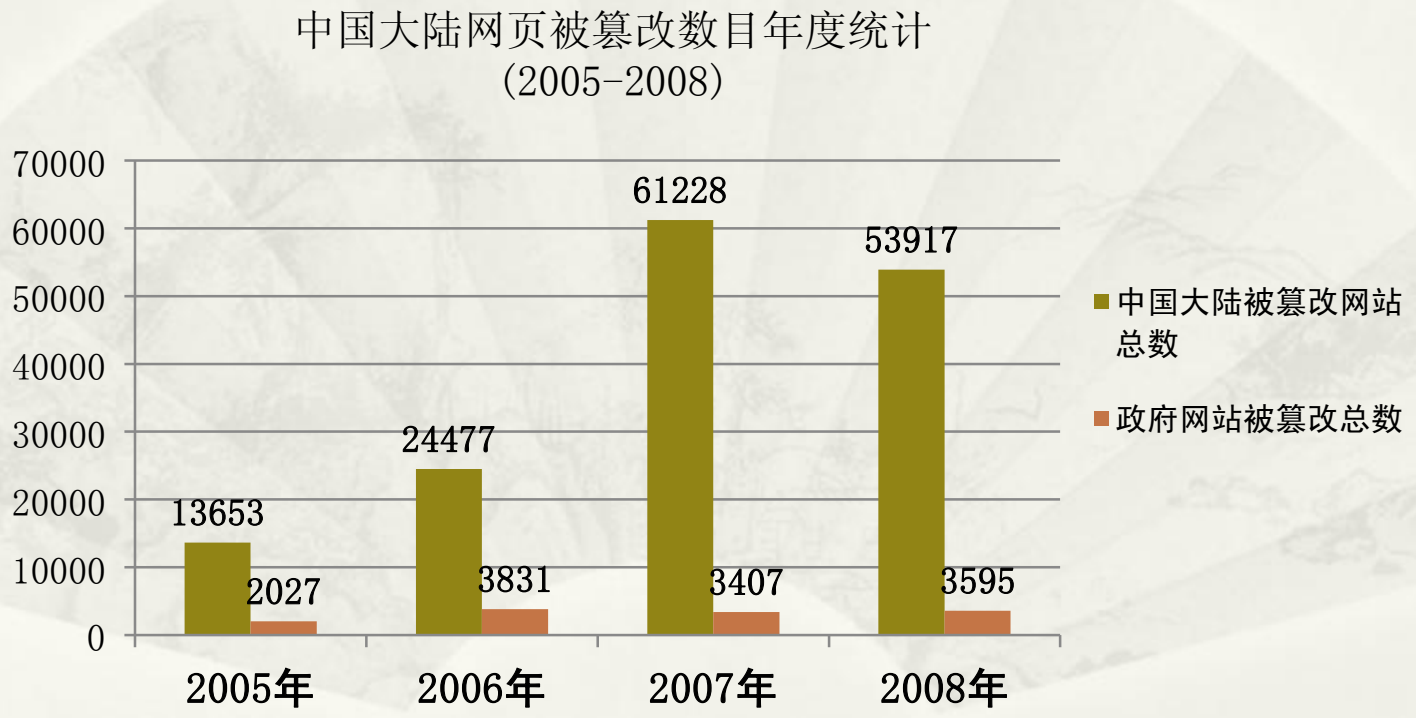
名称	特点
Win32.Troj.Generic	该病毒通过网页下载的方式传播，会释放C:\Documents and Settings\All Users\Application Data\Tencent\QQDownload\QQ.exe和QQ.exe；在开始菜单启动文件夹和run创建启动项，指向C:\Documents and Settings\All Users\Application Data\Tencent\QQDownload\QQ.exe；在run下创建启动项，指向C:\Documents and Settings\All Users\Application Data\Tencent\QQDownload\QQ.exe
Win32.Troj.Agent.xb	该病毒通过网页下载的方式传播，会修改winlogon，指向C:\WINDOWS\system32\init.exe；在run下创建启动项，指向C:\WINDOWS\windowsmp.exe；在各盘根目录下释放explorer.exe创建autorun.inf，autorun.inf指向explorer；创建服务4LLI
Win32.Troj.Scar	该病毒通过网页下载到的方式传播，会释放创建文件.C:\Documents and Settings\Administrator\Application Data\rundx.dll和c:\ documents and settings \ administrator \ application data\microsoft\windows\3dtext.scr；添加开机启动项3dtext.scr；设置文件夹隐藏属性
Win32.TrojDownloader.Agent	该病毒通过网页下载的方式传播，会在后台安装快快、百度浏览器、百度地址栏、UUSee及RKLauncher；在桌面、开始菜单和快速启动栏里释放浏览器上网.lnk、淘喜欢.lnk，指向C:\Program Files\ilovetb\TheWorld.exe，C:\Program Files\iloveu\TheWorld.exe；将主页篡改为http://www.sky238.com/?107m；在开始菜单启动文件夹里释放脚本；修改http关联，指向http://www.sky238.com/?1076.[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run]创建启动项
Win32.Loader.bx.368640	该网购木马病毒通过网页下载的方式传播，会利用暴风影音的升级程序，加载StormUpdate.dll，后打开verifier.exe进程，在把同目录下的加密后version.dat解密，然后注入系统verifier.exe进程，在用户使用网银充值时，在支付页面前，劫持到一个正常的中国联通充值卡的网站，让用户在这里购买手机充值卡，然后在付款后，购买的充值卡落入病毒作者之手

2011-12-19-25日

名称	
Hack.Exploit.Script.JS.Agent.ji	该脚本 该病毒会 话才会攻 溢出后会 者指定的
Trojan.Script.JS.Pop.a	该脚本 恶意弹窗
Trojan.Win32.StartPage.qfq	该木马 杀毒软件
Macro.Xl4Poppy	该宏 当用户再 开的文件
Worm.Win32.FakeFolder.c	该蠕 向恶意网

2005-2008网页篡改年度统计对比

中国大陆网页被篡改总数年度统计，可以看到，2007、2008年被篡改总数均超过50000，政府网站被篡改数2006年起均超过3400。



2011年1-11月：近3.5万个网站被篡改，政府网站2644个

2005-2008网页篡改年度统计对比

2007、2008年政府网站（.gov.cn）被篡改总数与2006年基本持平，但比例已经降低，不过仍旧高于当年.gov.cn占.cn网站的比例，2008年底.gov.cn占.cn网站总数的1.1%。