国家互联网应急中心

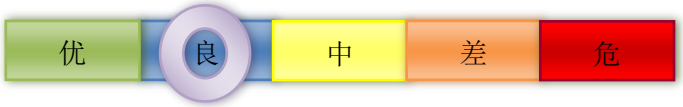
2017 年第 33 期

8 月 7 日-8 月 13 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

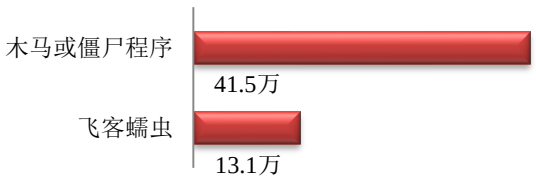


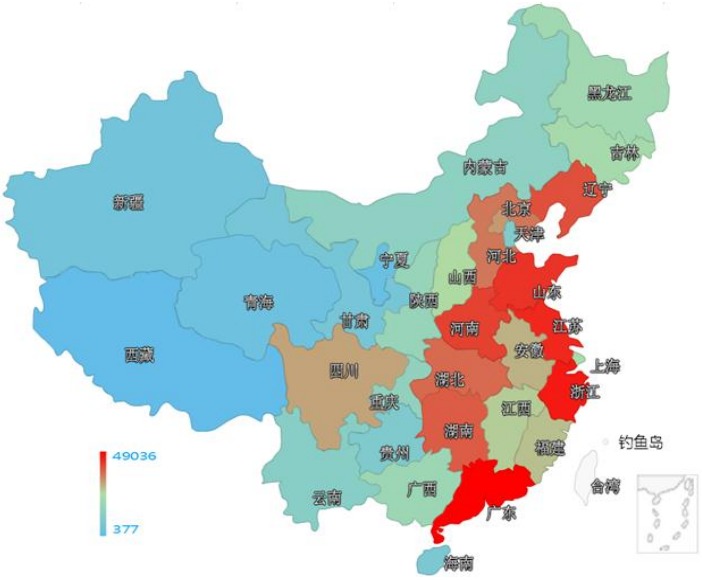
境内感染网络病毒的主机数量	•54.6万	↑ 32.4%
境内被篡改网站总数 其中政府网站数量	•2692 •64	↑ 28.6% ↑ 6.7%
境内被植入后门网站总数 其中政府网站数量	•927 •62	↓ 39.3% ↓ 48.8%
针对境内网站的仿冒页面数量	•117	↓ 66.7%
新增信息安全漏洞数量 其中高危漏洞数量	•302 •107	↑ 42.5% ↑ 18.9%

= 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 54.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.5 万以及境内感染飞客（conficker）蠕虫的主机约 13.1 万。





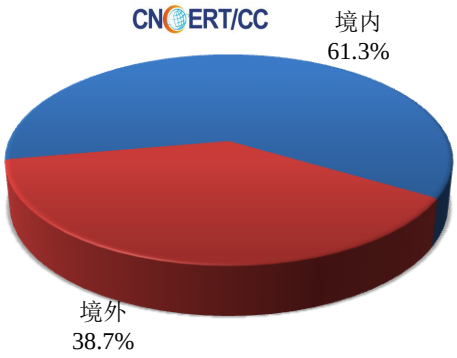
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

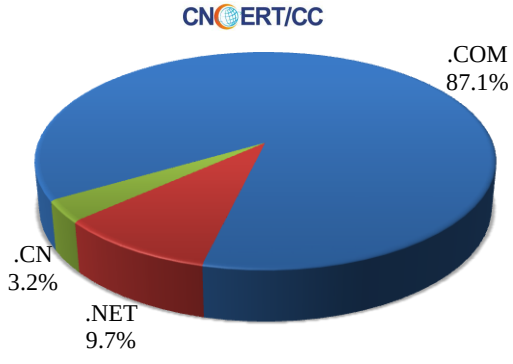
广东省	• 约4.9万个（约占中国大陆总感染量的11.8%）
浙江省	• 约4.5万个（约占中国大陆总感染量的10.9%）
江苏省	• 约3.5万个（约占中国大陆总感染量的8.5%）

