国家互联网应急中心

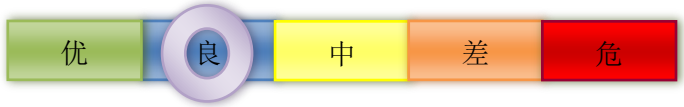
网络安全信息与动态周报

2017 年第 32 期

7 月 31 日-8 月 6 日

CNCERT/CC

本周网络安全基本态势

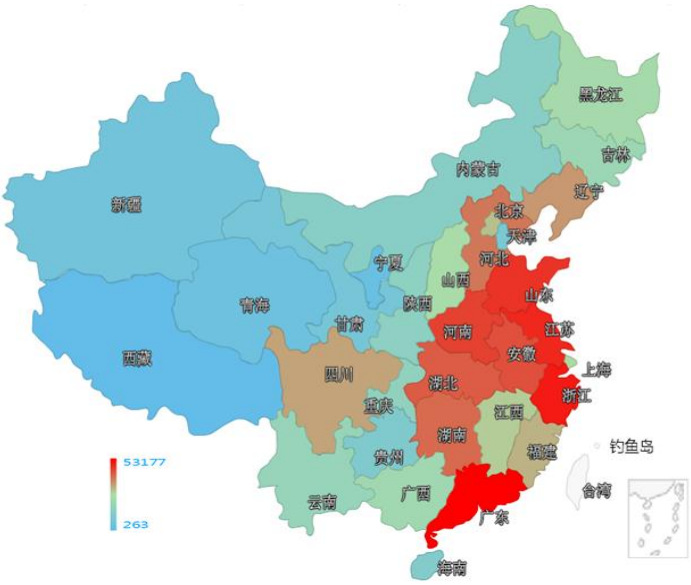


境内感染网络病毒的主机数量	•41.1万	
境内被篡改网站总数 其中政府网站数量	•2094 •60	↓14.5% ↑15.4%
境内被植入后门网站总数 其中政府网站数量	•1527 •121	↑92.6% ↑188.1%
针对境内网站的仿冒页面数量	•351	↑17.4%
新增信息安全漏洞数量 其中高危漏洞数量	•212 •90	↓23.2% ↓11.8%

═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

本周境内被木马或被僵尸程序控制的主机约 41.1 万。



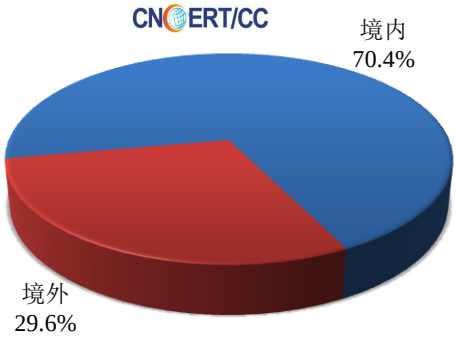
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

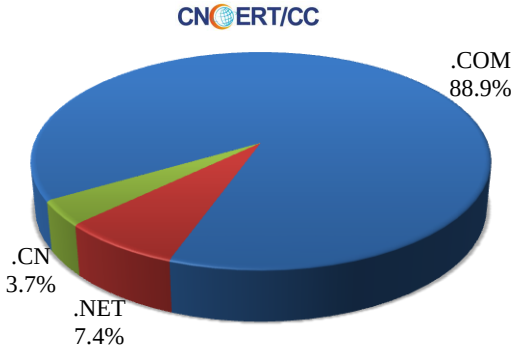
广东省	•约5.3万个（约占中国大陆总感染量的12.9%）
浙江省	•约4.0万个（约占中国大陆总感染量的9.7%）
江苏省	•约3.6万个（约占中国大陆总感染量的8.8%）

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 27 个，涉及 IP 地址 50 个。在 27 个域名中，有 29.6%为境外注册，且顶级域为.com 的约占 88.9%；在 50 个 IP 中，有约 6.0%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 2 个 IP。

本周放马站点域名注册所属境内外分布
(7/31-8/6)



本周放马站点域名所属顶级域的分布
(7/31-8/6)



