国家互联网应急中心

2015 年第 33 期

8 月 10 日-8 月 16 日

网络安全信息与动态周报

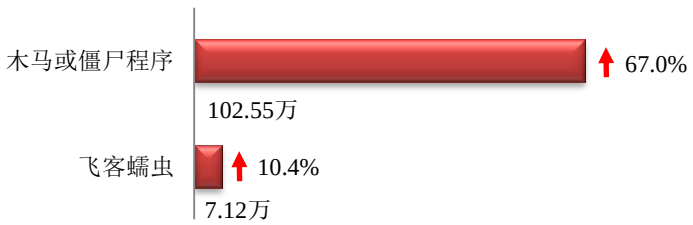
本周网络安全基本态势

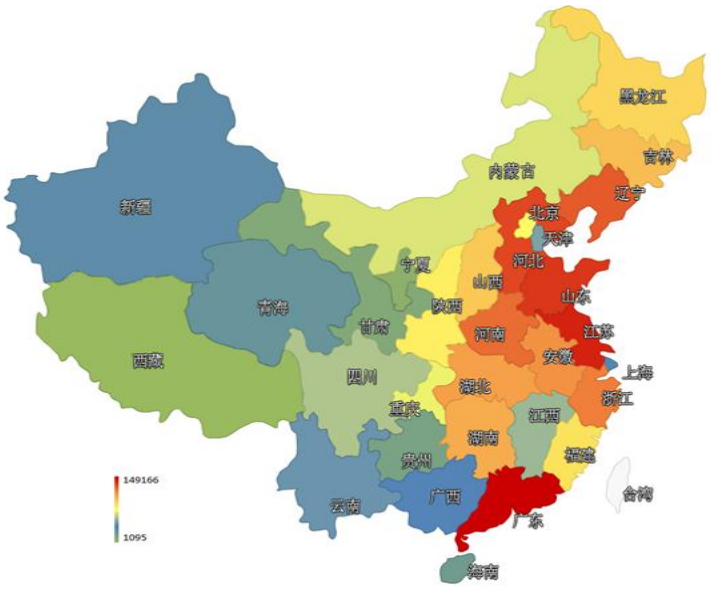
境内感染网络病毒的主机数量	•109.67万	↑61.6%
境内被篡改网站总数 其中政府网站数量	•5421 •115	↑9.9% ↑8.5%
境内被植入后门网站总数 其中政府网站数量	•2702 •134	↓6.3% ↑7.2%
针对境内网站的仿冒页面数量	•6359	↑23.3%
新增信息安全漏洞数量 其中高危漏洞数量	•130 •60	↑51.2% ↑30.4%

=表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 109.67 万个，其中包括境内被木马或被僵尸程序控制的主机约 102.55 万以及境内感染飞客（conficker）蠕虫的主机约 7.12 万。



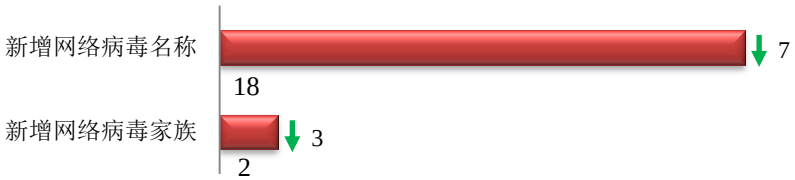


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和山东省。

TOP3

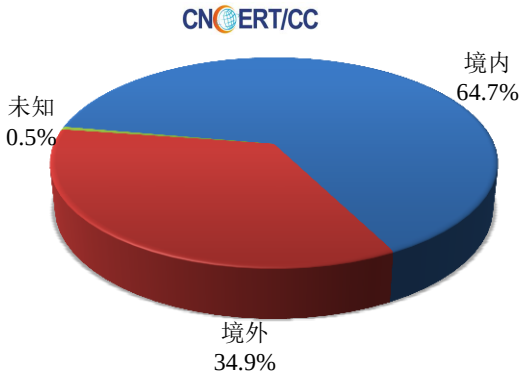
广东省	•约14.9万个（约占中国大陆总感染量的14.6%）
江苏省	•约10.3万个（约占中国大陆总感染量的10.0%）
山东省	•约9.7万个（约占中国大陆总感染量的9.5%）