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 31 个，涉及 IP 地址 44 个。在 31 个域名中，有 38.7%为境外注册，且顶级域为.com 的约占 87.1%；在 44 个 IP 中，有约 6.8%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 1 个 IP。

本周放马站点域名注册所属境内外分布
(8/7-8/13)



本周放马站点域名所属顶级域的分布
(8/7-8/13)



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。

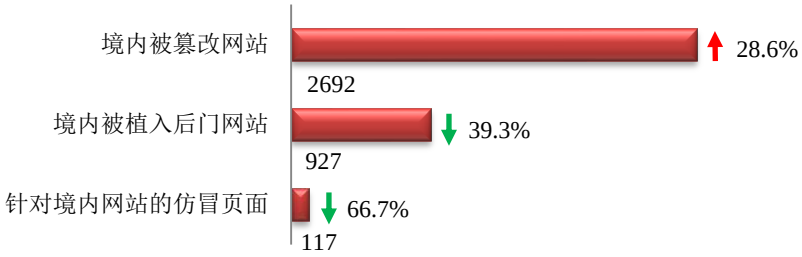
ANVA恶意地址黑名单发布地址

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。

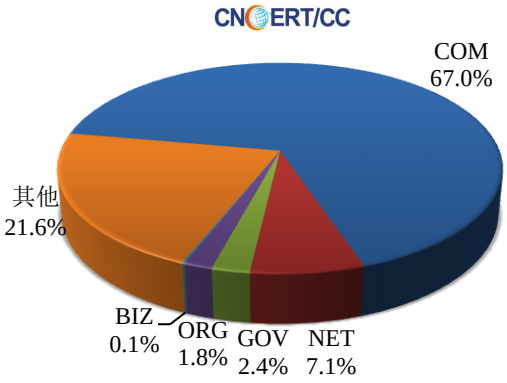
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2692 个；境内被植入后门的网站数量为 927 个；针对境内网站的仿冒页面数量为 117。

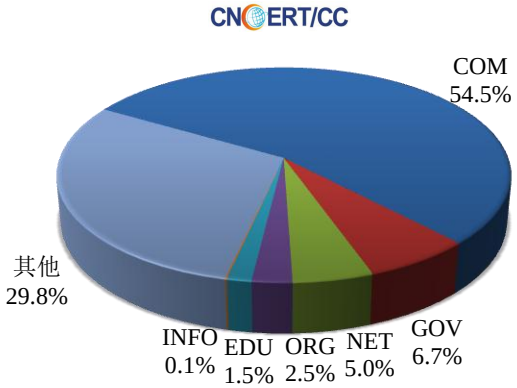


本周境内被篡改政府网站（GOV 类）数量为 64 个（约占境内 2.4%），较上周环比上升了 6.7%；境内被植入后门的政府网站（GOV 类）数量为 62 个（约占境内 6.7%），较上周环比下降了 48.8%；针对境内网站的仿冒页面涉及域名 103 个，IP 地址 60 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/7-8/13)

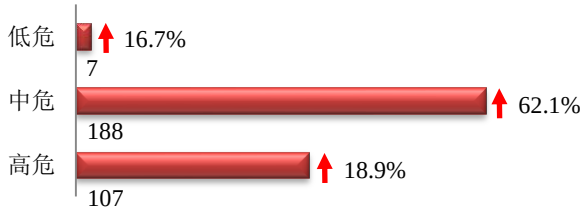


本周我国境内被植入后门网站按类型分布
(8/7-8/13)