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。

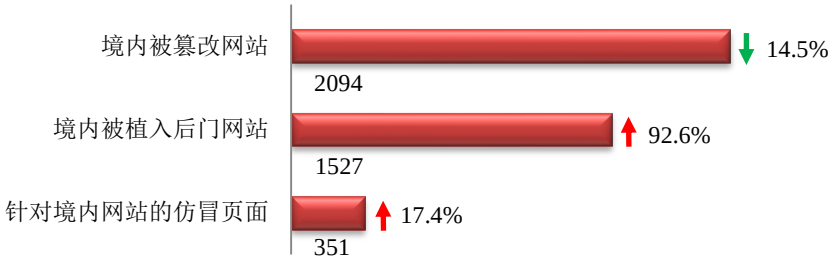
ANVA恶意地址黑名单发布地址

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。

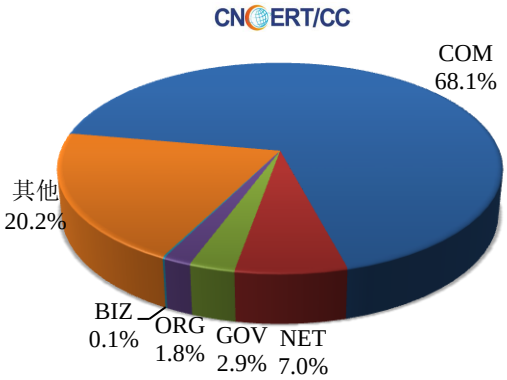
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2094 个；境内被植入后门的网站数量为 1527 个；针对境内网站的仿冒页面数量为 351。

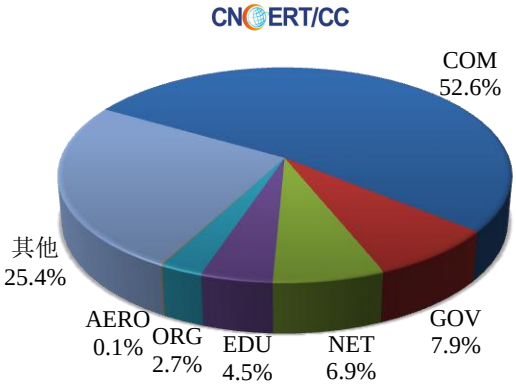


本周境内被篡改政府网站（GOV 类）数量为 60 个（约占境内 2.9%），较上周环比上升了 15.4%；境内被植入后门的政府网站（GOV 类）数量为 121 个（约占境内 7.9%），较上周环比上升了 188.1%；针对境内网站的仿冒页面涉及域名 304 个，IP 地址 144 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/31-8/6)

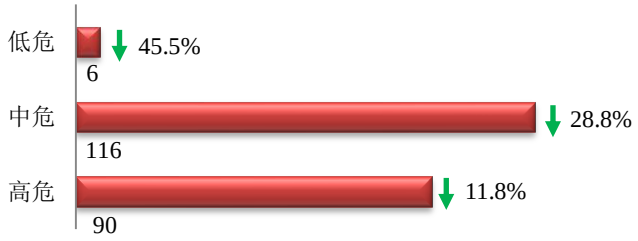


本周我国境内被植入后门网站按类型分布
(7/31-8/6)

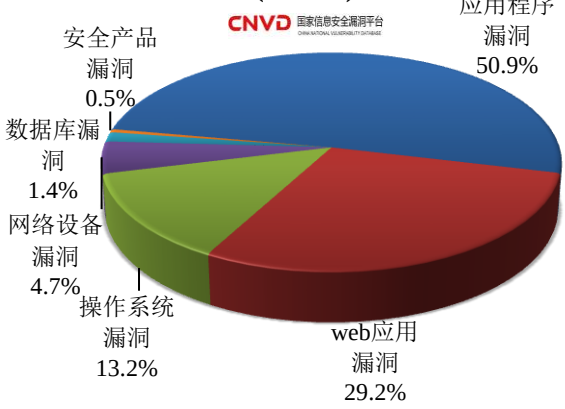


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 212 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
(7/31-8/6)