本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 18 个，按网络病毒家族统计新增 2 个。

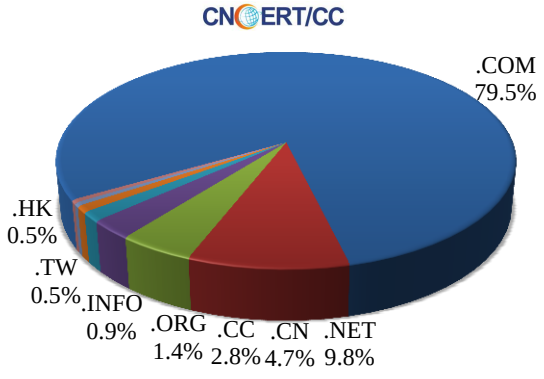


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 215 个，涉及 IP 地址 341 个。在 215 个域名中，有约 34.9%为境外注册，且顶级域为.com 的约占 79.5%；在 341 个 IP 中，有约 19.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 50 个 IP。

本周放马站点域名注册所属境内外分布
(8/10-8/16)



本周放马站点域名所属顶级域的分布
(8/10-8/16)



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

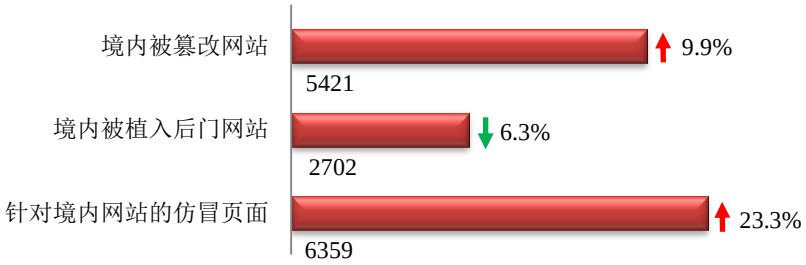
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

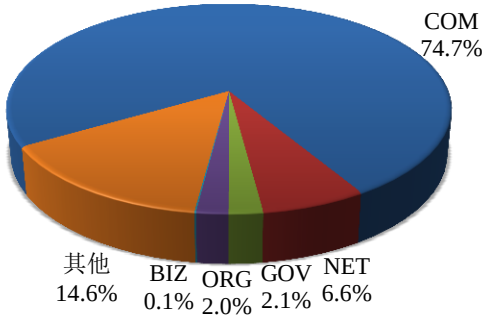
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 5421 个；境内被植入后门的网站数量为 2702 个；针对境内网站的仿冒页面数量为 6359。

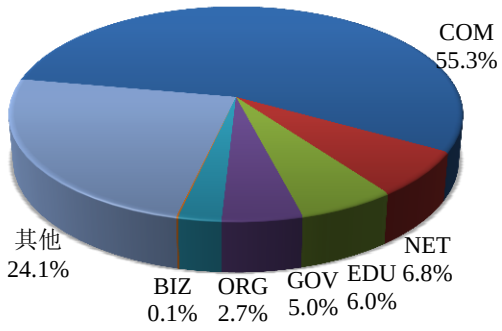


本周境内被篡改政府网站(GOV 类)数量为 115 个（约占境内 2.1%），较上周环比上升了 8.5%；境内被植入后门的政府网站(GOV 类)数量为 134 个（约占境内 5.0%），较上周环比上升了 7.2%；针对境内网站的仿冒页面涉及域名 5310 个，IP 地址 851 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/10-8/16)

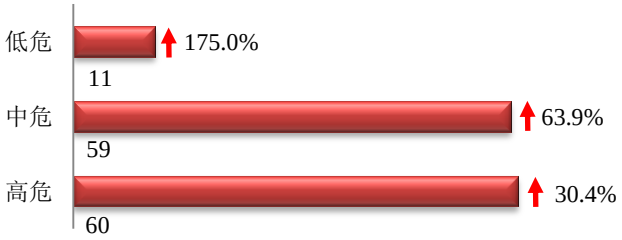


本周我国境内被植入后门网站按类型分布
(8/10-8/16)

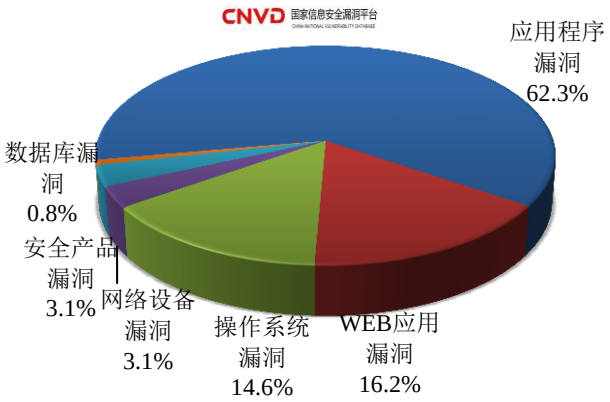


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 130 个，信息安全漏洞威胁整体评价级别为中。



本周CNVD收录漏洞按影响对象类型分布
(8/10-8/16)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是 WEB 应用漏洞和操作系统漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