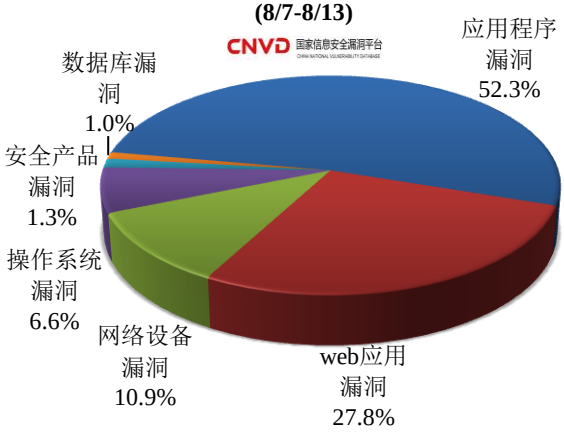


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 302 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
(8/7-8/13)



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 应用漏洞和网络设备漏洞。

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

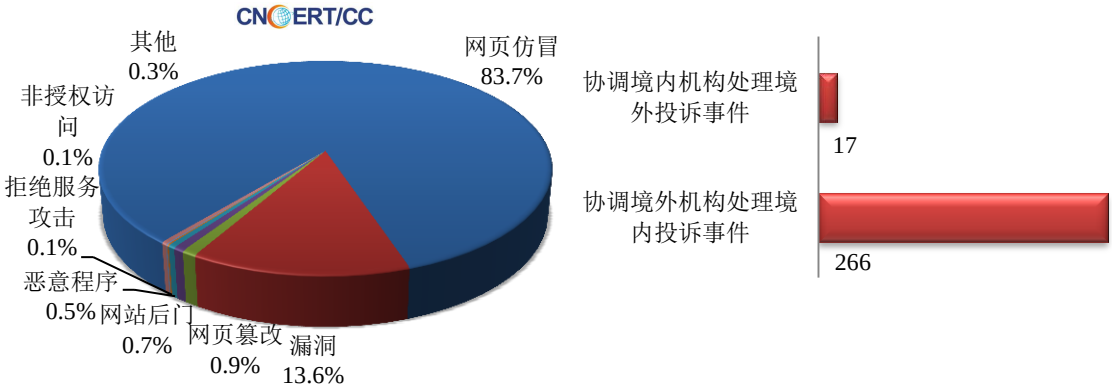
http://www.cnvd.org.cn/webinfo/list?type=4

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

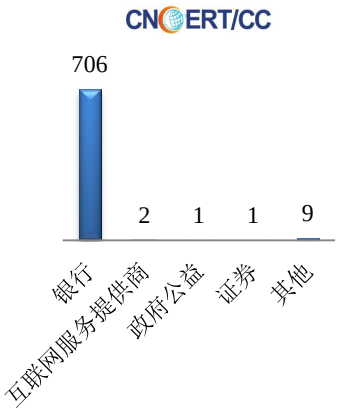
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 859 起，其中跨境网络安全事件 283 起。

本周CNCERT处理的事件数量按类型分布
(8/7-8/13)

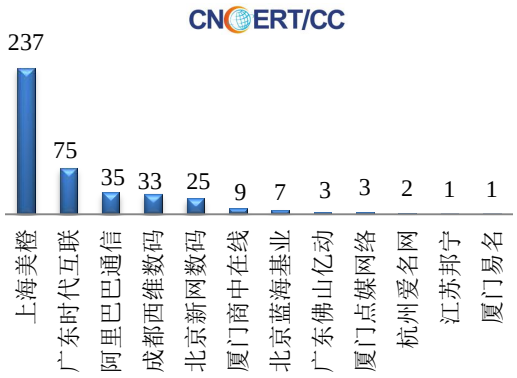


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 719 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 706 起和互联网服务提供商仿冒事件 2 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/7-8/13)

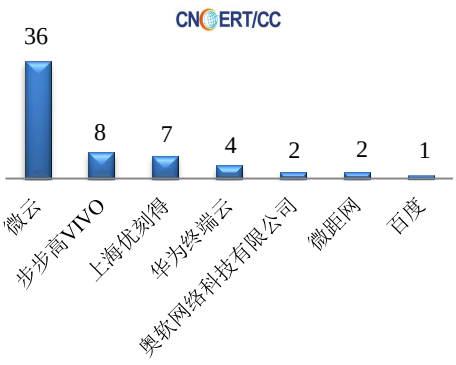


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/7-8/13)