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

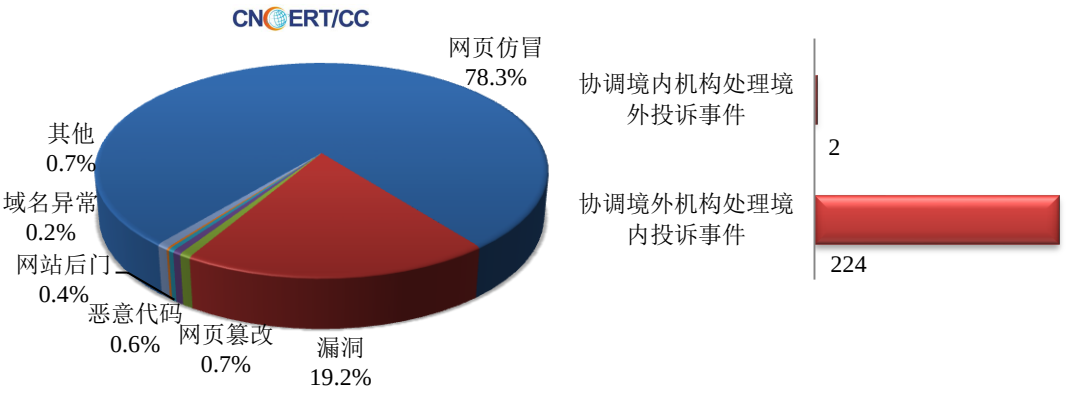
http://www.cnvd.org.cn/webinfo/list?type=4

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

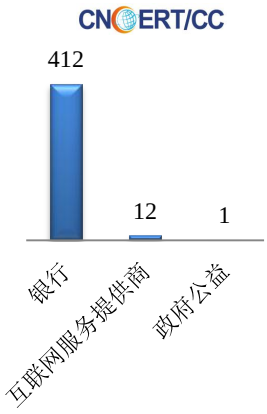
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 543 起，其中跨境网络安全事件 226 起。

本周CNCERT处理的事件数量按类型分布
(7/31-8/6)

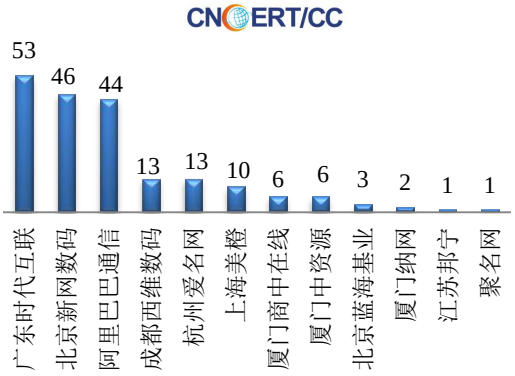


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 425 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 412 起和互联网服务提供商仿冒事件 12 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(7/31-8/6)

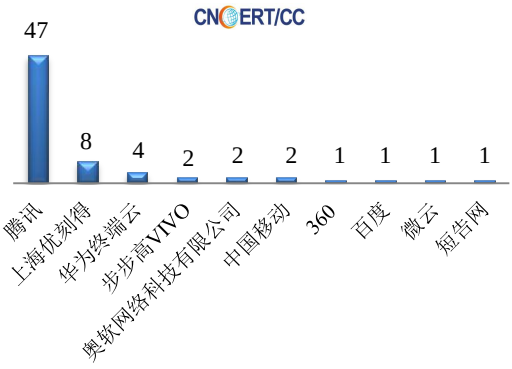


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/31-8/6)



本周，CNCERT 协调 10 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 69 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
(7/31-8/6)



业界新闻速递

1、工信部加快车联网等领域安全防护技术攻坚

新华社 7 月 31 日消息 记者 7 月 31 日从工信部获悉，工信部将聚焦电信和互联网行业网络安全保障关键环节，开展网络安全试点示范工作，引导企业加强技术手段建设，增强防范和应对网络安全威胁的能力，特别是车联网、物联网等新业务和融合领域的网络安全防护能力。工信部网络安全管理局有关负责人表示，工信部将车联网等新领域和新业态的网络安全工作作为今年重点，提出加强面向公共云服务、物联网、车联网、工业互联网等领域典型应用场景的安全防护，研发先进技术，提供特定、可行、有效的安全保护手段。他说，工信部鼓励企业在互联网安全防护上先试先行，并将针对新业务及融合领域网络安全、网络安全创新应用、域名系统安全等领域遴选试点示范企业，加强技术研发和应用落地。