CNVD漏洞周报发布地址

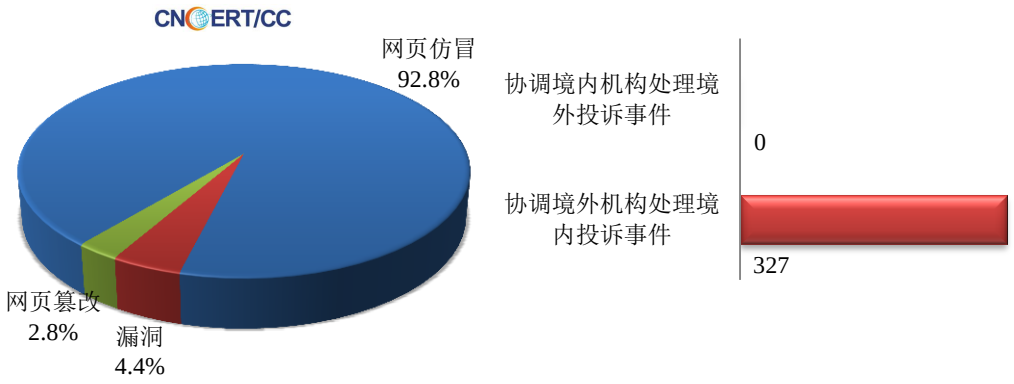
http://www.cnvd.org.cn/webinfo/list?type=4

国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

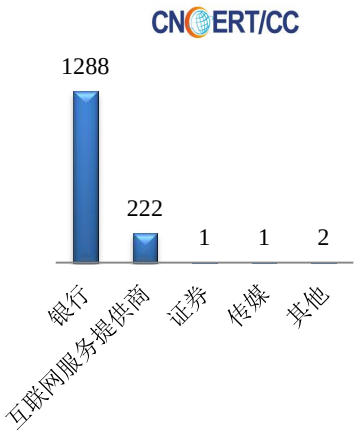
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1631 起，其中跨境网络安全事件 327 起。

本周CNCERT处理的事件数量按类型分布
(8/10-8/16)

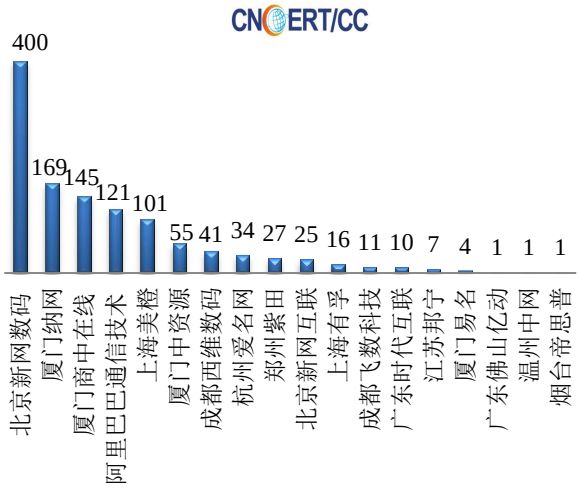


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1514 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1288 起和互联网服务提供商仿冒事件 222 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/10-8/16)



本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/10-8/16)



本周，CNCERT 协调 3 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 4 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名 (8/10-8/16)

业界新闻速递

1、公安部：推进网站信息安全等级保护工作

中国网信网 8 月 10 日消息 公安部在近日召开的全国重点互联网站和服务企业安全管理工作会议上透露，公安部门将与互联网管理部门密切合作，就推进互联网安全管理和网络社会法治建设工作推出一系列举措。公安部有关负责人介绍，随着互联网新业务新应用的快速发展，网络攻击、网络传播暴力恐怖信息、网络诈骗、窃取网民个人信息，以及网络黄赌毒等违法犯罪活动多发，已成为影响国家安全和社会稳定的突出问题。为进一步强化互联网安全管理，公安机关将与互联网管理部门密切合作，全面推进网站信息安全等级保护工作，提升网站防范非法入侵破坏、保护网民个人信息的能力；全面推行网警网上公开巡查执法，及时发现制止各类违法活动；在重点网站和互联网企业设立“网安警务室”，第一时间掌握网上涉嫌违法犯罪情况，服务和指导网站