本周，CNCERT 协调 7 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 60 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
(8/7-8/13)



业界新闻速递

1、英国制定新安全法案，加强关键基础设施网络防御体系

HackerNews.cc8 月 10 日消息 据外媒 8 月 8 日报道，英国政府于近期推出一项新安全法案，旨在保障国家关键基础设施安全。该法案指出，提供能源与交通等基本服务的供应商需要制定一份安全紧急方案，以解决电力故障或环境灾难所带来的严重影响。倘若此类公司未能有效实施网络安全措施，或将面临巨额罚款 ，其金额最高可达 1700 万英镑。目前，该法案集数字、文化、媒体与运动为一体，符合欧盟《网络与信息安全指令》（NIS 指令）的要求并将于明年 5 月生效执行。NIS 指令于 2016 年 7 月 6 日通过审核后在同年 8 月生效，旨在促进成员国安全战略协作与信息共享、提升欧盟网络安全水平。此外，欧盟成员国需要在 NIS 指令生效的 21 个月内将其纳入国家立法，并另有 6 个月可识别指令涉及的主体范围。调查显示，由于英国提供关键基础设施的组织于近期在勒索软件 WannaCry 与 NotPetya 攻击事件中普遍遭受影响，因此政府不得不加快安全法案的制定。

2、英国政府出台《智能汽车网络安全新指南》

cnBeta.COM8 月 7 日消息 为了鼓励汽车制造商们在机动车网络安全上多上点心，英国政府已于今日出台了一套全新的指南。交通大臣卡兰南勋爵（Lord Callanan）表示，随着该国道路上自动驾驶和联网汽车的增长，制造商理应为消费者提供最基础的防护，比如抵御网络攻击、控制个人资料、甚至远程控制车辆。这份指南的全称为《面向联网和自动驾驶汽车的网络安全关键原则》，目标是将之拓展到汽车制造和供应链上的每一方。

3、爱尔兰国有电力供应商 EirGrid 遭入侵，疑似政府黑客所为

HackerNews.cc8 月 9 日消息 据外媒 8 月 7 日报道，英国情报机构（NCSC）发现黑客于今年 4 月针对爱尔兰与北爱尔兰国有电力供应商 EirGrid 展开攻击，或有政府背景。调查显示，黑客在入侵 EirGrid 使用的沃达丰（Vodafone）网络系统后利用恶意软件拦截威尔士与北爱尔兰 Web 路由器中传输的所有未加密通信数据。此外，NCSC 还发现黑客通过多个英国 IP 地址入侵其他先进国家基础设施、攻击能源与制造行业的系统网络。知名媒体 Independent8 月 6 日透露，调查人员将监视并检测依赖沃达丰被黑互联网专线接入（DIA）服务的所有通信记录与文件。虽然目前并不清楚爱尔兰电网控制系统是否被安装恶意软件，但他们注意到，一旦如此，或将导致大规模停电现象。EirGrid 发言人 David Martin 表示，对于 EirGrid 来说，计算机网络与电力控制系统的安全至关重要。虽然 EirGrid 就网络安全具体操作问题不做任何公开评论，但能源企业与国家基础设施显然已成为黑客重点攻击对象。此外，英国政府通信总部（GCHQ）也警示合作伙伴密切关注能源行业的黑客攻击活动。

4、匈牙利三大国有银行连遭黑客网络钓鱼攻击

HackerNews.cc8 月 11 日消息 据外媒报道，匈牙利国民银行（MNB）于 8 月 8 日发表声明，指出黑客自 6 月以来针对匈牙利三大国有银行展开一系列网络钓鱼攻击活动，但并未提及受影响金融机构与可疑黑客组织的名称。MNB 作为匈牙利共和国中央银行、国家金融市场监管机构以及欧洲中央银行系统（ESCB）成员公开表示，黑客通过网络钓鱼电子邮件与短信方式大规模攻击银行客户，骗取帐户持有者泄露银行帐户详细信息与登录凭据。据悉，黑客此次使用的克隆网站较以往更加令人信服，不依赖任何翻译软件，直接使用匈牙利语误导