2、美司法部发布《在线系统漏洞披露计划框架》，帮助企业建立漏洞披露计划

E 安全 8 月 4 日消息 美国司法部（DOJ）犯罪科网络安全部门 7 月发布《在线系统漏洞披露计划框架》，以帮助组织机构制定正规的漏洞披露计划。越来越多的组织机构认识到，漏洞悬赏计划对于发现网络及应用程序中的安全漏洞相当奏效。大多数大型私有企业数年来一直在实施此类计划，美国政府这方面也采取了重要举措。美国国防部通过安全漏洞披露平台“HackerOne”运营三大漏洞悬赏计划（“黑进五角大楼”——Hack the Pentagon，“黑进陆军”——Hack the Army 和“黑进空军”——Hack the Air Force）推动这项工作。美国总务管理局（GSA）5 月也宣布启动漏洞悬赏计划。此外，参议员也提出一项新法案在国土安全部（DHS）构建漏洞悬赏试点计划。司法部制定的框架可以帮助公共和私有部门的组织机构设计漏洞披露计划。此框架不会规定漏洞披露计划的形式或目标，而是侧重描述授权发现与披露行为，以减少在民事或刑事上违反《计算机欺诈与滥用法》（CFAA）的可能性。

3、英国投资 1900 万美元计划 3 年内新设网络安全技术开发创新中心

E 安全 8 月 3 日消息 英国政府近期宣布，未来三年将投资 1900 万美元（约合人民币 12823 万）设立创新中心，以壮大国家网络安全人才，并改进技术。英国政府表示，新创新中心将为网络安全技术大型企业和初创企业之间提供合作机会。创新中心还将为英国网络安全行业的企业提供技术指导、业务支持和建议。英国数字、文化、媒体与体育部（The Department for Digital, Culture, Media and Sport，DCMS）会通过竞争的方式选出获胜者负责设计开发创新中心。今年早些时候，英国在切尔滕纳姆也开办了创新中心。新创新中心将设立在伦敦，该城市同时也是英国政府通讯总部（GCHQ）国家网络安全中心所在地。英国政府表示，在 PETRAS 研究中心 3300 万美元国家投资的推动下，伦敦未来三年还将成为研究项目的孵化地。这些研究项目在检验互联设备如何让社会受益的同时也力求保持安全性和弹性。

4、俄罗斯屏蔽 VPN 的法律将于 11 月 1 日生效

HackerNews.cc8 月 1 日消息 俄罗斯总统普京此前签署禁止提供 VPN 和其它匿名技术访问被屏蔽网站的法律。据悉，该法律将于今年 11 月 1 日正式生效。俄罗斯议会下院国家杜马于 10 天前对该法案进行投票表决并

获得一致通过，要求 ISP 屏蔽 VPN 和其它匿名网络技术。国家杜马信息政策委员会负责人 Leonid Levin 称，法律无意对守法公民实施限制，只是想要屏蔽非法内容。暂时不清楚俄罗斯将会采取什么技术手段屏蔽匿名网络技术。

5、巴基斯坦政府官网遭黑客入侵 播印度国歌

环球网 8 月 5 日消息 据香港东网 5 日报道，印度与巴基斯坦近日就克什米尔的主权纠纷，接连爆发冲突。8 月 14 日及 15 日分别是巴基斯坦与印度的独立日。两国黑客率先在互联网上较劲。一名印度黑客成功入侵巴基斯坦政府官网，不但将网站页面设为纯黑色，更播放印度国歌，极为挑衅。报道称，印度黑客入侵巴基斯坦政府官网后，大肆篡改其页面设计及留言，庆祝印度独立日。还有留言写道：思想有自由，说话有信念，我们的灵魂有自尊。请向那些伟大的人致敬，他们让这一切都成真。不久，巴基斯坦政府派人修复网站，但印度黑客纷纷在网上高呼取得胜利。

6、太阳能逆变器的一个 bug 可能导致欧洲电网大崩溃

cnBeta.COM8 月 4 日消息 据外媒报道，一名荷兰安全研究人员在某些太阳能面板上发下了一个严重的漏洞，若被利用，可能导致欧洲电网的崩溃。来自 ITsec 的 Willem Westerhof 在率先曝光此事的荷兰报媒 Volkskrant 上提到：他在所谓的逆变器部分发现了一个漏洞，而这个漏洞可以在欧洲成千上万的联网逆变器中找到。作为太阳能电板上的一个基本组成部分，逆变器负责将直流电转换为交流电。与其它易受攻击的物联网设备一样，黑客能够控制大量逆变器、然后将它们同时关掉，从而导致整个电网出现不均衡——瞬间击垮欧洲地区的大部分电网。为了让大家更好地意识到这种问题的规模，Westerhof 研究得出了 170 亿瓦这个数字。如果黑客真的得逞，那结果将是灾难性的。

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：饶毓

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158