提高安全管理防范能力；严厉打击网络非法入侵破坏、窃取网民个人信息、网络盗窃、网络诈骗和制造传播网络谣言等多发性网络违法犯罪，全面清理整治网上暴恐、涉枪涉爆和涉黄赌毒等违法信息，依法保护互联网企业和广大网民的合法权益。根据会议要求，重点网站和互联网企业须落实网站安全管理的组织、人员，健全、规范安全管理制度；坚守法律和道德底线，不渲染可能诱发犯罪的敏感案事件，不登载传播低俗有害信息；妥善处理网民的举报投诉，及时发现并向公安机关提供网络违法犯罪线索，并主动配合做好调查取证工作。

2、美国将发布《联邦民用网络安全战略》

网易 8 月 10 日消息 在美国联邦人事管理办公室遭遇严重的数据泄露事件后，美国政府发起了为期 30 天的网络安全冲刺。美国行政管理和预算局下设的电子政府和信息技术办公室、国家安全委员会网络安全理事会、国土安全部和国防部的网络安全专家组成了多个跨部门的网络冲刺小组，研究如何支撑联邦政府的系统安全，以避免类似联邦人事管理办公室泄露事件的网络入侵再次发生。美国行政管理和预算局将于近期发布《联邦民用网络安全战略》。冲刺小组从总体上审视了各个部门及联邦政府的网络安全政策以最终确定哪些部门的政策合乎标准，或者找出严重的漏洞。他们的研究主要致力于以下 8 个领域。保护数据：更好地保护静态的和传输中的数据；提升态势感知能力：增加检测与预警；提高人员的网络安全专业素养：确保吸引网络安全专业人员的能力；增强网络安全意识：从整体上提升安全风险意识；使程序标准化、自动化：减少网络配置和为漏洞安装补丁的时间；网络安全事故的控制和恢复：抑制恶意软件的扩散和特权用户的增加，快速识别、处置网络安全事故；强化系统的生命周期安全：通过采购更安全的系统提升平台的内在安全，并及时淘汰陈旧的系统；缩小攻击面：降低网络防御者实施保护的复杂程度。

3、英国强化个人信息安全屏障

人民网 8 月 14 日消息 据英国《卫报》报道，在欧洲有着上千家分店的英国知名手机零售商“汽车手机仓库”日前承认近期遭到“蓄意策划”的网络黑客袭击，导致大约 240 万用户的个人信息及 9 万名用户的信用卡资料泄露。由于这家手机零销商还运营着多家网站，这些相关网站的信息也可能遭到黑客破坏。英国信息监管局在接到报案后，开始联合警方展开调查。英国信息监管局的发言人强调说，这些被泄露的个人信息“很可能会被用于欺诈活动中，比如用来盗刷银行卡等”，因此建议可能受影响的用户尽快采取“预防措施”，以加强对自身敏感信息数据的保护。在英国，政府十分重视保护个人信息数据，尤其是涉及银行、金融等敏感而重要的个人资料，一些法律条文甚至还规定对泄露个人数据的公司和个人实施经济重惩等。为保证个人信息安全，英国议会早在 1984 年就通过了《数据保护法》，并设立数据保护登记官一职，以确保该法得到监管执行。1998 年，议会对这一法案进行了修订，加大了对公民个人数据的保护力度。此后，英国又陆续通过了《调查权法》、《通信管理条例》和《通信数据保护指导原则》等一系列旨在保护公民个人数据信息的法律、法规和条例。眼下，越来越多英国民众的网络信息安全意识正在不断提高，英国政府适时推出了一个总额 6.5 亿英镑的“网络安全战略”，意在整体提升国家的网络安全水平，净化和优化民众的上网环境，为公司和个人的网络安全信息数据构筑一道安全屏障。

4、网络安全军火商泄露惊天内幕：国际黑客联系针对中国发起攻击

赛迪网 8 月 11 日消息 Hacking Team 是一家在意大利米兰注册的软件公司，主要向各国政府及法律机构销售入侵及监视功能的软件。其远程控制系统可以监测互联网用户的通讯、解密用户的加密文件及电子邮件，记