用户认为站点合法安全。虽然该起攻击活动并未造成用户资金损失，但受影响金融机构已积极采取安全补救措施，加强自身网络系统防御体系建设。尽管如此，MNB 警示，其他银行仍可能于近期遭受类似攻击。

5、乌克兰国家邮政服务机构 Ukrposhta 两日连遭 DDoS 攻击

HackerNews.cc8 月 10 日消息 据外媒 8 月 8 日报道，乌克兰国家邮政服务机构 Ukrposhta 近期遭受黑客为期两天的分布式拒绝服务（DDoS）攻击，导致计算机网络系统运行缓慢，甚至出现中断现象。据 Interfax 通讯社消息，受害计算机网络系统与包裹在线跟踪系统有关。黑客利用僵尸网络向 Ukrposhta 服务器发送大规模流量，强制网站离线。Ukrposhta 发言人表示，此次攻击活动导致官网与相应服务普遍遭受影响。当前，技术人员正努力解决上述问题，以便尽快恢复工作流程。7 月下旬，Ukrposhta 曾在一份季度报告中证实，黑客通过乌克兰会计公司使用的 MeDoc 软件自动更新传播勒索病毒 NotPetya，导致公司自动化邮件系统完全崩溃。截至目前，NotPetya 已感染 60 多个国家不同行业的网络系统，与 5 月中旬爆发的勒索软件 WannaCry 具有明显相似之处。

6、委内瑞拉遭遇网络攻击 700 万手机通讯瘫痪

E 安全 8 月 13 日消息 当地时间周四，委内瑞拉政府表示，政府网站本周早些时候遭遇大规模网络攻击，导致 700 万手机用户无法使用通信服务。一支自称“The Binary Guardians”的组织宣称对此负责。攻击使委内瑞拉政府、最高法院和国会的网站关闭。科技部长胡格博·罗亚将这些攻击称为恐怖行动，称攻击者周三攻陷了运营商 Movilnet 的 GSM 平台，导致 700 万手机用户无法使用通信服务。罗亚表示，委内瑞拉本周一开始遭遇一波攻击，几十个政府和私企公司网站被黑。罗亚还指出，委内瑞拉光纤网被切断，影响了 7 个州。这些攻击在外国特工的帮助下实施，再一次破坏了委内瑞拉的网络连接。罗亚表示，委内瑞拉仍在调查该事件。

7、德国 SMA 太阳能电池板逆变器漏洞严重威胁欧洲电网

E 安全 8 月 8 日消息 安全公司 ITsec 一名荷兰安全研究人员威廉维斯特霍夫发现太阳能电池板组件中存在严重漏洞，该漏洞存在于太阳能电池板逆变器中，逆变器的主要作用是将直流电转换成交流电，若被黑客利用，会导致欧洲电网大范围停电。此漏洞影响的是德国领先企业 SMA 制造的逆变器。维斯特霍夫于 2016 年 12 月将该问题报告给了 SMA 公司，然而令人遗憾的是，6 个月后之后，SMA 仍未解决问题。维斯特霍夫发布了详细的漏洞分析报告及被称为“荷鲁斯场景”（Horus Scenario）的攻击场景。“荷鲁斯场景”是用来描述针对重要电气基础设施的大规模网络攻击场景。维斯特霍夫通过理论与实践证明了这种场景的存在。据荷兰媒体 Volkskrant 报道，维斯特霍夫声称该安全漏洞影响了欧洲电网使用的数千台联网逆变器。一旦黑客控制了大量逆变器，并将其关闭，这会造成欧洲大范围停电。维斯特霍夫的研究表明，存在漏洞的太阳能电池板控制着约 17GW 的电力，若黑客成功发起网络攻击，必然会带来灾难性的后果。

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 2016 年，CNCERT 与 69 个国家和地区的 185 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：肖崇蕙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158