录 Skype 及其它 VoIP 通信，也可以远程激活用户的麦克风及摄像头。其总部在意大利，雇员 40 多人，并在安纳波利斯和新加坡拥有分支机构，其产品在几十个国家使用。7 月 5 日晚，Hacking Team 服务器被攻击，其掌握的 400GB 数据泄露出来，由此引发的动荡，引起了业界一片哗然，里面有 Flash 0day, Windows 字体 0day, iOS enterprise backdoor app, Android selinux exploit, WP8 trojan 等等核武级的漏洞和工具，其远程控制系统可以突破系统默认以及杀毒软件的安全防护，后台监控用户的网络通讯、解密用户的加密文件及电子邮件， 记录 Skype 和其它 VoIP 工具的聊天内容，以及远程激活用户的麦克风及摄像头。在 Hacking Team 泄露的 400GB 数据当中，查到韩国和哈萨克斯坦曾跟 Hacking Team 合作利用其开发漏洞利用工具发起针对中国攻击的证据。这些已泄露额信息可以表明，中国才是国际化网络攻击的受害者。在报告中发现一些亚洲地区国家对我国进行的网络攻击窃密的铁证，甚至一些攻击已经得手，成功的控制了国内目标的 PC 或手机。攻击方还会对新发现的问题做针对性的要求，保证更隐秘的监控和机密信息的回传。

5、美报披露美电信巨头协助情报机构进行大规模监听

新华网 8 月 16 日消息 美国《纽约时报》15 日披露，电信业巨头美国电话电报公司对美国国家安全局的大规模网络和电信监听能力提供协助，近日曝光的国家安全局秘密文件称双方长达 20 余年的合作伙伴关系为“高度协作”，并且美国电话电报公司“极为愿意”提供协助。这些文件由前防务承包商雇员爱德华·斯诺登提供，标注时间为 2003 年至 2013 年。文件透露，国安局与美国电话电报公司的合作时间最长，始于 1985 年，代号为“锦绣”，而与另一个电信业巨头韦里孙通信公司的合作代号为“风暴酝酿”。文件表明，国安局与美国电话电报公司的合作独特且特别富有成效，在规模上远超与韦里孙通信公司的合作。据报道，国安局的大规模监听活动依赖于同美国电话电报公司非同寻常的合作，双方合作涉及范围广泛的秘密活动。美国电话电报公司依据不同的法律规定，通过多种方式，使国安局获取利用该公司位于美国本土网络系统的数十亿封电子邮件。根据最新的文件披露，到 2011 年，美国电话电报公司开始每天向国安局发送 11 亿份国内手机通话记录。这个数据让人触目惊心，因为美国情报官员曾经称，出于技术原因，他们主要收集固定电话通话记录。同年，国安局为与美国电话电报公司的合作花费了约 1.89 亿美元，是与韦里孙通信公司合作预算的两倍多。美国电话电报公司在它至少 17 个位于美国本土的互联网中心安装了监视设备，公司工程师总是最先试用国安局开发的监听技术。另外，国安局秘密文件还显示，美国电话电报公司并非简单地向国安局提供数据，由后者自行筛选，而是事先对数据进行了筛选，再把政府认为可以合法收集的信息传送给国安局。

6、以色列多个官方网站遭黑客组织“匿名者”攻击

环球网 8 月 12 日消息 据伊朗英语新闻电视台“Press TV”报道，黑客组织“匿名者”日前攻击了大量以色列官方网站，对报复以色列释放一起纵火袭击案犯罪嫌疑人的做法。据报道，这起针对一个巴勒斯坦家庭的纵火案导致一名婴儿及其父亲遇难。据报道，包括以色列总理办公室、以色列军方以及外交部长和财政部长在内大约 54 个网站都遭受攻击，它们在多达 12 小时内处于离线状态或遭遇技术故障。随后，黑客组织“匿名者”发布了一份声明，声称他们的攻击是对“犯罪国家”释放纵火案嫌疑人的回应。特拉维夫 9 日释放了所有被扣留的与近日一起纵火袭击有关的嫌疑人，他们涉嫌在 7 月 31 号用燃烧弹袭击了约旦河西岸 Duma 村的一所巴勒斯坦民居。18 个月大的婴儿 Ali Dawabsheh 在袭击中被烧死，婴儿的父亲随后也不治身亡。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2014 年，CNCERT 与 63 个国家和地区的 144 个组织建立了“CNCERT 国际合作伙伴”关系。

联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：何世平

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82991373